MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI

ROSSI S.P.A.

AI SENSI DEL DECRETO LEGISLATIVO N. 231/2001

"RESPONSABILITÀ AMMINISTRATIVA DELLA SOCIETÀ"

PARTE SPECIALE C

REATI INFORMATICI

Approvato dal Consiglio di Amministrazione della Rossi S.p.A. in data 19/01/2022

INDICE

1. PREMESSA

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D. Lgs. 231/2001 è collegato il regime di responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

L'art. 24-bis del D. Lgs. 231/2001 dispone:

"*1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.*

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, e dei delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105, si applica all'ente la sanzione pecuniaria sino a quattrocento quote (2) .

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)".

2. REATI APPLICABILI

In base all'analisi dei rischi effettuata, tra i reati richiamati dall'art. 24-bis del D. Lgs. 231/2001 sono risultati potenzialmente realizzabili nel contesto aziendale di ROSSI le seguenti fattispecie:

FATTISPECIE DI REATO	DESCRIZIONE FATTISPECIE
Documenti informatici (art. 491-bis c.p.)	Costituito dalle ipotesi di falsità, materiale o ideologica, commesse su atti pubblici, certificati, autorizzazioni, scritture private o atti privati, da parte di un rappresentante della Pubblica Amministrazione ovvero da un privato, qualora le stesse abbiano ad oggetto un "*documento informatico pubblico avente efficacia probatoria*", ossia un documento informatico munito quanto meno di firma elettronica semplice. Per "*documento informatico*" si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (tale delitto estende la penale perseguibilità dei reati previsti all'interno del Libro II, Titolo VII, Capo III del Codice Penale).
Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)	Costituito dalla condotta di chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo. La norma prevede un aumento della pena nei casi (i) di uso di violenza sulle cose o alle persone, (ii) in cui dal fatto derivi la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. *In via esemplificativa*, potrà rispondere del reato in esame la Società che, reperiti abusivamente i codici di accesso al sistema informatico di un competitor, si introduca nello stesso, al fine di consultare e asportare i dati aziendali ivi registrati, ovvero di distruggere le informazioni e i dati contenuti.
Detenzione e diffusione abusiva di codici di accesso a sistemi informativi o telematici (art. 615-quater c.p.)	Costituito dalla condotta di chi, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si

	procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo. *In via esemplificativa*, potrà rispondere del reato in esame la Società che, al fine di trarre un profitto, reperisca in modo abusivo i codici di accesso al sistema informatico di un competitor o di un Ente Certificatore.
Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615- quinquies c.p.)	Costituito dalla condotta di chi, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o a esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna, o, comunque, mette a disposizione di altri, apparecchiature, dispositivi o programmi informatici. *In via esemplificativa*, potrà rispondere del reato in esame la Società che, volendo danneggiare il sistema informatico dei competitor, diffonda programmi malevoli (c.d. virus informatici).
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)	Costituito dalla condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe. Risponde del medesimo reato chi rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni. *In via esemplificativa*, potrà rispondere del reato in esame la Società che, mediante un programma appositamente inserito nel sistema, intercetta le comunicazioni di posta elettronica in entrata e in uscita dalle caselle di posta dei propri dipendenti.

Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)	Costituito dalla condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico, ovvero intercorrenti fra più sistemi. *In via esemplificativa*, potrà rispondere del reato in esame la Società che installi apparecchiature capaci di copiare i codici di accesso degli utenti (ad esempio i commerciali di un competitor) di un sistema informatico.
Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)	Costituito dalla condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato. *In via esemplificativa*, potrà rispondere del reato in esame la Società che cancelli un numero significativo di file contenenti dati aziendali da un *device* di proprietà di un terzo soggetto (un competitor o una controparte in un contenzioso).
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.)	Costituito dalla condotta di chi commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, salvo che il fatto non costituisca più grave reato.
Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)	Costituito dalla condotta di chi, mediante le condotte di cui al 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento, salvo che il fatto costituisca più grave reato. *In via esemplificativa*, potrà rispondere del reato in esame la Società che distrugge il sistema informatico di un terzo soggetto (competitor o controparte in un contenzioso).
Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)	Costituito dalla condotta descritta al precedente articolo 635-quater, qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o

	telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

3. SCOPO E AMBITO DI APPLICAZIONE

In questa Parte Speciale sono individuati i principi di riferimento per la costruzione del Modello, specificamente previsti in relazione ai Processi e alle Attività Sensibili individuati al fine di prevenire la commissione dei reati informatici.

La presente Parte Speciale si riferisce a comportamenti posti in essere:

- dagli organi sociali,
- dai dipendenti,
- dai consulenti,
- da tutti coloro che svolgono un'attività per conto di Rossi S.p.A., come meglio definiti nella Parte Generale, coinvolti nelle Attività Sensibili individuate.

L'obiettivo perseguito è quello di garantire che i soggetti sopra individuati mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati sopra indicati.

4. ATTIVITA' SENSIBILI

L'art. 6, comma 2, lett. a) del D. Lgs. 231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette "Attività Sensibili", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D. Lgs. 231/2001.

L'analisi dei processi aziendali della Società ha consentito di individuare processi e attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24-bis del D. Lgs. 231/2001:

PROCESSO	ATTIVITA' SENSIBILI	DESCRIZIONE DELLE ATTIVITA' SENSIBILI
GESTIONE DEL SISTEMA INFORMATICO	**Gestione degli accessi**	Gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione e autorizzazione con particolare riferimento agli Amministratori di Sistema
	Gestione della sicurezza fisica	Gestione della sicurezza fisica, ambientale (compresa la sicurezza delle apparecchiature, cablaggi, dispositivi di rete, informazioni) e delle attività di censimento dei beni, oltre all'acquisto di strumenti, programmi e applicazioni a protezione dei dati
	Gestione delle attività on line	Gestione degli aspetti infrastrutturali della navigazione in rete con riferimento anche alle transazioni on line
	Gestione di documenti elettronici con valore probatorio	Gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni e della prevenzione di frodi documentali
	Gestione delle attività di monitoraggio	Gestione del monitoraggio e della verifica periodica del sistema informatico che comprende anche la gestione degli incidenti informatici e dei problemi di sicurezza informatica

5. RISCHI DI REATO A CUI LE ATTIVITÀ SENSIBILI SONO POTENZIALMENTE ESPOSTE

I reati informatici potenzialmente realizzabili sono stati suddivisi per le Attività Sensibili sopra individuate sulla base del Risk Assessment effettuato.

A questo proposito, si segnala che l'esposizione al rischio può essere "diretta", nei casi in cui l'attività aziendale sia condotta in un modo improprio al fine di commettere il reato, ma anche "indiretta" o "strumentale", allorché l'attività sia condotta in modo improprio al fine di agevolare od occultare la commissione di un reato nell'ambito di altra attività aziendale.

Nella specie, i reati identificati come a rischio per le Attività Sensibili oggetto della presente Parte Speciale sono quelli indicati al precedente paragrafo 2 e riportati nel Report di Risk Assessment. Non si esclude, tuttavia, che tali Attività Sensibili possano essere esposte, in via residuale, ad altri reati sanzionati dal D. Lgs. 231/2001[1].

Per questa ragione, tutti i principi di comportamento e i presidi di controllo previsti dalla Parte Speciale Protocollo devono essere sempre scrupolosamente osservati, poiché nel loro complesso possono risultare utili a prevenire anche reati che non siano stati associati alla specifica Attività Sensibile.

6. PRINCIPI GENERALI DI COMPORTAMENTO

Sulla base degli standard di riferimento internazionali, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Secondo tale approccio, gli obiettivi fondamentali della sicurezza informatica che la Società si pone sono i seguenti:

- **Riservatezza**: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- **Integrità**: garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che

[1] Si vedano, a titolo esemplificativo, il reato di Frode informatica ai danni dello Stato o di altro ente pubblico, disciplinato dall'art. 640-ter c.p. e richiamato nella sezione dedicata ai Reati contro la Pubblica Amministrazione (art. 24 D.Lgs 231/01), o il reato di Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori, disciplinato dall'art. 171-bis L. n. 633/1941 comma 1 e richiamato nella sezione dedicata ai Delitti in materia di violazione del diritto d'autore (art. 25 *nonies* D.Lgs 231/01).

le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati;

- **Disponibilità**: garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali, dei Dipendenti, dei Soggetti Terzi e di tutti coloro che svolgono un'attività per conto della Società (limitatamente agli obblighi contemplati nelle specifiche procedure o nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-bis del D.Lgs. 231/2001);
- violare i principi e le procedure aziendali previste nella presente Parte Speciale.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
- accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;
- svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati,

le informazioni, i dati o i programmi in esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

- svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;
- istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
- svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
- svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
- distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

a) osservare scrupolosamente quanto previsto dal Codice Etico aziendale e dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici;
b) astenersi da qualsiasi condotta che possa compromettere la sicurezza, riservatezza e integrità delle informazioni e dei dati, sia aziendali che di terzi;
c) utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
d) non prestare o cedere a terzi alcuna apparecchiatura informatica, senza la preventiva autorizzazione dell'Amministratore di Sistema;
e) in caso di smarrimento o furto, informare tempestivamente il Responsabile di Funzione e gli Uffici Amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
f) evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso,

nonché applicazioni/software che non siano state preventivamente approvata o la cui provenienza sia dubbia;

g) evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;

h) evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, etc.);

i) evitare l'utilizzo di password di altri utenti aziendali, anche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione dell'Amministratore di Sistema; qualora l'utente venisse a conoscenza della password di altro utente è tenuto a darne immediata notizia all'Amministratore di Sistema;

j) evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

k) utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;

l) rispettare le procedure e gli standard previsti, segnalando senza ritardo alle Funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;

m) segnalare senza ritardo alla Funzione IT eventuali incidenti di sicurezza informatica, anche solo dubbi, fornendo tutte le informazioni e l'eventuale documentazione necessaria per procedere a una corretta valutazione del caso;

n) impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;

o) astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

p) astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

q) osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società.

7. PRINCIPI DI RIFERIMENTO RELATIVI ALLA REGOLAMENTAZIONE DELLE ATTIVITÀ SENSIBILI

Ai fini dell'attuazione delle regole e divieti sopra elencati, oltre che dei principi già contenuti nella Parte Generale del presente Modello e dei principi generali di comportamento precedentemente individuati, nell'adottare le procedure specifiche con riferimento alle Attività Sensibili dovranno essere osservati anche i seguenti principi di riferimento:

1. Esistenza di una normativa aziendale relativa alla gestione del rischio informatico che individui le seguenti fasi:

- identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità ovvero delle carenze di protezione relativamente a una determinata minaccia - con riferimento alle seguenti componenti: (i) infrastrutture (incluse quelle tecnologiche quali le reti e gli impianti), (ii) hardware, (iii) software, (iv) documentazione, (v) dati/informazioni, (vi) risorse umane;
- individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse, raggruppabili nelle seguenti tipologie: (i) errori e malfunzionamenti, (ii) frodi e furti, (iii) software dannoso, (iv) danneggiamenti fisici, (v) sovraccarico del sistema, (vi) mancato rispetto della legislazione vigente;
- individuazione dei danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della loro probabilità di accadimento;
- identificazione delle possibili contromisure;
- effettuazione di un'analisi costi/benefici degli investimenti per l'adozione delle contromisure;
- definizione di un piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare;
- documentazione e gestione del rischio residuo.

2. Esistenza di una normativa aziendale nell'ambito della quale siano disciplinati i seguenti aspetti:

- definizione del quadro normativo riferito a tutte le strutture aziendali, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;
- costituzione di un polo di competenza in azienda che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche del trattamento dei dati personali e della tutela legale del software;
- puntuale pianificazione delle attività di sicurezza informatica;
- progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;
- periodica effettuazione di backup delle informazioni e dei dati aziendali;
- definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la *business continuity* attraverso meccanismi di superamento di situazioni anomale;
- applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute;

3. Redazione, diffusione e conservazione dei documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle Funzioni a ciò preposte;
4. Attuazione di una politica di formazione e/o di comunicazione inerente alla sicurezza, volta a sensibilizzare tutti gli utenti e/o particolari figure professionali sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali;
5. Installazione di software di protezione (antivirus, antimalware, etc.) regolarmente aggiornati su tutti i dispositivi utilizzati;
6. Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di networking;
7. Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano, che contempli una puntuale conoscenza dei beni

(materiali e immateriali) che costituiscono il patrimonio dell'azienda oggetto di protezione (risorse tecnologiche e informazioni);

8. Predisposizione e aggiornamento di un censimento dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale;
9. Predisposizione e mantenimento del censimento degli applicativi che si interconnettono con la Pubblica Amministrazione o con Autorità di Vigilanza e loro specifici software in uso;
10. Attuazione di un sistema di protezione idoneo a identificare e autenticare univocamente gli utenti che intendono ottenere l'accesso a un sistema elaborativo o trasmissivo. L'identificazione e l'autenticazione devono essere effettuate prima di ulteriori interazioni operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accessibili solo dagli utenti autorizzati;
11. Predisposizione e attuazione di una policy aziendale che stabilisce (i) le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi e (ii) un insieme di procedure di controllo idonee a verificare se l'accesso è consentito o negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive;
12. Attuazione di un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si esplichi attraverso la verifica e la gestione dei diritti d'accesso;
13. Attuazione di un sistema che prevede la segnalazione e il tracciamento delle operazioni che possono abbassare i livelli di protezione in termini di sicurezza o che rendano possibili violazioni delle politiche di protezione dei dati personali;
14. Proceduralizzazione ed espletamento di attività di analisi degli eventi registrati volte a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce;
15. Previsione di specifiche clausole per terzi/outsourcer aventi a oggetto il rispetto del Modello;

16. Flussi informativi periodici verso l'Organismo di Vigilanza e previsione di segnalazione immediata a detto organo di eventuali incidenti relativi alla sicurezza dei dati.

8. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

L'attività dell'Organismo di Vigilanza sarà svolta in stretta collaborazione con le Funzioni aziendali preposte ai Sistemi Informativi; in tal senso dovrà essere previsto un flusso informativo completo e costante tra dette Funzioni e l'Organismo di Vigilanza al fine di ottimizzare le attività di verifica e lasciando all'Organismo di Vigilanza il precipuo compito di monitorare il rispetto e l'adeguatezza del Modello.

I controlli svolti dall'Organismo di Vigilanza saranno diretti a verificare la conformità delle attività aziendali in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante, inerente alle Attività Sensibili interessate.

Di detti controlli l'Organismo di Vigilanza riferisce al Consiglio di Amministrazione e al Collegio Sindacale, secondo le modalità previste nella Parte Generale del presente Modello.