MODELLO DI ORGANIZZAZIONE E GESTIONE AI SENSI DEL D. LGS. 8 GIUGNO 2001, N. 231

ECOLOGICA

PARTE SPECIALE “D”

REATI INFORMATICI

INDICE PARTE SPECIALE D

1. I "REATI INFORMATICI" DI CUI ALL'ART. 24 *BIS* DEL D.LGS N. 231/2001

Si provvede, qui di seguito, a riportare le singole fattispecie di "reati informatici", richiamate dall'art. 24 *bis* del D.lgs n. 231/2001, così come definite e disciplinate dal codice penale, fornendo, altresì, con riferimento a ciascuna di esse, delle brevi note di commento. Le fattispecie di cui all'art. 24 bis del Decreto ritenute astrattamente rilevanti per Ecologica S.p.A. risultano essere le seguenti:

* * *

Art. 491-bis c.p. – Falsità in documenti informatici

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici .

La norma stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un Documento Informatico, pubblico o privato, avente efficacia probatoria (in quanto rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti).

* * *

Art. 615-ter c.p. – Accesso abusivo ad un sistema informatico o telematico

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva 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.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Costituito dalla condotta di chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Viene sanzionato l'accesso virtuale, che quindi non comporta condotte di aggressione fisica al sistema cui si accede a distanza su reti telematiche. La presenza di un sistema di protezione da accessi abusivi implica un'espressa volontà contraria del soggetto di far accedere altri al proprio sistema.

* * *

Art. 615-quater c.p. – Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Chiunque, 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, è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro.

La pena è della reclusione da uno a tre anni e della multa da cinquemilacentosessantaquattro euro a diecimilatrecentoventinove euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

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. Si ritiene che tra le condotte perseguite rientrino anche quella consistente nell'attivazione di un telefono cellulare clonato su un numero intesto ad altro soggetto, nonchè quella di clonazione dei decoder necessari per la ricezione di determinati programmi televisivi trasmessi via satellite.

* * *

Art. 615-quinquies c.p. – Diffusione ed installazione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

Costituito dalla condotta di chi diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Si tratta di un reato di pericolo quindi per integrare il reato non è richiesto che si verifichi il danneggiamento o l'interruzione, essendo sufficiente la mera elaborazione di un sistema, apparecchiatura o programma idoneo a creare il rischio di un danneggiamento.

* * *

Art. 617-quater c.p. – Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato.

Costituito dalla condotta di chi fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe. Vi rientrano tutti i casi in cui vi è una registrazione o presa di cognizione di una connessione intersistemica tra terminali e elaboratori d dati, che non sia diretta al soggetto agente. La norma estende la punibilità delle condotte incriminate dall'art. 617. La dottrina ritiene si tratti di un'autonoma fattispecie di reato, stante comunque la natura sussidiaria, confermata dalla clausola di apertura.

* * *

Art. 617-quinquies c.p. – Detenzione, diffusione e installazione di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri ho installa apparecchiature, programmi, codici, parole chiave ho altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

Costituito dalla condotta di chi, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico ovvero intercorrenti tra più sistemi. La norma estende la punibilità delle condotte incriminate dall'art. 617 bis.

* * *

Art. 635-bis c.p. – Danneggiamento di informazioni, dati e programmi informatici

Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

Costituito dalla condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui. Tale disposizione ricalca quanto previsto dall'art. 635 in materia di danneggiamento qui diretto a dati e programmi di natura informatica.

* * *

Art. 635-ter c.p. – Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Salvo che il fatto costituisca più grave reato, chiunque 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, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata..

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. Si tratta di un'ipotesi autonoma di reato e non quindi un'ipotesi aggravata di quanto previsto dall'art. 635 bis, che si qualifica quale delitto di attentato, per cui la condotta perseguita deve essere diretta a causare il danneggiamento informatico, ma anche idonea allo stesso sulla base della considerazione di condizioni storiche e sociali presenti al momento del fatto.

* * *

Art. 635-quater c.p. – Danneggiamento di sistemi informatici o telematici

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 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 è punito con la reclusione da uno a cinque anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Costituito dalla condotta di chi, salvo che il fatto non costituisca più grave reato, mediante le condotte di cui all'art. 635bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, rende, il

tutto o in parte, inservibili sistemi informatici o telematica altrui o ne ostacola gravemente il funzionamento. Si tratta dunque di un'ipotesi autonoma di reato, originariamente ricompresa nell'ambito dell'art. 635 bis.

* * *

Art. 635-quinquies c.p. – Danneggiamento di sistemi informatici o telematici di pubblica utilità

Se il fatto di cui all'articolo 635 quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

Costituito dalla condotta di chi distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. La pubblica utilità è il tratto determinate della disposizione in esame, che fa acquisire ai beni informatici e telematici in oggetto una maggiore sensibilità, in quanto utilizzati dalle pubbliche amministrazioni o destinati all'utilizzo o godimento collettivo. Si tratta di un delitto di attentato, per cui la condotta perseguita deve essere diretta a causare il danneggiamento informatico, ma anche idonea allo stesso sulla base della considerazione di condizioni storiche e sociali presenti al momento del fatto.

* * *

Art. 640-quinquies c.p. – Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.

Costituito dalla condotta del soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. Si tratta di un'ipotesi specifica adi frode informatica, che però può essere commessa solo da tali soggetti, qualificandosi dunque la disposizione in esame alla stregua di reato proprio.

2. I DESTINATARI DELLA PARTE SPECIALE

Destinatari della presente parte speciale sono:

- l'Amministratore.
- il Direttore Generale.
- i Sindaci e la società di revisione
- i Responsabili di Funzione.
- i Dipendenti sottoposti ai soggetti apicali innanzi menzionati.

- l'OdV.
- i Consulenti e/o i Partners aziendali.

Nell'espletamento di tutte le operazioni attinenti alla gestione sociale, i Destinatari della presente Parte Speciale devono, in generale, conoscere e rispettare tutte le disposizioni e prescrizioni contenute nei seguenti documenti e, precisamente:

- nella "Parte Generale" del Modello;
- nel Codice Etico;
- nel Manuale del Sistema di Gestione Integrato Qualità ed Ambiente e Sicurezza e nei relativi allegati
- nel documento di Politica integrata;
- nel Documento di Valutazione dei Rischi (DVR) redatto ai sensi del TUS;
- in tutte le procedure, le disposizioni e le istruzioni operative aziendali, la modulistica ed i documenti di appoggio in materia di sicurezza ed igiene sul lavoro;
- nel CCNL di riferimento.

3. OBIETTIVO E FUNZIONE DELLA PARTE SPECIALE

Obiettivo della presente Parte Speciale è la riduzione del rischio di commissione dei reati nelle seguenti aree di attività aziendale ("Aree di Rischio"): i) Reati informatici; ii) Trattamento illecito dei dati.

Funzione della presente Parte Speciale è fornire ai Destinatari a vario titolo coinvolti nello svolgimento di attività nei "Processi Sensibili", così come individuati nel successivo paragrafo:

- i principi generali e le regole di comportamento, nonché i protocolli a presidio dei processi sensibili a cui i destinatari della presente Parte Speciale, come innanzi individuati, in relazione al tipo di rapporto in essere con la Società e/o il Gruppo, sono tenuti ad attenersi ai fini di una corretta applicazione del Modello;
- con riferimento, in particolare, all'OdV e ai Responsabili delle altre funzioni aziendali chiamati a cooperare con lo stesso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica previste.

4. LE POTENZIALI AREE A RISCHIO ED I PROCESSI SENSIBILI

A seguito dell'attività di analisi dei rischi potenziali e della conseguente mappatura, così come analiticamente descritte nella Parte Generale del presente Modello, i processi sensibili individuati nell'ambito delle aree aziendali ritenute potenzialmente a rischio in relazione ai reati ed alle condotte criminose sopra esplicitate sono le seguenti:

1. Gestione di accessi, account e profili;

2. Gestione e utilizzo di sistemi software e banche dati;
3. Gestione dei sistemi hardware;
4. Gestione degli accessi fisici ai siti ove risiedono le strutture IT;
5. Gestione dei servizi di rete;
6. Servizi di key management e gestione della documentazione in formato digitale;
7. Gestione e protezione della postazione di lavoro;
8. Gestione dei dispositivi di memorizzazione connessi agli strumenti elettronici (es: USB, CD);
9. Gestione attività di inventariazione dei beni;
10. Gestione trasferimento dati personali all'esterno dell'organizzazione;
11. Gestione dei flussi informativi elettronici con la pubblica amministrazione.

Al contempo, si ritiene opportuno precisare che tali attività, individuate in fase di mappatura preliminare delle attività sensibili, sono state mantenute anche se, in seguito all'effettuazione delle indagini svolte in sede di *risk analysis* non sono emersi, con riferimento alle stesse, alcun profilo di rischio degno di rilievo. La decisione è motivata dal fatto che sebbene tali attività presentino, attualmente, un rischio reato tendente a zero, non di meno sono state ritenute di specifica considerazione nell'ambito del sistema di organizzazione, gestione e controllo della società tenuto conto della frequenza e del rilievo delle stesse in ambito aziendale.

5. MAPPATURA

L'attività di ***risk assessment*** è stata effettuata attraverso:

- la **raccolta e l'analisi della documentazione interna** ed esterna (funzionigrammi, procure e poteri di firma, procedure operative, comunicazioni, ecc.);
- **interviste** con i soggetti in posizione apicale;
- **interviste** con il personale operativo della Ecologica S.p.A. che, sulla base delle attività che è chiamato a svolgere, potrebbe essere coinvolto in reati previsti dal Decreto (soggetti sottoposti all'altrui direzione).

I risultati dell'*assessment* sono sintetizzati nella seguente tabelle:

		Funzioni Aziendali							
		Legale Rappresentante	Responsabile Tecnico	Funzione Amministrazione / Personale	Responsabile Cantiere	Responsabile Sistema di Gestione Integrato	Funzione Commerciale	Gestione Operativa	Responsabile Sicurezza
REATI INFORMATICI	Falsità di documenti informatici	SÌ	NO	SÌ	NO	NO	NO	NO	NO
	Accesso abusivo ad un sistema automatico o telematico	NO	NO	NO	NO	NO	NO	NO	NO
	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici	SÌ	NO	SÌ	NO	NO	NO	NO	NO
	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	NO	NO	NO	NO	NO	NO	NO	NO
	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche	SÌ	NO	NO	NO	NO	NO	NO	NO
	Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche	SÌ	NO	NO	NO	NO	NO	NO	NO
	Danneggiamento di informazioni, dati e programmi informatici	SÌ	NO	NO	NO	NO	NO	NO	NO
	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico	SÌ	NO	NO	NO	NO	NO	NO	NO
	Danneggiamento di sistemi informatici o telematici	SÌ	NO	NO	NO	NO	NO	NO	NO
	Danneggiamento di sistemi informatici o telematici di pubblica utilità	SÌ	SÌ	NO	NO	NO	NO	NO	NO
	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica	NO	NO	NO	NO	NO	NO	NO	NO

Tabella 1 – Mappatura dei rischi delle Funzioni Aziendali

6. PRINCIPI GENERALI E REGOLE DI COMPORTAMENTO

Tutti i Destinatari del Modello, come individuati nella Parte Generale, adottano regole di condotta conformi ai principi contenuti nel Codice Etico della Società, al fine di prevenire il verificarsi dei delitti di criminalità organizzata.

In particolare, costituiscono presupposto e parte integrante dei protocolli di prevenzione di cui al presente paragrafo i principi di comportamento individuati nel Codice Etico, che qui si intende integralmente richiamato.

Nell'espletamento delle attività considerate a rischio, i destinatari dovranno attenersi ai seguenti principi generali ed alle consequenziali regole di comportamento e di controllo.

1. È vietato ai collaboratori della Società accedere abusivamente (intendendosi qui per modalità abusiva quella caratterizzata dall'assenza di autorizzazione all'accesso ad un sistema protetto) ad alcun sistema informatico o telematico della Società o di terze parti anche con finalità che possano direttamente o indirettamente produrre un vantaggio o un interesse per la Società (ad es. reperendo informazioni e dati);
2. è vietato ai collaboratori della Società ricevere, detenere o diffondere abusivamente (la detenzione abusiva o la diffusione si caratterizzano dall'assenza di legittimazione alla detenzione o alla diffusione dei codici) e in qualsiasi forma, codici di accesso per accedere a sistemi informativi o telematici della Società o di terze parti, anche qualora tale comportamento possa direttamente o indirettamente produrre un vantaggio o un interesse per la Società (ad es. utilizzando tali codici per accedere a sistemi altrui e compiere operazioni illecite);
3. è vietato a tutti i collaboratori della Società procurarsi, diffondere apparecchiature, dispositivi o programmi informatici, attraverso strumenti aziendali, personali o di terze parti, diretti a danneggiare o interrompere un sistema informatico o telematico anche con finalità che possano direttamente o indirettamente produrre un vantaggio o un interesse per la Società;
4. sono assolutamente vietate le pratiche di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, e di semplice installazione di strumenti che possano conseguire tali scopi, anche con finalità che possano direttamente o indirettamente produrre un vantaggio o un interesse per la Società;
5. è vietato a tutti i collaboratori della Società di eseguire azioni od operazioni che possano causare il danneggiamento di informazioni, dati e programmi informatici di terze parti, in particolare se utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità.

7. I PROTOCOLLI A PRESIDIO DEI PROCESSI SENSIBILI

La Ecologica S.p.A. ha da tempo definito un sistema integrato di gestione aziendale, regolarmente certificato. La Società, si è dotata di un sistema di gestione integrato qualità, ambiente e sicurezza conforme alle norme UNI EN ISO 9001:2015, UNI EN ISO 14001:2015 e BS OHSAS 45001:2018

Il sistema integrato di gestione, così come innanzi delineato, deve essere costantemente mantenuto ed implementato in conformità alle norme tecniche di riferimento delle ottenute certificazioni.

Ciò precisato, si indicano qui di seguito i protocolli specifici che i Destinatari, in relazione al tipo di rapporto in essere con la Ecologica S.p.A. ed alla funzione espletata, sono tenuti a rispettare in accordo con il Manuale, le procedure, le disposizioni, le istruzioni operative nonché tutti gli ulteriori documenti di riferimento dei ridetti sistemi di gestione.

Per le operazioni riguardanti la gestione di accessi, account e profili, la gestione dei sistemi software e banche dati, e la protezione delle postazioni di lavoro, i protocolli di prevenzione prevedono che:

- il processo sia formalizzato in una procedura operativa o policy interna;
- siano definiti formalmente dei requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;
- i codici identificativi (user-id) per l'accesso alle applicazioni ed alla rete siano individuali ed univoci;
- la corretta gestione delle password sia definita da linee guida, comunicate a tutti gli utenti per la selezione e l'utilizzo della parola chiave;
- siano definiti i criteri e le modalità per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (es. lunghezza minima della password, regole di complessità, scadenza);
- gli accessi effettuati dagli Amministratori di sistema ai sistemi informativi aziendali siano registrati ed oggetto di verifiche periodiche, come previsto dal codice della Privacy;
- le applicazioni tengano traccia di tutti gli accessi effettuati dagli utenti;
- siano definiti i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- sia predisposta una matrice autorizzativa - applicazioni/profili/richiedente - allineata con i ruoli organizzativi in essere;

- siano eseguite verifiche periodiche dei profili utente al fine di verificare che siano coerenti con le responsabilità assegnate;
- la documentazione riguardante ogni attività critica che possa impattare sulla sicurezza fisica o logica dei sistemi informativi (per esempio la creazione di un nuovo utente con profilo Administrator), sia archiviata allo scopo di garantire la completa tracciabilità della stessa;
- siano definiti i criteri e le modalità per la gestione dei sistemi software che prevedano la compilazione e manutenzione di un inventario aggiornato del software in uso presso la società, l'utilizzo di software formalmente autorizzato e certificato e l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;
- siano definiti i criteri e le modalità per il change management (inteso come aggiornamento o implementazione di nuovi sistemi/servizi tecnologici interni alla Società);
- siano adottate misure tecniche finalizzate a garantire la continuità dei sistemi a supporto dei processi di Business ritenuti critici;
- siano chiuse le sessioni inattive dopo un limitato periodo di tempo (per esempio, screen saver per le postazioni di lavoro).

Per le operazioni riguardanti la gestione dei sistemi hardware, la gestione degli accessi fisici ai siti ove risiedono le strutture IT, la gestione dei servizi di rete e il trasferimento dati personali all'esterno dell'organizzazione i protocolli di prevenzione prevedono che:

- siano definite le responsabilità per la gestione delle reti;
- siano implementati criteri di sicurezza al fine di garantire la riservatezza dei dati interni alla rete e in transito su reti pubbliche;
- siano adottati meccanismi di segregazione delle reti e di monitoraggio del traffico di rete;
- siano implementati meccanismi di tracciatura degli eventi di sicurezza sulle reti (ad es. accessi anomali per frequenza, modalità, temporalità);
- sia regolamentata l'implementazione e la manutenzione delle reti telematiche mediante la definizione di responsabilità e modalità operative, di verifiche periodiche sul funzionamento delle reti e sulle anomalie riscontrate;
- siano definiti i criteri e le modalità per le attività di back up che prevedano la frequenza dell'attività, le modalità, il numero di copie, il periodo di conservazione dei dati;

- la documentazione riguardante ogni attività critica che possa impattare sulla sicurezza fisica o logica dei sistemi informativi (per esempio attività di manutenzione su apparecchiature hardware, modifiche alla configurazione dei firewall), sia archiviata allo scopo di garantire la completa tracciabilità della stessa;

- siano definiti i criteri e le modalità per la gestione dei sistemi hardware che prevedano la compilazione e la manutenzione di un inventario aggiornato dell'hardware in uso presso la Società e che regolamentino le responsabilità e le modalità operative in caso di implementazione e/o manutenzione di hardware;

- siano definite le misure di sicurezza adottate, le modalità di vigilanza e la relativa frequenza, la responsabilità, il processo di reporting delle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza, le contromisure da attivare;

- siano definite le credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT quali, a titolo esemplificativo, badge e codici di accesso;

- siano adottate adeguate misure di protezione da software pericoloso (es. worm e virus);

- siano previsti strumenti di protezione idonei a garantire la sicurezza nello scambio di informazioni critiche per il business aziendale e di carattere confidenziale;

- venga effettuata una verifica periodica dei log che registrano gli eventi e le attività degli utilizzatori;

- vengano definite e recepite regole per la corretta custodia dei dispositivi di memorizzazione (es. telefonini, chiavi USB, CD, hard disk esterni, ecc).

Per le operazioni riguardanti la gestione dei servizi di key management e la gestione della documentazione in formato digitale, la gestione dei flussi informativi elettronici con la pubblica amministrazione, i protocolli prevedono che:

- il processo sia formalizzato in una procedura operativa o policy interna che costituisce parte integrante del presente Modello;
- siano definiti criteri e modalità per la generazione, distribuzione, revoca ed archiviazione delle chiavi (smart card);
- sia formalmente disciplinata la eventuale gestione dei documenti in formato digitale da parte di soggetti terzi;
- siano definiti i controlli per la protezione delle chiavi da possibili modifiche, distruzioni e utilizzi non autorizzati;

- la documentazione di supporto alle attività effettuate con l'utilizzo dei documenti in formato digitale sia tracciabile e adeguatamente archiviata.

Per le attività inerenti l'inventariazione dei beni, i protocolli prevedono che:

- l'azienda effettui l'inventariazione degli asset aziendali, comprese le base dati in essi contenute, adoperati ai fini dell'operatività del sistema informatico e adotta politiche di conformità legale (copyright) laddove applicabili.

Costituiscono parte integrante del Modello le procedure aziendali che danno attuazione ai principi e alle misure di prevenzione sopra indicate per prevenire i reati informatici.

8. LE FUNZIONI ED I COMPITI DELL'ORGANISMO DI VIGILANZA

Le segnalazioni possono avvenire per iscritto e in forma non anonima, attraverso appositi canali di informazione riservati con le seguenti modalità:

- e-mail: **odv@ecologicaspa.com**

- lettera (anche anonima): all'indirizzo:

  Ecologica Spa
  Via per Statte 7050,
  74123 Taranto TA
  Alla c.a. del Presidente dell'Organismo di Vigilanza

- attraverso la piattaforma dedicata whistleblowing accessibile dal sito aziendale.

Fermo restando il potere discrezionale dell'OdV di attivarsi con specifici controlli, anche a seguito delle segnalazioni ricevute, oltre alle attività di verifica e controllo analiticamente specificate nella "Parte Generale" del Modello, lo stesso è tenuto ad effettuare periodicamente controlli a campione sui processi sensibili nell'ambito delle aree potenzialmente a rischio di reati informatici, diretti a verificare il rispetto dei principi e delle regole di cui alla presente parte speciale.

A tal fine, l'Amministratore, il Direttore Generale e il Capo dell'Unità Organizzativa (così come il Collegio Sindacale) sono tenuti ad una specifica reportistica all'OdV.

La presente Sezione e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'OdV, secondo quanto previsto nella Parte Generale, al fine di garantire il raggiungimento delle finalità del presente Modello.

- SCHEDE EVIDENZA ASSOCIATE

NUMERO SCHEDA EVIDENZA	PROCESSO SENSIBILE
15	Utilizzo e rete software