**PARTE SPECIALE F**

**REATI INFORMATICI**

1. **DESTINATARI DELLA “PARTE SPECIALE D”**

La presente Parte Speciale del Modello di Organizzazione e Gestione si rivolge agli amministratori, ai dirigenti, che operano nell’ambito delle attività e/o processi sensibili individuati ai sensi della presente Parte Speciale, nonché a tutti coloro che, anche in virtù di vincoli contrattuali (appaltatori, consulenti, partners, ecc.), intrattengono rapporti con SAP inerenti profili di gestione informatica.

L’obiettivo della Presente Parte Speciale è dunque di far sì che tutti i destinatari del Modello, nell’ambito delle attività e/o dei processi sensibili come individuati adottino, nei limiti dei propri compiti e delle connesse responsabilità, regole di condotta conformi ai principi contenuti nel Modello (sia nella Parte Generale che nella presente Parte Speciale) e nel Codice Etico al fine di prevenire la commissione dei reati considerati rilevanti ai sensi dell’articolo 24-bis e 25-nonies del Decreto.

In particolare, la presente Parte Speciale ha lo scopo di:

1. indicare le “regole di comportamento” e le procedure che i destinatari del Modello (amministratori, dirigenti, organi sociali, consulenti e collaboratori esterni) sono tenuti ad osservare al fine di una corretta ed efficace applicazione del Modello stesso;

2. fornire all’OdV ed alle funzioni aziendali che con lo stesso collaborano, gli strumenti effettivi per lo svolgimento delle attività di vigilanza, controllo e monitoraggio sull’applicazione del Modello.

1. **I REATI RELATIVI AI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI INTRODOTTI DELL’ART. 24-BIS DEL DECRETO LEGISLATIVO 231/01 E DEI DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE INTRODOTTI DALL’ ART. 25-NONIES DEL DECRETO LEGISLATIVO 231/01**

In questo capitolo introduttivo vengono descritte le fattispecie di reati contemplati nella presente Parte Speciale del Modello Organizzativo 231, così come indicati agli artt. 24-bis e 25-nonies del Decreto.

Pur rilevando che le due tipologie di reati tutelino interessi giuridici differenti, si è ritenuto opportuno procedere alla predisposizione di un'unica Sezione in quanto:

* entrambe le fattispecie hanno un comune presupposto: il corretto utilizzo delle risorse informatiche e principi etici da parte degli utenti;
* le aree di rischio risultano, in virtù di tale circostanza, in parte sovrapponibili;
* i principi procedurali mirano, in entrambi i casi, a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

Le aziende moderne hanno una forte dipendenza dagli strumenti informatici, come appunto la E.G.U.A. s.r.l.

L’illecito impiego delle nuove tecnologie permette la commissione di specifici reati che sono sempre più diffusi nella realtà odierna.

La prevenzione dei reati tecnologici è diventata una priorità non solo per l’introduzione delle specifiche norme ma per la crescita di sensibilità che avviene nelle strutture dirigenziali.

Gli articoli 24-bis prima e 25-nonies dopo, hanno affrontato una serie di illeciti la cui prevenzione è indispensabile in ogni struttura organizzata per poter sopravvivere in un mercato sempre più competitivo ed attento.

L’obiettivo del Modello Organizzativo è principalmente la prevenzione e, in secondo luogo, il monitoraggio e la valutazione dei dati disponibili al fine di garantire informazioni utili all’individuazione dell’utente che, eventualmente, commette un illecito. Il tutto permette all’Ente di disporre di una struttura monitorata ove, senza commettere alcun illecito in materia di privacy o in lesione degli artt. 4 e 8 dello Statuto dei Lavoratori, si acquisiscono dati utili a poter ricondurre un’eventuale condotta ad un’utente della rete. Informazioni che, opportunamente utilizzate, costituiscono un ottimo deterrente al fine preventivo.

L’organizzazione dei sistemi informativi deve tenere conto che l’attività di lavoro o un’eventuale attività illecita possano essere gestite con lo stesso strumento, per cui solo la prevenzione ed il monitoraggio possono permettere di ottenere un risultato.

Si procede con l’elencazione degli articoli del Codice Penale introdotti dagli articoli del D.Lgs. 231/01 al fine di conoscerne i dettagli, le pene inflitte, e le possibili modalità di commissione. Conoscere la fattispecie di reato è già di per se un deterrente alla commissione. Spesso il reato informatico non viene nemmeno percepito come tale e rientra in una ormai normale “cattiva abitudine”.

Verranno affrontate una ad una tutte le fattispecie di reato previste nel D.Lgs. 231/01.

Per ogni reato viene introdotto il testo, le pene previste dal codice, e :

* modalità di commissione : la percezione del reato informatico è spesso molto bassa e la sola descrizione della modalità di commissione permette all’utente di comprendere quando la propria condotta rientra in una fattispecie di reato ed evitarlo;
* modalità di prevenzione : descrizione delle misure messe in atto per la prevenzione del reato;
  + rischio : grado di rischio dell’ente nello specifico reato internazionale delle specie animali e vegetali in via di estinzione ex Legge 150/92 e violazione dei divieti di scarico (sversamento) in mare di sostanze e/o materiali inquinanti da navi ed aeromobili stabiliti da convenzioni internazionali ratificate dall’Italia).
* **Art. 491-bis cod.pen - Falsità in documenti informatici**

Norma : “Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, avente efficacia probatoria3, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. La norma stabilisce che tutti i delitti relativi alla falsità in atti disciplinati dal Codice Penale (cfr. Capo III, Titolo VII, Libro II), 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).

La falsità può essere materiale e/o ideologica, in dettaglio:

* Falsità materiale: si ha quando un documento viene formato o sottoscritto da persona diversa da quella indicata come mittente o sottoscrittore, con divergenza tra autore apparente e autore reale del documento (contraffazione) ovvero quando il documento è artefatto (e, quindi, alterato) per mezzo di aggiunte o cancellazioni successive alla sua formazione.
* Falsità ideologica: Si ha quando un documento non è veritiero nel senso che, pur non essendo né contraffatto né alterato, contiene dichiarazioni non vere. Nel falso ideologico è lo stesso autore del documento che attesta fatti non rispondenti al vero. Integra comunque il delitto di falsità in Documenti Informatici la condotta di chi falsifichi documenti aziendali oggetto di flussi informatizzati o la condotta di chi alteri informazioni a valenza probatoria presenti sui propri sistemi allo scopo di eliminare dati considerati “sensibili” in vista di una possibile attività ispettiva.

Modalità di commissione :

Realizzazione di un documento contenente informazioni non corrispondenti al vero realizzato da utente differente dal firmatario indicato. Sono casi estremamente difficili da prevenire in quanto lo strumento informatico trova la stessa applicazione sia nella gestione di dati corretti che in quelli falsi.

Modalità di prevenzione :

l’unica modalità di prevenzione di questo reato avviene attraverso il monitoraggio del file system dei server – soprattutto – ma anche – ove è possibile – dei terminali, al fine di poter individuare il reale utente della rete che crea / modifica / stampa il

documento.

Per la prevenzione di questo reato è importante dare continuità ad attività di formazione in cui vengano spiegate le conseguenze derivanti dal reato.

Rischio :

La rete è ben strutturata e permette di individuare l’utente che ha gestito un documento. La possibilità che il reato venga commesso è medio. Attualmente il sistema informatico non dispone di un software di auditing automatico del file system ma è stato accertato che, attraverso normali attività di analisi, è possibile individuare le credenziali dell’utente che ha creato / modificato un documento.

L’introduzione di un sistema automatico di monitoraggio permetterebbe nel tempo di ridurre ulteriormente il rischio.

* **Art. 615-ter cod. pen.- Accesso abusivo ad un sistema informatico o telematico**

Norma : “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”. Tale reato si concretizza quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza.

Viene punito l'accesso abusivo ad un sistema informatico o telematico comunque questo venga compiuto, e dunque anche quando ad esempio all'accesso non segua un vero e proprio danneggiamento di dati: ciò si verifica quando un soggetto acceda abusivamente ad un sistema informatico e proceda alla stampa di un documento contenuto nell’archivio del personal computer altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire l’accesso.

L’accesso abusivo è, normalmente,– propedeutico ad altri reati come la copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura). La suddetta fattispecie delittuosa si realizza anche nell’ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, si sia trattenuto contro la volontà del titolare del sistema, oppure abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Modalità di commissione : Il delitto potrebbe essere configurabile nell’ipotesi in cui un soggetto acceda abusivamente ai sistemi informatici di proprietà di terzi (outsider hacking), per prendere cognizione di dati riservati altrui nell’ambito di una negoziazione commerciale, o acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso in vista del compimento di atti ulteriori nell’interesse della società stessa. Tipici , nella commissione di questo reato, sono gli accessi ad un sistema informatico di un precedente datore di lavoro, per acquisire dati e sfruttarli nell’interesse del nuovo datore di lavoro. I dipendenti dovranno essere anche valutati in termini di performance con particolare riferimento ad attività concorrenziali nei riguardi di precedenti datori di lavoro.

Modalità di prevenzione : Monitoraggio delle connessioni attraverso la raccolta e storicizzazione dei files di log dei firewall posti a garantire la sicurezza della rete informatica. Attività che è stata delegata dall’ente a società esterna.

Rischio : La rete è ben strutturata e permette di individuare l’utente che ha gestito una connessione. La possibilità che il reato venga commesso è molto bassa.

* **Art. 615-quater cod. pen. - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici**

Norma : “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 ad un anno e con la multa sino a lire dieci milioni. La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell’articolo 617 quater.”

Il reato si realizza qualora un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei (sia a livello software che hardware) all’accesso di un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee a raggiungere tale scopo. Conseguentemente L’art. 615-quater cod. pen., punisce le condotte preliminari all’accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico. Importante che i sistemi informatici, come già nel caso precedente, sono intesi protetti a livello normativo quando sono gestiti attraverso un qualsiasi livello di protezione (password, firewall, etc.).

I dispositivi che consentono l’accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (quali badge o smart card). Ma anche da tool software e/o hardware che trovano un ampio mercato sulla rete internet.

In conclusione tale fattispecie si configura tra l’altro:

* quando il soggetto, in possesso legittimamente dei dispositivi di cui sopra (ad esempio, un operatore di sistema), li comunichi senza autorizzazione a terzi soggetti;
* quando il soggetto si procuri illecitamente uno di tali dispositivi.

L’art. 615-quater cod.pen. punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Modalità di commissione : Molto diffuso è il caso di un soggetto A che passando da un’azienda X ad un’azienda Y continui ad accedere ai dati della società X attraverso gli strumenti della società Y e tragga vantaggio per se e per l’azienda Y dai dati acquisiti dal sistema informativo della società X.  
Modalità di prevenzione : Monitoraggio dei contenuti delle memorie di massa attraverso programmi antivirus/antispyware che permettano di individuare presenza di files maligni anche in forma installativa. La rete è ben strutturata e dotata di opportuni programmi che garantiscono un livello di log adeguato e funzionale.  
Rischio : La rete è ben strutturata e gestita con software di elevato livello. La possibilità che il reato venga commesso è molto bassa.

* **Art. 615-quinquies cod. pen. - Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico**

Norma : “ 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.” Tale fattispecie di reato si realizza quando qualcuno, 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, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Modalità di commissione : Tale reato potrebbe configurarsi qualora un dipendente si procuri un Virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico aziendale in modo da distruggere documenti “sensibili” in relazione ad un procedimento penale a carico della società.

Modalità di prevenzione : Monitoraggio dei contenuti delle memorie di massa attraverso programmi antivirus / antispyware che permettano di individuare presenza di files maligni anche in forma installativa. La rete è ben strutturata e dotata di opportuni programmi che garantiscono un livello di log adeguato e funzionale. La struttura server è ben organizzata e parzialmente dislocata esternamente alla struttura aziendale, rendendola inaccessibile a utenti che intendessero aggredirla anche in modo fisico.

Rischio : La rete è ben strutturata e gestita. La possibilità che il reato venga commesso è molto bassa.

* **Art. 617-quater cod. pen. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche**

Norma : “Chiunque fraudolentemente intercetta comunicazioni relative ad 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.

Tale fattispecie di reato si realizza quando un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione.

Modalità di commissione : Il reato potrebbe configurarsi con il vantaggio concreto della società, nel caso in cui un dipendente impedisca una determinata comunicazione in via informatica al fine di evitare che un’impresa concorrente trasmetta i dati e/o l’offerta per la partecipazione ad una gara. Altra modalità attraverso cui è possibile compiere il reato è quello di intercettare una comunicazione informatica (tra cui sono comprese anche quelle tra apparati mobili) da cui acquisire dati utili ad attività vantaggiose per l’ente per da cui si dipende. Modalità di prevenzione : Il reato è possibile tecnicamente a seguito di un accesso abusivo. La specificità tecnica e la necessità di elevate conoscenze, unite alle strumentazioni attive per il monitoraggio della rete (antivirus) e della protezione (firewall) garantiscono un ottimo livello di prevenzione.

Rischio : La rete è ben strutturata e gestita. La possibilità che il reato venga commesso è molto bassa.

* **Art. 617-quinquies cod. pen. - Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche**

Norma : “Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte 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.” Questa fattispecie di reato si realizza nel caso in cui qualcuno, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. La condotta vietata dall’art. 617-quinquies cod. pen. è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate, purché le stesse abbiano una potenzialità lesiva.

Modalità di commissione : Un dipendente si introduca fraudolentemente presso la sede di una potenziale controparte commerciale al fine di installare apparecchiature idonee all’intercettazione di comunicazioni informatiche o telematiche rilevanti in relazione ad una futura negoziazione. Tipico il caso di un ex-dipendente che si reca presso la precedente società datrice di lavoro ed avvicina ex-colleghi con qualsivoglia scusa al fine di poter installare uno strumento di intercettazione da cui trarre dati da utilizzarsi a vantaggio dell’attuale datore di lavoro.

Modalità di prevenzione : Il reato ha una bassa specificità tecnica. La prevenzione deriva da un periodico monitoraggio delle apparecchiature e delle periferiche al fine di valutare l’eventuale introduzione di strumenti hardware esterni. I dipendenti dovranno essere anche valutati in termini di performance con particolare riferimento ad attività concorrenziali nei riguardi di precedenti datori di lavoro. Rischio : La rete è ben strutturata e gestita. La possibilità che il reato venga commesso è molto bassa.

* **Art. 635-bis cod. pen. - Danneggiamento di informazioni, dati e programmi  
  informatici**

Norma : “Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni. Se ricorre una o più delle circostanze di cui al secondo comma dell’articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.” La fattispecie di reato si realizza qualora un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui.

Modalità di commissione : Il danneggiamento potrebbe essere commesso a vantaggio della società laddove l’eliminazione o l’alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte di un fornitore della società o al fine di contestare il corretto adempimento delle obbligazioni da parte del medesimo o, ancora, nell’ipotesi in cui vengano danneggiati dei dati aziendali “compromettenti”.

Modalità di prevenzione : Come per la falsificazione di dati digitali la prevenzione può essere attuata solo con il monitoraggio del file system delle memorie di massa a disposizione degli strumenti informatici. La rete ben strutturata e monitorabile permette di individuare gli utenti che hanno gestito uno specifico file.

Rischio : La rete è ben strutturata e gestita. La possibilità che il reato venga commesso è media.

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

Norma : “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 ricorre la circostanza di cui al numero 1) del secondo comma dell’articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata. Tale reato si realizza qualora un soggetto commetta 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. Tale delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità. E’ una fattispecie di reato che deve essere tenuta in considerazione con molta attenzione da parte dell’ente SAP in quanto l’oggetto della propria attività è la trattazione di dati provenienti anche da enti pubblici (es. Città di Torino).

Modalità di commissione : Tale reato potrebbe essere commesso nell’interesse della società qualora un dipendente compia atti diretti a distruggere o alterare documenti informatici provenienti dall’ente pubblico.

Modalità di prevenzione : Come per il reato precedente la prevenzione può essere attuata solo con il monitoraggio del file system delle memorie di massa a disposizione degli strumenti informatici. La rete ben strutturata e monitorabile permette di individuare gli utenti che hanno gestito uno specifico file.

Rischio : La rete è ben strutturata e gestita. La possibilità che il reato venga commesso è media.

* **Art. 635-quater cod. pen. - Danneggiamento di sistemi informatici o telematici**

Norma : 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 ricorre la circostanza di cui al numero 1) del secondo comma dell’articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata”.

Questo reato si realizza qualora un soggetto mediante le condotte di cui all’art. 635-bis cod. pen., ovvero attraverso l’introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento.

Modalità di commissione : La commissione del reato richiede specifiche competenze tecniche e l’esecuzione di un accesso abusivo al sistema informatico per poter essere messo a compimento. Modalità di prevenzione : Il monitoraggio messo a punto attraverso i firewall garantisce la valutazione di accessi abusivi volti al danneggiamento di dati su sistemi di terzi.

Rischio : La rete è ben strutturata e gestita. La possibilità che il reato venga commesso è molto bassa.

* **Art. 635-quinquies cod. pen. - Danneggiamento di sistemi informatici o telematici di pubblica utilità**

Norma : 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 ricorre la circostanza di cui al numero 1) del secondo comma dell’articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Questo reato si configura quando la condotta di cui al precedente art. 635- quater cod. pen. è diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Come già citato in precedenza, l’ente deve tenere conto del fatto che tratta dati ed il sistema informatico è interconnesso anche con quello di enti pubblici.

Modalità: vedasi paragrafo precedente.

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

Norma : 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.

Questo reato si configura quando un soggetto che presta servizi di certificazione di Firma Elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Tale reato è dunque un reato cd. proprio in quanto può essere commesso solo da parte dei certificatori qualificati, o meglio, i soggetti che prestano servizi di certificazione di Firma Elettronica qualificata.

Modalità : Non applicabile

Si precisa in ogni caso che la commissione di uno dei Delitti Informatici sopra descritti assume rilevanza, per le finalità di cui al Decreto, solo qualora la condotta, indipendentemente dalla natura aziendale o meno del dato/informazioni/programma/sistema informatico o telematico, possa determinare un interesse o vantaggio per SAP. Pertanto, nell’ambito della descrizione delle singole fattispecie criminose, così come nella successiva descrizione dei Delitti in Violazione del Diritto d'Autore, si è tenuto conto di tale rilevante aspetto per l’elaborazione dei casi pratici proposti.

Le sanzioni applicabili all’Ente nell’ipotesi di commissione dei Delitti Informatici possono essere di natura pecuniaria, da 100 a 500 quote (considerato che il valore di ogni quota può essere determinato, sulla base delle condizioni economiche e patrimoniali dell’Ente, tra un minimo di Euro 258 ed un massimo di Euro 1.549 e le stesse possono variare da un minimo di circa Euro 26.000 ad un massimo di circa Euro 800.000) e di natura interdittiva, che variano a seconda della fattispecie criminosa realizzata.

I destinatari del presente Parte Speciale dovranno prestare attenzione alla correlazione e concorso tra i reati con l’attribuzione della responsabilità penale per più reati informatici nel caso di una violazione commessa (es. di correlazione: detenzione abusiva dei codici d’accesso/accesso abusivo/diffusione di software dannosi). La specificità dei reati informatici è tale che difficilmente potrà essere commesso un reato unico. Ad esempio l’accesso abusivo (635 ter) è da intendersi a livello tecnico un reato di tipo propedeutico alla commissione di ulteriori fattispecie. Come già citato sarà molto importante valutare le performance del singolo soggetto lavoratore al fine di accertare anomalie di risultati che potrebbero evidenziare l’utilizzo illecito di dati, la cui provenienza potrebbe derivare da una condotta fraudolenta compiuta attraverso un reato informatico tra quelli in precedenza descritti.

* **Le tipologie di delitti in violazione del diritto d'autore introdotte dall’ art. 25-nonies del decreto legislativo 231/01**

L'art. 25-nonies contempla alcuni reati previsti dalla Legge sul Diritto d'Autore (e, in particolare, dagli artt. 171, 171-bis, 171-ter, 171-septies e 171-octies della Legge 22/04/1941) quali, a titolo d’esempio:

* l'importazione, la distribuzione, la vendita o la detenzione a scopo commerciale o imprenditoriale di programmi contenuti in supporti non contrassegnati dalla SIAE;
* la riproduzione o il reimpiego del contenuto di banche dati;
* l'abusiva duplicazione, la riproduzione, la trasmissione o la diffusione in pubblico, di opere dell'ingegno destinate al circuito televisivo o cinematografico;
* l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.

Si provvede pertanto a fornire qui di seguito una breve descrizione delle due fattispecie di cui all’art. 25-nonies del D. Lgs. 231/2001.

* Art. 171 comma 1 lett. a bis e comma 3 Legge sul diritto d’autore - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio

In relazione alla fattispecie delittuosa di cui all'art. 171, il Decreto ha preso in considerazione esclusivamente due fattispecie, ovvero:

1. la messa a disposizione del pubblico, attraverso l’immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un’opera di ingegno protetta o di parte di essa;
2. la messa a disposizione del pubblico, attraverso l’immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un’opera di ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

Modalità di commissione : Tale reato potrebbe essere commesso nell’interesse della società qualora venissero caricati sul sito Internet aziendale dei contenuti coperti dal diritto d'autore.

* **Art. 171 bis Legge sul diritto d’Autore. - Protezione del diritto d'autore e di altri diritti connessi al suo esercizio**

La norma in esame è volta a tutelare il corretto utilizzo dei software e delle banche dati. Per i software, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata". Il reato in ipotesi si configura nel caso in cui chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla SIAE.

Modalità di commissione :

Tale reato potrebbe essere commesso nell’interesse della società qualora venissero utilizzati, per scopi lavorativi, programmi non originali al fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un software originale. Le sanzioni applicabili all’Ente nell’ipotesi di commissione dei Delitti in Violazione del Diritto d'Autore possono essere di natura pecuniaria fino a 500 quote (e dunque fino ad un massimo di circa Euro 800.000) e di natura interdittiva, quali l'interdizione dall'esercizio dell'attività o la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito per una durata non superiore ad un anno. Nel corso dell’anno 2013 è stato pubblicato il Decreto Legge 93/2013, che poi non ha trovato conversione in legge. L’articolo aveva introdotto nel catalogo dei reati presupposti l’ Art. 640 Ter. Considerato che l’Ente aveva valutato l’esigenza di procedere ad integrare il modello tenendo conto dell’articolo penale, tenuto conto anche dell’importanza di detto articolo da un punto di vista tecnico, ed ipotizzato che possa essere a breve reintrodotto nel catalogo dei reati presupposti, l’Ente ritiene di tenere in considerazione tale articolo ed adeguare già la propria organizzazione alle condotte punite.

* **Art.640-ter cod. pen. - Frode informatica**

Norma : Chiunque, alterando 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 o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante. Si tratta di un’importante innovazione concettuale della prevenzione dei reati in quanto impone una gestione della sicurezza attraverso sistemi di monitoraggio del file system estremamente capillari e complessi. Tale necessità deriva dall’affermazione inclusa nella norma “intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti” dove la prevenzione è ipotizzabile solamente ove il sistema informatico sia presidiato in modo continuo attraverso procedure automatizzate in quanto le informazioni relative all’eventuale alterazione di informazioni sono difficilmente ricostruibili successivamente alla commissione del reato.

Modalità di commissione : si tratta di un reato la cui commissione non richiede specifiche competenze tecniche, le stesse competenze necessarie alle funzioni lavorative possono essere impiegate per la gestione di una falsa identità finalizzata alla modifica o all’intervento in qualsiasi modalità su dati (files) o informazioni ad essi pertinenti.

Modalità di prevenzione : Il controllo messo a punto attraverso sistemi di monitoraggio continuo dei file system sono l’unica soluzione utile a garantisce la valutazione eventuali alterazioni intervenute sui dati o l’utilizzo improprio di informazioni / utenze.

Rischio : La rete della società è ben strutturata e gestita. È necessario comunque inserire un sistema di auditing continuo della rete, considerabile l’unica soluzione esaustiva alla prevenzione della tipologia di reato, parallelamente ad uno specifico piano di formazione indirizzato alla sensibilizzazione dei dipendenti utilizzatori di strumenti informatici e/o telematici.

**3. Processi Sensibili di E.G.U.A. per I Delitti Informatici**

* **Aree a Rischio**

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute in genere a rischio risultano essere, ai fini della presente Sezione, le seguenti:

- tutte le attività aziendali svolte dai Destinatari tramite l’utilizzo dei Sistemi Informativi aziendali, del servizio di posta elettronica e dell'accesso ad Internet;

- gestione dei Sistemi Informativi aziendali al fine di assicurarne il funzionamento e la manutenzione, l’evoluzione della piattaforma tecnologica e applicativa IT nonché la Sicurezza Informatica;

- gestione dei flussi informativi elettronici con la pubblica amministrazione;

- utilizzo di software e banche dati;

I destinatari del presente Parte Speciale sono in generale gli incaricati della gestione dei dati nei sistemi contabili ed informatici facendo riferimento in particolare agli organi sociali e di amministrazione.

Anche relativamente a tale aspetto si precisa che la E.G.U.A. non dispone di personale alle proprie dirette dipendenze infatti l’articolo 7 dello statuto della società E.G.U.A. s.r.l. obbliga la Società dell’Acqua Potabile s.r.l. (società mandataria della Associazione Temporanea di Impresse costituita con la mandante VIVENDI s.r.l., nell’interesse della quale agisce) in qualità di socio privato a fornire alla suddetta Società E.G.U.A. s.r.l. specifiche prestazioni accessorie al fine di coadiuvare la stessa nella gestione del “ciclo integrato delle acque”. In virtù di tale obbligo statutario, in data 21 febbraio 2008, tra le due società è stato sottoscritto un contratto di fornitura di prestazioni con quale la Società dell’Acqua Potabile si è impegnata a fornire gratuitamente alla E.G.U.A. s.r.l. diverse prestazioni.

E.G.U.A. s.r.l. non dispone di proprio personale tecnico dipendente appoggiandosi alla SAP s.r.l. pertanto l’analisi dei processi sensibili in materia di reati ambientali è stata condotta anche da quest’ultima società relativamente al personale tecnico alle proprie dipendenze e le risultanze sono state inserite all’interno del proprio modello di organizzazione, gestione e controllo.

Le attività sensibili relative ai reati informatici ai fini del D.Lgs. 231/2001 Le attività sensibili individuate, in riferimento ai Reati Informatici richiamati dall’art. 24-bis del D.Lgs. 231/2001, sono tra l’altro le seguenti: - Gestione e monitoraggio degli accessi ai sistemi informatici e telematici, nell’ambito della quale sono ricomprese le attività di: gestione del profilo utente e del processo di autenticazione; gestione e protezione della postazione di lavoro;

gestione degli accessi verso l’esterno;

gestione e protezione delle reti;

gestione degli output di sistema e dei dispositivi di memorizzazione;

- Sicurezza fisica (sicurezza cablaggi, dispositivi di rete, ecc.)

Utilizzo e gestione di dati aziendali con strumenti informatici dotati di software standard (commerciali) e/o piattaforma gestionale aziendale (fornita da gestore esterno);

4. Procedure adottate

4.1 Il sistema procedurale La presente Parte Speciale si riferisce a comportamenti posti in essere dagli utenti della rete informatica della società E.G.U.A., chiamati Destinatari. Obiettivo della presente Sezione è che tali Destinatari si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento delle attività rientranti nelle Aree a Rischio e in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti di E.G.U.A., a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Delitti Informatici e di quelli commessi in violazione del diritto d’autore.

In particolare, la presente Sezione ha la funzione di:

* fornire un elenco dei principi generali nonché dei principi procedurali specifici cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
* fornire all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandato.

Nell’espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, tutti i dirigenti, e consulenti dell’ente sono tenuti, in generale, a rispettare tutte le regole e i principi contenuti nei seguenti documenti, per le parti di proprio interesse:

- Organigramma aziendale e schemi organizzativi;

- Controllo degli accessi logici alle risorse informative rendendo riservati e personali i propri codici di accesso e le proprie password;

- Procedure interne di gestione password provvedendo alla sostituzione come previsto e senza ideare metodologie elusive delle logiche di sicurezza;

- Verifica periodica deli files di Log obbligatori da parte degli amministratori di sistema (accessi amministrativi e posta elettronica);

- Valutazione periodica del livello di sicurezza informatica, che per sua natura si riduce con il passar del tempo, se non vengono gestiti opportuni investimenti;

- Verifica periodica degli investimenti svolti in materia informatica, con particolare riferimento all’aggiornamento degli strumenti, compreso quelli di rete, e dei software.

Gli obiettivi fondamentali della sicurezza informatica che E.G.U.A. 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 risultano 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. Risulta garantito che le informazioni risultano trattate in modo tale che non possono essere manomesse o modificate da soggetti non autorizzati, e comunque, in caso di manomissione identificare l’esecutore;

- 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 lavoratori dipendenti e dei consulenti di SAP (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati 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 e art. 25-nonies 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:

1. alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
2. accedere abusivamente al sistema informatico o telematico proprio o di terzi di soggetti pubblici o privati;
3. accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e/o cancellare dati e/o informazioni, o di sottrarle al fine di poterle reimpiegare in attività concorrenziali e di vantaggio per l’ente;
4. 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.
5. 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;
6. 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;
7. 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;
8. installare apparecchiature per l’intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
9. svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
10. svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
11. distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.
12. acquisire, distribuire, vendere o detenere a scopo commerciale o imprenditoriale programmi in supporti non contrassegnati dal marchio SIAE, opere tutelate dal diritto d’autore o banche dati e software pirati.
13. Installare o utilizzare software tutelati dal diritto d’autore, non autorizzati da E.G.U.A., ed installati dal personale tecnico interno, per qualsivoglia attività lavorativa e di gestione di dati di proprietà E.G.U.A.;

Pertanto, i soggetti sopra indicati, devono rispettare i seguenti principi:

L’uso dei sistemi informatici deve svolgersi nel rigoroso rispetto delle norme vigenti, del Codice Etico in vigore e nel rispetto dei regolamenti emanati dall’ente;

- La società rispetta tutte le normative in materia di Privacy al quale tutti gli amministratori ed i collaboratori sono tenuti ad attenersi;

- Tutti i software installati nei sistemi della società risultano regolarmente licenziati e nessuno è autorizzato alla loro rimozione, reinstallazione, o modifica;

Ogni utente è personalmente responsabile dell’integrità (fisica e funzionale) dei sistemi medesimi, dei dati, delle informazioni e dei programmi ad essi relativi, ed alla loro custodia quando trasferiti all’esterno del perimetro aziendale (dispositivi mobili) ove possono essere oggetto di furto mirato all’acquisizione di dati aziendali;

- La società può altresì revocare, in tutto o in parte l’uso dei sistemi informatici, ovvero impedire, in tutto o in parte, l’accesso alle reti informatiche aziendali e non, ad uno o più utenti (a titolo d’esempio, facendo uso di filtri);

- Amministratori, dipendenti e collaboratori aderiscono ai predetti principi generali di utilizzo dei sistemi informatici e, quindi, espressamente accettano anche l’accesso ai medesimi, senza limitazione alcuna, da parte dei propri superiori, dell’amministratore di sistema o dei suoi delegati;

- L’utilizzo delle firme elettroniche certificate avviene su apposita delega scritta del rappresentante legale dell’azienda;

- E’ vietato qualsiasi uso dei sistemi informatici per scopi incompatibili con quello per il quale essi sono concessi in uso agli utenti.

In particolare è vietato:

l’uso ludico dei sistemi informatici;

operare il download, il caricamento o l’installazione di software (musicali, film, foto, programmi, ecc…) non autorizzati e, comunque, in violazione del diritto d’autore;

utilizzare supporti rimovibili (es. chiavetta USB) non controllati preventivamente e comunque in modo esclusivo per attività attinenti alle mansioni lavorative;

rendere in qualsiasi modo noto a terzi non autorizzati, o comunque consentire a questi la conoscenza di dati, informazioni, formule, descrizioni di processi, documenti, materiale di qualsiasi natura, coperto da riservatezza o la cui conoscenza da parte di soggetti terzi potrebbe recare danno alla società;

produrre, detenere, diffondere, in qualsiasi forma e modo, materiale pornografico, pedopornografico, di propaganda od istigazione a fini terroristici, ovvero offensivo dell’onore o dignità di terzi;

violare registri ed archivi informatici della società e/o falsificare dati, informazioni o documenti informativi di qualsiasi specie;

comunicare a terzi, cedere, trasmettere rendere noto o mettere a disposizione, in qualsiasi forma o modo, e a qualunque titolo, password di accesso a sistemi informatici della società o di terzi dei quali i destinatari della procedura siano in possesso in ragione dell’attività svolta;

porre in essere una delle condotte previste dall’art. 24bis d. lgs. 231/2001 ovvero anche altra condotta strumentale alle medesime.

- L’accesso a sistemi informatici di soggetti esterni alla Società (a titolo d’esempio la P.A.) è limitato ai soli utenti a ciò espressamente autorizzati attraverso l’attribuzione di specifici codici di accesso. Costoro sono tenuti a mantenere strettamente riservate, non divulgare e conservare al sicuro ed al riparo da atti di impossessamento o appropriazione le chiavi di accesso ai predetti sistemi;

- Nei casi di cessazione dei rapporti con la società, ovvero di cambio di mansioni dell’utente, le password e gli user-ID relativi ai sistemi informatici della società sono revocati; la società si fa inoltre carico di avvisare gli enti esterni dei quali l’utente sia in possesso di password e User-Id per conto della Società. La verifica del rispetto delle regole sopra elencate è delegata ad un consulente, che effettuerà controlli periodici producendo un apposito report per l’ Organismo di Vigilanza.

1. **PRINCIPI GENERALI DI COMPORTAMENTO**

I Principi generali di controllo possono essere sintetizzati come segue:

- Esistenza di procedure/norme/circolari: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.

- Poteri autorizzativi e di firma: i poteri autorizzativi e di firma devono:

i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l’indicazione delle soglie di approvazione delle spese;

ii) essere chiaramente definiti e conosciuti all’interno della Società.

Formazione: verrà programmato un corso di formazione sulla sicurezza informatica e sull’utilizzo dei sistemi informatici e ove saranno sensibilizzati i valori etici e morali nell’uso di sistemi informatici riepilogati nel presente documento.

1. **I CONTROLLI DELL’ODV**

I controlli dell’O.d.V. consistono in un’attività di analisi dei rischi reato ex D.Lgs. 231/2001 secondo quanto previsto nel presente Modello Organizzativo. A tal fine, all’O.d.V. viene garantito libero accesso a tutta la documentazione aziendale rilevante. Inoltre, l’O.d.V. può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella “Parte Generale”. Durante la propria attività l’ODV dovrà mantenere la massima discrezione e riservatezza avendo come unici referenti gli Organi Sociali di cui alla “Parte Generale”.