



DOCUMENTO DI SINTESI

relativo al

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

PARTE SPECIALE

Approvato in data 16/09/2026

INDICE

1. PREMESSA	10
2. LA STRUTTURA DELLA PARTE SPECIALE.....	10
3. LE AREE A RISCHIO REATO.....	15
3.1. GESTIONE DEI SERVIZI DI CASSA E DI TESORERIA A FAVORE DELLA PUBBLICA AMMINISTRAZIONE	17
3.1.1. Reati astrattamente ipotizzabili	17
3.1.2. Unità organizzative/funzioni aziendali coinvolte	18
3.1.3. Attività sensibili	18
3.1.4. Principi generali di comportamento.....	18
3.1.5. Controlli preventivi	20
3.2. APPROVVIGIONAMENTO DI BENI, LAVORI, SERVIZI E CONSULENZE PROFESSIONALI	21
3.2.1. Reati astrattamente ipotizzabili	21
3.2.2. Unità organizzative/funzioni aziendali coinvolte	23
3.2.3. Attività sensibili	24
3.2.4. Principi generali di comportamento.....	24
3.2.5. Controlli preventivi	26
3.3. GESTIONE DEL CONTENZIOSO PASSIVO E DEI RELATIVI RAPPORTI CON L'AUTORITÀ GIUDIZIARIA	29
3.3.1. Reati astrattamente ipotizzabili	29
3.3.2. Unità organizzative/funzioni aziendali coinvolte	30
3.3.3. Attività sensibili	30
3.3.4. Principi generali di comportamento.....	30
3.3.5. Controlli preventivi	32
3.4. GESTIONE DEL CONTENZIOSO ATTIVO E DEI RELATIVI RAPPORTI CON L'AUTORITÀ GIUDIZIARIA	34
3.4.1. Reati astrattamente ipotizzabili	34
3.4.2. Unità organizzative/funzioni aziendali coinvolte	34
3.4.3. Attività sensibili	35

3.4.4.	<i>Principi generali di comportamento.....</i>	35
3.4.5.	<i>Controlli preventivi</i>	37
3.5.	GESTIONE DEI SISTEMI INFORMATIVI	38
3.5.1.	<i>Reati astrattamente ipotizzabili</i>	39
3.5.2.	<i>Unità organizzative/funzioni aziendali coinvolti</i>	40
3.5.3.	<i>Attività sensibili</i>	40
3.5.4.	<i>Principi generali di comportamento.....</i>	41
3.5.5.	<i>Controlli preventivi</i>	43
3.6.	GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E LE AUTORITÀ DI VIGILANZA	46
3.6.1.	<i>Reati astrattamente ipotizzabili</i>	46
3.6.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	47
3.6.3.	<i>Attività sensibili</i>	47
3.6.4.	<i>Principi generali di comportamento.....</i>	48
3.6.5.	<i>Controlli preventivi</i>	50
3.7.	GESTIONE DEI RAPPORTI CON I PARTNER COMMERCIALI/MEDIATORI CREDITIZI/AGENTI.....	52
3.7.1.	<i>Reati astrattamente ipotizzabili</i>	52
3.7.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	52
3.7.3.	<i>Attività sensibili</i>	53
3.7.4.	<i>Principi generali di comportamento.....</i>	53
3.7.5.	<i>Controlli preventivi</i>	54
3.8.	GESTIONE DEGLI OMAGGI E DELLE SPESE DI RAPPRESENTANZA	55
3.8.1.	<i>Reati astrattamente ipotizzabili</i>	56
3.8.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	57
3.8.3.	<i>Attività sensibili</i>	57
3.8.4.	<i>Principi generali di comportamento.....</i>	57
3.8.5.	<i>Controlli preventivi</i>	59
3.9.	GESTIONE DELLA COMUNICAZIONE ESTERNA.....	60

3.9.1.	<i>Reati astrattamente ipotizzabili</i>	60
3.9.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	61
3.9.3.	<i>Attività sensibili</i>	61
3.9.4.	<i>Principi generali di comportamento.....</i>	62
3.9.5.	<i>Controlli preventivi</i>	63
3.10.	GESTIONE DELLE LIBERALITÀ E DELLE SPONSORIZZAZIONI	64
3.10.1.	<i>Reati astrattamente ipotizzabili</i>	64
3.10.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	65
3.10.3.	<i>Attività sensibili</i>	65
3.10.4.	<i>Principi generali di comportamento.....</i>	66
3.10.5.	<i>Controlli preventivi</i>	67
3.11.	GESTIONE DEGLI ADEMPIMENTI SOCIETARI	69
3.11.1.	<i>Reati astrattamente ipotizzabili</i>	69
3.11.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	69
3.11.3.	<i>Attività sensibili</i>	69
3.11.4.	<i>Principi generali di comportamento.....</i>	69
3.11.5.	<i>Controlli preventivi</i>	71
3.12.	CONTABILITÀ GENERALE, BILANCIO E ALTRE COMUNICAZIONI SOCIALI.....	72
3.12.1.	<i>Reati astrattamente ipotizzabili</i>	72
3.12.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	74
3.12.3.	<i>Attività sensibili</i>	74
3.12.4.	<i>Principi generali di comportamento.....</i>	75
3.12.5.	<i>Controlli preventivi</i>	77
3.13.	GESTIONE DEI SERVIZI DI ASSICURAZIONE E PREVIDENZA VERSO LA CLIENTELA	80
3.13.1.	<i>Reati astrattamente ipotizzabili</i>	80
3.13.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	81
3.13.3.	<i>Attività sensibili</i>	81

3.13.4.	<i>Principi generali di comportamento.....</i>	82
3.13.5.	<i>Controlli preventivi</i>	83
3.14.	SELEZIONE E ASSUNZIONE DEL PERSONALE	84
3.14.1.	<i>Reati astrattamente ipotizzabili</i>	84
3.14.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	85
3.14.3.	<i>Attività sensibili</i>	85
3.14.4.	<i>Principi generali di comportamento.....</i>	85
3.14.5.	<i>Controlli preventivi</i>	87
3.15.	GESTIONE DEL PERSONALE.....	89
3.15.1.	<i>Reati astrattamente ipotizzabili</i>	89
3.15.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	90
3.15.3.	<i>Attività sensibili</i>	90
3.15.4.	<i>Principi generali di comportamento.....</i>	91
3.15.5.	<i>Controlli preventivi</i>	92
3.16.	GESTIONE DELLA SALUTE E SICUREZZA SUL LAVORO ...	94
3.16.1.	<i>Reati astrattamente ipotizzabili</i>	94
3.16.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	95
3.16.3.	<i>Attività sensibili</i>	95
3.16.4.	<i>Principi generali di comportamento.....</i>	95
3.16.5.	<i>Controlli preventivi</i>	97
3.17.	GESTIONE DEGLI ASPETTI AMBIENTALI.....	103
3.17.1.	<i>Reati astrattamente ipotizzabili</i>	103
3.17.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	105
3.17.3.	<i>Attività sensibili</i>	105
3.17.4.	<i>Principi generali di comportamento.....</i>	105
3.17.5.	<i>Controlli preventivi</i>	106
3.18.	GESTIONE DEGLI INVESTIMENTI DELLA CLIENTELA	107
3.18.1.	<i>Reati astrattamente ipotizzabili</i>	107

3.18.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	109
3.18.3.	<i>Attività sensibili</i>	109
3.18.4.	<i>Principi generali di comportamento.....</i>	109
3.18.5.	<i>Controlli preventivi</i>	111
3.19. DEI VALORI	GESTIONE DEL DENARO CONTANTE, DELLE GARANZIE E 114	
3.19.1.	<i>Reati astrattamente ipotizzabili</i>	114
3.19.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	114
3.19.3.	<i>Attività sensibili</i>	114
3.19.4.	<i>Principi generali di comportamento.....</i>	115
3.19.5.	<i>Controlli preventivi</i>	116
3.20.	GESTIONE DELLA FINANZA E DELLA TESORERIA	117
3.20.1.	<i>Reati astrattamente ipotizzabili</i>	118
3.20.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	119
3.20.3.	<i>Attività sensibili</i>	119
3.20.4.	<i>Principi generali di comportamento.....</i>	119
3.20.5.	<i>Controlli preventivi</i>	121
3.21.	GESTIONE DEGLI ADEMPIMENTI ANTIRICICLAGGIO E ANTITERRORISMO	124
3.21.1.	<i>Reati astrattamente ipotizzabili</i>	124
3.21.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	124
3.21.3.	<i>Attività sensibili</i>	125
3.21.4.	<i>Principi generali di comportamento.....</i>	125
3.21.5.	<i>Controlli preventivi</i>	129
3.22.	PIANIFICAZIONE E CONTROLLO DI GESTIONE	132
3.22.1.	<i>Reati astrattamente ipotizzabili</i>	132
3.22.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	132
3.22.3.	<i>Attività sensibili</i>	133
3.22.4.	<i>Principi generali di comportamento.....</i>	133

3.22.5.	<i>Controlli preventivi</i>	134
3.23.	GESTIONE DI NUOVI PRODOTTI/SERVIZI E/O AGGIORNAMENTO DI QUELLI ESISTENTI E RELATIVO INSERIMENTO IN NUOVI MERCATI	136
3.23.1.	<i>Reati astrattamente ipotizzabili</i>	136
3.23.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	136
3.23.3.	<i>Attività sensibili</i>	136
3.23.4.	<i>Principi generali di comportamento.....</i>	137
3.23.5.	<i>Controlli preventivi</i>	137
3.24.	GESTIONE DEGLI ADEMPIMENTI FISCALI	139
3.24.1.	<i>Reati astrattamente ipotizzabili</i>	139
3.24.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	140
3.24.3.	<i>Attività sensibili</i>	141
3.24.4.	<i>Principi generali di comportamento.....</i>	141
3.24.5.	<i>Controlli preventivi</i>	143
3.25.	GESTIONE DEI FINANZIAMENTI VERSO LA CLIENTELA.	145
3.25.1.	<i>Reati astrattamente ipotizzabili</i>	145
3.25.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	146
3.25.3.	<i>Attività sensibili</i>	147
3.25.4.	<i>Principi generali di comportamento.....</i>	147
3.25.5.	<i>Controlli preventivi</i>	148
3.26.	GESTIONE DELLE OPERAZIONI DI MERCATO AI FINI DELLA PREVENZIONE DEGLI ILLECITI PENALI E AMMINISTRATIVI IN TEMA DI ABUSI DI MERCATO	151
3.26.1.	<i>Reati astrattamente ipotizzabili</i>	151
3.26.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	151
3.26.3.	<i>Attività sensibili</i>	152
3.26.4.	<i>Principi generali di comportamento.....</i>	152
3.26.5.	<i>Controlli preventivi</i>	154

3.27.	GESTIONE DEI RAPPORTI CON LA CLIENTELA - OPERATORE ESTERO	157
3.27.1.	<i>Reati astrattamente ipotizzabili</i>	157
3.27.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	158
3.27.3.	<i>Attività sensibili</i>	158
3.27.4.	<i>Principi generali di comportamento.....</i>	158
3.27.5.	<i>Controlli preventivi</i>	159
3.28.	GESTIONE DEGLI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E DELLE PIATTAFORME DI PAGAMENTO IN USO	161
3.28.1.	<i>Reati astrattamente ipotizzabili</i>	161
3.28.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	162
3.28.3.	<i>Attività sensibili</i>	163
3.28.4.	<i>Principi generali di comportamento.....</i>	163
3.28.5.	<i>Controlli preventivi</i>	166
3.29.	GESTIONE DEL PATRIMONIO CULTURALE DELLA BANCA	169
3.29.1.	<i>Reati astrattamente ipotizzabili</i>	169
3.29.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	170
3.29.3.	<i>Attività sensibili</i>	170
3.29.4.	<i>Principi generali di comportamento.....</i>	171
3.29.5.	<i>Controlli preventivi</i>	172
3.30.	GESTIONE DEL PATRIMONIO IMMOBILIARE DELLA BANCA	173
3.30.1.	<i>Reati astrattamente ipotizzabili</i>	173
3.30.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	174
3.30.3.	<i>Attività sensibili</i>	174
3.30.4.	<i>Principi generali di comportamento.....</i>	174
3.30.5.	<i>Controlli preventivi</i>	175
3.31.	GESTIONE DEI RAPPORTI CON INTERLOCUTORI TERZI - PUBBLICI O PRIVATI - NELLO SVOLGIMENTO DELLE PROPRIE ATTIVITÀ LAVORATIVE PER CONTO E/O NELL'INTERESSE DELLA BANCA.....	176

3.31.1.	<i>Reati astrattamente ipotizzabili</i>	176
3.31.2.	<i>Unità organizzative/funzioni aziendali coinvolte</i>	177
3.31.3.	<i>Attività sensibili</i>	177
3.31.4.	<i>Principi generali di comportamento.....</i>	177
3.31.5.	<i>Controlli preventivi</i>	178

1. PREMESSA

La Parte Speciale del Modello, dedicata alle categorie di reato considerate rilevanti all'esito delle attività di *risk assessment*, identifica le "aree a rischio reato", pari a n. 31, ossia le aree aziendali nel cui ambito è possibile la commissione, nell'interesse o a vantaggio della Banca, dei 'reati presupposto' previsti dal Decreto 231 (ivi incluse le aree c.d. "strumentali", ovvero quelle attività nelle quali possono realizzarsi le condizioni di fatto che rendono possibile l'eventuale commissione di 'reati presupposto' nell'ambito delle aree a rischio reato "dirette").

2. LA STRUTTURA DELLA PARTE SPECIALE

Al fine di garantirne la massima fruibilità per i Destinatari del Modello, la presente Parte Speciale è stata costruita seguendo il c.d. "approccio per aree a rischio" e contiene, pertanto, 31 sezioni, ognuna delle quali dedicata ad una "area a rischio reato" rilevante per la Banca. Per ciascuna "area a rischio reato" sono indicate le seguenti informazioni:

- le categorie di reato applicabili ed i relativi principali reati presupposto astrattamente perpetrabili (per la descrizione dei reati presupposto previsti dal Decreto si rimanda all'Allegato 1);
- le attività "sensibili", ovvero quelle al cui espletamento è connesso il rischio di commissione dei reati presupposto;
- i ruoli aziendali coinvolti nelle attività "sensibili" e che, astrattamente, potrebbero commettere i reati presupposto previsti dal Decreto nell'interesse o a vantaggio della Banca, sebbene tale individuazione dei/delle ruoli/funzioni non debba considerarsi, in ogni caso, tassativa, atteso che ciascun soggetto della Banca potrebbe, in linea teorica, essere coinvolto, anche a titolo di concorso;
- i principi di comportamento, generali e specifici, finalizzati a prevenire la commissione dei reati identificati ed a ridurre il rischio di condotte irregolari o illecite, i quali possono riguardare a titolo esemplificativo: sistema delle deleghe, poteri di firma e poteri autorizzativi, segregazione delle responsabilità, tracciabilità, obblighi di monitoraggio, formazione specifica, obblighi di segnalazione di determinate operazioni, flussi informativi/reporting.

Si riporta di seguito l'elenco delle categorie di reato di cui al Decreto 231:

1. reati contro la Pubblica Amministrazione (artt. 24 e 25, Decreto);
2. delitti informatici e trattamento illecito dei dati (art. 24-bis, Decreto);
3. delitti di criminalità organizzata (art. 24-ter, Decreto);

4. delitti in materia di falsità in monete, in carte di pubblico credito, in valori in bollo e in strumenti o segni di riconoscimento (art. 25-bis, Decreto);
5. delitti contro l'industria e il commercio (art. 25-bis.1, Decreto);
6. reati societari (art. 25-ter, Decreto);
7. delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater, Decreto);
8. pratiche di mutilazione degli organi genitali femminili (art. 25-quarter.1, Decreto);
9. delitti in materia di personalità individuale (art. 25-quinquies, Decreto);
10. reati di abuso di mercato (art. 25-sexies, Decreto);
11. reati di omicidio colposo o lesioni gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro (art. 25-septies, Decreto);
12. reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies, Decreto);
13. delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1, Decreto);
14. reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25-octies.2, Decreto);
15. delitti in materia di violazione del diritto d'autore (art. 25-novies, Decreto);
16. delitti di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies, Decreto);
17. reati ambientali (art. 25-undecies, Decreto);
18. delitti di impiego di cittadini di Paesi terzi di cui il soggiorno è irregolare (art. 25-duodecies, Decreto);
19. reati in materia di razzismo e xenofobia (art. 25-terdecies, Decreto);
20. reati in materia di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies, Decreto);
21. reati tributari (art. 25-quinquedecies, Decreto);
22. contrabbando (art. 25-sexiesdecies, Decreto);
23. delitti contro il patrimonio culturale (art. 25-septiesdecies, Decreto);

- 24. riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevicies, Decreto);
- 25. delitti contro gli animali (art. 25- undevicies, Decreto);
- 26. reati transnazionali (art. 10 L. 146/2006).

All'esito della condotta attività di *risk assessment*, è stato costruito il raccordo (di cui alla tabella che segue) tra le categorie di reato sopra indicate e le 31 “aree a rischio reato” individuate cui le categorie di reato rilevanti sono applicabili.

N	AREE A RISCHIO REATO	CATEGORIE DI REATO																										
		Reg. UE 2023/1114	26. l. n. 146/2006	25. 25-undevicies	24. 25-duodevicies	23. 25-septesdecies	22. 25-sexiesdecies	21. 25-quinquedecies	20. 25-quaterdecies	19. 25-terdecies	18. 25-duodecies	17. 25-undecies	16. 25-decies	15. 25-novies	14. 25-octies.2	13. 25-octies.1	12. 25-octies	11. 25-septies	10. 25-sexies	9. 25-quinquies	8. 25-quarter.1	7. 25-quarter	6. 25-ter	5. 25-bis.1	4. 25-bis	3. 24-ter	2. 24-bis	1. 24-25
1	GESTIONE DEI SERVIZI DI CASSA E DI TESORERIA A FAVORE DELLAPUBBLICA AMMINISTRAZIONE																✓						✓	✓	✓			✓
2	APPROVVIGIONAMENTO DI BENI, LAVORI, SERVIZI E CONSULENZE PROFESSIONALI							✓						✓	✓	✓	✓			✓		✓	✓	✓	✓			✓
3	GESTIONE DEL CONTENZIOSO PASSIVO E DEI RELATIVI RAPPORTI CON L'AUTORITÀ GIUDIZIARIA											✓											✓					✓
4	GESTIONE DEL CONTENZIOSO ATTIVO E DEI RELATIVI RAPPORTI CON L'AUTORITÀ GIUDIZIARIA											✓											✓					✓
5	GESTIONE DEI SISTEMI INFORMATIVI													✓													✓	
6	GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E LE AUTORITÀ DI VIGILANZA											✓											✓				✓	
7	GESTIONE DEI RAPPORTI CON I PARTNER COMMERCIALI/MEDIATORI CREDITIZI/AGENTI																✓					✓						
8	GESTIONE DEGLI OMAGGI E DELLE SPESE DI RAPPRESENTANZA																✓					✓						✓
9	GESTIONE DELLA COMUNICAZIONE ESTERNA													✓									✓		✓			✓
10	GESTIONE DELLE LIBERALITÀ E DELLE SPONSORIZZAZIONI																✓					✓						✓
11	GESTIONE DEGLI ADEMPIMENTI SOCIETARI																						✓					
12	CONTABILITÀ GENERALE, BILANCIO E ALTRE COMUNICAZIONI SOCIALI															✓						✓						✓
13	GESTIONE DEI SERVIZI DI ASSICURAZIONE E PREVIDENZA VERSO LA CLIENTELA																✓					✓						
14	SELEZIONE E ASSUNZIONE DEL PERSONALE								✓								✓						✓					
15	GESTIONE DEL PERSONALE															✓	✓						✓				✓	
16	GESTIONE DELLA SALUTE E SICUREZZA SUL LAVORO										✓																	✓
17	GESTIONE DEGLI ASPETTI AMBIENTALI																✓					✓						✓
18	GESTIONE DEGLI INVESTIMENTI DELLA CLIENTELA																✓		✓			✓						✓
19	GESTIONE DEL DENARO CONTANTE, DELLE GARANZIE E DEI VALORI				✓																							
20	GESTIONE DELLA FINANZA E DELLA TESORERIA																✓					✓						✓
21	GESTIONE DEGLI ADEMPIMENTI ANTIRICICLAGGIO E ANTITERRORISMO															✓						✓						
22	PIANIFICAZIONE E CONTROLLO DI GESTIONE																✓					✓						✓

N	AREE A RISCHIO REATO	CATEGORIE DI REATO																										
		1. 24-25	2. 24-bis	3. 24-ter	4. 25-bis	5. 25-bis.1	6. 25-ter	7. 25-quater	8. 25-quater.1	9. 25-quinquies	10. 25-sexies	11. 25-septies	12. 25-octies	13. 25-octies.1	14. 25-octies.2	15. 25-novies	16. 25-decies	17. 25-undecies	18. 25-duodecies	19. 25-terdecies	20. 25-quaterdecies	21. 25-quinquiesdecies	22. 25-sexiesdecies	23. 25-septiesdecies	24. 25-duodevicies	25. 25-undevicies	26. L. n. 146/2006	Reg. UE 2023/1114
23	GESTIONE DI NUOVI PRODOTTI/SERVIZI E/O AGGIORNAMENTO DI QUELLI ESISTENTI E RELATIVO INSERIMENTO IN NUOVI MERCATI				✓	✓																						
24	GESTIONE DEGLI ADEMPIMENTI FISCALI	✓	✓				✓						✓									✓						
25	GESTIONE DEI FINANZIAMENTI VERSO LA CLIENTELA	✓					✓	✓					✓		✓													
26	GESTIONE DELLE OPERAZIONI DI MERCATO AI FINI DELLA PREVENZIONE DEGLI ILLECITI PENALI E AMMINISTRATIVI IN TEMA DI ABUSI DI MERCATO						✓				✓																	
27	GESTIONE DEI RAPPORTI CON LA CLIENTELA - OPERATORE ESTERO						✓	✓					✓		✓													
28	GESTIONE DEGLI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E DELLE PIATTAFORME DI PAGAMENTO IN USO	✓					✓	✓					✓	✓	✓													
29	GESTIONE DEL PATRIMONIO CULTURALE DELLA BANCA	✓					✓	✓					✓											✓	✓			
30	GESTIONE DEL PATRIMONIO IMMOBILIARE DELLA BANCA	✓					✓	✓					✓									✓						
31	GESTIONE DEI RAPPORTI CON INTERLOCUTORI TERZI - PUBBLICI O PRIVATI - NELLO SVOLGIMENTO DELLE PROPRIE ATTIVITÀ LAVORATIVE PER CONTO E/O NELL'INTERESSE DELLA BANCA			✓																							✓	

3. LE AREE A RISCHIO REATO

In considerazione dell'organizzazione adottata, del *business* e dei processi della Banca, ad esito delle attività di *risk assessment* sono state individuate le seguenti “aree a rischio reato”, trattate nelle successive sezioni della presente Parte Speciale:

1. gestione dei servizi di cassa e di tesoreria a favore della Pubblica Amministrazione;
2. approvvigionamento di beni, lavori, servizi e consulenze professionali;
3. gestione del contenzioso passivo e dei relativi rapporti con l'Autorità giudiziaria;
4. gestione del contenzioso attivo e dei relativi rapporti con l'Autorità giudiziaria;
5. gestione dei sistemi informativi;
6. gestione dei rapporti con la Pubblica Amministrazione e le Autorità di Vigilanza;
7. gestione dei rapporti con i *partner* commerciali/mediatori creditizi/agenti;
8. gestione degli omaggi e delle spese di rappresentanza;
9. gestione della comunicazione esterna;
10. gestione delle liberalità e delle sponsorizzazioni;
11. gestione degli adempimenti societari;
12. contabilità generale, bilancio e altre comunicazioni sociali;
13. gestione dei servizi di assicurazione e previdenza verso la clientela;
14. selezione e assunzione del personale;
15. gestione del personale;
16. gestione della salute e sicurezza sul lavoro;
17. gestione degli aspetti ambientali;
18. gestione degli investimenti della clientela;
19. gestione del denaro contante, delle garanzie e dei valori;
20. gestione della finanza e della tesoreria;
21. gestione degli adempimenti antiriciclaggio e antiterrorismo;
22. pianificazione e controllo di gestione;
23. gestione di nuovi prodotti/servizi e/o aggiornamento di quelli esistenti e relativo inserimento in nuovi mercati;
24. gestione degli adempimenti fiscali;
25. gestione dei finanziamenti verso la clientela;
26. gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato;
27. gestione dei rapporti con la clientela – operatore estero;

28. gestione degli strumenti di pagamento diversi dai contanti e delle piattaforme di pagamento in uso;
29. gestione del patrimonio culturale della Banca;
30. gestione del patrimonio immobiliare della Banca;
31. gestione dei rapporti con interlocutori terzi – pubblici o privati – nello svolgimento delle proprie attività lavorative per conto e/o nell'interesse della Banca.

L'attività della Banca, nell'ambito delle "aree a rischio reato" si ispira, oltre a quelli indicati nelle sezioni successive, ai seguenti principi generali di controllo trasversali:

- esistenza di un sistema di deleghe e procure nonché di un sistema organizzativo (compiti, ruoli e responsabilità formalizzati);
- esistenza di specifica regolamentazione interna aziendale disciplinare ruoli, responsabilità, attività, modalità operative e controlli;
- segregazione di responsabilità nell'esecuzione dei processi;
- tracciabilità e verificabilità *ex post* di ogni operazione relativa alle attività "sensibili";
- archiviazione della documentazione al fine di garantire la tracciabilità del processo.

Nelle sezioni successive, per ogni "area a rischio reato", sono illustrate, per sottopunti: (i) le categorie di reato applicabili ed i relativi principali reati presupposto astrattamente perpetrabili, (ii) le unità organizzative/funzioni aziendali coinvolte, (iii) le attività "sensibili", (iv) principi generali di comportamento (v) principali controlli preventivi a presidio dei rischi.

In particolare, si precisa che, in termini generali:

- al fine di prevenire e impedire il verificarsi di reati di cui al presente Protocollo, i Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto delle disposizioni di legge in materia, della normativa interna, delle previsioni del Codice Etico e, in misura non esaustiva, dei principi generali di comportamento di seguito indicati per ciascuna Area;
- i controlli, preventivi rappresentano, ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca a prevenzione della commissione dei sopra indicati reati.

1.1. GESTIONE DEI SERVIZI DI CASSA E DI TESORERIA A FAVORE DELLA PUBBLICA AMMINISTRAZIONE

1.1.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Peculato (art. 314 c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Peculato mediante profitto dell'errore altrui (art. 316 c.p.);
- Concussione (art. 317 c.p.);
- Turbata libertà degli incanti (art. 353 c.p.);
- Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.);
- Frode nelle pubbliche forniture (art. 356 c.p.);
- Truffa ai danni dello Stato o di altro Ente pubblico (art. 640, comma 2, n. 1 c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- Frode informatica (art. 640-ter, c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

5) Delitti contro l'industria e il commercio (art. 25-bis.1)

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Autoriciclaggio (648 ter 1 c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).

1.1.2. Unità organizzative/funzioni aziendali coinvolte

- Area Affari (CCO):
 - Sviluppo e Gestione Corporate/ Istituzionali:
 - Tesoreria Enti;
- Area Crediti (CLO).

1.1.3. Attività sensibili

- a) Gestione tesoreria Enti.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- negoziazione, stipulazione, esecuzione di contratti con soggetti pubblici ai quali si perviene mediante gare ad evidenza pubblica (aperte o ristrette) o affidamento diretto;
- gestione delle operazioni di incasso e pagamento per conto degli Enti Pubblici;
- rendicontazione periodica agli Enti Pubblici circa le operazioni effettuate.

1.1.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- l'instaurazione ed il mantenimento da parte dei Destinatari di qualsiasi rapporto con la P.A. e con soggetti terzi incaricati di una pubblica funzione o di un pubblico servizio, devono essere caratterizzati dal pieno rispetto dei ruoli istituzionali, delle previsioni di legge in materia e delle procedure aziendali, dando puntuale e sollecita esecuzione alle relative prescrizioni e adempimenti richiesti;
- gli adempimenti nei confronti della P.A. e delle Autorità di Vigilanza e la edisposizione della relativa documentazione devono essere effettuati nel rispetto delle previsioni di legge in materia, con diligenza e professionalità, in modo da fornire informazioni accurate, complete e veritiere, evitando e comunque segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;
- i soggetti coinvolti nei processi con responsabilità di firma di atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;
- la trasmissione, anche informatica, di dati e documenti alla P.A. e alle Autorità di Vigilanza, deve essere curata da parte di Esponenti Aziendali/dipendenti e soggetti formalmente autorizzati e nei limiti delle proprie competenze e mansioni;

- il personale non deve dar seguito a qualunque tentativo di estorsione o concussione in cui sia coinvolto un funzionario della P.A.. Ogni notizia al riguardo, se già non denunciata all'Autorità, deve essere riportata al proprio superiore gerarchico per i provvedimenti e le azioni di competenza;
- vengono stabiliti limiti all'impiego delle risorse finanziarie mediante soglie quantitative coerenti con le competenze gestionali e le responsabilità organizzative.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- promettere o effettuare erogazioni in denaro a favore di rappresentanti della P.A., italiana o straniera, per finalità diverse da quelle istituzionali e di servizio e in violazione delle prescrizioni aziendali;
- porre in essere comportamenti intimidatori e fraudolenti con lo scopo di allontanare gli altri offerenti nelle procedure di gara pubblica, nonché porre in essere comportamenti collusivi con gli altri offerenti volti a condizionare il normale svolgimento delle offerte;
- promettere o concedere vantaggi di qualsiasi natura (es.: promesse di assunzione, contributi, etc.) in favore di rappresentanti della P.A., italiana o straniera, al fine di influenzarne l'indipendenza di giudizio od assicurare un qualsiasi vantaggio per la Banca;
- dare o promettere denaro o altra utilità a soggetti intermediari affinché utilizzino relazioni esistenti con soggetti pubblici, allo scopo di indurre questi ultimi a compiere un atto contrario ai doveri d'ufficio costituente reato od a remunerarli per l'esercizio delle loro funzioni allo scopo di condizionare l'azione pubblica a vantaggio della Società;
- concedere finanziamenti senza la sussistenza dei necessari requisiti ad un cliente che vanti relazioni con esponenti della P.A., al fine di ottenere un indebito vantaggio per la Banca grazie all'eventuale mediazione illecita da parte del cliente;
- esibire documenti e dati falsi o alterati ed omettere informazioni dovute al fine di orientare a proprio favore le decisioni della P.A.;
- alterare il funzionamento di sistemi informativi e telematici o manipolare i dati in essi contenuti;
- compiere atti di concorrenza sleale;

- operare in una situazione di conflitto di interessi;
- eseguire le operazioni per le quali si sospetta vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo;
- instaurare relazioni personali di favore o influenza per condizionare, direttamente o indirettamente, l'esito del rapporto con esponenti della P.A.;
- sollecitare o persuadere un funzionario pubblico, attraverso un'intesa illecita, al compimento di un atto illegittimo (in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità o, ancora, in violazione dell'obbligo di astensione in caso di conflitto di interesse);
- divulgare informazioni sensibili relativi al processo di gara (e.g. prezzo, dettagli tecnici) in occasione di eventuali interazioni con terze parti (e.g. competitors);
- violare il dovere di buona fede nell'esecuzione delle obbligazioni e del contratto di pubblica fornitura nonché, nell'ambito di un appalto pubblico, omettere di informare la P.A. su circostanze sopravvenute in corso di esecuzione dell'opera che comportino una modifica della prestazione.

1.1.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca in base allo specifico ruolo attribuito loro dalla normativa interna della Banca, nonché ai sensi del vigente sistema dei poteri e delle deleghe;
- controllo della documentazione relativa alla stipula dei rapporti contrattuali da parte del Responsabile della struttura aziendale competente o dei soggetti a ciò facoltizzati;
- verifica della documentazione predisposta dalla Banca per rispondere ad inviti a presentare offerte a clienti/potenziati clienti, ovvero a bandi di gara pubblici, in termini di veridicità e congruità sostanziale e formale, da parte del Responsabile della struttura aziendale competente in virtù dell'oggetto del contratto o da soggetti a ciò facoltizzati;

- formale definizione delle modalità e dei criteri per la selezione dei bandi di gara pubblica ai quali partecipare;
- formale definizione delle modalità di raccolta e verifica delle informazioni necessarie per la predisposizione della documentazione per la partecipazione alla gara pubblica;
- presenza di controlli automatici del sistema informatico in merito alle operazioni di incasso/pagamento disposte dall'Ente;
- controlli periodici in merito ai saldi risultanti dalle operazioni di incasso / pagamento;
- flussi informativi periodici tra le funzioni preposte della Banca e gli Enti;
- verifica e formale approvazione della documentazione raccolta / predisposta, da inoltrare agli Enti pubblici ai fini della rendicontazione delle operazioni effettuate;
- profilazione degli accessi agli applicativi informatici utilizzati per disporre le operazioni di tesoreria, tutte riservate al solo personale autorizzato;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna struttura è responsabile dell'archiviazione e della conservazione della documentazione di competenza, relativa anche alle singole operazioni, prodotta anche in via telematica o elettronica, nonché degli accordi/convenzioni/contratti definitivi, nell'ambito delle attività proprie del processo della stipula di rapporti con la Pubblica Amministrazione.

1.2. APPROVVIGIONAMENTO DI BENI, LAVORI, SERVIZI E CONSULENZE PROFESSIONALI

1.2.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.);

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.);

- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Art. 2 Convenzione internazionale per la repressione del finanziamento del terrorismo 9 dicembre 1999.

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Autoriciclaggio (648 ter 1 c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.).

21) Reati Tributari (art. 25-quinquiesdecies)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000);
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000);
- Indebita compensazione (art. 10 D.Lgs. n. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000).

9) Delitti contro la personalità individuale (art. 25-quinquies)

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Approfittamento della vittima di riduzione in schiavitù o di tratta (art. 601.1 c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.).

18) Delitti di impiego di cittadini di Paesi terzi di cui il soggiorno è irregolare (art. 25-duodecies)

- Impiego di cittadini terzi il cui soggiorno è irregolare (art. 22, comma 12 bis, D.Lgs. n. 286/1998).

14) Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25-octies.2)

- Violazione delle misure restrittive dell'Unione europea (art. 275-bis c.p.);
- Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione Europea (art. 275-ter c.p.);
- Violazione delle condizioni dell'autorizzazione allo svolgimento di attività (art. 275-quater c.p.).

15) Delitti in materia di violazione del diritto d'autore (art. 25-novies)

- Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171 L. 633/1941);
- Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-bis L. 633/1941);
- Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (art. 171-ter L. 633/1941).

5) Delitti contro l'industria e il commercio (art. 25-bis.1)

- Turbata libertà dell'industria o del commercio (art. 513 c.p.).

13) Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1)

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.);
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.);
- Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.);
- Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1, comma 2).

1.2.2. Unità organizzative/funzioni aziendali coinvolte

- Area Operativa (COO):
 - Acquisti, Fornitori ed Esternalizzazioni;

- Legale;
- Area Pianificazione e Amministrazione (CFO):
 - Pianificazione e Controllo di Gestione;
 - Amministrazione:
 - Contabilità e Bilancio;
- Ufficio aziendale richiedente (*Centri di Responsabilità*);
- Soggetti autorizzati alla spesa sulla base della normativa interna vigente.

1.2.3. Attività sensibili

- a) Approvvigionamento di beni, lavori, servizi e consulenze professionali.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- definizione e gestione del budget;
- anagrafica fornitori;
- selezione, qualifica e monitoraggio dei fornitori/consulenti/professionisti esterni;
- predisposizione e approvazione delle autorizzazioni di spesa;
- predisposizione, stipula e gestione del contratto / ordine d'acquisto;
- ricezione di beni, lavori, servizi e consulenze professionali;
- gestione della fatturazione;
- gestione ed emissione del benestare al pagamento.

1.2.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- i soggetti coinvolti nei processi con responsabilità di firma di atti o documenti con rilevanza all'esterno della Banca devono essere appositamente delegati;
- stabilire limiti all'impiego delle risorse finanziarie mediante soglie quantitative di spesa coerenti con le competenze gestionali e le responsabilità organizzative; segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione delle procedure acquisitive;
- la stipula da parte della Banca di contratti con i fornitori deve essere condotta in conformità con la normativa vigente e con i principi, i criteri e le disposizioni di cui alle procedure aziendali;

- negli accordi contrattuali stipulati con fornitori, collaboratori e/o consulenti esterni deve essere contenuta un'apposita dichiarazione con cui gli stessi confermano di essere a conoscenza della normativa di cui al D. lgs. 231/2001 ed al Codice Etico della Banca;
- assicurare per ciascun contratto e/o ordine di acquisto emesso dalla Banca, attraverso opportune modalità di controllo, la completezza dei dati, la corrispondenza con la relativa richiesta di acquisto debitamente autorizzata, la correttezza dell'importo e dei termini di pagamento;
- assicurare la corretta contabilizzazione delle operazioni di acquisto, cessione / dismissione di immobilizzazioni immateriali, materiali e finanziarie e relative plusvalenze o svalutazioni;
- verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- evitare di accettare pagamenti in contanti e non effettuare fatturazioni nei confronti dei soggetti diversi da quelli che assumono il ruolo di controparti contrattuali e in assenza di adeguata giustificazione; effettuare le opportune verifiche sulla tesoreria;
- verificare l'attendibilità commerciale e professionale dei fornitori e delle controparti contrattuali; verificare che i dati raccolti relativamente ai rapporti con terzi siano completi ed aggiornati sia per la corretta e tempestiva individuazione dei medesimi, sia per una valida valutazione del profilo;
- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza o la vicinanza a organizzazioni criminali o comunque illecite.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- autorizzare il pagamento di beni/servizi in assenza di verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- favorire indebitamente, nei processi di acquisto, collaboratori, fornitori, consulenti o altri soggetti terzi, in quanto indicati dagli interlocutori/referenti privati;
- effettuare prestazioni o pagamenti di compensi in favore di collaboratori, fornitori, consulenti, partner o altri soggetti terzi che operino per conto della Società, che non

trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e/o in relazione al tipo di incarico da svolgere dalle prassi vigenti;

- effettuare pagamenti delle spettanze verso i soggetti terzi attraverso sistemi inusuali, artificiosamente elaborati e/o triangolazioni con ulteriori soggetti esterni;
- assegnare incarichi di fornitura a terzi nei casi in cui si abbia notizia, o anche solo il sospetto, dell'utilizzo di lavoratori sottoposti a condizioni di sfruttamento, riduzione o mantenimento in stato di soggezione continuativa ovvero di riduzione o mantenimento in schiavitù o in servitù;
- affidare appalti / sub-appalti a società che impiegano lavoratori stranieri privi di permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, o risulti revocato o annullato;
- è vietato porre in essere, anche indirettamente, operazioni commerciali in violazione di misure restrittive dell'Unione Europea o delle relative disposizioni nazionali di attuazione, ivi incluse, a titolo meramente esemplificativo e non esaustivo, operazioni con stati terzi sottoposti a embargo o verso soggetti inseriti in c.d. blacklist dell'Unione Europea.

1.2.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- i soggetti che esercitano poteri autorizzativi e/o negoziali e i soggetti aventi facoltà di rappresentare la Banca nell'ambito delle attività presidiate nel presente Protocollo, sono individuati e autorizzati in base allo specifico ruolo attribuito loro nella normativa interna;
- previsione del Referente per le attività esternalizzate, con il compito di assicurare il governo di tutti i servizi acquisiti in regime di esternalizzazione, oltre che di sovrintendere ai processi di valutazione propedeutici a una qualsiasi decisione di outsourcing, garantendo efficacia e omogeneità alle attività di reportistica e controllo sulle attività esternalizzate;
- gli incarichi a fornitori, collaboratori e/o consulenti esterni sono redatti per iscritto, con evidenza di tutte le condizioni applicabili e con indicazione del compenso pattuito;

- l'eventuale affidamento a terzi – da parte dei fornitori della Banca – di attività in sub-appalto, è contrattualmente subordinato ad un preventivo assenso da parte della struttura della Banca che ha stipulato il contratto;
- formalizzazione del budget annuale e formale processo di approvazione delle spese extra budget con delibera ai massimi livelli di responsabilità;
- monitoraggio costante dei dati di budget e delle performance realizzate con discussione degli esiti e delle eventuali azioni correttive in sede di CdA;
- verifiche dei limiti di spesa e della pertinenza della stessa;
- verifica della regolarità, completezza, correttezza e tempestività delle scritture contabili;
- previsione di controlli di coerenza delle spese sostenute rispetto al budget assegnato al Responsabile di riferimento;
- verifica del rispetto dei criteri individuati dalla normativa aziendale per la scelta dei fornitori e dei professionisti/consulenti;
- la scelta dei fornitori di beni e servizi e dei professionisti avviene tra i nominativi selezionati all'interno dell'Albo fornitori, in base a criteri individuati nell'ambito della normativa interna;
- l'anagrafica fornitori deve essere aggiornata e riflettere correttamente tutti gli elementi di esistenza/qualificazione degli stessi;
- l'inserimento o la modifica a sistema dell'anagrafica dei fornitori deve essere supportato da apposita documentazione giustificativa;
- monitoraggio periodico sulla qualifica del fornitore/consulente/professionista esterno presente nell'albo attraverso la verifica periodica della sussistenza dei requisiti (tecnici, professionali, onorabilità, etc.) in capo ai soggetti già qualificati;
- verifica del rispetto delle norme di legge che vietano o subordinano a determinate condizioni il conferimento di incarichi di qualunque tipologia;
- previsione di controlli formali circa il possesso dei requisiti di onorabilità e professionalità (necessarie competenze ed esperienze) del consulente/professionista esterno in fase di selezione dello stesso;
- l'approvazione della richiesta di acquisto, l'emissione dell'ordine, il conferimento di incarico e il perfezionamento del contratto spettano esclusivamente a soggetti muniti

di idonei poteri in base al sistema di poteri, deleghe e procure in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno, così come definiti all'interno della normativa interna;

- invito di un numero adeguato di operatori economici qualificati (minimo due) per la categoria merceologica oggetto della richiesta di Acquisto;
- in deroga a quanto sopra previsto è possibile richiedere una sola offerta nei seguenti casi e con espressa motivazione scritta da allegare agli atti: (i) eventuali difficoltà nel reperire il numero di offerte minimo (due), nei casi di servizi o beni prodotti da un numero limitato di fornitori; (ii) in casi di comprovata urgenza per l'avvio di un'attività facendo ricorso a fornitori/consulenti di comprovata esperienza e di elevato standing;
- negli accordi contrattuali stipulati con fornitori, collaboratori e/o consulenti esterni deve essere contenuta un'apposita dichiarazione con cui gli stessi confermano di essere a conoscenza della normativa di cui al D. lgs. 231/2001 ed al Codice Etico della Banca;
- verifica periodica da parte delle competenti strutture/funzioni sulla gestione dei contratti con i fornitori e sulla corretta esecuzione dei processi di acquisto in modo da testarne e verificarne l'effettività, l'applicabilità e l'utilizzo corrente;
- verifica e certificazione, supportata da adeguata documentazione giustificativa, della corrispondenza tra il bene/lavoro/servizio/consulenza e prestazione di opera intellettuale ricevuta e quanto previsto nell'OdA/contratto (dal punto di vista qualitativo e quantitativo);
- verifiche periodiche in merito alla qualità dell'operato degli outsourcer e controllo sui costi derivati dall'attività svolta;
- il pagamento della prestazione o della fornitura sulla scorta della fattura/fattura elettronica o documento similare fiscalmente regolare emessa dal fornitore e inviato alla Banca;
- controlli sulle transazioni riguardano tutti i trasferimenti di fondi effettuati gli eventuali beni e servizi sottostanti agli stessi, per verificare che non siano stati violati provvedimenti di embargo o analoghe restrizioni di natura commerciale o finanziaria (a esempio, divieti o restrizioni all'accesso ai servizi finanziari, agli investimenti o alle transazioni di capitali);
- l'autorizzazione al pagamento della fattura spetta ai Responsabili delle Unità Organizzative per le quali è prevista l'assegnazione di un budget e delle relative facoltà

di spesa o ai soggetti all'uopo incaricati; può essere negata a seguito di formale contestazione delle inadempienze/carenze della fornitura adeguatamente documentata e dettagliata a cura delle predette Unità Organizzative;

- il pagamento delle fatture è effettuato da una specifica struttura/funzione aziendale dedicata;
- utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;
- documentabilità di ogni attività del processo con particolare riferimento alla fase di individuazione del fornitore di beni e/o servizi, o professionista/consulente, anche attraverso gare, in termini di motivazione della scelta nonché pertinenza e congruità della spesa;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione delle procedure acquisitive di beni e servizi.

1.3. GESTIONE DEL CONTENZIOSO PASSIVO E DEI RELATIVI RAPPORTI CON L'AUTORITÀ GIUDIZIARIA

1.3.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 317, 318, 319, 319-bis, 319-ter, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

16) Delitti di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies)

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

21) Reati Tributari (art. 25-quinquiesdecies)

- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000);
- Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000).

1.3.2. Unità organizzative/funzioni aziendali coinvolte

- Legale;
- Area Crediti Deteriorati:
 - Gestione Crediti Deteriorati;
 - Gestione Contenzioso.

1.3.3. Attività sensibili

- a) Gestione dei contenziosi passivi giudiziali e stragiudiziali (amministrativi, civili, penali, fiscali, giuslavoristici e previdenziali) e degli accordi transattivi.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- contenziosi giudiziali e stragiudiziali (sia con soggetti aventi natura privatistica che con Enti pubblici);
- definizione di accordi transattivi;
- reclami presentati alla Banca da parte della clientela (in relazione ai quali possono sorgere controversie definibili tramite transazioni o contenziosi).

1.3.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- i soggetti coinvolti nei processi con responsabilità di firma di atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;

- la trasmissione, anche informatica, di dati e documenti alla P.A. e alle Autorità di Vigilanza, deve essere curata da parte di Esponenti Aziendali/dipendenti e soggetti formalmente autorizzati e nei limiti delle proprie competenze e mansioni;
- gli incarichi a fornitori, collaboratori e/o consulenti esterni devono essere sempre redatti per iscritto, con l'evidenziazione di tutte le condizioni applicabili e l'indicazione del compenso pattuito; non è consentito riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del contenzioso e degli accordi transattivi, i contratti/lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- gli adempimenti nei confronti della P.A. e delle Autorità di Vigilanza e la predisposizione della relativa documentazione devono essere effettuati nel rispetto delle previsioni di legge in materia, con diligenza e professionalità, in modo da fornire informazioni accurate, complete e veritiere, evitando e comunque segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;
- nei rapporti con l'Autorità giudiziaria, i destinatari del Modello sono tenuti a prestare una fattiva collaborazione ed a rendere dichiarazioni veritiere, trasparenti ed esaurientemente rappresentative dei fatti;
- nei rapporti con l'Autorità giudiziaria, i destinatari e, segnatamente, coloro i quali dovessero risultare indagati o imputati in un procedimento penale, anche connesso, inerente all'attività lavorativa prestata in Banca, sono tenuti ad esprimere liberamente le proprie rappresentazioni dei fatti od a esercitare la facoltà di non rispondere accordata dalla legge;
- nei rapporti con l'Autorità giudiziaria ai Destinatari del Modello non è consentito accettare denaro o altra utilità, anche attraverso consulenti eventualmente incaricati dalla Banca medesima.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- promettere od offrire erogazioni in denaro o di altre utilità a favore di soggetti coinvolti in procedimenti giudiziari al fine di indurli ad occultare/omettere fatti che possano arrecare pene/sanzioni alla Banca, proteggendo o migliorando la posizione di quest'ultima;
- indurre un soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria nel corso di un procedimento penale, attraverso minaccia o violenza (coazione fisica o morale) al fine di occultare/omettere fatti che possano arrecare pene/sanzioni alla Banca;
- porre in essere (direttamente o indirettamente) qualsiasi attività che possa favorire o danneggiare una delle parti in causa, nel corso di procedimenti civili, penali o amministrativi;
- condizionare o indurre, in qualsiasi forma e con qualsiasi modalità, la volontà dei soggetti chiamati a rispondere all'Autorità Giudiziaria al fine di non rendere dichiarazioni o dichiarare fatti non rispondenti al vero;
- tenere una condotta ingannevole o comportamenti volti ad influenzare l'indipendenza di giudizio dei Giudici competenti, dei consulenti tecnici e dei loro ausiliari incaricati di svolgere gli accertamenti e le verifiche ispettive (es. al fine di evitare sanzioni per la Banca);
- presentare ai Giudici informazioni non veritiere e/o non complete o eludere obblighi di legge/normativi;
- affidare incarichi a professionisti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza.

1.3.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- accentramento delle responsabilità di indirizzo e/o gestione e monitoraggio delle singole fasi del processo in capo a specifiche strutture della Banca per la gestione dei contenziosi e degli accordi transattivi;

- approvazione e sottoscrizione degli atti che impegnano la Banca esclusivamente da parte di soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- adeguata tracciatura del processo che conduce ad un accordo transattivo e formalizzazione e sottoscrizione degli eventuali accordi transattivi in coerenza con il sistema autorizzativo in essere;
- verifica del corretto espletamento degli obblighi risultanti dall'accordo transattivo da parte della Banca;
- definizione delle modalità di individuazione dei legali esterni, previa accurata verifica delle necessarie qualifiche, competenze e requisiti;
- verifica di congruità tra le condizioni economico-finanziarie definite nei contratti con quanto previsto da tabelle professionali standard;
- definizione di controlli circa la corretta valorizzazione del servizio fornito dai legali esterni;
- formale dichiarazione relativa ad eventuali rapporti/conflitti di interesse con esponenti della Pubblica Amministrazione;
- interfaccia con i soggetti coinvolti in procedimenti giudiziari o chiamati a rendere dichiarazioni davanti all'Autorità Giudiziaria esclusivamente per il tramite di legali interni ed esterni (ove coinvolti) e le persone debitamente autorizzate;
- rilevazione e monitoraggio periodico delle controversie pendenti anche mediante informativa alla Direzione Generale ed al Consiglio di Amministrazione;
- monitoraggio periodico dello status dei contenziosi in corso, in coordinamento con i legali esterni incaricati;
- protocollazione ed archiviazione degli atti giudiziari in entrata;
- verifica e approvazione della documentazione da inviare all'Autorità Giudiziaria (mezzi probatori, atti di causa, scritti difensivi, etc.) da parte degli Uffici interni, dei legali esterni (ove coinvolti) e dei soggetti coinvolti nel procedimento;
- verifica del corretto espletamento degli obblighi risultanti dall'accordo transattivo da parte della Banca;

- archiviazione e conservazione di tutta la documentazione prodotta nell'ambito delle attività svolte, inclusa la copia di quella trasmessa all'Autorità Giudiziaria anche in via telematica;
- tutti i flussi informativi e documentali, interni ed esterni, sono scambiati a mezzo e-mail o posta cartacea protocollata e, in ogni caso, con modalità tali da garantirne la tracciabilità.

1.4. GESTIONE DEL CONTENZIOSO ATTIVO E DEI RELATIVI RAPPORTI CON L'AUTORITÀ GIUDIZIARIA

1.4.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 317, 318, 319, 319-bis, 319-ter, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

16) Delitti di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies)

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

21) Reati Tributari (art. 25-quinquiesdecies)

- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000);
- Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000).

1.4.2. Unità organizzative/funzioni aziendali coinvolte

- Legale;

- Area Crediti Deteriorati:
 - Gestione Crediti Deteriorati;
 - Gestione Contenzioso.

1.4.3. Attività sensibili

- a) Gestione dei contenziosi attivi giudiziali e stragiudiziali (amministrativi, civili, penali, fiscali, giuslavoristici e previdenziali) e degli accordi transattivi.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- contenziosi giudiziali e stragiudiziali (sia con soggetti aventi natura privatistica che con Enti pubblici);
- definizione di accordi transattivi;
- attività connesse alla gestione delle attività di recupero dei crediti.

1.4.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- i soggetti coinvolti nei processi con responsabilità di firma di atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;
- la trasmissione, anche informatica, di dati e documenti alla P.A. e alle Autorità di Vigilanza, deve essere curata da parte di Esponenti Aziendali/dipendenti e soggetti formalmente autorizzati e nei limiti delle proprie competenze e mansioni;
- gli incarichi a fornitori, collaboratori e/o consulenti esterni devono essere sempre redatti per iscritto, con l'evidenziazione di tutte le condizioni applicabili e l'indicazione del compenso pattuito; non è consentito riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del contenzioso e degli accordi transattivi, i contratti/lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;

- gli adempimenti nei confronti della P.A. e delle Autorità di Vigilanza e la predisposizione della relativa documentazione devono essere effettuati nel rispetto delle previsioni di legge in materia, con diligenza e professionalità, in modo da fornire informazioni accurate, complete e veritiere, evitando e comunque segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;
- nei rapporti con l'Autorità giudiziaria, i destinatari del Modello sono tenuti a prestare una fattiva collaborazione ed a rendere dichiarazioni veritiere, trasparenti ed esaurientemente rappresentative dei fatti;
- nei rapporti con l'Autorità giudiziaria, i destinatari e, segnatamente, coloro i quali dovessero risultare indagati o imputati in un procedimento penale, anche connesso, inerente all'attività lavorativa prestata in Banca, sono tenuti ad esprimere liberamente le proprie rappresentazioni dei fatti od a esercitare la facoltà di non rispondere accordata dalla legge;
- nei rapporti con l'Autorità giudiziaria ai Destinatari del Modello non è consentito accettare denaro o altra utilità, anche attraverso consulenti eventualmente incaricati dalla Banca medesima.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- promettere od offrire erogazioni in denaro o di altre utilità a favore di soggetti coinvolti in procedimenti giudiziari al fine di indurli ad occultare/omettere fatti che possano arrecare pene/sanzioni alla Banca, proteggendo o migliorando la posizione di quest'ultima;
- indurre un soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria nel corso di un procedimento penale, attraverso minaccia o violenza (coazione fisica o morale) al fine di occultare/omettere fatti che possano arrecare pene/sanzioni alla Banca;
- porre in essere (direttamente o indirettamente) qualsiasi attività che possa favorire o danneggiare una delle parti in causa, nel corso di procedimenti civili, penali o amministrativi;

- condizionare o indurre, in qualsiasi forma e con qualsiasi modalità, la volontà dei soggetti chiamati a rispondere all'Autorità Giudiziaria al fine di non rendere dichiarazioni o dichiarare fatti non rispondenti al vero;
- tenere una condotta ingannevole o comportamenti volti ad influenzare l'indipendenza di giudizio dei Giudici competenti, dei consulenti tecnici e dei loro ausiliari incaricati di svolgere gli accertamenti e le verifiche ispettive (es. al fine di evitare sanzioni per la Banca);
- presentare ai Giudici informazioni non veritiere e/o non complete o eludere obblighi di legge/normativi;
- affidare incarichi a professionisti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza.

1.4.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- la gestione dei contenziosi e degli accordi transattivi prevede l'accentramento delle responsabilità di indirizzo e/o gestione e monitoraggio delle singole fasi del processo in capo a specifiche strutture della Banca;
- gli atti che impegnano la Banca devono essere approvati e sottoscritti soltanto da soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- il processo che conduce ad un accordo transattivo è adeguatamente tracciato e gli eventuali accordi transattivi sono debitamente formalizzati e sottoscritti in coerenza con il sistema autorizzativo in essere;
- verifica del corretto espletamento degli obblighi risultanti dall'accordo transattivo da parte della Banca;
- definizione delle modalità di individuazione dei legali esterni, previa accurata verifica delle necessarie qualifiche, competenze e requisiti;
- verifica di congruità tra le condizioni economico-finanziarie definite nei contratti con quanto previsto da tabelle professionali standard;

- definizione di controlli circa la corretta valorizzazione del servizio fornito dai legali esterni;
- formale dichiarazione relativa ad eventuali rapporti/conflitti di interesse con esponenti della Pubblica Amministrazione;
- interfaccia con i soggetti coinvolti in procedimenti giudiziari o chiamati a rendere dichiarazioni davanti all'Autorità Giudiziaria esclusivamente per il tramite di legali interni ed esterni (ove coinvolti) e le persone debitamente autorizzate;
- rilevazione e monitoraggio periodico delle controversie pendenti anche mediante informativa alla Direzione Generale ed al Consiglio di Amministrazione;
- approvazione, nel rispetto delle deleghe in essere, delle strategie di gestione dei contenziosi giudiziali/stragiudiziali (ai fini del recupero dei crediti);
- predisposizione di un flusso informativo verso la Direzione Generale e il Consiglio di Amministrazione inerente alla situazione delle posizioni in contenzioso e dei “dubbi esiti”, evidenziando le pratiche destinate a buon fine, quelle di recuperabilità dubbia e quelle ove è prevedibile una perdita, collaborando con le Funzioni competenti alla relativa definizione;
- monitoraggio periodico dello status dei contenziosi in corso, in coordinamento con i legali esterni / società di recupero crediti incaricati;
- protocollazione ed archiviazione degli atti giudiziari in entrata;
- verifica e approvazione della documentazione da inviare all'Autorità Giudiziaria (mezzi probatori, atti di causa, scritti difensivi, etc.) da parte degli Uffici interni, dei legali esterni (ove coinvolti) e dei soggetti coinvolti nel procedimento;
- archiviazione e conservazione di tutta la documentazione prodotta nell'ambito delle attività svolte, inclusa la copia di quella trasmessa all'Autorità Giudiziaria anche in via telematica;
- tutti i flussi informativi e documentali, interni ed esterni, sono scambiati a mezzo e-mail o posta cartacea protocollata e, in ogni caso, con modalità tali da garantirne la tracciabilità.

1.5. GESTIONE DEI SISTEMI INFORMATIVI

1.5.1. Reati astrattamente ipotizzabili

2) Delitti informatici e trattamento illecito dei dati (art. 24-bis)

- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- Documenti informatici (art. 491 bis c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 615 quater c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- Danneggiamento di sistemi informatici di pubblica utilità (art. 635 quinquies c.p.);
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.);
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1 c.p.);
- Estorsione (art. 629, comma 3, c.p.);
- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105).

15) Delitti in materia di violazione del diritto d'autore (art. 25-novies)

- Divulgazione tramite reti telematiche di un'opera dell'ingegno protetta (Art. 171 L. 633/1941);
- Duplicazione, a fini di lucro, di programmi informatici o importazione, distribuzione, vendita, detenzione per fini commerciali di programmi contenuti in supporti non contrassegnati dalla SIAE (Art. 171-bis L. 633/1941);
- Duplicazione, riproduzione, trasmissione di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio (Art. 171-ter L. 633/1941);
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione

di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Frode informatica (art. 640 ter).

1.5.2. Unità organizzative/funzioni aziendali coinvolti

- Area Operativa (COO):
 - Sistemi e tecnologie;
 - Sicurezza informatica.
- Chief Risk Officer (CRO);
- DPO;
- tutte le figure professionali coinvolte nei processi aziendali e ivi operanti a qualsiasi titolo, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale, che utilizzano i sistemi informativi della Banca.

1.5.3. Attività sensibili

- a) Gestione dei profili di accesso e di autenticazione/autorizzazione alle apparecchiature informatiche, alla rete e ai sistemi nonché della sicurezza perimetrale fisica e logica e protezione delle apparecchiature;
- b) Sistema di gestione della sicurezza delle informazioni e dei dati;
- c) Gestione degli incidenti informatici;
- d) Gestione della riproduzione e diffusione all'interno dei sistemi informativi aziendali di opere tutelate dal diritto di autore e dai diritti connessi;
- e) Sviluppo, implementazione e manutenzione di software, apparecchiature, dispositivi, connessioni, reti o componenti tecniche connesse al sistema informatico.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- strutturazione del sistema informatico aziendale, gestione ed evoluzione della piattaforma tecnologica e applicativa IT;
- analisi del rischio e definizione dei requisiti di sicurezza informatica;
- gestione degli asset informativi;
- utilizzo della rete aziendale, del servizio di posta elettronica e accesso ad Internet;

- gestione di informazioni, dati e programmi informatici e della documentazione informatica.

1.5.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- definire e adottare opportune misure volte a garantire la massima riservatezza sulle informazioni raccolte negli archivi dei sistemi informativi, nonché le misure necessarie a garantire la sicurezza fisica e logistica degli stessi;
- impiegare sulle apparecchiature della Banca soltanto prodotti ufficialmente acquisiti;
- rispettare le procedure e gli standard previsti in materia di utilizzazione delle risorse informatiche, segnalando senza ritardo alle strutture competenti eventuali utilizzi e/o funzionamenti anomali di queste ultime;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- in caso di smarrimento o furto di qualsiasi apparecchiatura informatica, informare tempestivamente il responsabile della struttura competente alla gestione dei relativi sistemi/dispositivi informatici;
- le password di accesso alle applicazioni ed ai sistemi informativi della sono strettamente personali e in quanto tali non devono essere comunicate a terzi. Ciascun utente è responsabile della custodia delle proprie password e di qualsiasi operazione effettuata con la propria utenza;
- provvedere, entro le scadenze indicate dal responsabile della sicurezza informatica, alla modifica periodica della password;
- attenersi a quanto disposto dalle procedure aziendali e linee guida nell'ambito delle attività svolte mediante strumentazioni, piattaforme o sistemi informatici;
- i prodotti software installati (sia sulle apparecchiature assegnate all'utenza che relativi alla infrastruttura di rete) sono approvati dalla banca e correttamente licenziati; regolari contratti di manutenzione vigenti, prevedono il supporto necessario e l'accesso ai relativi aggiornamenti periodici. In particolare, per quanto relativo ai dispositivi mobili quali smartphone o tablet, sono vietate l'installazione e l'utilizzo di applicazioni

e software non licenziati (inclusi i software di sicurezza) o non presenti negli store ufficiali (quali Apple Store, Google Play Store);

- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- conformarsi alle prescrizioni del Regolamento U.E. n. 679/2016 ("GDPR") e d.lgs. n. 196/2003, T.U. Privacy, come modificato dal d.lgs. n. 101/2018 e alle direttive e raccomandazioni impartite dal Garante della Privacy a tutela della riservatezza dei dati personali di terzi.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- utilizzare i sistemi informatici aziendali per finalità non connesse alla mansione svolta;
- compromettere i controlli di sicurezza di sistemi informatici aziendali;
- eludere, anche attraverso programmi informatici, i blocchi apposti dalla Banca alla rete internet volti ad evitare l'indebito accesso a siti vietati;
- accedere in maniera non autorizzata ai sistemi informativi di terzi, alterarne il loro funzionamento, al fine di ottenere e/o modificare, senza diritto, dati, programmi o informazioni;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (ad esempio virus, worm, trojan, spyware, dialer, keylogger, rootkit) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- installare o comunque utilizzare strumenti software o hardware che potrebbero essere adoperati per analizzare o compromettere la sicurezza di sistemi informatici o telematici;
- divulgare, cedere o condividere con personale interno o esterno alla Banca le proprie credenziali di accesso ai sistemi ed alla rete aziendale o di terzi;
- violare i sistemi informatici di società concorrenti per acquisire la loro documentazione;

- danneggiare le infrastrutture tecnologiche di società concorrenti al fine di impedirne l'attività o danneggiarne l'immagine;
- danneggiare, distruggere o manomettere documenti informatici aventi efficacia probatoria, registrati presso Enti pubblici (es. polizia, uffici giudiziari, etc.), e relativi a procedimenti o indagini giudiziarie in cui la Banca sia coinvolta a qualunque titolo;
- produrre e trasmettere documenti in formato elettronico con dati/informazioni alterate;
- costringere chiunque a fare od omettere qualcosa attraverso la realizzazione o la minaccia di compiere condotte illecite in ambito informatico;
- utilizzare la posta elettronica per ricevere, memorizzare o spedire materiale – anche promozionale o di supporto ad eventi, workshop, presentazione di prodotti finanziari realizzati dalla Banca - che violi il copyright, il marchio o altre leggi sul diritto d'autore;
- utilizzare immagini, video, composizioni musicali, banche dati ovvero qualsiasi opera dell'ingegno protetta dal diritto d'autore senza aver ottenuto le necessarie licenze e permessi;
- utilizzare software, applicativi e banche dati non originali o sprovvisti del contrassegno SIAE, ovvero privi di valida ed efficace licenza di utilizzo e di certificazione, nonché con modalità non conformi alle prescrizioni contrattuali, nonché alle istruzioni impartite dal proprio Responsabile;
- elaborare prodotti informatici e/o il loro utilizzo, ove realizzati in house, privi dei requisiti di conformità, di funzionalità, di liceità e di conformità ad eventuali privative brevettuali di terzi;
- utilizzare sistemi di intelligenza artificiale, piattaforme o strumenti di IA non preventivamente autorizzati dalla Società.

1.5.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e dei soggetti aventi facoltà di rappresentare la Banca nell'ambito delle attività

sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna;

- formale approvazione del contratto con l'outsourcer e fornitori esterni sulla base di adeguati livelli autorizzativi;
- adozione di regolamenti e procedure aventi ad oggetto il corretto utilizzo delle risorse informatiche aziendali, la sicurezza informatica/telematica, la protezione dei dati sensibili;
- formale richiesta per la creazione/modifica/eliminazione di utenze abilitate all'utilizzo dei sistemi informativi aziendali;
- formale autorizzazione per la creazione di utenze abilitate all'utilizzo dei sistemi informativi aziendali, da parte di soggetti dotati dei poteri necessari;
- verifica di corrispondenza tra il ruolo del richiedente e la tipologia di utenza da abilitare/modificare/eliminare;
- previsione di controlli circa la sussistenza dei diritti di accesso ai sistemi e rimozione degli stessi al termine del rapporto di lavoro;
- definizione di criteri in merito alla corretta creazione e gestione delle password;
- definizione di appositi criteri per la creazione di "account speciali";
- definizione di credenziali di accesso univoche;
- accesso ai sistemi e ai dati consentito agli utenti unicamente per mezzo degli strumenti elettronici autorizzati, utilizzando le credenziali di autenticazione personali fornite;
- sistematica registrazione degli accessi ai sistemi informatici della Banca, tramite specifici sistemi di log management;
- tracciatura delle attività effettuate sui dati, compatibili con le leggi vigenti al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate;
- presidi di blocco automatico delle utenze in caso di ripetuti tentativi di accesso nei sistemi informatici aziendali con credenziali errate;
- previsione di attività di monitoraggio/controllo periodico dell'efficacia e operatività del sistema di gestione della sicurezza informatica;

- protezione e controllo delle aree fisiche in modo da scongiurare accessi non autorizzati, alterazione o sottrazione degli asset informativi;
- previsione di tecniche crittografiche e di firma digitale per garantire la riservatezza, l'integrità e il non ripudio delle informazioni archiviate o trasmesse;
- esistenza di regole formalizzate al fine di garantire un utilizzo corretto delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni;
- utilizzo di appositi software antivirus atti ad individuare e prevenire l'installazione di applicativi potenzialmente dannosi;
- utilizzo di specifico web filtering software (Firewall) al fine di bloccare l'accesso a siti Web che contengono contenuto limitato dalla politica aziendale o che potrebbero influire sulla sicurezza o le prestazioni operative della rete della Banca o dei sistemi informatici;
- previsione di regole formalizzate connesse alla gestione degli incidenti e dei problemi di sicurezza informatica;
- formale previsione di canali gestionali per la comunicazione degli Incidenti e Problemi (relativamente a tutta la catena tecnologica);
- gestione degli incidenti di sicurezza informatica, con l'obiettivo di identificare tempestivamente e minimizzare l'impatto di eventi avversi in ambito di sicurezza informatica, garantendo il tempestivo ripristino del regolare funzionamento dei servizi e delle risorse ICT coinvolte;
- adozione di specifiche soluzioni di continuità operativa di tipo tecnologico, organizzativo e infrastrutturale che assicurino la predetta continuità anche a fronte di situazioni di emergenza;
- verifica, da parte di adeguati livelli organizzativi, circa la riproduzione e diffusione all'interno dei sistemi informativi della Banca di opere tutelate dal diritto d'autore;
- previsione di controlli circa il rispetto dei termini delle licenze/contratto per l'utilizzo del software;
- identificazione dei soggetti preposti al coordinamento delle attività di gestione dei sistemi informativi della Banca;

- previsione della formale identificazione dei requisiti di sicurezza e di conformità tecnica in fase di acquisizione, sviluppo, fornitura e manutenzione del sistema informatico (inclusivo di componente hardware, software e delle componenti tecniche connesse);
- formale approvazione del contratto con la Società terza che si occupa di sviluppo, implementazione e manutenzione di software da parte di adeguati livelli autorizzativi;
- tracciabilità delle richieste di intervento di manutenzione (evolutiva, correttiva e ordinaria) sui sistemi informativi della Banca;
- formale autorizzazione degli interventi di manutenzione sui sistemi informativi della Banca;
- adeguata formazione del personale e dei fornitori sugli aspetti di sicurezza per sviluppare una maggiore sensibilità;
- il personale è tenuto a conformarsi alle regole, procedure e policy aziendali, di tempo in tempo applicabili, in merito all'utilizzo di strumenti di intelligenza artificiale.

1.6. GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E LE AUTORITÀ DI VIGILANZA

1.6.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-ter, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Concussione (art. 317 c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.);
- Truffa ai danni dello Stato o di altro Ente pubblico (art. 640, comma 2, n. 1 c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- Malversazione di erogazioni pubbliche (art. 316-bis c.p.);
- Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.);
- Turbata libertà degli incanti (art. 353 c.p.);
- Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.);
- Frode informatica (art. 640-ter, c.p.).

2) Delitti informatici e trattamento illecito dei dati (art. 24-bis)

- Documenti informatici (art. 491 bis c.p.).

6) Reati societari (art. 25-ter)

- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

16) Delitti di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-decies)

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.).

1.6.2. Unità organizzative/funzioni aziendali coinvolte

- Legale;
- Affari Societari, Soci e Investor Relations;
- Filiali;
- Aree Territoriali;
- Internal Audit;
- Chief Risk Officer (CRO);
- Compliance;
- Antiriciclaggio;
- DPO;
- Relazioni Esterne ed Attività Istituzionali;
- Area Affari (CCO);
- Area Crediti (CLO);
- Area Crediti Deteriorati;
- Gestione Personale;
- Area Operativa (COO);
- Area Finanza;
- Area Pianificazione e Amministrazione (CFO).

1.6.3. Attività sensibili

- a) Gestione dei rapporti, delle comunicazioni e degli adempimenti con Enti Pubblici, Organi di Polizia e le Autorità di Vigilanza, anche in occasione di ispezioni e accertamenti.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- esecuzioni di adempimenti;
- comunicazioni di dati e informazioni;
- ispezioni ed accertamenti;
- ottenimento di licenze o autorizzazioni amministrative;
- contratti/convenzioni per l'erogazione/gestione di finanziamenti agevolati;
- convenzioni con Enti pubblici per l'offerta rivolta ai dipendenti pubblici di prodotti e servizi bancari, d'investimento e assicurativi;
- negoziazione, stipulazione, esecuzione di contratti con soggetti pubblici ai quali si perviene mediante procedure negoziate (affidamento diretto o trattativa privata) o mediante gare ad evidenza pubblica (aperte o ristrette).

1.6.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- l'instaurazione ed il mantenimento da parte dei Destinatari di qualsiasi rapporto con la P.A. e con soggetti terzi incaricati di una pubblica funzione o di un pubblico servizio, devono essere caratterizzati dal pieno rispetto dei ruoli istituzionali, delle previsioni di legge in materia e delle procedure aziendali, dando puntuale e sollecita esecuzione alle relative prescrizioni e adempimenti richiesti;
- gli adempimenti nei confronti della P.A. e delle Autorità di Vigilanza e la predisposizione della relativa documentazione devono essere effettuati nel rispetto delle previsioni di legge in materia, con diligenza e professionalità, in modo da fornire informazioni accurate, complete e veritiere, evitando e comunque segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;
- i soggetti coinvolti nei processi con responsabilità di firma di atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;
- la trasmissione, anche informatica, di dati e documenti alla P.A. e alle Autorità di Vigilanza, deve essere curata da parte di Esponenti Aziendali/dipendenti e soggetti formalmente autorizzati e nei limiti delle proprie competenze e mansioni;
- il personale non deve dar seguito a qualunque tentativo di estorsione o concussione in cui sia coinvolto un funzionario della P.A.. Ogni notizia al riguardo, se già non

denunciata all'Autorità, deve essere riportata al proprio superiore gerarchico per i provvedimenti e le azioni di competenza;

- vengono stabiliti limiti all'impiego delle risorse finanziarie mediante soglie quantitative di spesa coerenti con le competenze gestionali e le responsabilità organizzative;
- in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali deve essere adottato un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, al fine di fornire all'azionista ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca;
- nei rapporti con l'Autorità giudiziaria, i destinatari del Modello sono tenuti a prestare una fattiva collaborazione ed a rendere dichiarazioni veritiere, trasparenti ed esaurientemente rappresentative dei fatti.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- promettere o effettuare erogazioni in denaro a favore di rappresentanti della P.A., italiana o straniera, per finalità diverse da quelle istituzionali e di servizio e in violazione delle prescrizioni aziendali;
- promettere o concedere vantaggi di qualsiasi natura (es.: promesse di assunzione, contributi, etc.) in favore di rappresentanti della P.A., italiana o straniera, al fine di influenzarne l'indipendenza di giudizio od assicurare un qualsiasi vantaggio per la Banca;
- dare o promettere denaro o altra utilità a soggetti intermediari affinché utilizzino relazioni esistenti con soggetti pubblici, allo scopo di indurre questi ultimi a compiere un atto contrario ai doveri d'ufficio costituente reato od a remunerarli per l'esercizio delle loro funzioni allo scopo di condizionare l'azione pubblica a vantaggio della Società;
- concedere finanziamenti senza la sussistenza dei necessari requisiti ad un cliente che vanti relazioni con esponenti della P.A., al fine di ottenere un indebito vantaggio per la Banca grazie all'eventuale mediazione illecita da parte del cliente;
- esibire documenti e dati falsi o alterati ed omettere informazioni dovute al fine di orientare a proprio favore le decisioni della P.A.;

- alterare il funzionamento di sistemi informativi e telematici o manipolare i dati in essi contenuti;
- instaurare relazioni personali di favore o influenza per condizionare, direttamente o indirettamente, l'esito del rapporto con esponenti della P.A.;
- sollecitare o persuadere un funzionario pubblico, attraverso un'intesa illecita, al compimento di un atto illegittimo (in violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità o, ancora, in violazione dell'obbligo di astensione in caso di conflitto di interesse);
- divulgare informazioni sensibili relativi al processo di gara (e.g. prezzo, dettagli tecnici) in occasione di eventuali interazioni con terze parti (e.g. competitors);
- violare il dovere di buona fede nell'esecuzione delle obbligazioni e del contratto di pubblica fornitura nonché, nell'ambito di un appalto pubblico, omettere di informare la P.A. su circostanze sopravvenute in corso di esecuzione dell'opera che comportino una modifica della prestazione;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità pubbliche di Vigilanza o degli Enti incaricati del controllo (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
- fornire informazioni fuorvianti sulla effettiva rappresentazione della situazione economica, patrimoniale e finanziaria della Banca;
- rappresentare e/o trasmettere - ai fini dell'elaborazione di documenti contabili, relazioni, prospetti, altre comunicazioni sociali - dati falsi, lacunosi o non rispondenti alla realtà.

1.6.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- identificazione dei soggetti/Funzioni incaricate ad interfacciarsi con istituzioni, Enti pubblici e Autorità di Vigilanza relativamente ad adempimenti, autorizzazioni, licenze ed ispezioni;
- identificazione dei soggetti/Funzioni incaricate a fornire idonea ed apposita documentazione a fronte di richieste da parte di istituzioni, Enti pubblici e Autorità di Vigilanza relativamente a adempimenti, autorizzazioni, licenze ed ispezioni;
- sottoscrizione degli atti che impegnano la Banca esclusivamente da soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- esecuzione delle attività in modo da garantire la veridicità, completezza, congruità e tempestività nella predisposizione di dati e informazioni a supporto delle attività o degli adempimenti verso la P.A./AdV;
- il Responsabile della struttura/funzione di volta in volta interessata assicura la corretta e completa predisposizione dei contenuti delle comunicazioni e il loro puntuale invio secondo le modalità e i tempi richiesti dalle Autorità/Istituzioni/Enti Pubblici;
- controlli di linea a cura di ciascuna Struttura interessata nello svolgimento delle attività inerenti all'esecuzione dei processi oggetto del presente Protocollo;
- qualora necessario, nell'ambito della gestione di visite ispettive da parte delle Autorità di Vigilanza, le strutture competenti individuano il coordinatore dell'ispezione al fine di assicurare il coordinamento fra tutti i responsabili delle strutture aziendali interessate e fungere da riferimento per tutte le richieste ricevute;
- in caso di accertamenti e ispezioni condotte presso la Banca dai competenti Enti o Autorità, è previsto il presidio da parte delle strutture organizzative competenti per materia, le quali si coordinano con tutti gli altri soggetti, strutture e Organi aziendali interessati. Il Responsabile della struttura interessata/il soggetto appositamente incaricato, ha l'obbligo di firmare per accettazione il verbale eventualmente redatto dai funzionari e di mantenerne copia unitamente ai relativi allegati;
- la struttura organizzativa di volta in volta interessata e/o i soggetti competenti, sono responsabili dell'archiviazione e della conservazione della documentazione di competenza trasmessa agli Enti Pubblici e alle Autorità di Vigilanza, nonché di tutta quella prodotta a supporto;

- tutti i flussi informativi e documentali, interni ed esterni, sono scambiati a mezzo e-mail o posta cartacea protocollata e, in ogni caso, mediante modalità tali da garantirne la tracciabilità;
- ogni comunicazione nei confronti delle Autorità, avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della Banca, è documentata/registrata in via informatica ed archiviata presso la struttura/funzione di competenza;

1.7. GESTIONE DEI RAPPORTI CON I PARTNER COMMERCIALI/MEDIATORI CREDITIZI/AGENTI

1.7.1. Reati astrattamente ipotizzabili

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.).

1.7.2. Unità organizzative/funzioni aziendali coinvolte

- Area Affari (CCO):
 - Sviluppo e Gestione Corporate/ Istituzionali;
 - Consulenza e Gestione Private;
 - Sviluppo e Gestione PMI/SB;
 - Sviluppo e Gestione Privati

- Marketing, Prodotti e Trasparenza;
- BU CQS.
- Filiali;
- Aree Territoriali.

1.7.3. Attività sensibili

a) Gestione dei rapporti con i partner commerciali/mediatori creditizi/agenti

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- individuazione e selezione dei rapporti con partner commerciali (compagnie di assicurazione)/mediatori creditizi/agenti;
- definizione di accordi di distribuzione con le compagnie assicurative circa i relativi prodotti;
- gestione e incasso delle provvigioni attive;
- rapporti con i mediatori creditizi/agenti;
- gestione e incasso delle provvigioni attive e passive.

1.7.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza o la vicinanza a organizzazioni criminali o comunque illecite;
- adottare criteri di trasparenza, correttezza, tracciabilità e oggettività nella selezione e gestione dei partner commerciali/mediatori creditizi/agenti;
- verificare preventivamente l'affidabilità, la reputazione e l'onorabilità dei partner commerciali, mediatori e agenti;
- assicurare che i rapporti siano formalizzati tramite accordi contrattuali scritti, completi e coerenti con le attività effettivamente svolte;
- garantire la tracciabilità dei flussi finanziari (provvigioni attive e passive), assicurando che siano giustificati da prestazioni reali e documentate;

- segnalare tempestivamente eventuali anomalie, criticità o situazioni sospette agli organi competenti.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- intrattenere rapporti con soggetti coinvolti, anche solo potenzialmente, in attività illecite (es. riciclaggio, criminalità organizzata, terrorismo);
- procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- effettuare o accettare pagamenti in contanti o tramite canali non tracciabili;
- omettere o alterare informazioni rilevanti nei processi di selezione, valutazione o gestione dei partner;
- aggirare i controlli aziendali od operare in violazione delle procedure interne.

1.7.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca nell'ambito delle attività sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna;
- definizione della modalità e dei criteri per la verifica preventiva dei presupposti di carattere strategico, economico e finanziario nonché dell'attuabilità dell'operazione alla base del contratto/convenzione;
- analisi di fattibilità dell'iniziativa commerciale mediante raccolta delle necessarie informazioni in merito a prodotti e servizi offerti dal partner;
- verifica preventiva/due diligence nella fase di selezione dei partner commerciali (compagnie di assicurazione)/mediatori creditizi/agenti;
- verifica periodica circa il mantenimento nel tempo del possesso dei requisiti di onorabilità e professionalità in caso ai partner commerciali/mediatori creditizi/agenti;

- verifica dei requisiti di indipendenza, di onorabilità e professionalità in capo agli agenti/mediatori creditizi;
- formalizzazione degli esiti dei colloqui con indicazione delle motivazioni dell'eventuale esclusione/ammissione dei candidati (mediatori creditizi/agenti);
- valutazione preliminare della partnership in termini di costi, ricavi e benefici degli accordi commerciali e di distribuzione;
- definizione dei criteri per la determinazione delle provvigioni attive;
- controllo di accuratezza delle erogazioni delle provvigioni attive e monitoraggio periodico;
- formale approvazione del contratto/accordo di distribuzione con il partner commerciale da parte di adeguati livelli autorizzativi;
- verifica della congruità delle provvigioni incassate rispetto a quanto definito nel contratto/accordo di distribuzione con le compagnie assicurative;
- previsione di controlli sull'operatività dei mediatori creditizi/agenti al fine di evidenziare eventuali comportamenti anomali e valutare le relative performance;
- previsione di controlli in merito al corretto invio, da parte di agenti in attività finanziaria che agiscono per conto della Banca, di una comunicazione contenente le informazioni e i dati acquisiti, anche con specifico riferimento alla documentazione prevista a supporto della pratica di finanziamento e al questionario sulla corretta identificazione della clientela sottoscritto dal richiedente il finanziamento e dall'agente;
- formale approvazione del contratto con i mediatori creditizi/agenti da parte di adeguati livelli autorizzativi;
- definizione dei criteri per la determinazione delle provvigioni da erogare ai mediatori creditizi/agenti;
- controllo di rispondenza tra le provvigioni da erogare ai mediatori creditizi/agenti definite nel contratto e quanto richiesto formalmente dagli stessi;
- formale approvazione delle provvigioni da erogare ai mediatori creditizi/agenti.

1.8. GESTIONE DEGLI OMAGGI E DELLE SPESE DI RAPPRESENTANZA

1.8.1.Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648-ter.1 c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

21) Reati Tributari (art. 25-quinquiesdecies)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000);
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000).

1.8.2. Unità organizzative/funzioni aziendali coinvolte

- Relazioni Esterne ed Attività Istituzionali;
- Filiali;
- Aree Territoriali.

1.8.3. Attività sensibili

- a) Gestione degli omaggi e delle spese di rappresentanza.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- distribuzione di omaggi - beni di modico valore - offerti, nell'ambito delle ordinarie relazioni di affari, al fine di promuovere l'immagine della Banca;
- spese di rappresentanza, in riferimento alle spese sostenute dalla Banca nell'espletamento delle relazioni commerciali, destinate a promuovere e migliorare l'immagine della Banca (ad es.: spese per colazioni e rinfreschi, spese per forme di accoglienza ed ospitalità, etc.).

1.8.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- le spese di rappresentanza devono essere congrue e non devono essere utilizzate come strumento per favorire impropriamente la Banca e/o influenzare il giudizio da parte di soggetti pubblici o privati coinvolti;
- gli omaggi devono essere congrui, proporzionati e coerenti con finalità di promozione dell'immagine aziendale. In particolare, gli omaggi:
 - o devono essere effettuati in buona fede, in relazione a finalità legittime di business e mai per ottenere vantaggi impropri;
 - o non devono essere motivati dal desiderio di esercitare influenze indebite o illecite né dall'aspettativa di reciprocità;
 - o non devono consistere in pagamenti in contanti né in forme non tracciabili di trasferimento di valore;
 - o devono essere ragionevoli in relazione a luogo, contesto, consuetudini e interlocutori coinvolti;

- devono essere conformi agli standard di cortesia professionale generalmente accettati nel settore;
- il valore economico deve intendersi quello percepito dal beneficiario dell'omaggio in base ai normali valori di mercato accessibili al pubblico;
- devono essere autorizzati preventivamente e deve essere garantita la tracciabilità degli omaggi in uscita e dei relativi destinatari. La tracciabilità deve essere garantita anche con riguardo agli omaggi in entrata (accettati o meno) e con riguardo alla società/soggetto fisico che ha effettuato tale offerta o fornito l'omaggio;

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale o comunque non conformi alle specifiche procedure aziendali;
- effettuare elargizioni/omaggi a favore di Enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persone ad essa collegate;
- promettere o concedere omaggi, atti di cortesia e di ospitalità, tali da poter essere interpretati come finalizzati a ottenere un trattamento di favore;
- distribuire omaggi e regali eccedenti le normali pratiche commerciali o di cortesia;
- condizionare tramite omaggi indebitamente un esponente (o un soggetto collegato) di una società terza fornitrice di beni o servizi, al fine di ottenere l'adozione di provvedimenti/misure compiacenti (e.g. al fine di ottenere forniture a prezzi altrimenti al di fuori dei valori di mercato);
- offrire, promettere o concedere omaggi o atti di ospitalità che possano essere interpretati come finalizzati a ottenere trattamenti di favore o vantaggi indebiti;
- utilizzare omaggi, atti di cortesia o spese di rappresentanza per incidere impropriamente sul giudizio o sul comportamento di soggetti pubblici o privati;
- porre in essere forme di intrattenimento o servizi non coerenti con finalità professionali o privi di adeguata giustificazione documentale;

- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparte o in relazione con la Banca, al fine di favorire indebitamente gli interessi della Banca;
- dare in omaggio beni per i quali non sia stata accertata la legittima provenienza ed il rispetto delle disposizioni che tutelano le opere dell'ingegno, i marchi e i diritti di proprietà industriale in genere nonché le indicazioni geografiche e le denominazioni di origine protette.

1.8.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione delle competenti strutture della Banca deputate alla gestione dell'omaggistica aziendale nonché in merito ai servizi di hospitality e spese di rappresentanza per lo svolgimento degli eventi/convegni;
- approvazione e sottoscrizione degli atti che impegnano contrattualmente la Banca ed eventuali variazioni ai relativi termini e condizioni da parte esclusivamente di soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- erogazione di omaggi e servizi di hospitality effettuati nel rispetto dei limiti di budget approvati, acquisendo documentazione a riprova della avvenuta e corretta esecuzione delle deliberazioni assunte;
- previsione di un processo di richiesta, verifica ed approvazione dell'erogazione di omaggi verso terzi;
- formale comunicazione al proprio Responsabile gerarchico/Responsabile della Funzione Internal Audit nel caso della ricezione di un omaggio;
- formale motivazione in merito al rifiuto dell'omaggio ricevuto;
- previsione di un processo di richiesta, verifica ed approvazione dell'organizzazione di eventi/convegni e delle spese di rappresentanza verso terzi;

- previsione di controlli circa il rispetto della capienza di budget con riferimento alle ospitalità e spese di rappresentanza;
- garantita la pertinenza e coerenza delle spese di rappresentanza sostenute mediante la verifica dei giustificativi a supporto delle spese di rappresentanza, nonché della documentazione relativa all'applicazione di specifiche agevolazioni verso terzi, al fine di assicurare il rispetto dei limiti prestabiliti, nonché a verificare l'inerenza delle spese sostenute rispetto alle attività lavorative svolte;
- tracciatura delle attività all'interno di un sistema informativo e documentale, con riferimento all'elenco dei destinatari di omaggi, alle caratteristiche delle iniziative sostenute, nonché ai documenti giustificativi delle spese anche di rappresentanza sostenute.

1.9. GESTIONE DELLA COMUNICAZIONE ESTERNA

1.9.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Traffico di influenze illecite (art. 346-bis).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

15) Delitti in materia di violazione del diritto d'autore (art. 25-novies)

- Divulgazione tramite reti telematiche di un'opera dell'ingegno protetta (art. 171 L. 633/1941);
- Duplicazione, a fini di lucro, di programmi informatici o importazione, distribuzione, vendita, detenzione per fini commerciali di programmi contenuti in supporti non contrassegnati dalla SIAE (art. 171-bis L. 633/1941);

- Duplicazione, riproduzione, trasmissione di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio (art. 171-ter L. 633/1941);
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941);
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

5) Delitti contro l'industria e il commercio (art. 25-bis.1)

- Turbata libertà dell'industria o del commercio (art. 513 c.p.).

21) Reati Tributari (art. 25-quinquiesdecies)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000);
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000).

1.9.2. Unità organizzative/funzioni aziendali coinvolte

- Relazioni Esterne ed Attività Istituzionali;
- Affari Societari, Soci e Investor Relations;
- Area Affari (CCO):
 - Marketing, Prodotti e Trasparenza.

1.9.3. Attività sensibili

- a) Gestione delle attività di marketing e comunicazione.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- aggiornamento del sito internet della Banca in relazione ai contenuti istituzionali;
- rapporti con i mass media;
- comunicazione esterna attraverso il sito web e i giornali;
- rapporti con l'agenzia pubblicitaria;

- organizzazione degli eventi.

1.9.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- i rapporti con la stampa, e più in generale con i mezzi di comunicazione e di informazione di massa, devono essere gestiti nel pieno rispetto dei principi di trasparenza, accuratezza, completezza e tempestività;
- l'aggiornamento del sito internet istituzionale deve garantire che tutte le informazioni pubblicate siano veritiere, complete, chiare e coerenti con la comunicazione istituzionale della Banca, assicurando al contempo il rispetto della normativa in materia di privacy, sicurezza informatica e flussi autorizzativi interni;
- i rapporti con le agenzie pubblicitarie devono garantire una collaborazione trasparente, tracciabile e improntata a criteri di imparzialità, assicurando che ogni materiale prodotto sia conforme alle policy interne, alla normativa di settore e ai valori di integrità, sobrietà e tutela della reputazione aziendale;
- l'organizzazione degli eventi deve assicurare che la pianificazione, la selezione dei fornitori, la gestione dei contenuti e la relazione con gli invitati siano conformi ai principi di trasparenza, responsabilità, economicità e coerenza con gli obiettivi istituzionali della Banca, garantendo al contempo il pieno rispetto delle policy interne e delle normative applicabili;
- è fatto obbligo di mantenere riservate tutte le informazioni e i documenti acquisiti nello svolgimento delle proprie funzioni, sia aventi ad oggetto la Banca e gli strumenti finanziari della stessa, sia riguardanti Società terze in rapporto d'affari con la Banca e gli strumenti finanziari di queste ultime nonché di utilizzare le informazioni o i documenti stessi esclusivamente per l'espletamento dei propri compiti lavorativi;
- i rapporti con i mass media non devono essere gestiti da personale non autorizzato, né devono diffondere anticipazioni, informazioni riservate, price sensitive o comunque non pubbliche, né prevedere trattamenti preferenziali, vantaggi indebiti o comportamenti che possano compromettere imparzialità e correttezza;
- la comunicazione esterna tramite sito web e stampa non deve diffondere informazioni ingannevoli, incomplete, sensazionalistiche o non coerenti con la realtà dei servizi

offerti, né divulgare contenuti regolamentati o price sensitive al di fuori dei canali previsti dalla normativa;

- l'organizzazione degli eventi non deve coinvolgere fornitori non autorizzati o non conformi alle policy interne, né utilizzare risorse economiche o materiali per finalità non coerenti o non tracciabili;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione della comunicazione esterna, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- diffondere sia ad altro personale sia all'esterno della Banca, attraverso qualsiasi canale informativo, compreso internet, informazioni, voci o notizie non corrispondenti alla realtà, ovvero informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti in relazione alla Banca;
- fatto salvo quanto previsto in materia di comunicazione al pubblico di informazioni privilegiate relative alla Banca, comunicare al mercato o ai media informazioni privilegiate relative alle società clienti della Banca.

1.9.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione delle competenti strutture della Banca deputate alla gestione delle attività in relazione alla comunicazione esterna ed all'organizzazione degli eventi;
- approvazione e sottoscrizione degli atti che impegnano contrattualmente la Banca ed eventuali variazioni ai relativi termini e condizioni esclusivamente da parte di soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- formale approvazione, da parte di adeguati livelli organizzativi, dei contenuti da diffondere agli organi di informazione;

- monitoraggio, da parte degli Uffici a ciò preposti, delle comunicazioni alla stampa o di altri mezzi di informazione al fine di prevenire il rischio di diffusione di notizie false o fuorvianti riguardanti la Banca;
- formale approvazione, da parte di adeguati livelli organizzativi, dei contenuti da pubblicare sul sito web della Banca e sui giornali;
- previsione di controlli sulla veridicità e correttezza del materiale pubblicitario;
- previsione di controlli sul consuntivo di spesa e sull'allineamento rispetto al preventivo;
- previsione di un processo di richiesta, verifica ed approvazione in merito all'organizzazione degli eventi;
- adozione di opportuni strumenti di controllo nell'ambito della promozione dell'immagine della banca e dell'attività commerciale;
- previsione di controlli preventivi sull'attinenza della qualifica degli invitati all'evento con la finalità dello stesso;
- formale definizione delle spese ammissibili e dei limiti di importo per l'organizzazione di eventi.

1.10. GESTIONE DELLE LIBERALITÀ E DELLE SPONSORIZZAZIONI

1.10.1. Reati astrattamente ipotizzabili

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (648 ter 1 c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

21) Reati Tributari (art. 25-quinquiesdecies)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000);
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000).

1.10.2. Unità organizzative/funzioni aziendali coinvolte

- Relazioni Esterne ed Attività Istituzionali;
- Filiali;
- Aree Territoriali.

1.10.3. Attività sensibili

- a) Gestione delle liberalità e delle sponsorizzazioni.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- iniziative di carattere liberale e valutazione dei destinatari delle liberalità;
- sponsorizzazioni ai fini della promozione, della valorizzazione ed il potenziamento dell'immagine della Banca;

1.10.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- per garantire coerenza ai contributi ed alle sponsorizzazioni effettuate, nella scelta delle proposte cui aderire deve essere, deve essere prestata particolare attenzione ad ogni possibile conflitto di interesse di natura personale o aziendale;
- effettuare un'adeguata verifica preventiva e debitamente documentata, in caso di contributi o sponsorizzazioni, del beneficiario nonché effettuare tutti i pagamenti esclusivamente sui conti intestati a quest'ultimo;
- assicurare che liberalità e sponsorizzazioni non siano motivate dal desiderio di esercitare influenze improprie o ottenere ritorni personali o aziendali illeciti;
- verificare che gli importi siano ragionevoli e proporzionati rispetto all'iniziativa o all'Ente destinatario.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- utilizzare sponsorizzazioni o liberalità per ottenere, direttamente o tramite terzi, favori, decisioni indebite o vantaggi non conformi alle norme interne e di legge.
- effettuare operazioni di sponsorizzazione o liberalità, anche correlate ad eventi, con terzi soggetti pubblici o privati, non debitamente autorizzate dagli Organi competenti o prive di adeguata documentazione giustificativa;
- promettere o concedere donazioni, benefici, atti di cortesia e di ospitalità, tali da poter essere interpretati come finalizzati a ottenere un trattamento di favore;
- concedere somme o benefici a soggetti con finalità non coerenti con la missione aziendale o privi di un ritorno reputazionale o istituzionale legittimo;
- effettuare erogazioni, per iniziative di beneficenza o di sponsorizzazione, a favore di Enti coinvolti vicende giudiziarie note o in pratiche non rispettose dei diritti umani;
- effettuare sponsorizzazioni che possano essere interpretate come strumenti per mascherare pagamenti illeciti;
- corrispondere – in qualsiasi forma, anche in via indiretta – ovvero organizzare la raccolta di contributi, donazioni, liberalità, effettuare sponsorizzazioni finanziare

iniziative, Enti o associazioni che possano configurare anche indirettamente finalità politiche, salvo espressa previsione normativa e autorizzazione formale;

- frazionare importi transattivi al fine di aggirare controlli, soglie o autorizzazioni;
- dare o promettere denaro o altra utilità a soggetti intermediari affinché utilizzino relazioni esistenti con soggetti pubblici, allo scopo di indurre questi ultimi a compiere un atto contrario ai doveri d'ufficio costituente reato od a remunerarli per l'esercizio delle loro funzioni allo scopo di condizionare l'azione pubblica a vantaggio della Banca;
- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero altre organizzazioni con la finalità di promuovere o favorire interessi della Banca, anche a seguito di illecite pressioni;
- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparte o in relazione con la Banca, al fine di favorire indebitamente gli interessi della Banca.

1.10.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione delle competenti strutture della Banca deputate alla gestione delle attività di sponsorizzazione ed erogazioni liberali;
- approvazione e sottoscrizione degli atti che impegnano contrattualmente la Banca e di eventuali variazioni ai relativi termini e condizioni esclusivamente da parte di soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- previsione di un processo relativo alle modalità operative per l'espletamento delle attività connesse alle sponsorizzazioni ed all'erogazione di liberalità;

- previsione di criteri e regole relative alle attività di selezione del destinatario della liberalità;
- esecuzione di una due-diligence dei destinatari delle iniziative, finalizzata a verificare i requisiti reputazionali, normativi, di onorabilità e competenza degli stessi; in particolare, la due-diligence è finalizzata ad accertare che:
 - o non vi siano condizioni di incompatibilità o conflitto di interessi, anche con riguardo ai rapporti di parentela o alle relazioni di carattere personale o professionale della controparte;
 - o la controparte non abbia subito condanne per reati né sia stata assoggettata a sanzioni da parte di Autorità nazionali o internazionali, rilevanti ai fini della sponsorizzazione;
 - o la controparte non sia residente o abbia sede in un Paese a regime fiscale privilegiato;
 - o la controparte - sia persona fisica sia giuridica - non sia iscritta nelle liste stilate dalle organizzazioni internazionali al fine di prevenire il finanziamento del terrorismo ed il riciclaggio, ovvero non sia residente in Paesi a rischio terrorismo;
- formale identificazione del gestore del contratto;
- formale approvazione del contratto da parte di adeguati livelli autorizzativi;
- previsione di controlli circa il corretto espletamento delle attività oggetto della sponsorizzazione
- previsione, con riferimento a tutte le forniture o alle richieste di sponsorizzazioni/liberalità, anche qualora siano coinvolti soggetti terzi non clienti, di un'attività di verifica consistente nell'accertamento da parte dell'Unità proponente in merito al profilo reputazionale del potenziale fornitore/richiedente al fine di escludere, almeno in via preventiva, possibili coinvolgimenti in attività criminose;
- coerenza delle iniziative di beneficenza o sponsorizzazione in termini di capienza del budget, target di destinatari, contenuti e scopi;
- tracciatura di tutte le attività in oggetto a livello di sistema informativo e documentale, con particolare riferimento all'elenco dei destinatari di beneficenze e sponsorizzazioni, alle caratteristiche delle iniziative sostenute, nonché ai documenti giustificativi.

1.11. GESTIONE DEGLI ADEMPIMENTI SOCIETARI

1.11.1. Reati astrattamente ipotizzabili

6) Reati societari (art. 25-ter)

- False comunicazioni sociali (artt. 2621 e 2622 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.);
- Illecita influenza dell'assemblea (art. 2636 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

1.11.2. Unità organizzative/funzioni aziendali coinvolte

- Affari Societari, Soci e Investor Relations;
- Tutte le Aree/Uffici aziendali coinvolti nella trasmissione di comunicazioni verso gli Organi Sociali;
- Legale.

1.11.3. Attività sensibili

- a) Gestione dei rapporti con gli Organi Sociali.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- comunicazione delle informazioni periodiche previste;
- comunicazione di informazioni e di dati societari e messa a disposizione della documentazione, sulla base delle richieste ricevute;
- gestione dei libri sociali e degli atti degli Organi Sociali;
- gestione delle attività connesse al funzionamento dell'assemblea dei soci (svolgimento e verbalizzazione).

1.11.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- assicurare il regolare funzionamento della Banca e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale nonché la libera e corretta formazione della volontà assembleare;
- trasmettere tempestivamente al Collegio Sindacale tutti i documenti relativi ad argomenti posti all'ordine del giorno di Assemblee e Consigli di Amministrazione o sui quali il Collegio debba esprimere un parere;
- mettere a disposizione del Collegio e della Società di Revisione i documenti sulla gestione della Società per le verifiche proprie dei due Organismi;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non impedendo in alcun modo l'esercizio delle funzioni di vigilanza da queste intraprese;
- dare notizia, da parte di ogni Amministratore, agli altri Amministratori e al Collegio Sindacale di situazioni di conflitto di interessi relative a una determinata operazione, precisandone la natura, i termini, l'origine e la portata e astenersi dal partecipare alla relativa deliberazione;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- fornire e/o tramettere informazioni fuorvianti sulla effettiva rappresentazione della situazione economica, patrimoniale e finanziaria della Banca; rappresentare e/o trasmettere - ai fini dell'elaborazione di documenti contabili, relazioni, prospetti, altre comunicazioni sociali - dati falsi, lacunosi o non rispondenti alla realtà;
- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;

- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Banca.

1.11.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- i rapporti con gli Organi Sociali intrattenuti dal Responsabile della struttura di riferimento o dai soggetti dal medesimo appositamente incaricati;
- approvazione e sottoscrizione degli atti che impegnano la Banca esclusivamente da parte di soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- tempestiva e completa evasione, a cura delle strutture competenti, delle richieste di documentazione specifica avanzate dagli Organi Sociali nell'espletamento della propria attività di vigilanza e controllo;
- previsione di flussi informativi periodici verso gli Organi Sociali;
- segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con gli Organi Sociali al fine di garantire, per tutte le fasi del processo, un meccanismo di maker e checker;
- verifica della regolarità, completezza e correttezza di tutti gli adempimenti e delle comunicazioni trasmesse, comprese le attività affidate a soggetti ed Enti terzi;
- adeguata gestione dei libri sociali obbligatori e degli atti del Consiglio di Amministrazione, da parte delle competenti strutture della Banca;
- definizione delle modalità di convocazione e svolgimento dell'Assemblea, in osservanza dei principi normativi e statutari adottati;
- formale previsione nello Statuto societario delle modalità di rappresentanza in Assemblea dei diritti di voto;
- previsione di verifiche circa il diritto di partecipazione all'Assemblea, anche per delega;
- previsione di regole volte ad assicurare la corretta verbalizzazione delle riunioni dell'Assemblea dei soci;

- definizione delle modalità di predisposizione, approvazione e trasmissione agli Organi societari ed ai Soci della documentazione inerente atti e deliberazioni, nonché relativa conservazione;
- previsione di riunioni periodiche formalizzate tra Soggetti Apicali della Banca e gli Organi societari e/o Soci; ciascuna struttura organizzativa coinvolta nelle attività inerenti ai rapporti con gli Organi Sociali è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta, recuperata o ricevuta da terzi, anche in via telematica o elettronica;
- scambio di tutti i flussi informativi e documentali, interni ed esterni, a mezzo e-mail o posta cartacea protocollata e, in ogni caso, con modalità tali da garantirne la tracciabilità.

1.12. CONTABILITÀ GENERALE, BILANCIO E ALTRE COMUNICAZIONI SOCIALI

1.12.1. Reati astrattamente ipotizzabili

6) Reati societari (art. 25-ter)

- False comunicazioni sociali (artt. 2621 e 2622 c.c.);
- Fatti di lieve entità (art. 2621-bis c.c.);
- Impedito controllo (art. 2625 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.);
- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.);
- False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.).

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

13) Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1)

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.);
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.);
- Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.);
- Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1, comma 2);
- Trasferimento fraudolento di valori (art. 512-bis c.p.).

21) Reati Tributari (art. 25-quinquiesdecies)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000);

- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000);
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000);
- Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000);
- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000);
- Indebita compensazione (art. 10-quater D.lgs. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000).

1.12.2. *Unità organizzative/funzioni aziendali coinvolte*

- Area Pianificazione e Amministrazione CFO:
 - Pianificazione e Controllo di Gestione:
 - Iniziative ESG;
 - Amministrazione:
 - Contabilità e Bilancio;
 - Fiscale e Tributario;
 - Anagrafe e Segnalazioni di Vigilanza.

1.12.3. *Attività sensibili*

- a) Gestione della contabilità e redazione del bilancio d'esercizio e delle comunicazioni sociali.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- registrazioni contabili;
- anagrafica/clienti;
- fatturazione attiva/passiva;
- situazioni contabili infrannuali;
- redazione ed approvazione del bilancio e delle altre comunicazioni sociali;
- svalutazione crediti;
- segnalazioni di Vigilanza;
- gestione dei pagamenti della Banca.

1.12.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca;
- rappresentare i fatti di gestione in modo corretto, completo e tempestivo nella contabilità e nei dati aziendali allo scopo di garantire la corretta e veritiera rappresentazione dei risultati economici, patrimoniali e finanziari della Banca;
- assicurare il rispetto dei principi contabili adottati e la tracciabilità nelle scritture di chiusura, assestamento e rettifica e le poste estimative/valutative;
- assicurare la corretta contabilizzazione delle operazioni di acquisto, cessione/dismissione di immobilizzazioni immateriali, materiali e finanziarie e relative plusvalenze o svalutazioni;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento della Banca e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- osservare le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando comportamenti che ne possano provocare una sensibile alterazione rispetto alla corrente situazione di mercato;
- garantire la corretta gestione dell'anagrafica fornitori/clienti ed il suo costante e tempestivo aggiornamento;
- effettuare controlli formali e sostanziali e garantire un costante monitoraggio dei flussi finanziari della Banca, con riferimento ai pagamenti verso terzi, tenendo conto della sede legale della società controparte, degli istituti di credito utilizzati, di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni od operazioni straordinarie;

- verificare che le operazioni che comportano l'utilizzo o l'impiego di risorse economiche o finanziarie debbano avere una causale espressa e siano documentate e registrate in conformità ai principi di correttezza e trasparenza contabile;
- garantire che gli incassi e i pagamenti della Società nonché i flussi di denaro siano sempre tracciabili e provabili documentalmente;
- procedere ad eventuali modifiche delle anagrafiche già esistenti solo a seguito di espressa e documentata richiesta ed in presenza della documentazione a supporto della modifica richiesta;
- assicurare il regolare funzionamento della Banca e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale nonché la libera e corretta formazione della volontà assembleare;
- mettere a disposizione del Collegio e della Società di Revisione i documenti sulla gestione della Società per le verifiche proprie dei due organismi;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste intraprese;
- mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei propri compiti e, in particolare, assicurare che la circolazione interna e verso Terzi di documenti contenenti informazioni potenzialmente privilegiate sia soggetta ad ogni necessaria attenzione e cautela, onde evitare pregiudizi ed indebite divulgazioni;
- dare notizia, da parte di ogni Amministratore, agli altri Amministratori e al Collegio Sindacale di situazioni di conflitto di interessi relative a una determinata operazione, precisandone la natura, i termini, l'origine e la portata e astenersi dal partecipare alla relativa deliberazione.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- effettuare registrazioni contabili in modo non accurato, non corretto e non veritiero;
- registrare operazioni senza un'adeguata documentazione di supporto che ne consenta "in primis" una corretta rilevazione contabile e successivamente una ricostruzione accurata;

- evitare di porre in essere operazioni simulate o diffondere notizie false sulla Società e sulle sue eventuali controllate, nonché sulla loro attività;
- effettuare prestazioni o pagamenti di compensi in favore di collaboratori, fornitori, consulenti, partner o altri soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e/o in relazione al tipo di incarico da svolgere dalle prassi vigenti;
- effettuare pagamenti delle spettanze verso i soggetti terzi attraverso sistemi inusuali, artificiosamente elaborati e/o triangolazioni con ulteriori soggetti esterni;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Banca e delle sue Controllate;
- fornire e/o tramettere informazioni fuorvianti sulla effettiva rappresentazione della situazione economica, patrimoniale e finanziaria della Banca; rappresentare e/o trasmettere - ai fini dell'elaborazione di documenti contabili, relazioni, prospetti, altre comunicazioni sociali - dati falsi, lacunosi o non rispondenti alla realtà;
- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di Vigilanza e/o degli Enti Pubblici svolgenti funzioni di controllo cui è soggetta l'attività aziendale, nonché la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette autorità;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Banca.

1.12.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- approvazione e sottoscrizione degli atti che impegnano la Banca esclusivamente da parte di soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;

- individuazione e autorizzazione dei soggetti che intervengono nella gestione delle attività inerenti alla predisposizione delle dichiarazioni fiscali, e nelle prodromiche attività di emissione/contabilizzazione delle fatture in base allo specifico ruolo attribuito ai sensi del vigente sistema dei poteri e delle deleghe;
- presenza di normativa interna che regola lo svolgimento del processo aziendale con indicazione di ruoli, responsabilità e modalità operative delle funzioni aziendali coinvolte nella gestione delle attività contabile e fiscale;
- attribuzione ad ogni struttura organizzativa coinvolta della responsabilità delle attività di competenza connesse alla produzione e/o alla valutazione delle voci contabili e degli eventuali relativi commenti presenti nell'informativa periodica;
- monitoraggio del rispetto dei principi che regolano la compilazione, tenuta e conservazione dei dati e delle informazioni contabili;
- produzione, per tutte le operazioni registrate in contabilità, di prima nota contabile, debitamente validata, e della relativa documentazione giustificativa;
- monitoraggio del piano dei conti;
- definizione e approvazione di controlli relativi alle operazioni di gestione del piano dei conti aziendale;
- formale definizione dei profili aziendali abilitati ad effettuare le operazioni di creazione, modifica, cancellazione e migrazione dei conti;
- formale definizione dei profili abilitati alle operazioni di creazione, modifica, cancellazione e migrazione dei saldi;
- previsione di sistemi automatici per la registrazione contabile;
- chiara individuazione dei soggetti aziendali autorizzati ad accedere al sistema aziendale dedicato alla gestione della contabilità mediante user ID e password personali;
- produzione, per tutte le operazioni registrate in contabilità, di prima nota contabile, debitamente validata, e della relativa documentazione giustificativa;
- riconciliazioni contabili complete ed accurate;
- formale definizione dei profili abilitati alle operazioni di inserimento/modifica/cancellazione delle anagrafiche fornitori a sistema;

- previsione della tracciabilità di inserimenti/modifiche/cancellazioni effettuate in anagrafica fornitori;
- previsione di controlli per l'apertura di codici fornitore per fornitori inesistenti;
- formale definizione dei profili abilitati nonché di tracciamento delle operazioni di inserimento/modifica/cancellazione delle anagrafiche clienti a sistema;
- controlli sulla corretta emissione, applicazione delle aliquote IVA e contabilizzazione delle fatture del ciclo attivo e sulla loro corrispondenza con i contratti e impegni posti in essere con i terzi;
- controlli sull'effettività del rapporto sottostante alle fatture passive ricevute e sulla corretta registrazione e contabilizzazione;
- controllo sull'effettività delle prestazioni rispetto alle fatture emesse;
- verifiche, con cadenza periodica, dei saldi di contabilità generale, dei conti lavorazione, transitori e similari;
- analisi degli scostamenti, attraverso il confronto dei dati esposti nel periodo corrente e quelli relativi a periodi precedenti;
- previsione di flussi informativi tra la Funzione preposta alla predisposizione del bilancio e le Funzioni che devono fornire le necessarie informazioni contabili;
- approvazione delle poste valutative incluse nel bilancio da parte dei soggetti abilitati;
- definizione di un processo approvativo e di controllo per le scritture di rettifica e assestamento;
- definizione di verifiche di correttezza, completezza ed accuratezza delle informazioni contenute nel bilancio;
- definizione di controlli sulla predisposizione della nota integrativa e della relazione sulla gestione;
- formale approvazione da parte del CdA della bozza di bilancio della Banca;
- approvazione definitiva del Bilancio d'esercizio da parte dell'Assemblea dei Soci;
- monitoraggio, da parte delle Funzioni Aziendali a ciò preposte, dell'anzianità dei crediti e delle conseguenti azioni di sollecito/piani di rientro;
- formale approvazione delle proposte di saldo e stralcio dei crediti;

- qualora siano identificate oggettive evidenze di una possibile perdita di valore, riduzione del valore del credito da parte della Banca mediante una svalutazione, tenendo conto di criteri di oggettività e prudenza ed in funzione dei flussi di cassa previsti e della mitigazione del rischio derivante dalle garanzie presenti, imputando la rettifica di valore al conto economico di esercizio. Conformemente alle disposizioni del principio contabile IFRS 9, il modello di valutazione si basa sulla stima delle perdite attese, ovvero perdite relative ad eventi non ancora manifestati alla data di valutazione, ma che possono in futuro manifestarsi;
- gestione proattiva da parte dell'Area Crediti Deteriorati dei crediti classificati come Crediti Scaduti Deteriorati, cercando di normalizzarne il rapporto mediante specifiche azioni e conseguenti piani di risanamento;
- monitoraggio del Piano NPE, dell'andamento del portafoglio UTP e dei piani di rientro, prevedendo tempestivi interventi anche con solleciti formali, attraverso il coinvolgimento dei Preposti di Filiale e dei Capi Area;
- ciascuna struttura organizzativa coinvolta nelle attività di cui al presente Protocollo è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta, recuperata o ricevuta da terzi, anche in via telematica o elettronica;
- la rilevazione, la trasmissione e l'aggregazione delle informazioni contabili finalizzate alle comunicazioni sociali avviene esclusivamente tramite il sistema informatico, il quale garantisce la tracciabilità dei singoli passaggi del processo di formazione dei dati e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- sistematica formalizzazione e verbalizzazione delle attività di verifica e controllo svolte dagli Organi Sociali.

1.13. GESTIONE DEI SERVIZI DI ASSICURAZIONE E PREVIDENZA VERSO LA CLIENTELA

1.13.1. Reati astrattamente ipotizzabili

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

1.13.2. Unità organizzative/funzioni aziendali coinvolte

- Area Affari (CCO):
 - Consulenza e Gestione Private;
 - Sviluppo e Gestione /PMI/SB;
 - Sviluppo e Gestione Privati
 - Condizioni;
 - Marketing, Prodotti e Trasparenza;
- Filiali;
- Aree Territoriali.

1.13.3. Attività sensibili

- a) Gestione delle attività di collocamento dei prodotti assicurativi e dei rapporti con i clienti.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- profilazione della clientela;
- stipula del contratto di assicurazione e previdenza;
- monitoraggio della fase post-vendita.

1.13.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- assumere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali;
- effettuare con tempestività correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste intraprese;
- informare preventivamente i clienti della Banca sulla reale natura, rischi e costi delle operazioni e dei servizi da essa offerti;
- nei prospetti richiesti ai fini della sollecitazione all'investimento, non esporre false informazioni o occultare dati o notizie in modo tale da indurre in errore i destinatari del prospetto.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- comunicare informazioni false e di occultare dati e notizie che potrebbero indurre in errore i destinatari di tali comunicazioni;
- proporre opportunità commerciali o di qualsiasi altro genere che possano, anche solo potenzialmente, procurare loro un indebito vantaggio, al fine di ottenere in cambio un favore per la Banca;
- tenere una condotta ingannevole che possa indurre, anche in via potenziale, in errore la clientela nella valutazione tecnico-economica dei prodotti o dei servizi offerti o comunque ricorrere a pratiche elusive, tendenti a forzare il giudizio o il comportamento del cliente.

1.13.5. *Controlli preventivi*

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- approvazione e sottoscrizione degli atti che impegnano la Banca esclusivamente da parte dei soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- verifica del corretto inserimento del cliente in anagrafica;
- accertamento della capacità e legittimità ad agire del cliente mediante la raccolta di informazioni e documenti idonei alla profilatura;
- esecuzione di una classificazione dei clienti in modo da poter eseguire, nei loro confronti, verifiche più o meno incisive e commisurate ad una delle quattro tipologie di profilo di rischio di riciclaggio o di finanziamento del terrorismo riscontrante, sulla base dell'elaborazione dei dati e delle informazioni acquisite in sede di censimento anagrafico, di accensione di rapporti continuativi o di esecuzione di operazioni occasionali e di monitoraggio dell'operatività posta in essere;
- previsione di un monitoraggio periodico dell'anagrafica clienti; in tale ambito, è richiesto all'Addetto di Filiale/Ufficio incaricato, la compilazione del questionario di Adeguata Verifica, anche mediante la compilazione delle necessarie informazioni richieste all'interno dell'applicativo utilizzato, l'accertamento dell'identità del cliente tramite e l'esecuzione delle opportune verifiche e valutazioni nel caso in cui si rilevino corrispondenze in sede di controllo automatico dell'applicativo. Con specifico riferimento alla clientela persona giuridica, la Funzione Antiriciclaggio provvede con cadenza annuale a monitorare i nominativi privi del questionario di Adeguata Verifica, sollecitando la Rete a raccogliere i dovuti questionari in ottemperanza degli obblighi di adeguata verifica della Clientela;
- formali controlli al fine di verificare che il cliente non sia presente nelle Liste Antiriciclaggio e Antiterrorismo;
- verifica da parte del Responsabile di filiale della corretta e completa sottoscrizione della modulistica da parte del contraente e dell'assicurato (se diverso dal contraente);
- verifica della disponibilità presente sul conto di addebito del cliente; eventuali variazioni delle condizioni sono valutate e autorizzate a livello direzionale dal Chief Commercial Officer/Direzione Generale;

- flussi informativi periodici da e verso i partner commerciali mediante l'inoltro della documentazione relativa al rapporto assicurativo.

1.14. SELEZIONE E ASSUNZIONE DEL PERSONALE

1.14.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-ter, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

18) Delitti di impiego di cittadini di Paesi terzi di cui il soggiorno è irregolare (art. 25-duodecies)

- Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 22 D.Lgs. n.286/1998);
- Disposizioni contro le immigrazioni clandestine (art. 12 D.lgs. 286/1998).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

Delitti contro la personalità individuale (art. 25 quinquies)

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Approfittamento della vittima di riduzione in schiavitù o di tratta (art. 601.1 c.p.);
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648-ter.1 c.p.).

1.14.2. Unità organizzative/funzioni aziendali coinvolte

- Gestione Personale.

1.14.3. Attività sensibili

- a) Selezione e assunzione del personale.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- valutazione e selezione dei candidati idonei;
- formalizzazione dell'assunzione;
- predisposizione e trasmissione della documentazione da inoltrare alle organizzazioni sindacali.

1.14.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- l'assunzione di personale o collaboratori deve seguire regole di trasparenza basandosi sulla valutazione di professionalità, preparazione tecnica, esperienza maturata e potenziale di sviluppo;
- la selezione deve essere effettuata tra una rosa di candidati, salvo il caso di personale specialistico qualificato, di categorie protette ovvero di figure destinate a posizioni manageriali;
- la valutazione comparativa dei candidati deve essere effettuata sulla base di criteri di competenza, professionalità ed esperienza in relazione al ruolo per il quale avviene l'assunzione;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo di selezione e assunzione del personale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- le informazioni richieste ai candidati in sede di colloquio conoscitivo devono essere rispettose della sfera privata e delle opinioni personali;

- la trasmissione, anche informatica, di dati e documenti alla P.A. e alle Autorità di Vigilanza, deve essere curata da parte di Esponenti Aziendali/dipendenti e soggetti formalmente autorizzati e nei limiti delle proprie competenze e mansioni;
- osservare e garantire l'osservanza, all'interno della Banca di tutte le norme a tutela del lavoratore;
- il personale deve essere assunto con regolare contratto di lavoro, stipulato nel rispetto del CCNL applicabile, e non è ammessa alcuna forma di lavoro irregolare;
- non utilizzare, assumere o impiegare manodopera, anche mediante l'attività di intermediazione, sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno;
- monitorare periodicamente la validità dei documenti dei dipendenti che risiedono in Paesi terzi e sollecitare questi ultimi, prima della scadenza del permesso di soggiorno, al rinnovo del medesimo;
- nella definizione del contratto di assunzione, garantire il rispetto delle condizioni di lavoro e del salario minimo dell'ultimo contratto collettivo nazionale CCNL sottoscritto;
- eventuali consulenti esterni coinvolti nei processi in esame devono sottoscrivere le clausole rilevanti ai fini del D. Lgs. 231/01.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- promettere o effettuare erogazioni in denaro a favore di rappresentanti della P.A., italiana o straniera, per finalità diverse da quelle istituzionali e di servizio e in violazione delle prescrizioni aziendali;
- promettere o concedere vantaggi di qualsiasi natura (es.: promesse di assunzione, contributi, etc.) in favore di rappresentanti della P.A., italiana o straniera, al fine di influenzarne l'indipendenza di giudizio od assicurare un qualsiasi vantaggio per la Banca;
- instaurare relazioni personali di favore o influenza per condizionare, direttamente o indirettamente, l'esito del rapporto con esponenti della P.A.;
- effettuare promesse di assunzione o assunzioni in favore di soggetti segnalati dall'interlocutore/referente privato;

- sottoporre i lavoratori a condizioni di sfruttamento ad esempio attraverso:
 - la reiterata corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque sproporzionato rispetto alla quantità e qualità del lavoro prestato;
 - la reiterata violazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie;
 - la sussistenza di violazioni delle norme in materia di sicurezza e igiene nei luoghi di lavoro;
 - l'esposizione lavoratori sfruttati a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro;
 - reclutare minori in età non lavorativa.

1.14.5. *Controlli preventivi*

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca nell'ambito delle attività sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna;
- definizione ed approvazione del budget dei costi connessi alle assunzioni (budget destinato per le nuove assunzioni e/o per la copertura di posizioni vacanti) nel rispetto delle deleghe in essere;
- rilevazione e rappresentazione dell'esigenza di una nuova assunzione da parte del Direttore Generale o del Responsabile di un singolo ufficio nell'ambito delle attività di periodico monitoraggio dei carichi lavorativi in essere;
- definizione da parte dell'Ufficio Gestione del Personale e del Responsabile dell'ufficio interessato dall'assunzione delle caratteristiche della figura oggetto di ricerca (mansione richiesta, tipologia e durata del contratto, qualifica e profilo del candidato ricercato);

- ricerca dei CV di potenziali candidati da parte dell'Ufficio Gestione del Personale attraverso le piattaforme di ricerca di cui la Banca si avvale (es. LinkedIn) ed eventuale affidamento della ricerca ad una agenzia di recruiting esterna (selezionata in base alle procedure aziendali che governano gli approvvigionamenti);
- formale approvazione del contratto con la Società di Recruiting da parte di adeguati livelli autorizzativi;
- verifica, in occasione di appositi colloqui di selezione, del possesso dei requisiti in capo ai candidati individuati; ogni candidato è valutato secondo requisiti oggettivi di competenza, soft skills necessarie in funzione del ruolo oggetto della ricerca ed esperienza pregressa;
- autorizzazione all'assunzione concessa soltanto dal personale espressamente facoltizzato secondo il vigente sistema dei poteri e delle deleghe;
- identificazione di potenziali conflitti di interesse e/o di rapporti di parentela con la PA da parte del candidato;
- formalizzazione degli esiti dei colloqui tecnico-motivazionali con indicazione delle motivazioni dell'eventuale esclusione/ammissione dei candidati;
- definizione dei criteri connessi alla predisposizione dell'offerta economica; l'Ufficio Gestione del Personale, in accordo con i soggetti delegati, formula una proposta contrattuale rispettando le previsioni del Contratto Collettivo vigente e la sottopone al candidato;
- a seguito di accettazione da parte del candidato, predisposizione della documentazione necessaria all'assunzione ed esecuzione di un controllo sulla regolarità della documentazione personale del candidato (anche in ordine al permesso di soggiorno, se si tratta di lavoratori extracomunitari);
- il dipendente è informato dell'esistenza e del contenuto delle norme comportamentali da seguire, anche in materia di salute e sicurezza sui luoghi di lavoro ed è tenuto a rispettare i contenuti del Codice Etico e del Modello di Organizzazione, Gestione e Controllo adottato dalla Banca;
- adeguata formazione al nuovo assunto sulle procedure aziendali da osservare, anche in materia di salute e sicurezza sui luoghi di lavoro, nonché sul contenuto e sulle finalità del Modello di Organizzazione, Gestione e Controllo adottato dalla Società;

- verifica formale della documentazione identificativa e di supporto necessaria all'assunzione del personale da parte della Funzione competente; in merito alle assunzioni obbligatorie, riguardanti cioè le persone appartenenti a categorie protette, la documentazione necessaria per l'assunzione è predisposta dall'Ufficio Gestione del Personale indicando il numero delle assunzioni da effettuare in virtù dei criteri definita dalla normativa esterna ed in virtù del numero di lavoratori della Banca, sui cui applicare la percentuale definita dalla legge;
- formale definizione degli accordi sindacali raggiunti e relativa validazione da parte di procuratori abilitati della Banca;
- archiviazione e conservazione di tutta la documentazione prodotta in forma cartacea, telematica o elettronica, nell'ambito del processo di selezione, assunzione, valutazione del personale.

1.15. GESTIONE DEL PERSONALE

1.15.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Malversazione di erogazioni pubbliche (art. 316-bis c.p.);
- Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.);
- Truffa (art. 640 c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- Frode informatica in danno dello Stato o di altro Ente pubblico (art. 640-ter c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.)
- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-ter, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648-ter.1 c.p.).

21) Reati Tributari (art. 25-quinquiesdecies)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000);
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000);
- Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000);
- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000).

2) Delitti informatici e trattamento illecito dei dati (art. 24-bis)

- Documenti informatici (art. 491-bis c.p.).

13) Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1)

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.).

1.15.2. *Unità organizzative/funzioni aziendali coinvolte*

- Gestione Personale:
 - Sviluppo e Formazione;
 - Amministrazione e Sicurezza;
- Area Pianificazione e Amministrazione (CFO):
 - Amministrazione:
 - Fiscale e Tributario.

1.15.3. *Attività sensibili*

- a) Amministrazione del personale.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- rilevazione presenze, straordinari, permessi, ferie e gestione anagrafica Dipendenti;
- calcolo e pagamento di salari, stipendi e corrispettivi;
- gestione dei benefit aziendali (utilizzo carte di credito aziendali);
- gestione trasferte, rimborsi spese;
- predisposizione, approvazione e invio delle dichiarazioni contributive, previdenziali e assistenziali.

1.15.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- la trasmissione, anche informatica, di dati e documenti alla P.A. e alle Autorità di Vigilanza, deve essere curata da parte di Esponenti Aziendali/dipendenti e soggetti formalmente autorizzati e nei limiti delle proprie competenze e mansioni;
- la gestione dei rimborsi spese avviene in accordo con la normativa, anche fiscale, applicabile;
- le uniche spese di trasferta rimborsabili sono quelle direttamente collegabili ad incarichi di lavoro;
- le note spese devono essere autorizzate e liquidate solo se inerenti all'attività svolta e supportate da idonea documentazione; eventuali deroghe alla mancata presentazione della documentazione giustificativa devono essere appositamente motivate dal dipendente (smarrimento, mancato rilascio) e approvate dal responsabile di riferimento;
- garantire che i pagamenti della Banca nonché i flussi di denaro siano sempre tracciabili e provabili documentalmente;
- garantire la massima correttezza nell'ambito dei rapporti con l'amministrazione fiscale e la massima trasparenza nella comunicazione di dati e informazioni alla stessa;
- procedere ad eventuali modifiche delle anagrafiche solo a seguito di espressa e documentata richiesta ed in presenza della documentazione a supporto della modifica richiesta;

- eseguire gli adempimenti fiscali nei tempi e nei modi definiti dalla normativa o dall'Autorità fiscale;
- garantire l'applicazione della legislazione nazionale riguardante la salute e la sicurezza nei luoghi di lavoro, il salario minimo vitale, l'adeguato orario di lavoro e la sicurezza sociale (previdenza e assistenza);
- eventuali consulenti esterni coinvolti nei processi in esame devono sottoscrivere le clausole rilevanti ai fini del D. Lgs. 231/01.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- promettere o effettuare erogazioni in denaro a favore di rappresentanti della P.A., italiana o straniera, per finalità diverse da quelle istituzionali e di servizio e in violazione delle prescrizioni aziendali;
- promettere o concedere vantaggi di qualsiasi natura (es.: promesse di assunzione, contributi, etc.) in favore di rappresentanti della P.A., italiana o straniera, al fine di influenzarne l'indipendenza di giudizio od assicurare un qualsiasi vantaggio per la Banca;
- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore.

1.15.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca nell'ambito delle attività sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna;
- formale approvazione del contratto con l'outsourcer sulla base di adeguati livelli autorizzativi;
- definizione dei profili abilitati ad accedere all'anagrafica dipendenti;

- inserimento completo ed accurato dei dati in fase di nuove assunzioni e/o in fase di modifiche in anagrafica dipendenti;
- tracciabilità delle variazioni dei dati anagrafici dei dipendenti;
- accurata rilevazione delle presenze dei dipendenti, ivi inclusi i dirigenti;
- formale approvazione di ferie, straordinari e permessi da parte dei Responsabili degli Uffici oltre che in osservanza delle norme vigenti, sulla base di un piano organizzativo della Funzione;
- previsione di un monitoraggio periodico sul sistema di rilevazione delle presenze;
- previsione di verifiche in merito alle richieste di rimborsi spese: è possibile richiedere un rimborso nei limiti delle soglie di spesa massima previsti per le diverse tipologie di esborso (vitto, alloggio, spese di viaggio). Sono, inoltre, individuate le tipologie di spesa suscettibili di rimborso. Il rimborso spese è disposto solo previa presentazione da parte del dipendente di apposita nota spese e giustificativi di supporto;
- rendicontazione completa ed accurata delle spese sostenute in trasferta: la liquidazione delle note spese è autorizzata previa verifica della pertinenza e della ragionevolezza delle spese dichiarate a cura del Responsabile diretto del richiedente;
- definizione di massimali di spesa rimborsabili in relazione alle spese sostenute tramite carte di credito aziendali;
- rendicontazione completa ed accurata delle spese sostenute in trasferta attraverso carte di credito aziendali;
- previsione di controlli sulle spese sostenute mediante carta di credito per uso aziendale;
- formale autorizzazione alla trasferta;
- definizione delle modalità e delle regole di concessione delle carte di credito aziendali;
- accurata elaborazione dei cedolini;
- previsione di verifiche sulla corretta elaborazione dei cedolini;
- formale approvazione del mandato di pagamento degli stipendi;
- previsione di meccanismi di valutazione periodica del personale basati sul raggiungimento degli obiettivi assegnati (valutazione quantitativa), nonché sulla

valutazione dei comportamenti agiti (valutazione qualitativa) durante il periodo di osservazione della performance;

- previsione di controlli di completezza ed accuratezza in fase di elaborazione delle dichiarazioni contributive, previdenziali e assistenziali;
- verifiche in merito alla corretta contabilizzazione delle competenze del Personale e dei connessi adeguamenti del fondo TFR, con riferimento a premi di rendimento, bonus aziendali, remunerazione, nonché al calcolo attuariale dei premi di fedeltà e del TFR, sulla base dei dati comunicati dall'Ufficio Personale e dallo studio attuariale incaricato;
- formale autorizzazione in merito ai documenti/dati da trasmettere alla Pubblica Amministrazione;
- utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, archiviazione e conservazione da parte delle Strutture di volta in volta interessate, della documentazione di competenza prodotta anche in via telematica o elettronica, inerente all'esecuzione degli adempimenti svolti nell'ambito della gestione delle attività sopra descritte.

1.16. GESTIONE DELLA SALUTE E SICUREZZA SUL LAVORO

1.16.1. Reati astrattamente ipotizzabili

11) Reati di omicidio colposo o lesioni gravi o gravissime, commesse con violazione delle norme sulla tutela della salute e della sicurezza sul lavoro (art. 25-septies)

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose (art. 590, comma 3, c.p.).

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e Istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321 e 322, 322-bis c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Traffico di influenze illecite (art. 346-bis, comma 2, c.p.).

1.16.2. Unità organizzative/funzioni aziendali coinvolte

- Gestione Personale:
 - Amministrazione e Sicurezza;
- Filiali;
- Aree Territoriali.

1.16.3. Attività sensibili

- a) Adempimenti relativi a salute e sicurezza sul luogo di lavoro e dei rapporti con Enti Pubblici per il rispetto delle cautele previste da leggi e regolamenti.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- organizzazione dei ruoli e delle attività connesse alla tutela della Salute e Sicurezza sul lavoro;
- attività di valutazione dei rischi e predisposizione delle conseguenti misure di prevenzione e protezione;
- gestione delle emergenze;
- attività di informazione, formazione e coinvolgimento dei lavoratori in tema di Salute e Sicurezza sul lavoro;
- gestione della sorveglianza sanitaria;
- rilevazione, registrazione e gestione degli infortuni e degli incidenti.

1.16.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- osservare rigorosamente tutte le norme poste dalla legge e dalle procedure aziendali interne in materia di salute, sicurezza ed igiene sul lavoro;
- garantire l'assegnazione di un budget adeguato a tutte le Funzioni aziendali responsabili (o per eventuali incarichi a terzi) per la salute e la sicurezza sui luoghi di lavoro, al fine di garantire un corretto adempimento di tutte le prescrizioni normative nonché la tempestiva risoluzione di anomalie riscontrate;

- assicurare un costante monitoraggio delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro, nonché la definizione dei ruoli dell'organizzazione aziendale che debbano provvedere alla loro attuazione;
- assicurare un costante monitoraggio dell'attuazione delle misure preventive e protettive predisposte per la gestione della salute e sicurezza sui luoghi di lavoro;
- promuovere ed attuare ogni ragionevole iniziativa finalizzata a minimizzare i rischi e a rimuovere le cause che possono mettere a repentaglio la sicurezza e la salute dei dipendenti e dei terzi che prestano la propria attività presso la Banca;
- compiere approfondita analisi con riferimento ad ogni infortunio sul lavoro verificatosi, al fine di individuare eventuali lacune nel sistema di gestione della salute e della sicurezza e di identificare le eventuali azioni correttive da intraprendere;
- adottare, direttamente attraverso il Datore di Lavoro ovvero tramite soggetto a ciò delegato, provvedimenti disciplinari, in conformità alle disposizioni contrattuali e legislative, nei confronti dei lavoratori che non osservino le misure di prevenzione e le procedure di sicurezza mettendo in pericolo, attuale o potenziale, la propria o altrui sicurezza;
- garantire trasparenza, correttezza e tracciabilità nei confronti degli adempimenti verso gli Enti esterni preposti al controllo in materia di sicurezza sul lavoro (A.S.L., Vigili del Fuoco, Ispettorato del Lavoro, etc.) in occasione di accertamenti ispettivi o in occasione del perfezionamento di altre pendenze;
- provvedere, nell'ambito dei contratti di appalto o di fornitura, ad informare le controparti sugli eventuali rischi in materia di sicurezza sul lavoro e ad elaborare le connesse misure preventive.

Le misure in ambito Salute e Sicurezza sul Lavoro (SSL) non devono in nessun caso comportare oneri finanziari per i lavoratori. È cura di ciascun lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite. I lavoratori devono in particolare:

- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro o dal suo delegato ai fini della protezione collettiva e individuale;
- utilizzare correttamente le apparecchiature da lavoro nonché gli eventuali dispositivi di sicurezza;

- segnalare immediatamente alle Funzioni aziendali competenti le deficienze dei mezzi e dei dispositivi dei punti precedenti, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli;
- non rimuovere o modificare, senza autorizzazione, i dispositivi di sicurezza, di segnalazione, di controllo;
- partecipare ai programmi di formazione e di addestramento organizzati dal Datore di Lavoro;
- sottoporsi ai controlli sanitari previsti nei loro confronti;
- contribuire, insieme al Datore di Lavoro o al suo delegato all'adempimento di tutti gli obblighi imposti dall'Autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

1.16.5. *Controlli preventivi*

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

ORGANIZZAZIONE DELLA SICUREZZA

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca nell'ambito delle attività sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna, nonché ai sensi del vigente sistema dei poteri e delle deleghe della Banca;
- chiara e formale identificazione del Datore di Lavoro;
- istituzione di un'articolazione di funzioni che assicura le competenze tecniche ed i poteri necessari per la verifica, valutazione, gestione e controllo del rischio mediante la definizione di uno specifico Organigramma della Sicurezza;
- formalizzazione del sistema di deleghe in materia di SSL;
- chiara identificazione del Responsabile per la Prevenzione e Protezione (RSPP);

- chiara identificazione e formale designazione degli addetti alle emergenze e degli addetti al primo soccorso;
- formale designazione dei soggetti cui sono affidati ruoli e responsabilità in materia di SSL (RSPP, RLS, etc.);
- nomina del Medico Competente per l'effettuazione della sorveglianza sanitaria, in base ai requisiti di cui all'articolo 38 del D. Lgs. 81/2008;
- tracciabilità della formale accettazione dell'incarico da parte dei soggetti designati.

VALUTAZIONE DEI RISCHI

- formale definizione di una Politica per la salute e sicurezza sul lavoro, volta a definire i compiti e le responsabilità in materia di sicurezza;
- valutazione di tutti i rischi presenti in azienda per la sicurezza e la salute dei lavoratori, compresi quelli collegati allo stress correlato alla specifica attività svolta. In merito, è stato redatto ed approvato il relativo "Documento di Valutazione dei Rischi".
- dotazione di DPI assegnati in funzione della specificità delle mansioni e in ragione della sussistenza di rischi infortunistici e rischi specifici in materia di SSL;
- convocazione (almeno annuale) e formale verbalizzazione della riunione periodica ai sensi dell'art. 35 del D.Lgs. 81/08.

SORVEGLIANZA SANITARIA

Il medico competente verifica i requisiti/idoneità del personale in via preliminare all'attribuzione delle mansioni e/o al cambio mansione ed a richiesta provvede inoltre a:

- collaborare con il Datore di Lavoro e con il Servizio di Prevenzione e Protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della Sorveglianza Sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori e all'attività di formazione e informazione nei loro confronti, per la parte di competenza considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro;
- effettuare e tracciare le visite di sorveglianza sanitaria (nuovi assunti, visite periodiche, cambio mansione o su richiesta del lavoratore);

- definire formalmente la documentazione sanitaria e di rischio da predisporre a cura del Medico Competete (es. Cartella Sanitaria);
- comunicare per iscritto in occasione della riunione periodica di cui all'art. 35 D.Lgs. 81/2008 i risultati anonimi collettivi della Sorveglianza Sanitaria effettuata, fornendo indicazioni sul significato di detti risultati ai fini dell'attuazione delle misure per la tutela della salute e della integrità psicofisica dei lavoratori.

Tutti gli ambienti di lavoro sono visitati e valutati da soggetti in possesso dei requisiti di legge e di adeguata formazione tecnica. Il Medico Competente, il Responsabile e gli addetti del Servizio Prevenzione e Protezione visitano i luoghi di lavoro ove sono presenti lavoratori esposti a rischi specifici ed effettuano a campione sopralluoghi negli altri ambienti.

Con specifico riferimento all'attività di analisi degli infortuni sul lavoro e delle malattie professionali, il processo prevede le seguenti fasi:

- accurata e tempestiva denuncia/comunicazione di infortunio;
- attivazione di una istruttoria preliminare che consiste in una attività di verifica e approfondimento tramite la raccolta di tutti gli elementi conoscitivi sia di natura testimoniale sia documentale;
- effettuazione di un sopralluogo - se necessario - per individuare la causa primaria dell'evento;
- definizione degli eventuali provvedimenti correttivi da adottare;
- formale definizione di regole per la rilevazione, registrazione e investigazione degli infortuni, degli incidenti e dei "mancati incidenti".

FORMAZIONE E SENSIBILIZZAZIONE

La Banca assicura l'adeguata e completa formazione di tutto il personale, pianificando le attività in ottemperanza a quanto stabilito dagli Accordi Stato-Regioni per la formazione in materia di salute e sicurezza sul lavoro mediante:

- predisposizione di un piano di formazione, nel quale sono elencati gli interventi formativi previsti per l'anno, con indicazione dell'argomento, del periodo in cui essi verranno pianificati e dei relativi destinatari. La formazione è, in ogni caso, erogata in

caso di assunzione. Le iniziative formative sono organizzate con il supporto dell'Ufficio Gestione del Personale, con il quale vengono valutate anche le modalità più idonee per la loro somministrazione (es. corsi in aula o in modalità e-learning).

- tracciabilità della formazione erogata ai lavoratori in materia di SSL sulla base di quanto definito dal programma di formazione;
- erogazione di formazione specifica alle figure aziendali designate in materia SSL;
- garanzia della qualità ed efficacia della formazione, nel caso di docenza esterna, assicurata attraverso il processo di scelta del professionista, nel rispetto delle regole di qualifica aziendali e dei requisiti richiesti dalla normativa applicabile;
- identificazione di regole formali per la gestione delle emergenze;
- formalizzazione del Piano di Emergenza e di evacuazione;
- svolgimento periodico delle prove di evacuazione e di simulazione delle situazioni di emergenza, incluse le modalità, frequenza e tracciabilità.

GESTIONE E DI COORDINAMENTO DELLE PRESTAZIONI D'OPERA E DI SERVIZI

Con riferimento ai singoli programmi, progetti o commesse implicanti la realizzazione di lavori per mezzo di cantieri temporanei o mobili ai sensi del Titolo IV del D.Lgs. 81/08 e s.m.i., il Datore di lavoro e/o suo delegato assicurano, anche attraverso la collaborazione delle Funzioni aziendali competenti:

- la verifica dell'idoneità tecnico professionale delle imprese appaltatrici/lavoratori autonomi in relazione all'affidamento nonché acquisisce in relazione alla sua tipologia ed entità, i certificati pubblici che attestino le caratteristiche di effettività, dimensione, regolarità contributiva e previdenziale, etc., dell'affidatario;
- le attività di vigilanza sull'operato dei soggetti nominati ai sensi di legge, previa verifica del possesso degli opportuni requisiti professionali definiti dalla normativa vigente, quali il Responsabile lavori, il Coordinatore della sicurezza in fase di progettazione (CSP) ed in fase di esecuzione (CSE), con riferimento in particolare alla redazione, aggiornamento, riesame e comunicazione alle parti interessate (ditte appaltatrice ed esecutrici) del Piano di Sicurezza e Coordinamento (PSC), del Piano Operativi per la Sicurezza (POS) e del Fascicolo tecnico, elaborati secondo le disposizioni normative

vigenti, nonché alle attività di monitoraggio e verifica da parte di detti soggetti circa il rispetto delle disposizioni ivi contenute;

- l'esecuzione degli adempimenti tecnico-amministrativi, notifiche e comunicazioni alla Pubblica Amministrazione, anche per il tramite dei professionisti incaricati;
- la stipula del contratto, con indicazione dei costi per la sicurezza e allegazione del piano di sicurezza e coordinamento/documento di valutazione dei rischi interferenziali;
- il coordinamento nell'esecuzione delle attività fra le imprese/lavoratori autonomi e controlli sul rispetto delle misure nel cantiere, anche per il tramite dei professionisti incaricati;
- con specifico riferimento alla gestione dei contratti di appalto, contratti d'opera, contratti di somministrazione rientranti nell'ambito di applicazione dell'art. 26 del D.Lgs. 81/08 e s.m.i., la Banca, in sede di affidamento di lavori, servizi e forniture:
 - o verifica l'idoneità tecnico professionale delle imprese appaltatrici/lavoratori autonomi in relazione all'affidamento nonché acquisisce in relazione alla sua tipologia ed entità, i certificati pubblici che attestino le caratteristiche di effettività, dimensione, regolarità contributiva e previdenziale, etc., dell'affidatario;
 - o fornisce agli stessi le necessarie informazioni sui rischi specifici esistenti nell'ambiente in cui sono chiamati a svolgere le proprie attività e sulle misure di prevenzione e di emergenza definite.

La Banca promuove la cooperazione ed il coordinamento degli interventi di protezione e prevenzione dei rischi, elaborando un documento di valutazione dei rischi che indichi le misure adottate per eliminare o, ove ciò non sia possibile, ridurre al minimo i rischi da interferenze (fatta eccezione per i contratti esclusi dall'obbligo di predisposizione dello stesso). Tale documento è allegato al contratto di appalto o di opera e va adeguato in funzione dell'evoluzione di lavori, servizi e forniture.

Infine, i lavoratori di aziende che svolgono per la Banca attività in regime di appalto e subappalto devono essere riconoscibili ed esporre apposita tessera di riconoscimento.

ATTIVITÀ DI MONITORAGGIO

Sono programmate e svolte attività di vigilanza sistematica con riferimento al rispetto delle procedure e delle istruzioni di lavoro impartite ai lavoratori e l'effettiva attuazione delle misure ed il rispetto delle disposizioni impartite per garantire una maggiore sicurezza.

Al termine dell'attività di monitoraggio, il sistema adottato dalla Banca per la gestione della salute e sicurezza dei lavoratori è sottoposto ad un riesame periodico da parte del Datore di Lavoro, al fine di accertare che lo stesso sia adeguatamente attuato e garantisca il raggiungimento degli obiettivi prefissati. L'attività di riesame dovrà tra l'altro basarsi su (i) statistiche infortuni; (ii) risultato dell'attività di monitoraggio effettuata; (iii) azioni correttive intraprese; (iv) rapporti sulle emergenze; (v) segnalazioni pervenute dall'Organismo di Vigilanza.

Della suddetta attività di riesame deve essere data evidenza su base documentale e gli esiti della stessa sono oggetto di discussione nell'ambito della riunione periodica ex art. 35 del Decreto Sicurezza.

TRACCIABILITÀ

Con specifico riferimento alla tracciabilità, si riportano di seguito ulteriori presidi di controllo operativi stabiliti dalla Banca a prevenzione della commissione dei sopra indicati reati:

- la struttura/funzione e/o i soggetti competenti sono responsabili dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, ivi compresa la documentazione comprovante i requisiti tecnico-professionali delle imprese appaltatrici, dei lavoratori autonomi e dei soggetti destinatari di deleghe in materia di sicurezza, nonché documentazioni e certificazioni obbligatorie di legge;
- ogni comunicazione nei confronti delle Autorità, avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della Banca, è documentata/registrata in via informatica ed archiviata presso la struttura/funzione di competenza.
- identificazione di regole formali per la gestione delle emergenze;
- formalizzazione del Piano di Emergenza e di evacuazione;
- svolgimento periodico delle prove di evacuazione e di simulazione delle situazioni di emergenza, incluse le modalità, frequenza e tracciabilità;

- tracciabilità della formazione erogata ai lavoratori in materia di SSL sulla base di quanto definito dal programma di formazione;
- erogazione di formazione specifica alle figure aziendali designate in materia SSL;
- effettuazione e tracciabilità delle visite di sorveglianza sanitaria (nuovi assunti, visite periodiche, cambio mansione o su richiesta del lavoratore);
- formale definizione della documentazione sanitaria e di rischio da predisporre a cura del Medico Competete (es. Cartella Sanitaria);
- dotazione di DPI assegnati in funzione della specificità delle mansioni e in ragione della sussistenza di rischi infortunistici e rischi specifici in materia di SSL;
- accurata e tempestiva denuncia/comunicazione di infortunio;
- formale definizione di regole per la rilevazione, registrazione e investigazione degli infortuni, degli incidenti e dei “mancati incidenti”.

1.17. GESTIONE DEGLI ASPETTI AMBIENTALI

1.17.1. Reati astrattamente ipotizzabili

17) Reati ambientali (art. 25-undecies)

- Abbandono di rifiuti in casi particolari (art. 255-bis T.U. Ambientale);
- Abbandono di rifiuti pericolosi (art. 255-ter T.U. Ambientale);
- Attività di gestione di rifiuti non autorizzata (art. 256 T.U. Ambientale);
- Combustione illecita di rifiuti (art. 256-bis T.U. Ambientale);
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (art. 257 D.lgs. 152/2006);
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 T.U. Ambientale);
- Spedizione illegale di rifiuti (art. 259 D.Lgs. 152/2006);
- Spedizione illegale di rifiuti (art. 259-ter D.lgs. 152/2006);
- Sanzioni (art. 279 T.U. Ambientale);
- Omessa bonifica (art. 452-terdecies c.p.);
- Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.);

- Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis T.U. Ambientale);
- Inquinamento ambientale (art. 452-bis c.p.);
- Disastro ambientale (art. 452-quater c.p.);
- Delitti colposi contro l'ambiente (art. 452-quinquies c.p.);
- Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.);
- Impedimento del controllo (art. 452-septies c.p.);
- Circostanze aggravanti (art. 452-octies c.p.);
- Circostanze aggravanti (art. 452-sexiesdecies c.p.);
- Misure a tutela dell'ozono stratosferico e dell'ambiente (art. 3, comma 6, L. 549/1993).

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e Istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321 e 322, 322-bis c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Traffico di influenze illecite (art. 346-bis, comma 2, c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Associazioni con finalità di terrorismo anche internazionale e di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

1.17.2. Unità organizzative/funzioni aziendali coinvolte

- Area Operativa (COO):
 - Archivio e Logistica;
- Filiali;
- Aree Territoriali.

1.17.3. Attività sensibili

- a) Attività relative alla raccolta e gestione dei rifiuti anche in rapporto con terze parti.

1.17.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- vigilare sul rispetto degli adempimenti in materia ambientale;
- assicurare il costante monitoraggio dei fornitori esterni incaricati dello smaltimento, verificando periodicamente il possesso delle necessarie certificazioni/permessi;
- effettuare la raccolta dei rifiuti assimilabili agli urbani, urbani e speciali in conformità alle normative e alle prassi di buona tecnica e di prevenzione ambientale;
- affidare i rifiuti speciali, pericolosi e non pericolosi a società di trasporto e recupero e smaltimento autorizzate ed iscritte ai relativi Albi, avendo cura di accertare il conseguimento, anche da parte di fornitori e consulenti, delle prescritte autorizzazioni, iscrizioni o comunicazioni;
- adempiere tempestivamente agli obblighi di messa in sicurezza dei siti e procedere con le opportune segnalazioni nei confronti delle Autorità competenti nonché con gli interventi di dovuta bonifica dei siti in caso di incidenti che abbiano causato l'inquinamento di suolo, sottosuolo e delle acque;
- assicurare il corretto espletamento degli obblighi di comunicazione normativamente definiti;
- considerare come requisito rilevante per la valutazione del fornitore, ove la natura della fornitura lo renda possibile e opportuno, le certificazioni ambientali;

- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es.: A.S.L., Vigili del Fuoco, ARPA, Comune, Provincia, etc.) in occasione di accertamenti/procedimenti ispettivi.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra cui si citano in via esemplificativa:

- instaurare rapporti con società esterne che non abbiano adeguate caratteristiche tecnico-professionali o di correttezza o non dispongano di tutte le autorizzazioni necessarie allo svolgimento delle attività di raccolta, trasporto e smaltimento di rifiuti per conto della Banca;
- effettuare attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione ovvero in violazione di alcuni dei requisiti normativamente previsti per lo svolgimento di dette attività;
- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- depositare i rifiuti al di fuori delle aree appositamente adibite e consegnare i rifiuti speciali così come definiti dalla vigente normativa interna a fornitori incaricati del trasporto che non siano autorizzati alla gestione dei rifiuti;
- in sede di realizzazione delle prescritte misure di controllo, perseguire l'obiettivo di risparmio costi e tempi a scapito della tutela dell'ambiente;
- non effettuare gli obblighi di comunicazione previsti dalle norme di legge vigenti (es. MUD), nei tempi e nei modi normativamente definiti;
- cedere, esportare, o comunque gestire abusivamente ingenti quantitativi di rifiuti effettuando operazioni ovvero ricorrendo a mezzi e attività continuative organizzate, al fine di conseguire un ingiusto profitto.

1.17.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- approvazione e sottoscrizione degli atti che impegnano la Banca esclusivamente da soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- definizione dei principali adempimenti da porre in essere in ambito aziendale in merito alla gestione delle diverse tipologie di rifiuti prodotti dalla Banca, in conformità a quanto stabilito dalle disposizioni normative vigenti;
- affidamento delle attività di trasporto, recupero e smaltimento dei rifiuti esclusivamente a imprese autorizzate e nel rispetto delle procedure aziendali relative alla selezione dei fornitori di servizi;
- scelta dei fornitori di beni e servizi e dei professionisti effettuata tra i nominativi selezionati in base a criteri individuati nell'ambito della normativa interna;
- verifica in sede contrattuale del possesso dei requisiti autorizzativi, ai sensi delle vigenti normative nazionali e regionali, alle ditte preposte allo smaltimento ed al trasporto dei rifiuti;
- formalizzazione dei rapporti con i fornitori di servizi ambientali e previsione di una clausola con la quale si chiede l'impegno al rispetto del Codice Etico e del D.Lgs. 231/01;
- verifica sulla corretta gestione da parte dell'appaltatore dei rifiuti derivanti dalle attività di manutenzione ordinaria e straordinaria e da ristrutturazioni immobiliari;
- controllo sul corretto espletamento, da parte dei fornitori, dei servizi di manutenzione/pulizia (Servizi all'Edificio, Servizi alle Persone, etc.) degli immobili;
- documentabilità di ogni attività inerente ai processi;
- archiviazione e conservazione di tutta la documentazione prodotta a supporto da parte di tutte le strutture organizzative di volta in volta interessate e/o i soggetti competenti;
- utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità e non alterabilità delle informazioni elaborate e delle operazioni svolte.

1.18. GESTIONE DEGLI INVESTIMENTI DELLA CLIENTELA

1.18.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies);

- Autoriciclaggio (art. 648 - ter 1 c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Riciclaggio (art. 648-bis c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Associazioni con finalità di terrorismo anche internazionale e di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

6) Reati societari (art. 25-ter)

- Aggiotaggio (art. 2637 c.c.);
- False comunicazioni sociali (artt. 2621 e 2622 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

10) Reati e illeciti amministrativi di abuso di mercato (art. 25-sexies)

- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 D.Lgs.58/1998);
- Manipolazione del mercato (art. 185 del D.Lgs. 24 febbraio 1998, n. 58).
-

1.18.2. Unità organizzative/funzioni aziendali coinvolte

- Area Affari (CCO):
 - Consulenza e Gestioni Private;
- Filiali;
- Area Operativa (COO):
 - Polo Back Office;
- Aree Territoriali;
- Compliance.

1.18.3. Attività sensibili

a) Negoziazione, collocazione e gestione di strumenti finanziari per conto della clientela.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- profilatura della clientela;
- esecuzione, ricezione e trasmissione ordini per conto della clientela.

1.18.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- assumere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca;
- osservare le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando comportamenti che ne possano provocare una sensibile alterazione rispetto alla corrente situazione di mercato;
- effettuare con tempestività correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste intraprese
- astenersi dal porre in essere qualsiasi comportamento idoneo a configurare un abuso delle informazioni privilegiate;

- informare preventivamente i clienti della Banca sulla reale natura, rischi e costi delle operazioni e dei servizi da essa offerti;
- assicurare la corretta contabilizzazione delle operazioni di acquisto, cessione/dismissione di immobilizzazioni immateriali, materiali e finanziarie e relative plusvalenze o svalutazioni;
- mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei propri compiti e, in particolare, assicurare che la circolazione interna e verso terzi di documenti contenenti informazioni potenzialmente privilegiate sia soggetta ad ogni necessaria attenzione e cautela, onde evitare pregiudizi ed indebite divulgazioni;
- nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati o nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, non esporre false informazioni od occultare dati o notizie in modo da indurre in errore i destinatari del prospetto;
- ove applicabile, le condotte elencate ai punti precedenti assumono rilevanza e pertanto sono vietate anche con riferimento a crypto-attività o qualora le attività siano svolte con l'ausilio di sistemi di intelligenza artificiale;

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- utilizzare informazioni rilevanti e privilegiate per acquistare, vendere o compiere altre operazioni su strumenti finanziari per conto proprio o per conto di terzi, anche per interposta persona;
- impartire ordini per l'acquisto di, uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere informazioni fuorvianti sullo strumento finanziario in modo da aumentarne il prezzo;
- effettuare operazioni di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interessi (a meno che esso non venga esplicitato nelle forme previste dalla normativa), allorquando tale operazione non sarebbe stata ragionevolmente effettuata in caso di assenza di conflitto di interessi;
- compiere operazioni od ordini di compravendita che consentano, anche tramite l'azione di concerto di più persone, di fissare il prezzo di mercato di strumenti finanziari ad un livello anomalo o artificiale;

- porre in essere operazioni simulate o diffondere notizie false sulla Società;
- comunicare informazioni false e occultare dati e notizie che potrebbero indurre in errore i destinatari di tali comunicazioni;
- proporre opportunità commerciali o di qualsiasi altro genere che possano, anche solo potenzialmente, procurare loro un indebito vantaggio, al fine di ottenere in cambio un favore per la Banca;
- tenere una condotta ingannevole che possa indurre, anche in via potenziale, in errore la clientela nella valutazione tecnico-economica dei prodotti o dei servizi offerti o comunque ricorrere a pratiche elusive, tendenti a forzare il giudizio o il comportamento del cliente;
- ove applicabile, le condotte elencate ai punti precedenti assumono rilevanza e pertanto sono vietate anche con riferimento a crypto-attività o qualora le attività siano svolte con l'ausilio di sistemi di intelligenza artificiale.

1.18.5. *Controlli preventivi*

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca nell'ambito delle attività sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna, nonché ai sensi del vigente sistema dei poteri e delle deleghe della Banca;
- applicazione di regole formali volte a disciplinare le modalità ed i criteri adottati dalla Banca per l'esecuzione e la trasmissione degli ordini di negoziazione di strumenti finanziari;
- esecuzione da parte della Banca delle disposizioni impartite dalla clientela in modo rapido, onesto, equo e professionale al fine di assicurare un'elevata qualità di esecuzione degli ordini nonché l'integrità e l'efficienza dei mercati. Sono, inoltre, previsti dispositivi idonei a garantire la continuità e la regolarità nella prestazione del servizio, utilizzando sistemi, risorse e procedure appropriati e proporzionati;

- identificazione da parte della Banca dei negoziatori ritenuti più adeguati ad assicurare il rispetto degli obblighi previsti in materia di Best Execution, allo scopo di assicurare il migliore risultato possibile per il cliente;
- scelta dei soggetti negoziatori effettuata sulla base della competenza ed esperienza degli stessi, nello svolgimento dell'attività di intermediazione finanziaria nonché delle opportune valutazioni relative al merito creditizio degli intermediari ed ai costi di collegamento;
- trasmissione da parte della clientela degli ordini tramite canali di comunicazione elettronici tramite piattaforma di Internet banking appositamente abilitata, nonché all'occorrenza tramite posta elettronica. Tramite tale procedura la Banca provvede all'identificazione del cliente, alla fornitura allo stesso di tutte le informazioni sullo strumento finanziario oggetto dell'ordine e sull'operazione, nonché alla conservazione delle informazioni relative all'operazione richiesta;
- raccolta degli ordini della clientela da parte del personale esclusivamente tramite apparecchiature telefoniche di proprietà della Banca e previsione che l'operatore presti il servizio di investimento tramite canale telefonico, al fine di assicurare che il cliente disponga di tutte le informazioni necessarie;
- verifica e aggiornamento periodico dell'anagrafica cliente mediante raccolta e controllo di informazioni e documenti idonei per una corretta profilazione;
- il Gestore di Filiale, mediante la consultazione degli applicativi in dotazione alla filiale, verifica:
 - o la sottoscrizione da parte del cliente del contratto relativo al servizio di investimento;
 - o la disponibilità e la capienza del conto corrente; qualora il controvalore presunto dell'operazione sia superiore al saldo, è previsto un sistema bloccante, che non consente la conclusione dell'ordine;
 - o la consistenza del deposito titoli, in conformità alle disposizioni nazionali in materia di short selling disposte in recepimento del Regolamento (UE) 236/2012;
 - o il riepilogo dell'ordine, generato tramite stampa a seguito dell'inserimento in procedura dei dati dell'operazione, che riporta le caratteristiche dell'ordine nonché la presenza di eventuali conflitti di interessi o profili di inadeguatezza;

la conformità della firma rispetto a quella apposta sul relativo contratto, qualora il cliente non sia personalmente conosciuto;

- il gestore è tenuto ad avvisare l'Ufficio Consulenza e Gestione Private per l'inoltro dell'ordine alla controparte se lo stesso supera i limiti di volume prudenzialmente impostati dalla Banca;
- nel caso di ordini provenienti da un delegato o procuratore, l'addetto verifica preventivamente l'esistenza e la validità della delega/procura;
- una copia dell'ordine, sottoscritta dal cliente e recante i dati dell'operazione inseriti in procedura, è consegnata al cliente, quale attestazione dell'ordine; l'originale è inoltrato all'Ufficio Polo Back Office e un'altra copia è archiviata presso la filiale secondo le modalità previste;
- eventuali richieste di variazione delle condizioni sono inoltrate dal Gestore di filiale all'Ufficio Consulenza e Gestione Private che previa autorizzazione da parte del CCO autorizza l'Ufficio Polo Back Office alle modifiche richieste.;
- verifica del rispetto della policy di valutazione e pricing in fase di determinazione dei prezzi delle obbligazioni emesse dalla Banca;
- monitoraggio delle attività di regolamento e contabilizzazione delle operazioni su strumenti finanziari effettuate;
- verifica della regolarità, completezza e correttezza di tutti gli adempimenti, comprese le attività affidate a soggetti terzi;
- controlli di linea a cura di ciascuna struttura interessata nello svolgimento delle attività inerenti all'esecuzione dei processi oggetto del presente Protocollo;
- utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle informazioni elaborate;
- predisposizione e trasmissione di dati e documenti specificamente richiesti dalle Autorità di vigilanza;
- archiviazione e conservazione da parte della struttura organizzativa di volta in volta interessata e/o i soggetti competenti, della documentazione di competenza trasmessa alle Autorità di Vigilanza, nonché di quella prodotta a supporto delle attività svolte.

1.19. GESTIONE DEL DENARO CONTANTE, DELLE GARANZIE E DEI VALORI

1.19.1. Reati astrattamente ipotizzabili

4) Delitti in materia di falsità in monete, in carte di pubblico credito, in valori in bollo e in strumenti o segni di riconoscimento (art. 25-bis)

- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.).

1.19.2. Unità organizzative/funzioni aziendali coinvolte

- Area Operativa (COO):
 - Cassa centrale;
- Filiali;
- Aree Territoriali.

1.19.3. Attività sensibili

a) Gestione e movimentazione dei valori.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- movimentazione dei valori (operazioni di sportello, cassa continua, gestione ATM/MTA, rimessa valori alle Filiali e versamenti in Banca d'Italia, contazione esterna);
- gestione dei valori ed in particolare delle banconote sospette di falsità;
- gestione delle garanzie (es. certificati di deposito, effetti cambiari a garanzia);

- gestione dei valori in bianco (es. assegni, libretti di risparmio);
- gestione delle segnalazioni dei dati statistici alla Banca d'Italia (es. riciclo contante, chiusura filiale).

1.19.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- astenersi da condotte commerciali finalizzate o comunque idonee a ledere la buona fede del consumatore/cliente ovvero il lecito affidamento degli interlocutori;
- ogni operazione e transazione avente ad oggetto monete metalliche o banconote, in euro o in altra valuta, deve essere effettuata correttamente, adeguatamente registrata e corredata da un supporto documentale (cartaceo od informatico) idoneo a consentire, in ogni momento, i controlli, nonché l'identità della controparte negoziale;
- in presenza di banconote sospette di falsità, gli addetti sono tenuti a predisporre tempestivamente un verbale di ritiro delle banconote sospette di falsità. Nello specifico, per quanto concerne le banconote in euro sospette di falsità, la normativa vigente prevede che l'addetto trasmetta una copia del verbale all'Ufficio Centrale Antifrode dei Mezzi di Pagamento (UCAMP) del Ministero dell'Economia e delle Finanze alla Filiale della Banca d'Italia competente per territorio.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- sostituire, occultare, intermediare, trasferire denaro (monete o banconote di qualsiasi valuta), metalli preziosi o cose di cui si conosca, o si presuma, la provenienza delittuosa e la condizione di falsità;
- effettuare pagamenti/incassare tramite contanti e assegni bancari per importi superiori ai limiti definiti dalla normativa vigente;
- effettuare operazioni idonee a favorire il riciclaggio di denaro proveniente da attività illecite o criminali, ovvero anche rimettere in circolazione banconote sospettate di falsità, ottenute in buona fede;

- agevolare in qualsiasi modo diretto o indiretto l'introduzione, detenzione, spendita, messa in circolazione di monete false o alterate;
- contravvenire a quanto previsto dalla normativa vigente in materia di ritiro dalla circolazione e trasmissione alla Banca d'Italia delle banconote denominate in euro sospette di falsità;
- alterare ovvero contraffare – attraverso qualsivoglia tipo di riproduzione – marchi o segni distintivi nazionali ed esteri depositati/registrati ovvero fare uso di marchi o segni distintivi alterati oppure contraffatti;
- alterare oppure contraffare – attraverso qualsivoglia tipo di riproduzione - brevetti, disegni, modelli industriali ovvero fare uso di brevetti, disegni o modelli industriali alterati oppure contraffatti.

1.19.5. *Controlli preventivi*

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca nell'ambito delle attività sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna, nonché ai sensi del vigente sistema dei poteri e delle deleghe della Banca;
- adozione di specifica normativa interna nella quale vengono disciplinate le modalità di gestione e movimentazione dei valori;
- verifica del rispetto del massimale di contante presente nelle filiali mediante l'applicativo gestionale;
- approvazione, da parte del Responsabile della Funzione preposta della Banca, della richiesta di "sovvenzione" di denaro contante alle filiali o di ritiro del denaro contante dalle filiali;
- verifica periodica a sistema del corretto svolgimento del servizio di sovvenzione e ritiro;
- presenza di apparecchiature di selezione e accettazione delle banconote, adatte alla verifica dell'autenticità delle banconote e in grado di individuare e separare gli esemplari contraffatti da quelli autentici in modo affidabile e regolare nel tempo;

- verifica del timbro del capo cassiere sulle fascette delle banconote ricevute dalla filiale;
- formale sottoscrizione dei documenti cartacei di accompagnamento per il servizio di trasporto delle mazzette di banconote false/deteriorate in Banca d'Italia;
- verifica dei documenti di accompagnamento per il servizio di "sovvenzione" del denaro contante, di ritiro del denaro contante e di invio delle banconote logore/false in Banca d'Italia;
- adeguata gestione degli aspetti contrattuali con i vettori incaricati al trasporto dei plichi di banconote/effetti a garanzia/valori in bianco;
- formale approvazione del contratto con i vettori incaricati al trasporto dei plichi di banconote/effetti a garanzia/valori in bianco da parte di adeguati livelli autorizzativi;
- verifica automatica del contante presente nei plichi e nelle mazzette in termini di numero e di presenza di banconote deteriorate o false;
- verifica della quantità di banconote di valuta estera presenti nei plichi, da vendere alla Banca Intesa SanPaolo;
- verifica da parte delle Funzioni della Banca preposte, dell'estinzione del finanziamento, prima dell'invio dei documenti di garanzia alla filiale;
- adeguata custodia delle garanzie (es. certificati di deposito, effetti cambiari a garanzia) e relativo divieto di accesso ai soggetti non autorizzati;
- richiesta formale, da parte della filiale, di ricezione dei valori in bianco di cui necessita per lo svolgimento dell'attività lavorativa (es. carnet di assegni, libretti di risparmio);
- adeguata custodia dei valori in bianco (es. assegni, libretti di risparmio) e relativo divieto di accesso ai soggetti non autorizzati;
- formale inoltro semestrale delle segnalazioni statistiche alla Banca d'Italia;
- accesso agli applicativi utilizzati da parte del personale autorizzato della Banca secondo i poteri assegnati;
- archiviazione e conservazione di tutta la documentazione prodotta nell'ambito della propria attività.

1.20. GESTIONE DELLA FINANZA E DELLA TESORERIA

1.20.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

6) Reati societari (art. 25-ter)

- False comunicazioni sociali (artt. 2621 e 2622 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

10) Reati e illeciti amministrativi di abuso di mercato (art. 25-sexies)

- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 D.Lgs.58/1998);
- Manipolazione del mercato (art. 185 del D.Lgs. 24 febbraio 1998, n. 58).

1.20.2. Unità organizzative/funzioni aziendali coinvolte

- Area Finanza:
 - Tesoreria Banca;
- Chief Risk Officer (CRO);
- Area Pianificazione e Amministrazione (CFO);
- Area Crediti (CLO).

1.20.3. Attività sensibili

- a) Negoziazione, collocazione e gestione di strumenti finanziari per conto proprio;
- b) Gestione di conti di corrispondenza della Banca.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- definizione delle linee guida in merito alla gestione del portafoglio titoli di proprietà;
- esecuzione, ricezione e trasmissione ordini per la gestione del portafoglio titoli in conto proprio;
- adempimenti di carattere amministrativo/normativo connessi alla esecuzione delle operazioni di negoziazione;
- operazioni di emissione delle obbligazioni;
- gestione della liquidità sul conto accentrato c/o Banca d'Italia e sui conti presso altre Istituzioni finanziarie.

1.20.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- assumere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca;
- osservare le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando comportamenti che ne possano provocare una sensibile alterazione rispetto alla corrente situazione di mercato;

- effettuare con tempestività correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste intraprese;
- astenersi dal porre in essere qualsiasi comportamento idoneo a configurare un abuso delle informazioni privilegiate;
- la possibilità di accesso alle specifiche informazioni rilevanti ed alle informazioni privilegiate deve essere circoscritta limitatamente alle persone che vi abbiano necessità di operare e di cui si provvede ad assicurare istantaneamente l'iscrizione nella relativa Lista di Monitoraggio o nel Registro;
- assicurare la corretta contabilizzazione delle operazioni svolte su strumenti finanziari;
- mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei propri compiti e, in particolare, assicurare che la circolazione interna e verso terzi di documenti contenenti informazioni potenzialmente privilegiate sia soggetta ad ogni necessaria attenzione e cautela, onde evitare pregiudizi ed indebite divulgazioni;
- ove applicabile, le condotte elencate ai punti precedenti assumono rilevanza e pertanto sono vietate anche con riferimento a crypto-attività o qualora le attività siano svolte con l'ausilio di sistemi di intelligenza artificiale.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- utilizzare informazioni rilevanti e privilegiate per acquistare, vendere o compiere altre operazioni su strumenti finanziari per conto proprio o per conto di terzi, anche per interposta persona;
- impartire ordini per l'acquisto di, uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere informazioni fuorvianti sullo strumento finanziario in modo da aumentarne il prezzo;
- effettuare operazioni di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interessi (a meno che esso non venga esplicitato nelle forme previste dalla normativa), allorquando tale operazione non sarebbe stata ragionevolmente effettuata in caso di assenza di conflitto di interessi;

- compiere operazioni o ordini di compravendita che consentano, anche tramite l'azione di concerto di più persone, di fissare il prezzo di mercato di strumenti finanziari ad un livello anomalo o artificiale;
- eseguire operazioni che non determinano alcuna variazione nella proprietà ovvero non comportano alcun trasferimento effettivo della proprietà di uno strumento finanziario;
- porre in essere operazioni simulate o diffondere notizie false sulla Società;
- comunicare informazioni false e occultare dati e notizie che potrebbero indurre in errore i destinatari di tali comunicazioni;
- proporre opportunità commerciali o di qualsiasi altro genere che possano, anche solo potenzialmente, procurare loro un indebito vantaggio, al fine di ottenere in cambio un favore per la Banca;
- compiere operazioni su strumenti finanziari della Banca e di società terze in rapporto d'affari con la Banca stessa, in relazione alle quali si posseggano informazioni privilegiate circa l'emittente o il titolo stesso conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse; tale divieto si applica a qualsiasi tipo di operazione in strumenti finanziari (ad esempio: azioni, obbligazioni, warrant, covered warrant, opzioni, futures);
- ove applicabile, le condotte elencate ai punti precedenti assumono rilevanza e pertanto sono vietate anche con riferimento a crypto-attività o qualora le attività siano svolte con l'ausilio di sistemi di intelligenza artificiale.

1.20.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e i soggetti aventi facoltà di rappresentare la Banca nell'ambito delle attività sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna, nonché ai sensi del vigente sistema dei poteri e delle deleghe della Banca;
- definizione di specifica normativa interna in relazione ai processi di cui al presente Protocollo;

- presenza di un registro delle persone che hanno accesso a informazioni privilegiate/confidenziali relative all'operatività sui mercati finanziari;
- adozione di strategie d'investimento, formalmente approvate dagli Organi Sociali, basate sulla diversificazione e la combinazione di varie categorie di strumenti finanziari, al fine di i) garantire rendimenti competitivi e assorbimenti patrimoniali in linea con gli obiettivi formulati nel piano industriale; ii) contenere il rischio complessivo associato al portafoglio di investimenti entro i limiti regolamentari e le soglie definite nel RAF;
- previsione di specifici limiti operativi ed autorizzativi in relazione alla gestione del portafoglio titoli di proprietà;
- previsione di flussi informativi verso gli Organi Sociali in relazione all'andamento in termini di rischio/rendimento del portafoglio titoli di proprietà;
- in riferimento alla gestione dei conflitti di interesse, previsione di una valutazione preliminare, condotta con il supporto delle strutture interne, circa l'eventuale presenza di collegamenti tra gli esponenti della Controparte e gli esponenti e relativi collegati, ai sensi della normativa interna in tema di Parti correlate, della Banca;
- valutazione del merito creditizio delle controparti per la sottoscrizione o l'acquisto di titoli di debito o derivati da questi emessi; le operazioni di acquisto e vendita di titoli sul portafoglio titoli di proprietà avvengono per il tramite di Controparti/Broker classificate come "controparti qualificate/professionali";
- previsione di criteri formali e di adeguata verifica per l'individuazione e selezione delle controparti;
- verifica che la controparte contrattuale non sia inserita nelle Liste di Riferimento (nelle quali sono indicati i soggetti coinvolti in attività di terrorismo, riciclaggio e attività illecite transazionali). In caso di esito positivo del controllo, astenersi dall'intrattenere rapporti con la suddetta controparte contrattuale; la controparte, una volta conclusa l'operazione sui mercati finanziari, invia il ticket elettronico riepilogativo di tutti i dati dell'operazione. L'operatore dopo aver controllato la corrispondenza di quanto riportato nel ticket con l'ordine impartito inoltra il ticket al reparto Contabilità e Bilancio ed al CRO e provvede ad inserire l'operazione nella procedura di Front Office. L'operazione, prima di essere processata dal reparto Contabilità e Bilancio, deve essere validata (secondo quanto stabilito nei poteri delegati), attraverso l'apposizione della conferma informatica nella procedura stessa;

- monitoraggio della riserva obbligatoria detenuta dalla Banca all'interno del conto presso la Banca d'Italia;
- monitoraggio della liquidità presente all'interno dei conti reciproci di corrispondenza presso altri Istituti Bancari per il regolamento di specifiche operazioni;
- previsione di specifici poteri autorizzativi in relazione al pagamento per il trasferimento della liquidità tra Banche;
- formale autorizzazione dei pagamenti gestiti tramite home banking;
- previsione di controlli sulla regolarità dei pagamenti assicurando piena coincidenza tra i destinatari dei pagamenti e le controparti effettivamente coinvolte nelle transazioni per le operazioni in titoli di proprietà;
- previsione di controlli su transazioni potenzialmente anomale, in termini di importo, tipologia, oggetto o frequenza;
- approvazione del programma annuale delle emissioni di titoli obbligazionari;
- verifica delle condizioni economiche delle singole emissioni;
- monitoraggio dell'efficacia e della correttezza delle metodologie adottate per determinare il fair value delle obbligazioni;
- monitoraggio delle attività di regolamento e contabilizzazione delle operazioni su strumenti finanziari effettuate;
- verifica della regolarità, completezza e correttezza di tutti gli adempimenti, comprese le attività affidate a soggetti terzi;
- controlli di linea a cura di ciascuna struttura interessata nello svolgimento delle attività inerenti all'esecuzione dei processi oggetto del presente Protocollo;
- utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle informazioni elaborate;
- predisposizione e invio della documentazione e delle segnalazioni periodiche alle Autorità di Vigilanza previste da leggi e regolamenti;
- predisposizione e trasmissione di dati e documenti specificamente richiesti dalle Autorità di Vigilanza;
- Archiviazione e conservazione da parte della struttura organizzativa di volta in volta interessata e/o dei soggetti competenti, della documentazione di competenza

trasmessa alle Autorità di Vigilanza, nonché di quella prodotta a supporto delle attività svolte.

1.21. GESTIONE DEGLI ADEMPIMENTI ANTIRICICLAGGIO E ANTITERRORISMO

1.21.1. Reati astrattamente ipotizzabili

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Associazioni con finalità di terrorismo anche internazionale e di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

14) Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25-octies.2)

- Violazione delle misure restrittive dell'Unione europea (art. 275-bis c.p.);
- Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione Europea (art. 275-ter c.p.);
- Violazione delle condizioni dell'autorizzazione allo svolgimento di attività (art. 275-quater c.p.).

1.21.2. Unità organizzative/funzioni aziendali coinvolte

- Antiriciclaggio;
- Alto Dirigente;
- Consigliere Delegato;

- Filiali;
- Aree Territoriali.

1.21.3. Attività sensibili

a) Adempimenti antiriciclaggio nella prestazione di servizi bancari, servizi d'investimento ed erogazione del credito alla clientela.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- adempimenti inerenti all'adeguata verifica della clientela in sede di apertura e gestione dei rapporti continuativi;
- attività di offerta fuori sede effettuata tramite la rete dei consulenti finanziari;
- trasferimento di fondi;
- operatività di sportello;
- trasferimento e deposito di valori mobiliari;
- espletamento delle verifiche semplificate e rafforzate eseguite periodicamente dalla Funzione Antiriciclaggio, tale da consentire il riconoscimento e la valutazione dei presupposti e degli esiti degli interventi effettuati, anche ai fini della segnalazione delle operazioni sospette (SOS).

1.21.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- devono essere osservate la normativa vigente e le procedure interne in materia di contrasto al riciclaggio, al finanziamento del terrorismo e all'eversione dell'ordine democratico; in particolare, deve essere rispettata la regolamentazione in materia di prevenzione del riciclaggio;
- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza o la vicinanza a organizzazioni criminali o comunque illecite;
- non realizzare operazioni finanziarie e/o commerciali con controparti che utilizzano strutture societarie opache e/o che impediscono l'identificazione univoca dell'assetto societario (proprietà) e/o dei reali beneficiari dell'operazione;

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione dell'anagrafica fornitori/clienti;
- eseguire un periodico aggiornamento delle informazioni relative alla clientela nell'ambito di rapporti continuativi;
- non accettare pagamenti e non emettere fatture nei confronti di soggetti diversi da quelli che assumono ruolo di controparte contrattuale e in assenza di adeguata giustificazione;
- evitare di accettare pagamenti in contanti e non effettuare fatturazioni nei confronti dei soggetti diversi da quelli che assumono il ruolo di controparti contrattuali e in assenza di adeguata giustificazione;
- sospendere/interrompere un rapporto con il cliente/fornitore/partner laddove, previa opportuna consultazione con il proprio responsabile di Funzione, qualora emergessero comportamenti del cliente non in linea con la normativa, le leggi e i principi di controllo statuiti nel presente documento;
- garantire la corretta gestione della politica fiscale, anche con riguardo alle eventuali transazioni con i Paesi di cui alla c.d. "black list" secondo le disposizioni normative vigenti e con quelli a regime fiscale privilegiato indicati al D.M. 23 gennaio 2002 e loro successive modifiche ed integrazioni;
- individuare ed attuare specifici programmi di controllo interno con particolare riguardo alla gestione dei pagamenti e della tesoreria, nonché ai rapporti con controparti aventi sede sociale e/o operativa in Paesi a fiscalità privilegiata;
- garantire piena e fattiva collaborazione alle Autorità competenti nelle attività di indagine nell'ambito di operazioni sospette di riciclaggio o di finanziamento del terrorismo o di eversione dell'ordine democratico;
- informare immediatamente il proprio superiore gerarchico in merito all'eventuale sussistenza di conflitti d'interesse nell'ambito delle attività valutative/autorizzative connesse al presidio del rischio di riciclaggio e finanziamento al terrorismo, nonché astenersi dalle attività medesime rimettendole ad altri soggetti competenti e autorizzati;

- attuare e partecipare ai programmi di formazione attuati ai sensi della normativa applicabile alla Banca in materia di contrasto al riciclaggio e al finanziamento del terrorismo.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- instaurare rapporti continuativi, o mantenere in essere quelli preesistenti, ed eseguire operazioni quando non è possibile attuare gli obblighi di adeguata verifica nei confronti del cliente, ad esempio per il rifiuto del cliente a fornire le informazioni richieste;
- eseguire le operazioni per le quali si sospetta vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo;
- ricevere od occultare denaro o cose provenienti da un qualsiasi delitto o compiere qualunque attività che ne agevoli l'acquisto, la ricezione o l'occultamento;
- sostituire o trasferire denaro, titoli, beni o altre utilità provenienti da illeciti, ovvero compiere in relazione ad essi altre operazioni che possano ostacolare l'identificazione della loro provenienza delittuosa;
- partecipare ad uno degli atti di cui ai punti precedenti, associarsi per commetterli, tentare di perpetrarli, aiutare, istigare o consigliare qualcuno a commetterli o agevolarne l'esecuzione;
- effettuare operazioni di sponsorizzazione o liberalità, anche correlate ad eventi, con terzi soggetti pubblici o privati, non debitamente autorizzate dagli Organi competenti e con evidenza documentale e tracciamento dei flussi finanziari;
- corrispondere – in qualsiasi forma, anche in via indiretta – ovvero organizzare la raccolta di contributi, donazioni, liberalità, effettuare sponsorizzazioni o concedere agevolazioni creditizie a partiti politici, organizzazioni politiche, anche locali ovvero internazionali, associazioni, comitati se non nel pieno rispetto della normativa vigente in materia di finanziamento delle organizzazioni politiche;
- effettuare operazioni che possano realizzare, direttamente o indirettamente – anche a titolo di concorso od agevolazione – anche a favore di beneficiari diversi dai formali titolari, il finanziamento ovvero erogare servizi finanziari, anche transfrontalieri, aventi ad oggetto merci, sostanze stupefacenti e psicotrope, materiali, armamenti anche da

guerra dei quali sia vietata importazione/esportazione, ovvero la movimentazione di somme e fondi soggetti a sequestro dall'Autorità Giudiziaria;

- eseguire operazioni che vedano coinvolti soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, erogazione del credito, rimessione di debito, rilascio di garanzie personali o reali, apertura di c/c, effettuazione di rimesse e trasferimento di fondi, anche transfrontalieri, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi);
- sostituire, occultare, intermediare, trasferire denaro, beni o cose di cui si conosca la provenienza delittuosa, ovvero compiere operazioni bancarie e finanziarie (a titolo meramente esemplificativo: prestazioni di garanzie, incasso per conto, girata di assegni, cessione di crediti, rinuncia a crediti, costituzione e tenuta di fondi occulti, etc.) di sostituzione o trasferimento di denaro, beni od altre utilità provenienti da un delitto non colposo, ovvero che possano celare od ostacolare l'identificazione della loro provenienza delittuosa e/o dell'autore del reato;
- porre in essere, anche indirettamente, operazioni monetarie o finanziarie in violazione di misure restrittive dell'Unione Europea o delle relative disposizioni nazionali di attuazione, ivi incluso, a titolo meramente esemplificativo e non esaustivo, omettere di adottare misure di congelamento su fondi designati ed incluse operazioni finanziarie con Stati terzi sottoposti ad embargo;
- omettere di fornire alle Autorità amministrative competenti, in violazione di misure restrittive dell'Unione Europea o delle relative disposizioni nazionali di attuazione, informazioni conosciute per ragione del proprio ufficio o della propria professione, relative a fondi o risorse economiche presenti nel territorio nazionale che appartengono a Soggetti Designati¹ o da questi posseduti, detenuti o controllati;
- impiegare in attività economiche o finanziarie denaro, beni o altre utilità provenienti da un delitto;
- nei rapporti intrattenuti con Intermediari Finanziari e con i soggetti di cui di cui all'art. 3, d.lgs. 25 maggio 2017 n. 90, tenere comportamenti che impediscano od ostacolino l'adempimento da parte loro degli obblighi di identificazione dei soggetti (e dei

¹ Soggetti Designati: una persona fisica o giuridica, un'entità o un organismo o gruppo assoggettati a misure restrittive dell'Unione Europea;

beneficiari finali dell'operazione), di registrazione e di segnalazione di operazioni sospette;

- realizzare operazioni di usura o, comunque, in violazione delle prescrizioni di cui alla legge n. 108/1996, al regolamento attuativo di cui al d.p.r. n. 315/1997 salvo altre;
- negoziare/stipulare e/o porre in essere contratti o rapporti con persone fisiche e giuridiche, gruppi ed entità dei quali sia conosciuto o sospetto il coinvolgimento in attività illecite.

Inoltre, è fatto divieto di:

- commercializzare prodotti attraverso canali distributivi non autorizzati dalla Banca;
- commercializzare polizze attraverso soggetti non autorizzati all'intermediazione dei prodotti assicurativi;
- indurre con frode, raggiri o artifici un consumatore a stipulare una polizza o ad acquistare un prodotto bancario/assicurativo.

1.21.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- definizione da parte della Funzione Antiriciclaggio, anche sulla base di un monitoraggio periodico della normativa rilevante in materia, delle politiche di governo, nonché del sistema delle procedure e dei controlli interni, rispettivamente finalizzati al contrasto e alla prevenzione dei rischi di riciclaggio e di attività terroristiche;
- formalizzazione all'interno della normativa della Banca dei soggetti, delle strutture organizzative e degli Organi a cui sono attribuiti specifici ruoli e responsabilità previsti dalla normativa applicabile in materia di contrasto al riciclaggio e al finanziamento del terrorismo;
- monitoraggio dell'evoluzione del quadro normativo di riferimento in ambito antiriciclaggio e antiterrorismo;
- rilevazione delle novità rivenienti dal quadro normativo di riferimento e la stretta integrazione tra i diversi presidi di prevenzione: dall'adeguata verifica, alla tracciabilità dei flussi finanziari, alla rilevazione e segnalazione di operazioni sospette;

- screening anagrafico effettuate in fase di onboarding sia nel corso del rapporto, consentono di confrontare i nominativi presenti all'interno delle liste dei soggetti designati pubblicate dalle Nazioni Unite, dall'Unione Europea e da altre autorità nazionali (es. OFAC);
- criteri generali di valutazione concernenti il cliente, l'eventuale titolare effettivo e, ove rilevante, l'esecutore ed in particolare il paese o l'area geografica di provenienza (anche dei fondi); le relazioni d'affari; l'attività svolta e i Paesi con i quali vi siano collegamenti significativi; il profilo economico e finanziario (in termini reddituali e patrimoniali);
- monitoraggio della puntuale acquisizione delle informazioni per l'identificazione e la profilatura della clientela;
- al fine di presidiare il rischio di violazione delle sanzioni finanziarie, monitoraggio continuo dei provvedimenti emessi dalle Autorità competenti (e.g. ONU, UE, OFAC);
- screening transazionale sull'ordinante o sul beneficiario del trasferimento (i.e. bonifico in ingresso/uscita) prima che i fondi vengano messi a disposizione del beneficiario;
- in caso di corrispondenza di soggetti destinatari di misure restrittive, applicazione di procedure tra cui la sospensione immediata, il congelamento e la segnalazione alle Autorità competenti;
- monitoraggio dell'affidabilità del sistema informatico per la gestione del profilo di rischio della clientela. La Funzione effettua nell'ambito della valutazione dei sistemi informatici adottati specifiche attività di valutazione preventiva sulle tabelle ed i criteri per l'assegnazione della profilatura della clientela coerentemente con la normativa di riferimento;
- verifica della corretta esecuzione degli adempimenti prescritti in materia di adeguata verifica della clientela;
- previsione di monitoraggio periodico dell'anagrafica clienti; in tale ambito, è richiesto all'Addetto di Filiale/Ufficio incaricato, la compilazione del questionario di Adeguata Verifica, anche mediante la compilazione delle necessarie informazioni richieste all'interno dell'applicativo utilizzato, l'accertamento dell'identità del cliente tramite l'esecuzione delle opportune verifiche e valutazioni nel caso in cui si rilevino corrispondenze in sede di controllo automatico. Inoltre, la Funzione Antiriciclaggio provvede con cadenza annuale a monitorare i nominativi privi del questionario di

Adeguate Verifica, sollecitando la Rete a raccogliere i dovuti questionari in ottemperanza degli obblighi di adeguata verifica della Clientela;

- monitoraggio continuo delle controparti che intrattengono rapporti continuativi con la Banca e della connessa operatività, sulla base della profilatura attribuita in sede di instaurazione del rapporto;
- aggiornamento/revisione delle informazioni sui clienti esistenti, finalizzati al rispetto del principio della “know your customer rule”;
- analisi e valutazione sulle liste sensibili ai fini AML/CFT;
- verifica – anche su base campionaria - che le causali AUI siano correttamente raccordate alle casuali degli applicativi gestionali che generano la movimentazione da registrare. In caso di anomalie, la Funzione Antiriciclaggio attiva prontamente tutti gli interventi idonei a rimuovere le criticità rilevate e segue il follow up degli stessi.
- previsione, a fronte della rilevazione di operazioni inattese e/o sospette, di un iter di valutazione strutturato su più livelli in cui intervengono soggetti distinti e a valle del quale può essere disposta la trasmissione all’Autorità competente di una Segnalazione di Operazione Sospetta (SOS);
- rilevazione delle infrazioni delle disposizioni in tema di limitazioni nell'utilizzo del contante e dei titoli al portatore;
- verifica, da parte dell’Alto Dirigente, con il supporto della Funzione AML, in merito all’adeguatezza delle misure adottate per mitigare in maniera efficace il rischio connesso al rapporto di corrispondenza intrattenuto o in corso di apertura con clientela PEP e/o ad alto rischio;
- definizione delle esigenze formative in materia antiriciclaggio e antiterrorismo;
- archiviazione sistematica presso le strutture di competenza di tutta la documentazione relativa all’operatività e ai controlli periodici effettuati sulle posizioni relative ai clienti;
- utilizzo obbligatorio di sistemi informatici di supporto che tracciano tutte le informazioni elaborate per l’esecuzione degli adempimenti;
- tracciabilità, registrazione in via informatica e archiviazione presso la struttura/Funzione di competenza di ogni comunicazione nei confronti delle Autorità.

1.22. PIANIFICAZIONE E CONTROLLO DI GESTIONE

1.22.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Art. 2 Convenzione internazionale per la repressione del finanziamento del terrorismo 9 dicembre 1999.

6) Reati societari (art. 25-ter)

- False comunicazioni sociali (art. 2621 c.c. e 2622 c.c.);
- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

1.22.2. Unità organizzative/funzioni aziendali coinvolte

- Area Pianificazione e Amministrazione (CFO):
 - Pianificazione e Controllo di Gestione;

- Filiali;
- Aree Territoriali.

1.22.3. Attività sensibili

- a) Predisposizione e monitoraggio del budget dei costi annuale.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- gestione del budget dei costi e approvazione degli extra – budget;
- produzione della reportistica e della rendicontazione;
- analisi degli scostamenti e identificazione degli interventi da implementare (revisione degli obiettivi).

1.22.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- rappresentare i fatti di gestione in modo corretto, completo e tempestivo nella contabilità e nei dati aziendali allo scopo di garantire la corretta e veritiera rappresentazione dei risultati economici, patrimoniali e finanziari della Banca;
- garantire che ogni variazione di budget (inclusi extra-budget) sia adeguatamente motivata, autorizzata e formalizzata;
- assicurare la tracciabilità e documentabilità di tutte le fasi del processo di pianificazione, approvazione e monitoraggio del budget;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- rappresentare in modo fuorviante la situazione economica, patrimoniale o finanziaria della società;

- approvare o giustificare costi fittizi, non documentati o non inerenti all'attività aziendale;
- effettuare operazioni o registrazioni finalizzate a occultare la reale destinazione delle risorse finanziarie;
- omettere controlli o aggirare i sistemi autorizzativi previsti per approvazioni e variazioni di budget;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà;
- ostacolare o impedire le attività di controllo e verifica da parte delle Funzioni competenti.

1.22.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- il Consiglio di Amministrazione, sulla base delle analisi fornite dall'Area Pianificazione e Amministrazione, definisce le strategie e gli obiettivi economici e finanziari;
- la normativa interna regola lo svolgimento del processo aziendale con indicazione di ruoli, responsabilità e modalità operative delle Funzioni aziendali coinvolte nella gestione delle attività di pianificazione e controllo di gestione;
- il processo di pianificazione strategica ha l'obiettivo di definire ed aggiornare il Piano Industriale della Banca, assicurando la coerenza con la propensione al rischio (e, di conseguenza, con il Risk Appetite Framework), la sostenibilità del business e il raggiungimento degli obiettivi economici, patrimoniali e organizzativi nel medio termine;
- l'attività di pianificazione strategica è coordinata dall'Ufficio Pianificazione e Controllo di Gestione, con il supporto delle unità preposte (CFO, Responsabile Area Finanza, CLO, CCO, COO, CRO e Reparto Iniziative ESG) e si concretizza nella predisposizione del Piano Industriale;

- l'attività di verifica e monitoraggio del Piano Industriale, da sottoporre al Consiglio di Amministrazione, viene svolta con cadenza trimestrale dal CFO, che si avvale del supporto dell'Ufficio Pianificazione e Controllo di Gestione;
- il Piano Industriale viene sottoposto a revisione in caso di proposte o valutazioni di modifiche al Risk Appetite Framework (RAF), sulla base della sua redazione annuale o in presenza di criticità emerse dal monitoraggio degli indicatori in esso previsti;
- la revisione del Piano può rendersi necessaria o comunque opportuna qualora si verificassero mutamenti significativi delle condizioni esogene o endogene che abbiano influenzato le linee di sviluppo originariamente definite, in caso di scostamenti rilevanti tra previsioni e consuntivi intermedi, oppure nel caso di operazioni straordinarie o investimenti con un impatto significativo sul percorso strategico delineato;
- il processo di pianificazione operativa ha l'obiettivo di definire il Budget della Banca, assicurando la coerenza con il Piano Strategico e la propensione al rischio (e, di conseguenza, con il Risk Appetite Framework), la sostenibilità del business e il raggiungimento degli obiettivi economici, patrimoniali e organizzativi nel breve termine;
- l'attività di pianificazione operativa è coordinata dall'Ufficio Pianificazione e Controllo di Gestione, con il supporto delle unità preposte (CFO, Responsabile Area Finanza, CLO, CCO, COO, CRO e Reparto Iniziative ESG) e si concretizza nella predisposizione del Budget;
- annualmente viene effettuata un'analisi adeguata dei dati per la costruzione della bozza di Budget annuale allineato rispetto alle politiche e agli obiettivi elaborati: il Budget, prima dell'approvazione del Consiglio di Amministrazione, è sottoposto a un processo di controllo da parte del Chief Risk Officer (CRO), e più in generale dell'Area Risk Management, e della Funzione Compliance;
- periodicamente viene effettuato un monitoraggio del budget (con cadenza giornaliera, mensile e trimestrale) ed un'analisi degli scostamenti rispetto agli obiettivi definiti mediante condivisione con il Direttore Generale e il Consiglio di Amministrazione;
- tutte le strutture organizzative di volta in volta interessate e/o i soggetti competenti, sono responsabili dell'archiviazione e della conservazione di tutta la documentazione prodotta a supporto;

- sono utilizzati sistemi informatici di supporto che garantiscono la tracciabilità e non alterabilità delle informazioni elaborate e delle operazioni svolte.

1.23. GESTIONE DI NUOVI PRODOTTI/SERVIZI E/O AGGIORNAMENTO DI QUELLI ESISTENTI E RELATIVO INSERIMENTO IN NUOVI MERCATI

1.23.1. Reati astrattamente ipotizzabili

5) Delitti contro l'industria e il commercio (art. 25-bis.1)

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.).

Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis)

- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

1.23.2. Unità organizzative/funzioni aziendali coinvolte

- Area Affari (CCO):
 - Marketing, Prodotti e Trasparenza;
 - Condizioni.

1.23.3. Attività sensibili

- a) Sviluppo e governo dei prodotti offerti verso la clientela.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- definizione delle esigenze commerciali;
- analisi preliminare e valutazione dei nuovi prodotti/servizi;
- autorizzazione e monitoraggio dei nuovi prodotti/servizi.

1.23.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- è fatto obbligo di mantenere un comportamento corretto, trasparente e collaborativo nei rapporti con il cliente;
- è fatto obbligo di porre la massima attenzione ed accuratezza in ogni attività finalizzata all'acquisizione, elaborazione ed illustrazione di dati e di informazioni relative a prodotti, propri o di terzi, oggetto di vendita;
- nell'ambito dei rapporti commerciali con i clienti è fatto divieto di tenere condotte che possano ledere la concorrenza;
- deve essere garantita un'adeguata formalizzazione in termini di descrizione del servizio/prodotto oggetto di vendita;
- non impedire o non ostacolare illegittimamente l'esercizio di un'industria o di un commercio ovvero compiere atti di concorrenza sleale;
- non usare nomi o segni distintivi nell'ambito della commercializzazione dei prodotti che siano idonei a produrre confusione con nomi o segni distintivi appartenenti o legittimamente usati da altre società;
- non effettuare una descrizione di un prodotto non esattamente corrispondente a quella reale;
- è fatto divieto di alterare ovvero contraffare – attraverso qualsivoglia tipo di riproduzione – marchi o segni distintivi nazionali ed esteri depositati/registrati ovvero fare uso di marchi o segni distintivi alterati oppure contraffatti.

1.23.5. *Controlli preventivi*

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca, in base allo specifico ruolo attribuito loro nella normativa interna, nonché ai sensi del vigente sistema dei poteri e delle deleghe della Banca;

- formalizzazione all'interno della normativa della Banca dei soggetti, delle strutture organizzative e degli Organi a cui sono attribuiti specifici ruoli e responsabilità previsti dalla normativa applicabile nell'ambito del presente Protocollo;
- approvazione formale delle strategie commerciali da parte del Consiglio di Amministrazione;
- sovrintendenza dell'attuazione delle strategie commerciali approvate dal Consiglio di Amministrazione da parte del Direttore Generale;
- monitoraggio del contesto di riferimento della Banca (mutamenti del contesto giuridico e regolamentare, rafforzamento del presidio dei rischi, etc.) al fine di introdurre nel mercato nuovi prodotti /servizi;
- verifica, nell'ambito dell'attività di collocamento e distribuzione di prodotti e servizi di terzi, di eventuali conflitti di interesse tra i fornitori di tali prodotti e servizi e la Banca;
- verifica da parte delle Funzioni di Controllo della conformità delle caratteristiche e dell'operatività dei nuovi prodotti/servizi rispetto alla regolamentazione vigente e alle regole interne applicabili;
- valutazione di fattibilità per la realizzazione dei nuovi prodotti/servizi, da parte dell'Area Affari e dei competenti Uffici della Banca;
- trasmissione della proposta di nuovo prodotto o di modifica sostanziale al Comitato Prodotti, che ne valuta l'adeguatezza sotto i profili strategico, economico, commerciale, organizzativo, informatico e contabile/segnaletico/fiscale, proponendo eventuali approfondimenti necessari al completamento delle analisi preventive richieste per il lancio commerciale;
- nell'ambito della distribuzione di prodotti di proprietà di Enti terzi, acquisizione dal Produttore di tutte le informazioni necessarie alla corretta distribuzione mediante un flusso informativo continuo, strutturato e tracciabile, che accompagna l'intero ciclo di vita del prodotto: dalla fase pre-lancio, alla commercializzazione, fino al monitoraggio post-vendita e agli eventuali aggiornamenti;
- Verifica della scheda prodotto/servizio da parte delle FAC e delle strutture competenti;
- approvazione formale per l'inserimento sul mercato del nuovo prodotto/servizio o la modifica di prodotti e servizi esistenti da parte del Comitato Prodotti (in caso di nuovi prodotti e servizi riconducibili a linee di business e canali già presidiati dalla banca, nonché di modifica a prodotti e servizi già esistenti) o del Consiglio di Amministrazione

(in caso di nuovi prodotti e servizi riconducibili a linee di business/mercati/canali non serviti previo parere motivato non vincolante del Comitato Prodotti ;

- verifica di conformità del materiale pubblicitario relativo al nuovo prodotto o servizio rispetto alle vigenti disposizioni normative e regolamentari (es. trasparenza, privacy, antitrust, etc.);
- definizione ed approvazione del pricing e delle condizioni da applicare ai nuovi prodotti/servizi;
- erogazione di specifiche sessioni formative per le tipologie di prodotto che richiedono una specifica preparazione tecnica del personale afferente alla Rete commerciale;
- distribuzione dei prodotti elaborati, nonché di quelli collocati per conto di terzi, attraverso modalità e canali coerenti con le caratteristiche del target market e del prodotto;
- monitoraggio dei nuovi prodotti o servizi al fine di verificare la rispondenza alle disposizioni e alle norme interne ed esterne;
- rendicontazione, alle Funzioni di Controllo (di secondo livello), con cadenza annuale, in merito agli esiti dei controlli effettuati in sede di monitoraggio ex post;
- archiviazione di tutta la documentazione rilevante da ciascuna Funzione/Ufficio, in modo da garantire la tracciabilità delle fasi chiave del processo al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle decisioni assunte.

1.24. GESTIONE DEGLI ADEMPIMENTI FISCALI

1.24.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Truffa ai danni dello Stato o di altro Ente pubblico (art. 640, comma 2, n. 1 c.p.);
- Frode informatica (art. 640-ter c.p.);
- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

2) Reati informatici e trattamento illecito di dati (art. 24-bis)

- Documenti informatici (art. 491 - bis c.p.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Autoriciclaggio (art. 648 - ter 1 c.p.).

6) Reati societari (art. 25-ter)

- False comunicazioni sociali (artt. 2621 e 2622 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Fatti di lieve entità (art. 2621-bis c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

21) Reati Tributarî (art. 25-quinquiesdecies)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000);
- Dichiarazione infedele (art. 4 D.lgs. 74/2000);
- Omessa dichiarazione (art. 5 D.lgs. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.lgs. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000);
- Indebita compensazione (art. 10-quater D.lgs. 74/2000);
- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000).

1.24.2. Unità organizzative/funzioni aziendali coinvolte

- Area Pianificazione e Amministrazione (CFO):
 - Amministrazione:
 - Contabilità e Bilancio;
 - Fiscale e Tributario.

1.24.3. *Attività sensibili*

a) Gestione adempimenti amministrativi e tributari.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- determinazione delle imposte dirette e indirette;
- predisposizione, approvazione e invio delle dichiarazioni fiscali o dei modelli di versamento;
- esecuzione dei versamenti relativi alle imposte dirette e indirette;
- fatturazione attiva/passiva;
- registrazioni contabili.

1.24.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca;
- il processo di determinazione delle imposte deve avvenire sulla base di una rappresentazione del Bilancio d'esercizio veritiera, secondo i principi contabili di riferimento;
- la compilazione e la trasmissione della dichiarazione dei redditi devono avvenire nel rispetto dei tempi e modi previsti dalla legge;
- nel caso in cui alcune attività siano eseguite da professionisti esterni, devono essere utilizzate figure professionali di comprovata esperienza e con adeguata formazione in materia;
- l'archiviazione di tutta la documentazione rilevante, in formato cartaceo ovvero elettronico, deve essere effettuata nel rispetto delle previsioni normative e secondo standard atti a garantire la tracciabilità, la veridicità, l'immediata recuperabilità dei documenti;
- conservare in modo adeguato delle scritture contabili e degli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali;

- garantire la massima correttezza nell'ambito dei rapporti con l'amministrazione fiscale e la massima trasparenza nella comunicazione di dati e informazioni alla stessa;
- tutti i pagamenti riferiti ad acquisti realizzati dalla Banca devono essere effettuati a fronte dell'inserimento a sistema della fattura corrispondente da parte del personale a ciò debitamente autorizzato, previa verifica della relativa regolarità formale e della congruità del pagamento con il contratto/ordine d'acquisto corrispondente.
- assicurare, nella gestione dei rapporti delle Funzioni aziendali competenti con i Revisori legali, la tracciabilità delle richieste pervenute e di quelle evase, con evidenza della documentazione prodotta.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- effettuare registrazioni contabili in modo non accurato, non corretto e non veritiero;
- presentare dichiarazioni relative alle imposte sui redditi o sul valore aggiunto contenenti elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti;
- presentare dichiarazioni relative alle imposte sui redditi o sul valore aggiunto contenenti elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri
- utilizzare mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria;
- occultare o distruggere documenti contabili;
- rappresentare e/o trasmettere, ai fini dell'elaborazione e rappresentazione in Bilancio, relazioni, prospetti o altre comunicazioni sociali, dati falsi, lacunosi o non rispondenti alla realtà;
- nell'ambito di sistemi transfrontalieri, rappresentare elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, ovvero omettere la presentazione della dichiarazione sul valore aggiunto ovvero il pagamento delle somme dovute utilizzando in compensazione crediti inesistenti o non spettanti, al fine di evadere le imposte sul valore aggiunto;

- emettere o rilasciare fatture o altri documenti per operazioni inesistenti al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto;
- ostacolare le attività di verifica e di controllo degli Organi/Funzioni preposti;
- occultare o distruggere in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari, al fine di evadere le imposte, ovvero di consentirne l'evasione a terzi;
- alienare simulatamente o compiere altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva, al fine di sottrarsi al pagamento delle imposte ovvero di interessi o sanzioni amministrative relativi a dette imposte;
- indicare nella documentazione presentata ai fini della transazione fiscale elementi attivi per un ammontare inferiore quello reale o elementi passivi fittizi per un ammontare complessivo superiore.

1.24.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- approvazione e sottoscrizione degli atti che impegnano la Banca esclusivamente da parte di soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- presenza di normativa interna che regola lo svolgimento del processo aziendale con indicazione di ruoli, responsabilità e modalità operative delle Funzioni aziendali coinvolte nella gestione delle attività in ambito contabile e fiscale. Ogni struttura organizzativa coinvolta è responsabile delle attività di competenza connesse alla produzione e/o alla valutazione delle voci contabili;
- verifiche di accuratezza e completezza della documentazione connessa alla registrazione delle scritture contabili;
- monitoraggio del rispetto dei principi che regolano la compilazione, tenuta e conservazione dei dati e delle informazioni contabili delle dichiarazioni di natura contabile e fiscale;

- definizione, di uno scadenziario fiscale e monitoraggio circa il rispetto delle scadenze;
- monitoraggio delle tempistiche da rispettare per le comunicazioni, denunce e adempimenti nei confronti dell'Amministrazione finanziaria;
- verifica circa la completezza e la correttezza dei dati necessari al calcolo delle imposte, della corretta compilazione dei relativi Modelli dichiarativi e di versamento, nonché della completa e corretta registrazione contabile;
- monitoraggio dell'evoluzione del quadro normativo di riferimento;
- formale definizione delle modalità di versamento relative alle imposte dirette e indirette;
- formale sottoscrizione delle dichiarazioni predisposte da parte del Legale Rappresentante (o soggetto formalmente delegato) e trasmissione (ivi inclusa trasmissione telematica) delle stesse alle Autorità competenti, nel pieno rispetto del sistema di deleghe, procure e responsabilità organizzative assegnate in essere;
- controlli sulla corretta emissione, applicazione delle aliquote IVA e contabilizzazione delle fatture del ciclo attivo e sulla loro corrispondenza con i contratti e impegni posti in essere con i terzi;
- controlli sull'effettività del rapporto sottostante alle fatture passive ricevute e sulla corretta registrazione e contabilizzazione;
- controllo sull'effettività delle prestazioni rispetto alle fatture emesse;
- verifiche di quadratura circa la corrispondenza degli importi dovuti a titolo di imposta sul valore aggiunto con i registri e i relativi conti di contabilità generale;
- verifica sul rispetto dei requisiti normativi relativamente alle eventuali compensazioni IVA effettuate;
- verifica della congruenza delle aliquote di ammortamento in base ai principi contabili internazionali e alla normativa fiscale vigente;
- verifica della congruità e della tempestività del versamento delle imposte tramite l'esame della quietanza rilasciata dall'Agenzia delle Entrate;
- archiviazione e conservazione da parte della struttura organizzativa di volta in volta interessata e/o dei soggetti competenti, di tutta la documentazione prodotta a supporto;

- adozione di misure informatiche tali da tracciare il momento e l'autore di ogni modifica/integrazione delle scritture contabili o di altri documenti rilevanti ai fini fiscali;
- archiviazione e conservazione delle attività di controllo, revisione e certificazione poste in essere dal Collegio Sindacale e dalla Società di revisione, nonché di tutte le evidenze raccolte a supporto e prodotte.

1.25. GESTIONE DEI FINANZIAMENTI VERSO LA CLIENTELA

1.25.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.);
- Truffa ai danni dello Stato o di altro Ente pubblico (art. 640, comma 2, n. 1 c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- Malversazione di erogazioni pubbliche (art. 316-bis c.p.);
- Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.);
- Turbata libertà degli incanti (art. 353 c.p.);
- Turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.);
- Frode informatica (art. 640-ter, c.p.);
- Frode ai danni del Fondo europeo agricolo (art. 2 Legge 23 dicembre 1986 n. 898).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

14) Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25-octies.2)

- Violazione delle misure restrittive dell'Unione europea (art. 275-bis c.p.);
- Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione Europea (art. 275-ter c.p.);
- Violazione delle condizioni dell'autorizzazione allo svolgimento di attività (art. 275-quater c.p.).

1.25.2. *Unità organizzative/funzioni aziendali coinvolte*

- Area Affari (CCO):
 - BU CQS;
 - Sviluppo e Gestione Corporate/ Istituzionali;
 - Sviluppo e Gestione /PMI/SB;
 - Sviluppo e Gestione Privati
 -
- Area Crediti (CLO):
 - Concessione Crediti;
 - Amministrazione Crediti;
 - Monitoraggio Crediti;
- Area Crediti Deteriorati (CNPE):
 - Gestione Crediti Deteriorati;

- Filiali;
- Aree Territoriali.

1.25.3. Attività sensibili

- a) Gestione dei crediti verso soggetti privati e pubblici.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- attività di istruttoria, valutazione dei requisiti, valutazione delle garanzie e delibera ai fini della concessione di finanziamenti alla clientela (es. cessione del quinto, mutui, leasing, etc.);
- monitoraggio dei finanziamenti ed eventuali rimodulazioni/sospensioni;
- rapporti operativi con Enti terzi agevolanti (es. Fondo ex Lege 662/96, Fondo Europeo degli Investimenti, Consorzi di Garanzia) per l'ottenimento delle garanzie e i successivi adempimenti;
- gestione dei crediti in sofferenza.

1.25.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- verificare, nell'ambito della concessione e gestione delle linee di credito alla clientela, la coerenza tra il finanziamento richiesto ed il profilo economico-finanziario del cliente, per una valutazione circa la (potenziale) esposizione a fenomeni di riciclaggio o di finanziamento del terrorismo;
- in sede di valutazione del cliente/prenditore, si devono tenere in considerazione tutte le informazioni, interne ed esterne (comprese anche dati esterne: es. protesti, pregiudizievoli, etc.), su eventuali eventi negativi a carico dei soggetti coinvolti nella richiesta di affidamento;
- eseguire un periodico aggiornamento delle informazioni relative alla clientela nell'ambito di rapporti continuativi;
- ogni operazione posta in essere deve essere legittima, coerente, congrua, autorizzata, verificabile, correttamente e adeguatamente registrata e corredata da un supporto documentale (cartaceo od informatico) idoneo a consentire, in ogni momento, i

controlli, la ricostruzione del processo decisionale, nonché l'identità della controparte negoziale;

- è vietato porre in essere, anche indirettamente, operazioni commerciali in violazione di misure restrittive dell'Unione Europea o delle relative disposizioni nazionali di attuazione, ivi incluse, a titolo meramente esemplificativo e non esaustivo, operazioni con stati terzi sottoposti a embargo o verso soggetti inseriti in c.d. blacklist dell'Unione Europea;
- divieto di instaurare, mantenere rapporti, essere coinvolto, partecipare o dirigere organismi associativi (di soggetti nazionali od esteri) per delinquere, facendo da ciò derivare un qualsiasi illecito vantaggio per la Banca.

1.25.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca nell'ambito delle attività sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna, nonché ai sensi del vigente sistema dei poteri e delle deleghe della Banca;
- definizione di specifica normativa interna in relazione ai processi di cui al presente Protocollo:
 - o all'inizio di ciascun esercizio, previa approvazione da parte del Consiglio di Amministrazione, l'Area Crediti, in un clima di condivisione continua e costante con la Funzione di Controllo dei Rischi, nel rispetto di quanto dichiarato nel Risk Appetite Framework, declina le Politiche Creditizie secondo framework differenziati per tipologia di controparte, al fine di dar seguito agli indirizzi complessivi di evoluzione del portafoglio crediti;
 - o i canali di distribuzione della Banca curano le relazioni con la clientela, anche al fine di individuarne le esigenze, le caratteristiche della richiesta finanziaria e lo strumento tecnico più adeguato a soddisfare la stessa;

- le decisioni creditizie sono assunte esclusivamente sulla base di criteri oggettivi, trasparenti e verificabili, quali il merito creditizio, la capacità di rimborso, il profilo di rischio, la conformità normativa e le politiche interne vigenti;
- nel caso di affidamenti rivolti ad entità appartenenti a Gruppi, la valutazione del merito creditizio deve tener conto, anche, dell'insieme di relazioni sottostanti al gruppo economico di appartenenza, in funzione delle relative connessioni giuridiche ed economiche;
- l'affidamento avviene attraverso la concessione di linee di credito che, ai fini dell'individuazione dell'Organo deliberante competente, vengono suddivise per tipologia di rischio e ordinate per rischiosità decrescente, raggruppando le operazioni che presentano un grado di rischio analogo;
- la Banca pone la massima attenzione agli operatori economici che, relativamente ai fattori ambientali, sociali e di governo societario dedicano attenzione all'utilizzo responsabile delle risorse naturali e agli effetti sugli ecosistemi, definiscono adeguate condizioni di sicurezza, salute, giustizia, parità e inclusione, generano reddito e lavoro nel rispetto di principi etici e delle migliori prassi di governo delle aziende.

Le fasi principali in cui si articola la concessione del credito consistono in: (i) attività di avvio; analisi istruttoria; (ii) delibera; (iii) perfezionamento del contratto e delle garanzie. A seguito delle suddette fasi si procede all'erogazione del credito concesso:

- l'analisi istruttoria consiste nell'insieme di verifiche, analisi e valutazione in relazione alla solvibilità e profittabilità del cliente. Essa viene effettuata dopo la verifica della bontà del supporto documentale e della corretta identificazione del cliente anche sotto l'aspetto del rischio di riciclaggio;

le linee di credito concesse diventano operative solo ad avvenuto perfezionamento del contratto e delle garanzie. In questa fase, è indispensabile verificare che le garanzie siano rispondenti ai dovuti requisiti di piena validità giuridica e ammissibilità prima dell'attivazione del fido.

Sono altresì previsti i seguenti presidi di controllo:

- verifica del censimento anagrafico del richiedente e degli eventuali garanti e coobbligati e della presenza di eventuali note anagrafiche negative sul richiedente;

- verifica della sottoscrizione dei documenti (dichiarazioni fiscali, bilancio, etc.) da parte del richiedente il fido;
- verifica sulle capacità economico-patrimoniali della controparte richiedente il fido (soggetto privato e Società) e sulle modalità di copertura dei piani finanziari oggetto di valutazione;
- verifica della conformità delle proposte di affidamento rispetto ai criteri qualitativi e di affidabilità stabiliti dal Consiglio di Amministrazione;
- verifica dell'idoneità e della congruità del profilo giuridico del garante (presenza di eventuali conflitti di interesse, carenza di poteri, procedure concorsuali in essere, elevata rischiosità del garante per età avanzata, etc.);
- determinazione dell'Organo competente a deliberare in via automatica, tenuto conto dei limiti alle deleghe di potere per categoria di rischio stabilite dal Consiglio di Amministrazione;
- definizione dei criteri e delle modalità di modifica/rimodulazioni e sospensione del finanziamento;
- monitoraggio delle posizioni creditizie finalizzato ad individuare tempestivamente sintomi di deterioramento e situazioni di criticità, al fine di intraprendere gli opportuni provvedimenti correttivi;
- qualora siano identificate oggettive evidenze di una possibile perdita di valore, riduzione da parte della Banca del valore del credito mediante una svalutazione, tenendo conto di criteri di oggettività e prudenza ed in funzione dei flussi di cassa previsti e della mitigazione del rischio derivante dalle garanzie presenti, imputando la rettifica di valore al conto economico di esercizio. Conformemente alle disposizioni del principio contabile IFRS 9, il modello di valutazione si basa sulla stima delle perdite attese, ovvero perdite relative ad eventi non ancora manifestati alla data di valutazione, ma che possono in futuro manifestarsi;
- gestione proattiva da parte dell'Area Crediti Deteriorati dei crediti classificati come Crediti Scaduti Deteriorati, cercando di normalizzarne il rapporto mediante specifiche azioni e conseguenti piani di risanamento;
- monitoraggio del Piano NPE, dell'andamento del portafoglio UTP e dei piani di rientro, prevedendo tempestivi interventi anche con solleciti formali, attraverso il coinvolgimento dei Preposti di Filiale e dei Capi Area;

- previsioni di flussi informativi tempestivi verso gli Organi Amministrativi (Consiglio di Amministrazione, Direzione Generale, etc.) relativamente all'andamento del credito finanziario;
- corretta registrazione sul sistema informatico della Banca delle attività di controllo effettuate in merito alla gestione del credito finanziato;
- definizione delle modalità e dei criteri posti alla base di eventuali modifiche e/o di rinnovi delle convenzioni stipulate;
- formale rendicontazione, da parte delle Funzioni coinvolte della Banca, nei confronti degli Enti terzi agevolanti in merito all'andamento del finanziamento agevolato o assistito da garanzie pubbliche;
- archiviazione e conservazione da parte della struttura organizzativa interessata e/o i soggetti competenti della documentazione di competenza;
- gestione di tutte le attività attraverso sistemi applicativi dedicati, nei quali sono mantenuti tutti i dettagli delle operazioni effettuate.

1.26. GESTIONE DELLE OPERAZIONI DI MERCATO AI FINI DELLA PREVENZIONE DEGLI ILLECITI PENALI E AMMINISTRATIVI IN TEMA DI ABUSI DI MERCATO

1.26.1. Reati astrattamente ipotizzabili

10) Reati e illeciti amministrativi di abuso di mercato (art. 25-sexies)

- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 del D.Lgs. 24 febbraio 1998, n. 58);
- Manipolazione del mercato (art. 185 D.Lgs.58/1998).

6) Reati societari (art. 25-ter)

- Aggiotaggio (art. 2637 c.c.).

1.26.2. Unità organizzative/funzioni aziendali coinvolte

- Compliance;

- Filiali;
- Affari Societari, Soci e Investor Relations;
- Relazioni Esterne e Attività Istituzionali;
- Area Affari (CCO);
- Area Operativa (COO):
 - Polo Back Office;
- Area Finanza:
 - Tesoreria Banca.

1.26.3. Attività sensibili

- a) Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato;
- b) Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abuso di mercato.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- individuazione e monitoraggio delle informazioni privilegiate;
- comunicazione al pubblico delle informazioni privilegiate.
- acquisizione/vendita/emissione o altre operazioni relative a strumenti finanziari, propri o di terzi, sui mercati regolamentati;
- monitoraggio, istruttoria e segnalazione delle operazioni per le quali si ravvisano possibili sospetti ai fini della disciplina degli abusi di mercato.

1.26.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- assumere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Banca;

- osservare le regole che presiedono alla corretta formazione del prezzo degli strumenti finanziari, evitando comportamenti che ne possano provocare una sensibile alterazione rispetto alla corrente situazione di mercato;
- effettuare con tempestività correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste intraprese
- astenersi dal porre in essere qualsiasi comportamento idoneo a configurare un abuso delle informazioni privilegiate;
- la possibilità di accesso alle specifiche informazioni rilevanti ed alle informazioni privilegiate deve essere circoscritta limitatamente alle persone che vi abbiano necessità di operare e di cui si provvede ad assicurare istantaneamente l'iscrizione nella relativa Lista di Monitoraggio o nel Registro;
- assicurare la corretta contabilizzazione delle operazioni svolte su strumenti finanziari;
- mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei propri compiti e, in particolare, assicurare che la circolazione interna e verso terzi di documenti contenenti informazioni potenzialmente privilegiate sia soggetta ad ogni necessaria attenzione e cautela, onde evitare pregiudizi ed indebite divulgazioni;
- ove applicabile, le condotte elencate ai punti precedenti assumono rilevanza e pertanto sono vietate anche con riferimento a crypto-attività o qualora le attività siano svolte con l'ausilio di sistemi di intelligenza artificiale.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- utilizzare informazioni rilevanti e privilegiate per acquistare, vendere o compiere altre operazioni su strumenti finanziari per conto proprio o per conto di terzi, anche per interposta persona;
- impartire ordini per l'acquisto di, uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere informazioni fuorvianti sullo strumento finanziario in modo da aumentarne il prezzo;
- effettuare operazioni di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interessi (a meno che esso non venga esplicitato nelle

forme previste dalla normativa), allorquando tale operazione non sarebbe stata ragionevolmente effettuata in caso di assenza di conflitto di interessi;

- compiere operazioni od ordini di compravendita che consentano, anche tramite l'azione di concerto di più persone, di fissare il prezzo di mercato di strumenti finanziari ad un livello anomalo o artificiale;
- eseguire operazioni che non determinano alcuna variazione nella proprietà ovvero non comportano alcun trasferimento effettivo della proprietà di uno strumento finanziario;
- porre in essere operazioni simulate o diffondere notizie false sulla Società;
- comunicare informazioni false e di occultare dati e notizie che potrebbero indurre in errore i destinatari di tali comunicazioni;
- proporre opportunità commerciali o di qualsiasi altro genere che possano, anche solo potenzialmente, procurare loro un indebito vantaggio, al fine di ottenere in cambio un favore per la Banca;
- compiere operazioni su strumenti finanziari della Banca e di società terze in rapporto d'affari con la Banca stessa, in relazione alle quali si posseggano informazioni privilegiate circa l'emittente o il titolo stesso conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse; tale divieto si applica a qualsiasi tipo di operazione in strumenti finanziari (ad esempio: azioni, obbligazioni, warrant, covered warrant, opzioni, futures);
- ove applicabile, le condotte elencate ai punti precedenti assumono rilevanza e pertanto sono vietate anche con riferimento a crypto-attività o qualora le attività siano svolte con l'ausilio di sistemi di intelligenza artificiale.

1.26.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- Individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca nell'ambito delle attività sensibili presidiate nel presente Protocollo, in base allo specifico ruolo attribuito loro nella normativa interna, nonché ai sensi del vigente sistema dei poteri e delle deleghe della Banca;

- definizione di specifica normativa interna in relazione ai processi di cui al presente Protocollo;
- identificazione ed accertamento da parte dell'Ufficio Affari Societari, Soci e Investor Relations, sulla base dei criteri deliberati dal CdA, dell'evento/informazione qualificabile come privilegiata, anche avvalendosi dei flussi informativi provenienti da altre strutture "c.d. funzioni organizzative competenti";
- verifica delle misure necessarie a mantenere il carattere privilegiato o riservato delle informazioni durante la loro circolazione interna;
- in caso di identificazione di un soggetto terzo, il quale ha avuto accesso ad informazioni privilegiate, tempestiva comunicazione al soggetto della natura privilegiata dell'informazione;
- esistenza di presidi volti a garantire che la circolazione delle informazioni privilegiate nell'ambito della Banca avvenga nel rispetto della oggettiva necessità di comunicazione in relazione all'attività svolta;
- presenza di un registro delle persone che hanno accesso a informazioni privilegiate/confidenziali relative all'operatività sui mercati finanziari da parte dell'Ufficio Affari Societari Soci e Investor Relations, il quale garantisce:
 - o la riservatezza delle informazioni ivi contenute assicurando che l'accesso all'Insider List sia limitato alle persone chiaramente identificate che devono accedervi per la natura della rispettiva funzione o posizione;
 - o l'esattezza delle informazioni presenti nell'Insider List;
 - o l'accesso e il reperimento delle versioni precedenti dell'Insider List;
 - o la conservazione per cinque anni dopo l'elaborazione o ciascun aggiornamento;
- formalizzazione di specifiche regole per l'identificazione di una informazione quale "privilegiata", formalizzate all'interno di apposita normativa interna e rese disponibili nella intranet aziendale;
- adeguate cautele, tra cui la predisposizione di utenze dedicate, volte a garantire la protezione e custodia del Registro in modo da impedire accessi a soggetti non autorizzati;
- individuazione dei soggetti cui compete il controllo delle informazioni privilegiate da trasmettere all'esterno;

- formale autorizzazione da parte del CdA e del Direttore Generale in merito ai contenuti dei documenti contenenti le informazioni privilegiate della Banca da trasmettere all'esterno;
- definizione di criteri utili ai fini del rilevamento di condotte sospette e di meccanismi idonei alla rilevazione delle stesse;
- analisi e valutazione delle operazioni sospette, anche attraverso l'utilizzo di una procedura informatica per la rilevazione di operazioni anomale. Tale procedura e la connessa conduzione di verifiche sono effettuate dalla Compliance, la quale:
 - o analizza quotidianamente le operazioni estratte automaticamente dalla procedura sulla base di soglie di attenzione preimpostate ed effettua gli approfondimenti al fine di concludere il test del ragionevole sospetto ed attivare, qualora ritenuto opportuno, l'iter segnaletico alla CONSOB;
 - o analizza eventuali segnalazioni provenienti dalle strutture di front e back office interessate dalla negoziazione di strumenti finanziari da parte della clientela;
 - o valuta con periodicità almeno annuale e con l'eventuale supporto dell'Ufficio Organizzazione, la coerenza delle regole, dei parametri e delle soglie impostati nella procedura di detecting rispetto all'operatività della banca e della propria clientela;
- conservazione della documentazione inerente all'analisi effettuata, anche nel caso in cui si è ritenuto di non procedere con la segnalazione all'Autorità;
- formale segnalazione alla Consob delle operazioni che, in base a ragionevoli motivi, possono ritenersi configurare una violazione delle norme sull'abuso di mercato;
- formalizzazione di procedure adeguate al fine di consentire la segnalazione all'interno della Società di eventuali violazioni commesse dai propri dipendenti in contrasto con le disposizioni in materia di abusi di mercato;
- sottoscrizione, da parte di tutti i soggetti censiti all'interno del Registro Insider, di apposita modulistica contenente gli obblighi giuridici e regolamentari, nonché le sanzioni applicabili in caso di abuso di informazioni privilegiate e di comunicazione illecita di tali informazioni;
- monitoraggio, da parte dell'Ufficio Polo Back Office, dei soggetti c.d. "internal dealing" in relazione alla loro operatività in strumenti finanziari emessi dalla Banca. In particolare, fermo restando che l'obbligo segnaletico alla CONSOB grava sui soggetti

c.d. internal dealing che hanno posto in essere operazioni su strumenti finanziari emessi dalla Banca, l'Ufficio Back Office - utilizzando estrazioni giornaliere di dati e notizie appositamente predisposte e messe a disposizione dello stesso – analizza l'eventuale operatività in strumenti finanziari emessi dalla Banca di tali soggetti e provvede a segnalare a mezzo comunicazione interna, nella prima giornata lavorativa utile, l'avvenuto superamento della soglia di 20.000€;

- archiviazione e conservazione della documentazione di competenza da parte della struttura organizzativa interessata e/o dei soggetti competenti;
- gestione delle operazioni di compravendita di strumenti finanziari attraverso sistemi applicativi dedicati, nei quali sono mantenuti tutti i dettagli delle transazioni effettuate.

1.27. GESTIONE DEI RAPPORTI CON LA CLIENTELA - OPERATORE ESTERO

1.27.1. Reati astrattamente ipotizzabili

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Art. 2 Convenzione internazionale per la repressione del finanziamento del terrorismo 9 dicembre 1999.

14) Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25-octies.2)

- Violazione delle misure restrittive dell'Unione Europea (art. 275-bis c.p.);
- Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione Europea (art. 275-ter c.p.);
- Violazione delle condizioni dell'autorizzazione allo svolgimento di attività (art. 275-quater c.p.).

1.27.2. Unità organizzative/funzioni aziendali coinvolte

- Area Crediti (CLO):
 - Amministrazione Crediti:
 - Estero;
- Filiali;
- Aree Territoriali.

1.27.3. Attività sensibili

- a) Operatività con l'estero.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- gestione delle attività di pagamento e incasso dall'estero;
- consegna "documenti esteri" (documenti rappresentativi della merce);
- verifica "documenti esteri" (documenti rappresentativi della merce).

1.27.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- assumere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali;
- assicurarsi che i pagamenti digitali vengano processati tramite l'adozione di procedure di sicurezza e su infrastrutture di comunicazione affidabili;
- operare nel rispetto degli obblighi di legge e assicurare la corretta attuazione delle politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo;

- segnalare tempestivamente ai soggetti competenti ogni circostanza per la quale si conosca, si sospetti, o si abbiano ragionevoli motivi per sospettare che siano state compiute, tentate o siano in corso operazioni di frode e/o falsificazione di mezzi di pagamento diversi dai contanti, riciclaggio, di finanziamento del terrorismo o che i fondi, indipendentemente dalla loro entità, provengano da un'attività criminosa;
- effettuare controlli formali e sostanziali e garantire un costante monitoraggio dei flussi finanziari della Banca, con riferimento ai pagamenti verso terzi, tenendo conto della sede legale della società controparte, degli istituti di credito utilizzati, di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni od operazioni straordinarie;
- è vietato porre in essere, anche indirettamente, operazioni commerciali in violazione di misure restrittive dell'Unione Europea o delle relative disposizioni nazionali di attuazione, ivi incluse, a titolo meramente esemplificativo e non esaustivo, operazioni con stati terzi sottoposti a embargo o verso soggetti inseriti in c.d. blacklist dell'Unione Europea;
- è vietato porre in essere, anche indirettamente, operazioni monetarie o finanziarie in violazione di misure restrittive dell'Unione Europea o delle relative disposizioni nazionali di attuazione, ivi incluso, a titolo meramente esemplificativo e non esaustivo, omettere di adottare misure di congelamento su fondi designati ed incluse operazioni finanziarie con Stati terzi sottoposti ad embargo.

1.27.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- formalizzazione all'interno della normativa della Banca dei soggetti, delle strutture organizzative e degli Organi a cui sono attribuiti specifici ruoli e responsabilità previsti dalla normativa applicabile in materia di contrasto al riciclaggio e al finanziamento del terrorismo nonché in violazione o elusione delle Misure Restrittive;
- screening anagrafico effettuate sia in fase di onboarding sia nel corso del rapporto, consentono di confrontare i nominativi presenti all'interno delle liste dei soggetti designati pubblicate dalle Nazioni Unite, dall'Unione Europea e da altre autorità nazionali (es. OFAC);

- controlli sulle transazioni che riguardano i trasferimenti di fondi effettuati nonché gli eventuali beni e servizi sottostanti agli stessi, volti a verificare che non siano stati violati provvedimenti di embargo o analoghe restrizioni di natura commerciale o finanziaria (ad esempio, divieti o restrizioni all'accesso ai servizi finanziari, agli investimenti o alle transazioni di capitali);
- qualsiasi operazione da o verso Paesi sottoposti a misure restrittive deve essere sottoposta a verifiche preventive idonee a escludere qualsiasi rischio di violazione dei regimi sanzionatori internazionali; tali verifiche ricomprendono la natura e finalità dell'operazione, i beni/ servizi coinvolti, le rotte commerciali, le controparti coinvolte e la documentazione di supporto;
- la Banca applica rigorosamente le misure di congelamento dei fondi e delle risorse economiche detenuti o controllati da soggetti designati, ossia persone fisiche, giuridiche, Enti o organismi inclusi nelle liste sanzionatorie emanate da Autorità sovranazionali, europee o nazionali (es. ONU e UE);
- verifica della presenza di eventuali note anagrafiche negative sul richiedente/ricevente del pagamento estero;
- verifica della presenza del cliente richiedente/ricevente all'interno delle blacklist;
- verifica del corretto svolgimento delle operazioni di incasso e pagamento da e verso l'estero;
- verifica del rispetto della normativa vigente antiriciclaggio nell'ambito delle operazioni da e verso l'estero;
- verifica della sottoscrizione dei documenti necessari all'espletamento della pratica (modello di richiesta del pagamento estero);
- verifica della completezza della documentazione allegata ad ogni singola operazione da e verso l'estero;
- verifica della conformità della documentazione rappresentativa della merce emessa con la lettera di credito ricevuta;
- verifica della conformità della documentazione rappresentativa della merce ricevuta con la lettera di credito emessa;
- approvazione delle attività istruttorie ai fini dell'accettazione e dell'effettuazione del pagamento dall'estero;

- utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni;
- al fine di consentire l'agevole ricostruzione delle responsabilità e l'adeguata tracciatura delle motivazioni alla base delle decisioni assunte, conservazione, anche in modalità elettronica, della documentazione riguardante tutte le pratiche di pagamento e regolamento internazionale da parte delle strutture aziendali.

1.28. GESTIONE DEGLI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E DELLE PIATTAFORME DI PAGAMENTO IN USO

1.28.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648 - ter 1 c.p.).

13) Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1)

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.);
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.);

- Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.);
- Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1, comma 2).

14) Reati in materia di violazione di misure restrittive dell'Unione Europea (art. 25-octies.2)

- Violazione delle misure restrittive dell'Unione europea (art. 275-bis c.p.);
- Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione Europea (art. 275-ter c.p.);
- Violazione delle condizioni dell'autorizzazione allo svolgimento di attività (art. 275-quater c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

1.28.2. Unità organizzative/funzioni aziendali coinvolte

- Area Operativa (COO):
 - Sistemi e Tecnologie;
 - Sicurezza Informatica;
 - Polo Back Office;
 - Cassa Centrale;
- Area Affari (CCO):
 - Sviluppo e Gestione /PMI/SB;
 - Sviluppo e Gestione Privati
 -
 - Marketing, Prodotti e Trasparenza;
 - Sviluppo e Gestione Corporate/ Istituzionali;
- Filiali.

1.28.3. Attività sensibili

- a) Gestione delle attività connesse ai sistemi informatici, applicazioni e servizi di monetica, aziendali e/o forniti da soggetti esterni nell'ambito dei servizi di pagamento elettronico.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- gestione e monitoraggio di carte di pagamento, servizi di incasso e pagamento e di servizi di banca virtuale;
- gestione e monitoraggio dei conti correnti;
- monitoraggio delle attività connesse ai sistemi informatici, applicazioni e servizi di monetica, aziendali e/o forniti da partner esterni nell'ambito dei servizi di pagamento elettronico;
- gestione delle attività amministrative e contabili relative agli assegni, agli effetti (cartacei ed elettronici), ai flussi relativi ai servizi telematici (CBI, Remote Banking, HomeBanking) e ai bonifici;
- gestione delle convenzioni e offerta di modalità di pagamento tramite piattaforme di pagamenti online (es. Satispay, MyBank, XPay, PayByLink, PagoPA, etc.);

1.28.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- assumere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali;
- in caso di immissione nel circuito economico di strumenti di pagamento diversi dal contante evidentemente falsificati e/o alterati, o anche semplicemente sospetti di falsità, darne comunicazione alle Autorità competenti;
- assicurarsi che i pagamenti digitali vengano processati tramite l'adozione di procedure di sicurezza e su infrastrutture di comunicazione affidabili;
- operare nel rispetto degli obblighi di legge e assicurare la corretta attuazione delle politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo;

- segnalare tempestivamente ai soggetti competenti ogni circostanza per la quale si conosca, si sospetti, o si abbiano ragionevoli motivi per sospettare che siano state compiute, tentate o siano in corso operazioni di frode e/o falsificazione di mezzi di pagamento diversi dai contanti, riciclaggio, di finanziamento del terrorismo o che i fondi, indipendentemente dalla loro entità, provengano da un'attività criminosa;
- effettuare controlli formali e sostanziali e garantire un costante monitoraggio dei flussi finanziari della Banca, con riferimento ai pagamenti verso terzi, tenendo conto della sede legale della società controparte, degli istituti di credito utilizzati, di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni od operazioni straordinarie;
- verificare che le operazioni che comportano l'utilizzo o l'impiego di risorse economiche o finanziarie debbano avere una causale espressa e siano documentate e registrate in conformità ai principi di correttezza e trasparenza contabile;
- garantire che gli incassi e i pagamenti della Società nonché i flussi di denaro siano sempre tracciabili e provabili documentalmente;
- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta dalla Banca e per le specifiche finalità assegnate;
- rispettare le procedure e gli standard previsti in materia di utilizzazione delle risorse informatiche, segnalando senza ritardo alle Funzioni competenti eventuali utilizzi e/o funzionamenti anomali di queste ultime;
- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- realizzare ogni forma di frode e di falsificazione dei mezzi di pagamento anche diversi dai contanti che possano costituire una minaccia alla sicurezza ovvero favorire forme di finanziamento per la criminalità organizzata e rendere possibili altre forme criminali;
- utilizzare, al fine di trarne profitto, per sé o per altri, indebitamente e non essendone titolare carte di credito o qualsiasi altro strumento di pagamento che abiliti al prelievo di denaro contante o all'acquisto di beni e/o prestazione di servizi;

- utilizzare in modo fraudolento, consapevole e senza diritto uno strumento di pagamento diversi dai contanti illecitamente ottenuto ovvero oggetto di illecita appropriazione;
- falsificare o alterare gli strumenti di pagamento diversi dai contanti, ovvero possedere, cedere o acquisire tali strumenti o documenti di provenienza illecita, o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi;
- acquisire in maniera fraudolenta i codici segreti della clientela;
- aprire conti correnti in forma anonima o con intestazione fittizia, nonché creare e/o utilizzare strumenti di pagamento con tali caratteristiche, al fine di ottenere, dall'utilizzo e gestione degli stessi, un indebito vantaggio;
- immettere nella rete internet, dati ricognitivi e/o operativi di una carta di credito intestata ad un terzo (o di altro strumento di pagamento diverso dal contante), acquisiti fraudolentemente, al fine di effettuare transazioni economiche a vantaggio e/o nell'interesse della Società;
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti, al fine di ottenere un indebito vantaggio procurando un altrui danno qualora il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, trojan, spyware, dialer, etc.) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- accedere abusivamente ad un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti, al fine di alterare/manipolare e trasmettere dei dati non veritieri alle Autorità di Vigilanza;
- accedere abusivamente, direttamente o per interposta persona, ad un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate o di utilizzare indebitamente, falsificare o alterare strumenti di pagamento diversi dai contanti;
- detenere, produrre e/o diffondere apparecchiature/programmi informatici in grado di realizzare un indebito utilizzo di strumenti di pagamento diversi dal contante della

clientela (es. manomissione POS/ATM, piattaforma home banking), al fine di ottenere vantaggi per la Banca;

- porre in essere, anche indirettamente, operazioni commerciali in violazione di misure restrittive dell'Unione Europea o delle relative disposizioni nazionali di attuazione, ivi incluse, a titolo meramente esemplificativo e non esaustivo, operazioni con stati terzi sottoposti a embargo o verso soggetti inseriti in c.d. blacklist dell'Unione Europea;
- porre in essere, anche indirettamente, operazioni monetarie o finanziarie in violazione di misure restrittive dell'Unione Europea o delle relative disposizioni nazionali di attuazione, ivi incluso, a titolo meramente esemplificativo e non esaustivo, omettere di adottare misure di congelamento su fondi designati ed incluse operazioni finanziarie con Stati terzi sottoposti ad embargo.

-

1.28.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- approvazione e sottoscrizione degli atti che impegnano contrattualmente la Banca ed eventuali variazioni ai relativi termini e condizioni esclusivamente da soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- formalizzazione all'interno della normativa della Banca dei soggetti e delle strutture organizzative a cui sono attribuiti specifici ruoli e responsabilità previsti dalla normativa applicabile nell'ambito del presente Protocollo;
- accesso ai dati ed alle applicazioni aziendali limitato esclusivamente al personale autorizzato. I permessi sono assegnati secondo procedura debitamente formalizzata e viene periodicamente verificata la coerenza sia tramite sistemi automatici, sia attraverso il coinvolgimento dei responsabili degli utenti;
- presenza di un sistema di sicurezza informatico e applicativo sui servizi di incasso e pagamento elettronico nell'ambito dei rapporti con le controparti, con specifico riferimento alla gestione dei prodotti e servizi bancari offerti alla clientela in grado sia di garantire un'operatività coerente con la volontà dei titolari dei rapporti che di prevenire condotte di natura fraudolenta;

- controlli di linea sulle disposizioni di pagamento gestite per conto della clientela;
- previsione da parte della società emittente le carte di presidi di controllo nel continuo per il corretto utilizzo delle carte, in grado di evidenziare operatività anomala tali da consentire il blocco operativo della carta;
- controlli di linea assegnati alle strutture organizzative della Banca relativamente alla gestione dei pagamenti (e dei relativi regolamenti) eseguiti con corrispondenti estere;
- controlli sulle transazioni riguardano tutti i trasferimenti di fondi effettuati dalla clientela e gli eventuali beni e servizi sottostanti agli stessi, per verificare che non siano stati violati provvedimenti di embargo o analoghe restrizioni di natura commerciale (ad esempio, divieti o limitazioni all'import/export di merci, beni e tecnologie a duplice uso) o finanziaria (ad esempio, divieti o restrizioni all'accesso ai servizi finanziari, agli investimenti o alle transazioni di capitali);
- verifica del corretto inserimento del cliente in anagrafica;
- adeguata verifica della clientela attraverso l'identificazione del titolare effettivo;
- verifica del merito creditizio del cliente al fine di determinare il plafond della carta di pagamento richiesto;
- esecuzione dell'Adeguata Verifica nei confronti del cliente/esercente richiedente il servizio di pagamento e/o il conferimento di strumenti POS, attraverso compilazione del questionario KYC;
- aggiornamento periodico delle informazioni relative ai rapporti intrattenuti con la clientela al fine di consentire una costante valutazione del profilo economico e finanziario della stessa;
- formalizzazione di specifiche regole per l'emissione e la compilazione di assegni bonifici, le quali prevedono la corretta identificazione del cliente ordinante e il reperimento dei dati anagrafici, sia dell'ordinante che del beneficiario;
- adozione di meccanismi tecnici e/o organizzativi, a presidio dei principali rischi operativi/IT, nonché costante aggiornamento della normativa interna disciplinante l'operatività inerente ai sistemi di pagamento dalla stessa offerti;
- previsione formale di restrizioni/blocchi delle operazioni relative alle carte di credito e/o conti correnti per i quali sussista il sospetto di una relazione con il riciclaggio o con il finanziamento del terrorismo;

- monitoraggio delle eventuali operazioni anomale relative alle operazioni effettuate con le carte di credito e di debito da parte dei clienti;
- presenza di apposita normativa interna che formalizza gli adempimenti da porre in essere, in capo a ciascuna Filiale, nel caso di frode/duplicazioni di carte e altri strumenti di pagamento, nonché specifico controllo sulla movimentazione del conto corrente collegato alla Carta di Debito per accertare eventuali utilizzi non riconosciuti (blocco carte, segnalazioni alle autorità, etc.).
- esecuzione, da parte dell'Ufficio Anagrafe e Segnalazioni di Vigilanza, con il supporto del Polo Back Office, di segnalazioni semestrali nei confronti di Banca d'Italia in materia di "Fraud Reporting;
- adozione di un sistema antifrode evoluto che, agendo a livello transazionale, analizza l'operatività dell'utente sulla base di dati storici;
- formazione del personale della Banca sul tema della cybersecurity al fine di aumentare la consapevolezza sui rischi di attacchi informatici che si possono realizzare tramite phishing, smishing e ransomware;
- verifiche periodiche da parte dell'Area Operativa in merito ai KPI e ai livelli di servizio dell'outsourcer informatico responsabile della gestione dei Servizi di Pagamento prestati via internet e del trattamento dei dati sensibili inerenti alle operazioni di pagamento effettuate tramite tale canale;
- esecuzione di un assessment annuale sui rischi operativi e di sicurezza relativi ai servizi di pagamento;
- presenza di specifici blocchi che limitano l'operatività fraudolenta nel caso di operatività sospetta proveniente da Paesi a Rischio AML/circuiti inattendibili/categorie commerciali/codice esercente;
- presenza di specifiche clausole 231 all'interno dei contratti con outsourcer e partner commerciali in merito al rispetto delle regole definite nel Modello, nonché al rispetto delle misure di sicurezza per l'erogazione di servizi di pagamento;
- presenza di controlli sulla presenza di assegni versati negli ATM remoti/comunicazioni alle filiali delle eventuali giacenze da confermare tramite CIT/verifica eventuali irregolarità dei titoli per ritiro urgente tramite vigilanza ed avvio azioni di back up;
- esecuzioni di controllo delle operazioni di prelievo sospette e/o fraudolente effettuate tramite gli ATM;

- corretta archiviazione delle immagini relative ad assegni, nonché invio delle stesse a provider terzi o autorità su richiesta;
- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, archiviazione e conservazione da parte della Funzione di volta in volta interessata di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo descritto;
- utilizzo di sistemi e strumenti informatici a supporto dell'operatività che garantiscano la registrazione e l'archiviazione dei dati e delle informazioni acquisite nell'ambito del processo descritto.

1.29. GESTIONE DEL PATRIMONIO CULTURALE DELLA BANCA

1.29.1. Reati astrattamente ipotizzabili

24) Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevices)

- Riciclaggio di beni culturali (art. 518-sexies c.p.);
- Devastazione e saccheggio di beni culturali e paesaggistici (art. 518-terdecies c.p.).

23) Delitti contro il patrimonio culturale (art. 25-septiesdecies)

- Furto di beni culturali (art. 518-bis c.p.);
- Appropriazione indebita di beni culturali (art. 518-ter c.p.);
- Ricettazione di beni culturali (art. 518-quater c.p.);
- Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.);
- Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.);
- Importazione illecita di beni culturali (art. 518-decies c.p.);
- Uscita o esportazione illecite di beni culturali (art. 518-undecies c.p.);
- Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies c.p.);
- Contraffazione di opere d'arte (art. 518-quaterdecies c.p.).

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);

- Traffico di influenze illecite (art. 346-bis).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648-ter.1 c.p.).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

1.29.2. Unità organizzative/funzioni aziendali coinvolte

- Relazioni Esterne ed Attività Istituzionali.

1.29.3. Attività sensibili

- a) Gestione del patrimonio artistico della Banca.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- attività amministrative e commerciali legate al patrimonio artistico (e.g. prestito a titolo gratuito);
- attività di restauro e conservazione legate al patrimonio artistico.

1.29.4. *Principi generali di comportamento*

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- verificare la documentazione attestante l'autenticità o la probabile attribuzione del bene culturale;
- verificare la documentazione attestante la lecita provenienza del bene, o in mancanza, una dichiarazione contenente tutte le informazioni disponibili;
- verificare la completezza e la corretta compilazione di tutta la documentazione di supporto al trasferimento del bene;
- ottemperare alle prescrizioni della Soprintendenza competente per territorio relative alle modalità di conservazione o di custodia dei beni culturali;
- in ipotesi di trasferimento/movimentazione dei beni culturali, attenersi durante il trasporto alle prescrizioni impartite dalla Soprintendenza competente per territorio;
- custodire e gestire i beni culturali, con la massima cura e scrupolo oltre che nel rispetto delle prescrizioni impartite dalle Autorità competenti, al fine di garantirne la conservazione e la trasmissibilità alle generazioni future;
- con riferimento ai beni dichiarati di interesse culturale, ottenere l'autorizzazione al prestito dalla Soprintendenza di spettanza, presentando la denuncia di trasferimento della detenzione di tali beni alla entro il termine previsto dalla normativa vigente;
- curare, con riferimento ai beni dichiarati di interesse culturale, le attività di autorizzazione alla movimentazione del bene dalla Soprintendenza di spettanza.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- distruggere, deturpare, danneggiare, disperdere qualsiasi bene culturale o paesaggistico o comunque renderlo in tutto o in parte inservibile o non fruibile;
- utilizzare un bene culturale in modo non compatibile con il relativo carattere storico-artistico o in pregiudizio della relativa conservazione o integrità.

1.29.5. *Controlli preventivi*

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione delle competenti strutture della Banca deputate alla gestione del patrimonio artistico dichiarati di interesse culturale nonché deputate al mantenimento dei contatti istituzionali (e.g. Soprintendenze, Musei, Fondazioni);
- approvazione e sottoscrizione degli atti che impegnano contrattualmente la Banca e di eventuali variazioni ai relativi termini e condizioni esclusivamente da parte di soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- verifica dell'ottenimento delle autorizzazioni previste dalle Autorità competenti prima di procedere ad interventi sui beni soggetti a vincoli culturali;
- verifica per tutti i beni del patrimonio culturale oggetto di acquisizione dell'esistenza di: (i) una perizia redatta da un esperto indipendente attestante la legittima provenienza e l'autenticità dei beni mobili culturali o della dichiarazione della Sovrintendenza archivistica e bibliografica attestante l'interesse storico particolarmente importante dei beni archivistici; (ii) una perizia per i beni immobili tutelati con l'indicazione dei vincoli diretti;
- verifica al momento della cessione, anche a titolo non oneroso, ovvero della donazione dei beni del patrimonio culturale della Banca, dell'esistenza della perizia o della dichiarazione della Sovrintendenza archivistica e bibliografica di cui al punto precedente, dell'ottenimento delle autorizzazioni previste, del corretto espletamento delle denunce alle Autorità competenti e del rispetto dei termini di prelazione a favore del Ministero o, nel caso della Regione o di altro Ente pubblico territoriale interessato;
- verifica, in caso di trasferimento all'estero di beni mobili appartenenti al patrimonio culturale della Banca, dell'esistenza attestato di libera circolazione o licenza di esportazione;
- ogni atto dispositivo (compravendite, prestiti, cessioni anche a titolo non oneroso, donazioni) è formalizzato in un documento, debitamente firmato/approvato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
- per i beni eventualmente destinati a iniziative con finalità sociali e/o culturali oggetto di comodato, locazione, vendita o altre operazioni immobiliari, svolgimento di attività di due diligence del beneficiario finalizzata ad analizzare (i) il tipo di Ente e la finalità

per la quale è costituito; (ii) l'affidabilità e la reputazione dell'Ente, con particolare attenzione ai precedenti e/o alle imputazioni penali.

1.30. GESTIONE DEL PATRIMONIO IMMOBILIARE DELLA BANCA

1.30.1. Reati astrattamente ipotizzabili

1) Reati contro la Pubblica Amministrazione (artt. 24-25)

- Corruzione e istigazione alla corruzione (artt. 318, 319, 319-bis, 319-quater, 320, 321, 322 e 322-bis c.p.);
- Traffico di influenze illecite (art. 346-bis).

6) Reati societari (art. 25-ter)

- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635 bis c.c.).

12) Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-octies)

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648-ter.1 c.p.).

7) Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater)

- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (artt. 270-bis ss. c.p.);
- Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.);
- Finanziamento al terrorismo (art. 2 Convenzione internazionale di New York per la repressione del finanziamento al terrorismo, 9 dicembre 1999).

21) Reati tributari (art. 25-quinquiesdecies)

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000);
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000);
- Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000);
- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000);
- Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000).

1.30.2. Unità organizzative/funzioni aziendali coinvolte

- Archivio e Logistica.

1.30.3. Attività sensibili

- a) Gestione del patrimonio immobiliare della Banca.

Con riferimento all'attività sensibile in esame, sono stati individuati i seguenti ambiti:

- acquisizione e vendita degli immobili;
- gestione contratti locazione/comodato;
- gestione e amministrazione degli immobili e degli impianti
- progettazione, manutenzione ed esecuzione lavori;
- richieste di utilizzo – a titolo gratuito - delle sale e degli spazi di proprietà per incontri pubblici, convegni e seminari.

1.30.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- non promettere o concedere beni immobili a condizioni diverse da quelle di mercato, fatti salvi i casi di concessione di beni destinati a iniziative con finalità sociali e/o culturali; non promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di

cortesie di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a soggetti della Pubblica Amministrazione ovvero a esponenti apicali e/o persone a loro subordinate di società aventi natura privatistica con la finalità di promuovere o favorire interessi della Banca;

- non affidare incarichi a consulenti/professionisti esterni eludendo criteri documentabili e obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza;
- preventivamente alla stipula di contratti di locazione/vendita relativi agli immobili di proprietà della Banca, le offerte pervenute dai potenziali locatari/acquirenti devono essere verificate, sulla base di parametri economici, potenziale locatario/acquirente, condizioni di locazione/vendita;
- preventivamente alla stipula di contratti di locazione/vendita relativi agli immobili di proprietà della Società, effettuare un'attività di due diligence sulla controparte (compratore/locatario) con particolare riguardo a quanto stabilito dalle;
- curare, con riferimento ai beni culturali immobili, le attività di autorizzazione alla cessione/manutenzione del bene dalla Soprintendenza di spettanza;
- sugli edifici e nelle aree tutelati come beni culturali o paesaggistici, è vietata l'affissione di cartelli o altri mezzi di pubblicità che possono danneggiare l'aspetto, il decoro o la pubblica fruizione di detti immobili.

1.30.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- approvazione e sottoscrizione degli atti che impegnano la Banca da parte di soggetti appositamente autorizzati ai sensi del vigente sistema dei poteri e delle deleghe;
- formalizzazione di ogni atto dispositivo (compravendite, locazioni, prestiti, cessioni anche a titolo non oneroso, donazioni e comodati) in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;
- verifica della correttezza e della completezza dei dati presenti in fattura al fine di accertarne la coerenza con i contratti di locazione attiva;

- verifica degli importi da liquidare (rispetto a quanto definito contrattualmente e al servizio/bene ricevuto) prima di procedere all'autorizzazione del pagamento di fatture passive nell'ambito delle attività connesse alla gestione del patrimonio immobiliare e culturale della Banca;
- verifica della congruità del prezzo di compravendita degli immobili anche attraverso l'acquisizione di perizie redatte da esperti indipendenti;
- per i beni eventualmente destinati a iniziative con finalità sociali e/o culturali oggetto di comodato, locazione, vendita o altre operazioni immobiliari, svolgimento di attività di due diligence del beneficiario finalizzata ad analizzare (i) il tipo di Ente e la finalità per la quale è costituito; (ii) l'affidabilità e la reputazione dell'Ente, con particolare attenzione ai precedenti e/o alle imputazioni penali;
- esecuzione di opere e lavori di qualunque genere su beni culturali, e/o a qualsivoglia intervento in materia di edilizia solo in forza delle autorizzazioni previste dalla normativa esterna di riferimento;
- esecuzione di adeguata verifica della società esecutrice dei lavori in materia di edilizia sui beni culturali, tenendo conto, in particolare, della natura giuridica, della prevalente attività svolta, della struttura organizzativa, nonché del possesso dei mezzi necessari a garantire la tutela, la sicurezza e la conservazione dei beni culturali nel corso delle opere.

1.31. GESTIONE DEI RAPPORTI CON INTERLOCUTORI TERZI - PUBBLICI O PRIVATI - NELLO SVOLGIMENTO DELLE PROPRIE ATTIVITÀ LAVORATIVE PER CONTO E/O NELL'INTERESSE DELLA BANCA

1.31.1. Reati astrattamente ipotizzabili

3) Delitti di criminalità organizzata (art. 24-ter)

- Associazione per delinquere (art. 416 c.p.);
- Associazione a delinquere di stampo mafioso anche straniera (art. 416 bis c.p.);
- Scambio elettorale politico-mafioso (art. 416 ter c.p.).

26) Reati transnazionali (art. 10 L. 146/2006)

- Associazione per delinquere (art. 416 c.p.);

- Associazione a delinquere di stampo mafioso anche straniero (art. 416 bis c.p.);
- Favoreggiamento personale (art. 378 c.p.).

1.31.2. Unità organizzative/funzioni aziendali coinvolte

- Tutte le Unità Organizzative/Funzioni aziendali.

1.31.3. Attività sensibili

Le analisi condotte hanno identificato le attività aziendali della Banca nell'ambito della quale si potrebbe configurare la commissione dei delitti di criminalità organizzata di cui all'art. 24-ter del D. Lgs. 231/2001. Sono da considerare sensibili potenzialmente tutti i processi quando il reato preveda il coinvolgimento di tre o più persone e, a tal proposito, la fattispecie di associazione a delinquere deve essere considerata come aggravante di un reato presupposto.

In particolare, è stata individuata la seguente attività sensibile, applicabile a tutte le strutture della Banca nonché a tutti i processi considerati sensibili ai sensi del D. Lgs. 231/2001:

- a) Gestione dei rapporti con interlocutori terzi - pubblici o privati - nello svolgimento delle proprie attività lavorative per conto e/o nell'interesse della Banca.

1.31.4. Principi generali di comportamento

I Destinatari del Modello coinvolti nelle attività sensibili individuate, sono tenuti al rispetto dei seguenti principi generali di condotta:

- tenere un comportamento corretto, trasparente e collaborativo conformemente ai principi stabiliti dalle norme di legge e dalle procedure aziendali interne;
- osservare rigorosamente le norme poste dalla legge a tutela del diritto – costituzionalmente garantito - ad associarsi per scopi e fini che non siano vietati ai singoli dalla legge penale;
- garantire che l'iniziativa economica non si svolga in contrasto con l'utilità sociale e, quindi, l'ordine pubblico;
- assicurare il regolare funzionamento della Banca e degli Organi sociali, garantendo ed agevolando ogni forma di controllo interno sulle attività societarie che possano essere

strumentali all'attuazione di comportamenti o condotte non conformi ai principi normativi sopra richiamati;

- non ostacolare in alcun modo lo svolgimento di eventuali indagini e iniziative da parte degli Organi sociali, o più in generale da qualsiasi Organo/Autorità/Ente ispettivo, finalizzate a rilevare e combattere condotte illecite in relazione all'ipotesi dei reati associativi considerati.

In particolare, è fatto divieto di porre in essere comportamenti (o concorrere alla realizzazione di condotte) che possano rientrare nelle fattispecie di cui ai reati sopra indicati, tra i quali si citano in via esemplificativa:

- promuovere, costituire, organizzare ovvero partecipare ad associazioni di tre o più soggetti con lo scopo di commettere uno o più delitti o, più in generale, tenere condotte direttamente o indirettamente vietate dalla legge penale;
- implementare e svolgere qualsivoglia iniziativa economica che, nella forma associativa e con le modalità di cui sopra, si ponga in contrasto con l'utilità sociale, recando danno alla sicurezza e alla libertà altrui, con conseguente violazione dell'ordine economico e dell'ordine pubblico;
- attuare – anche strumentalizzando attività riconducibili alla comune gestione societaria – condotte che si concretino in un'attiva e stabile partecipazione all'associazione illecita;
- contribuire – anche attraverso il proprio assetto organizzativo – a creare e garantire nel tempo una struttura organizzativa che, seppur minima, sia comunque idonea e adeguata alla realizzazione di obiettivi delittuosi nell'interesse dell'associazione illecita;
- predisporre - ovvero contribuire a predisporre – i mezzi attraverso i quali supportare l'operatività della associazione illecita;
- promuovere o comunque proporre, la realizzazione di obiettivi delittuosi di volta in volta individuati come utili o necessari nell'ottica del conseguimento di un vantaggio per la Banca.

1.31.5. Controlli preventivi

Ad integrazione delle regole comportamentali di carattere generale, gli ulteriori presidi di controllo operativi stabiliti dalla Banca sono:

- individuazione e autorizzazione dei soggetti che esercitano poteri autorizzativi e/o negoziali e aventi facoltà di rappresentare la Banca, in base allo specifico ruolo attribuito loro dalla normativa interna della Banca, nonché ai sensi del vigente sistema dei poteri e delle deleghe;
- gestione dei rapporti con i rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza, Organi di Polizia, Autorità giudiziaria in genere attribuita ai soggetti appositamente incaricati ai sensi del sistema dei poteri e delle deleghe della Banca;
- in caso di accertamenti e ispezioni in materia fiscale, assistenziale o previdenziale ovvero di ispezioni condotte direttamente presso la Banca dai competenti Enti o Autorità, previsto il presidio da parte delle strutture organizzative competenti per materia, le quali si coordinano con tutti gli altri soggetti, strutture e Organi aziendali interessati;
- definizione di un sistema dei poteri e delle deleghe che stabilisca le autonomie gestionali per natura di spese ed impegni, nei confronti della clientela;
- gestione dei rapporti con la clientela in esecuzione degli impegni di natura contrattuale assunti demandata organizzativamente a specifiche strutture della Banca che si occupano della erogazione dei prodotti/servizi oggetto del contratto, diverse da quelle di stipula del contratto medesimo;
- relativamente al processo del credito, segregazione tra i soggetti incaricati della fase istruttoria rispetto a quelli preposti alla delibera del finanziamento;
- svolgimento delle attività in modo da garantire la veridicità, completezza, congruità e tempestività nella predisposizione di dati e informazioni a supporto degli adempimenti. In particolare, laddove questi comportino l'elaborazione di dati è effettuato un controllo sulla correttezza delle elaborazioni stesse da parte di soggetti diversi da quelli che le hanno effettuate;
- adempimenti di adeguata verifica delle controparti e profilatura del rischio, posti in essere, secondo le previsioni contenute nella normativa interna, a cura di strutture differenti a seconda della specifica operatività;
- stipula da parte della Banca di contratti con i fornitori condotta in conformità con la normativa vigente e con i principi, i criteri e le disposizioni di cui alle procedure aziendali;

- corretta conservazione ed archiviazione da parte di ogni struttura referente della documentazione di pertinenza, con modalità idonee a osservare le misure di sicurezza per la protezione delle informazioni ed assicurare l'unicità del fascicolo per il finanziamento verso la clientela;
- formalizzazione di ogni accordo con le controparti in un documento, debitamente sottoscritto dalle stesse e dai soggetti della Banca muniti di idonei poteri secondo il sistema dei poteri e delle deleghe in essere ed archiviato a cura della competente struttura organizzativa;
- esecuzione degli adempimenti mediante l'utilizzo di sistemi informatici di supporto che tracciano tutte le informazioni elaborate.

Poiché i delitti di criminalità organizzata possono essere finalizzati anche alla commissione dei reati già analizzati nelle singole Parti Speciali, si ritiene opportuno specificare che l'attività a rischio sopra menzionata deve intendersi integrata con le altre specificatamente individuate in relazione a ciascuna fattispecie oggetto di trattazione all'interno dei Protocolli di cui al presente Modello.