Protocollo Reati Informatici
Allegato modello organizzativo 231/2001

Principi procedurali specifici
Principi procedurali da osservare nelle singole operazioni a rischio

Si indicano di seguito i principi procedurali che in relazione ad ogni singola Area a Rischio gli Esponenti Aziendali sono tenuti a rispettare e che, ove opportuno, devono essere implementati in specifiche procedure aziendali ovvero possono formare oggetto di comunicazione da parte del ODV:

1. si deve richiedere l'impegno dei Partner, Fornitori e parti terze al rispetto degli obblighi di legge in tema di Reati Informatici;

2. la selezione delle controparti destinate a fornire i servizi di **I.T.** (*Information Thecnology*), siano essi Partner, Fornitori o parti terze deve essere svolta con particolare attenzione e in base ad apposita procedura interna.
In particolare, l'affidabilità di tali Partner o Fornitori e parti terze deve essere valutata, ai fini della prevenzione dei Reati di cui anche attraverso specifiche indagini *ex ante*;

3. deve essere rispettata da tutti gli Esponenti Aziendali la previsione del Codice etico diretta a vietare comportamenti tali che siano in contrasto con la prevenzione dei Reati informatici contemplati ;

4. nel caso in cui l'Odv riceva segnalazioni di violazione delle norme del Decreto da parte degli Esponenti Aziendali e/o Collaboratori Esterni, è tenuta ad intraprendere le iniziative più idonee per acquisire ogni utile informazione al riguardo;

5. in caso persistano dubbi sulla correttezza di comportamenti dei Collaboratori Esterni, l'ODV emetterà una raccomandazione per il Comitato di Controllo e/o per gli Organi Direttivi delle Società interessate.

Rapporti con parti terze
Nei contratti con i Consulenti, i Partner i Fornitori e parti terze deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché del Modello.

Gli Organi di *Governance* devono aver adottato e fatto adottare da tutte le Unità Operative le necessarie procedure per prevenire la commissione dei reati sotto elencati:

• Accesso abusivo ad un sistema informatico e telematico (Art. 615-ter c.p.)

• Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (Art. 615 quater c.p.)

• Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (Art. 615 quinquies c.p.)

• Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617 quater c.p.)

• Installazione di apparecchiature o soppressione di contenuto di comunicazioni informatiche o telematiche (Art. 617 quinquies c.p.)

Danneggiamento di sistemi informatici e telematici (Art. 635 bis c.p)

• Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilita` (Art. 635 ter c.p)

• Danneggiamento di sistemi informatici o telematici di cui (Art. 635 quarter c.p)

• Danneggiamento di sistemi informatici o telematici di pubblica utilita`(Art. 635 quinquies c.p

• Frode informatica del soggetto che presta servizi di certificazione di firma elettronica(art. 640 quinquies c.p)

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

Ci si riferisce a comportamenti posti in essere da amministratori, dirigenti e dipendenti operanti nelle aree di attività a rischio nonché da Collaboratori esterni e Partner, come già definiti nella Parte Generale (qui di seguito, tutti definiti i “Destinatari”).
In via generale, a tali soggetti è richiesto di:

non 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);
non violare i principi e le procedure aziendali previste nella presente parte speciale;
non porre in essere comportamenti in contrasto con leggi e regolamenti in materia di protezione e sicurezza di dati personali e sistemi informatici (in particolare, Codice in materia di protezione dei dati personali; provvedimenti del Garante della Privacy, ecc.).

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

a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;
b) accedere abusivamente al sistema informatico o telematico di soggetti pubblici o privati;
c) accedere abusivamente al proprio sistema informatico o telematico al fine alterare e /o cancellare dati e/o informazioni;
d) 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;
e) 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;
f) 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;
g) 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;
h) istallare apparecchiature per l’intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;

i) svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;
j) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
k) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i collaboratori e dipendenti indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. non prestare o cedere a terzi qualsiasi apparecchiatura informatica;
3. segnalare alle funzioni competenti il furto, il danneggiamento o lo smarrimento di tali strumenti; inoltre, qualora si verifichi un furto o si smarrisca un'apparecchiatura informatica di qualsiasi tipo, l'interessato, o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire alla funzione competente l'originale della denuncia all'Autorità di Pubblica Sicurezza;
4. evitare di introdurre e/o conservare in Società (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;
5. evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC;
7. evitare l'utilizzo di passwords di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi;
8. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
9. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
10. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
11. impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;
12. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
13. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
14. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
15. astenersi dall'utilizzare gli strumenti informatici per il collegamento a chat, social network, (facebook, instagram, whatsapp etc..)
15. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici

Il sistema dei controlli, adattato dalla Società prevede, con riferimento alle singole aree a rischio individuate, una serie di protocolli di controllo di seguito descritti e applicabili a tutte le aree a rischio − deve essere formalizzata una politica in materia di sicurezza del sistema informativo che preveda, fra l'altro:

− le modalità di comunicazione anche a terzi;

− le modalità di riesame della stessa, periodico o a seguito di cambiamenti significativi.

− deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici. − deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità per l'identificazione e la classificazione degli assets aziendali (ivi inclusi dati e informazioni).

− deve essere adottato e attuato uno strumento normativo che assicuri la correttezza e la sicurezza dell'operatività dei sistemi informativi tramite policy e procedure.

In particolare, tale strumento normativo deve assicurare:

il corretto e sicuro funzionamento degli elaboratori di informazioni;
la protezione da software pericoloso;
il backup di informazioni e software;
la protezione dello scambio di informazioni attraverso l'uso di tutti i tipi di strumenti per la comunicazione anche con terzi;
gli strumenti per effettuare la tracciatura della attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza;
il controllo sui cambiamenti agli elaboratori e ai sistemi;
la gestione di dispositivi rimovibili.
− deve essere adottato e attuato uno strumento normativo che disciplini i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell'efficienza ed efficacia del sistema di gestione della sicurezza informatica. − deve essere adottato e attuato uno strumento normativo che preveda:

la valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;
specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi;
l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, token di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
la destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta.

Con riferimento all'attività di gestione dei profili utente e del processo di autenticazione la Società si conforma ai seguenti principi di controllo:

− deve essere adottato e attuato uno strumento normativo che disciplini gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. In particolare, tale strumento normativo deve prevedere:

l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;

l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;
la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati;
i piani e le procedure operative per le attività di telelavoro.

− deve essere adottato e attuato uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tale strumento normativo deve prevedere:

appropriati canali gestionali per la comunicazione degli Incidenti e Problemi;
l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause;
la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;
l'analisi di report e trend sugli Incidenti e sui Problemi e l'individuazione di azioni preventive;
appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;
l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;
l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;
la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi workaround e le soluzioni definitive, identificate o implementate;
la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa.
− deve essere adottato e attuato uno strumento normativo che preveda l'implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche. − deve essere adottato e attuato uno strumento normativo che definisca:

l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
la confidenzialità, autenticità e integrità delle informazioni;
la sicurezza nel processo di sviluppo dei sistemi informativi.
Con riferimento all'attività di gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio la Società si conforma ai seguenti principi di controllo:

− deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi. − deve essere adottato e attuato uno strumento normativo che definisca:

l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;

la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
la confidenzialità, autenticità e integrità delle informazioni;
la sicurezza nel processo di sviluppo dei sistemi informativi.

Con riferimento all'attività di gestione degli accessi da e verso l'esterno la Società si conforma ai seguenti principi di controllo:

− deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi. − deve essere adottato e attuato uno strumento normativo che disciplini gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. In particolare, tale strumento normativo deve prevedere:

l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle

applicazioni aziendali;
la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati;
i piani e le procedure operative per le attività di telelavoro.

− deve essere adottato e attuato uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tale strumento normativo deve prevedere:

appropriati canali gestionali per la comunicazione degli Incidenti e Problemi;
l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause;
la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;
l'analisi di report e trend sugli Incidenti e sui Problemi e l'individuazione di azioni preventive;
appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;
l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;
l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;

la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi workaround e le soluzioni definitive, identificate o implementate;
la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa.
− deve essere adottato e attuato uno strumento normativo che preveda l'implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche. − deve essere adottato e attuato uno strumento normativo che definisca:

l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
la confidenzialità, autenticità e integrità delle informazioni;
la sicurezza nel processo di sviluppo dei sistemi informativi.

Con riferimento all'attività di gestione e protezione delle reti la Società si conforma ai seguenti principi di controllo:

− deve essere adottato e attuato uno strumento normativo che definisca i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi.

− deve essere adottato e attuato uno strumento normativo che disciplini gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni. In particolare, tale strumento normativo deve prevedere:

l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura;
le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
una procedura di registrazione e deregistrazione per accordare e revocare l'accesso a tutti i sistemi e servizi informativi;
la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti usando un processo formale;
la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto che attribuiva il diritto di accesso;
l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete;
la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi delle applicazioni aziendali;
la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
la custodia dei dispostivi di memorizzazione (ad es. chiavi USB, CD, hard disk esterni, etc.) e l'adozione di regole di clear screen per gli elaboratori utilizzati;
i piani e le procedure operative per le attività di telelavoro.
− deve essere adottato e attuato uno strumento che definisca adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. In particolare, tale strumento normativo deve prevedere:

appropriati canali gestionali per la comunicazione degli Incidenti e Problemi;
l'analisi periodica di tutti gli incidenti singoli e ricorrenti e l'individuazione della root cause;

la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva;
l'analisi di report e trend sugli Incidenti e sui Problemi e l'individuazione di azioni preventive;
appropriati canali gestionali per la comunicazione di ogni debolezza dei sistemi o servizi stessi osservata o potenziale;
l'analisi della documentazione disponibile sulle applicazioni e l'individuazione di debolezze che potrebbero generare problemi in futuro;
l'utilizzo di basi dati informative per supportare la risoluzione degli Incidenti;
la manutenzione della basi dati contenente informazioni su errori noti non ancora risolti, i rispettivi workaround e le soluzioni definitive, identificate o implementate;
la quantificazione e il monitoraggio dei tipi, dei volumi, dei costi legati agli incidenti legati alla sicurezza informativa.
− deve essere adottato e attuato uno strumento normativo che preveda l'implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche. − deve essere adottato e attuato uno strumento normativo che definisca:

l'identificazione di requisiti di sicurezza in fase di progettazione o modifiche dei sistemi informativi esistenti;
la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
la confidenzialità, autenticità e integrità delle informazioni;
la sicurezza nel processo di sviluppo dei sistemi informativi.

Con riferimento all'attività di gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD) (e.6) la Società si conforma ai seguenti principi di controllo:

Deve essere adottato e attuato uno strumento normativo che preveda:
l'implementazione e lo sviluppo sull'uso dei controlli crittografici per la protezione delle informazioni e sui meccanismi di gestione delle chiavi crittografiche.

Detto Protocollo sarà divulgato a tutti i destinatari di tutte le unità operative.

19.06.2015