PROTOCOLLO VI

GESTIONE DEI SISTEMI INFORMATIVI

EDIZIONE APPROVATA CON DELIBERA DEL CONSIGLIO DI AMMINISTRAZIONE DI IGS DEL 28.07.2020

INDICE

PROTOCOLLO VI

1. PREMESSA

Nell'ambito del processo **Gestione dei sistemi informativi**, il presente documento ha quale principale obiettivo definire:

- i profili di rischio-reato;
- le attività sensibili (cosi come definite nella Parte Generale);
- i principi di controllo e di comportamento che i Destinatari devono osservare al fine di applicare correttamente le prescrizioni del Modello.

2. PROFILI DI RISCHIO REATO

Si riportano di seguito i reati potenzialmente rilevanti con riguardo al processo **Gestione dei sistemi informativi**:

Reati contro la Pubblica Amministrazione ed il suo patrimonio (Art. 24 del Decreto)

- Frode informatica (Art. 640-t*er* c.p.)

Delitti informatici e trattamento illecito di dati (Art. 24-*bis* del Decreto)

- Accesso abusivo ad un sistema informatico o telematico (Art. 615-*ter* c.p.)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-*quater* c.p.)
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617-*quinquies* c.p.)
- Danneggiamento di informazioni, dati e programmi informatici (Art. 635-*bis* c.p.)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635-*ter* c.p.)
- Danneggiamento di sistemi informatici o telematici (Art. 635-*quater* c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-*quinquies* c.p.)
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615-*quater* c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615-*quinquies* c.p.)
- Documenti informatici (Art. 491-*bis* c.p.)
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640-*quinquies* c.p.)

Reati in materia di violazione del diritto d'autore (Art. 25-*novies* del Decreto)

- Tutela penale del software e delle banche dati (Art. 171-*bis*, comma 1, L. 22 aprile 1941, n. 633)

Si rimanda all'Allegato A "I reati e gli illeciti amministrativi rilevanti ai sensi del D.Lgs.231/2001" per una descrizione completa ed esaustiva delle sopra elencate fattispecie.

3. ATTIVITÀ SENSIBILI

Si riportano di seguito le attività sensibili che possono essere svolte nell'ambito del processo in oggetto e nell'ambito delle quali, potenzialmente, potrebbero essere commessi i reati di cui al precedente paragrafo:

- Gestione dei sistemi informativi

4. PRINCIPI DI CONTROLLO E DI COMPORTAMENTO

Di seguito sono elencati alcuni dei principi di carattere generale da considerarsi applicabili ai Destinatari del presente Modello, come definiti nella Parte Generale.

In generale, è fatto divieto di porre in essere comportamenti o concorrere alla realizzazione di condotte che possano rientrare nelle fattispecie di reato innanzi indicate; sono altresì proibite le violazioni ai principi ed alle regole previste nel Codice Etico.

In particolare:

Con riferimento all'attività sensibile "Gestione dei sistemi informativi" ai Destinatari è fatto obbligo di:

- garantire che tutte le operazioni svolte nell'ambito dell'attività sensibile in oggetto, e con particolare riferimento – a titolo esemplificato e non esaustivo – nella:
  - gestione degli accessi,
  - gestione dei sistemi di autenticazione
  - gestione delle utenze,
  - gestione dei backup,
  - gestione della sicurezza,
  - gestione di virus e di malware, siano rispettati i principi previsti dal corpo procedurale della Società;
- utilizzare le risorse informatiche assegnate per l'espletamento della propria attività lavorativa, limitando l'utilizzo di internet a fini personali;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- verificare il corretto aggiornamento dei sistemi di protezione antivirus e antispyware e, in caso di non regolare aggiornamento, evitare l'utilizzo della risorsa informatica segnalando il problema al proprio Responsabile;
- assicurare meccanismi di protezione dei file, quali password, conversione dei documenti in formato non modificabile;
- garantire la tracciabilità dei documenti prodotti attraverso l'archiviazione delle varie versioni dei documenti o comunque garantire meccanismi di tracciabilità delle modifiche;
- segnalare tempestivamente all'OdV eventuali situazioni di anomalia e criticità riscontrate.

Ed inoltre, nell'ambito della medesima attività sensibile ai Destinatari è fatto divieto di:

- effettuare il download non controllato o programmato di update o upgrade di applicazioni installate dalla Società;
- effettuare il download di dati non inerenti all'attività lavorativa (musica, ecc.);
- installare applicazioni senza l'autorizzazione della Società;

- alterare documenti elettronici, pubblici o privati, con finalità probatoria;
- accedere, senza averne la autorizzazione, ad un sistema informatico o telematico o trattenersi contro la volontà espressa o tacita di chi ha diritto di escluderlo (il divieto include sia l'accesso ai sistemi informativi interni che l'accesso ai sistemi informativi di enti concorrenti, pubblici o privati, allo scopo di ottenere informazioni su sviluppi commerciali o industriali);
- procurarsi, riprodurre, diffondere, comunicare, ovvero portare a conoscenza di terzi codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure nel fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui protetto da misure di sicurezza;
- procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici 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, l'alterazione del suo funzionamento (il divieto include la trasmissione di virus con lo scopo di danneggiare i sistemi informativi di enti concorrenti);
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici (il divieto include l'intrusione non autorizzata nel sistema informativo di società concorrente, con lo scopo di alterare informazioni e dati di quest'ultima);
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui o di pubblica utilità o di ostacolarne gravemente il funzionamento;
- installare software/programmi aggiuntivi rispetto a quelli esistenti e/o autorizzati dalla Società;
- porre in essere, nell'ambito delle proprie attività lavorative e/o mediante utilizzo delle risorse della Società, comportamenti di qualsivoglia natura atti a ledere diritti di proprietà intellettuale altrui;
- introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita o comunque mettere in circolazione - al fine di trarne profitto - beni/opere realizzati usurpando il diritto d'autore o brevetti di terzi;
- diffondere - tramite reti telematiche - un'opera dell'ingegno o parte di essa;
- duplicare, importare, distribuire, vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale - o comunque per trarne profitto - programmi per elaboratori, banche dati, opere a contenuto letterario, musicale, multimediale, cinematografico, artistico per i quali non siano stati assolti gli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi al suo esercizio.