PROTOCOLLO VII

GESTIONE DEI SISTEMI INFORMATIVI

EDIZIONE APPROVATA CON DELIBERA DEL CONSIGLIO DI AMMINISTRAZIONE DI IGS DEL 26 SETTEMBRE 2024

INDICE

PROTOCOLLO VII

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.

***

Stante la potenziale ed astratta configurabilità, tra le altre, di fattispecie corruttive (cfr. infra) nell'ambito del processo *de quo*, la Società ha inteso dotarsi di un Sistema di gestione per la Prevenzione della Corruzione (il "**SGAC**"), secondo lo standard internazionale ISO 37001:2016 "Sistemi di gestione per la prevenzione della corruzione". I presidi contenuti nella documentazione componente il SGAC, si intendono qui integralmente richiamati e costituiscono, insieme con i principi di comportamento di cui al presente Protocollo di Parte Speciale, presidio che la società ha inteso porre a prevenzione dei reati contro la pubblica amministrazione. Per maggiore dettaglio, si rinvia al capitolo 3.5 della Parte Generale, nonché ai singoli documenti componenti il SGAC.

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 (Artt. 24 e 25 del Decreto)
- Delitti informatici e trattamento illecito di dati (Art. 24-*bis* del Decreto)
- Reati in materia di violazione del diritto d'autore (Art. 25-*novies* del Decreto)

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

La **Gestione dei sistemi informativi** nel suo complesso è stata individuata quale attività sensibile che può essere svolta nell'ambito del processo in oggetto e nell'ambito della quale, potenzialmente, potrebbero essere commessi i reati di cui al precedente paragrafo.

4. PRINCIPI DI CONTROLLO E DI COMPORTAMENTO

4.1. Principi generali 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.

Inoltre, ai Destinatari è fatto divieto di alterare documenti elettronici, pubblici o privati, con finalità probatoria.

I Destinatari sono tenuti all'applicazione delle best practices in materia di sicurezza informatica come di volta in volta riflesse nelle procedure interne della Società.

I Destinatari debbono altresì segnalare tempestivamente all'OdV eventuali situazioni di anomalia e criticità riscontrate.

4.2 Principi specifici di comportamento e controllo

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:

(i) gestione degli accessi,
(ii) gestione dei sistemi di autenticazione,
(iii) gestione delle utenze,
(iv) gestione dei backup,
(v) gestione della sicurezza,
(vi) 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, nel rispetto delle policies e delle procedure aziendali;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- assicurare, ricorrendo anche al supporto delle funzioni aziendali competenti, il corretto aggiornamento dei sistemi di protezione antimalware 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, e conversione dei documenti in formato non modificabile, laddove sia tecnicamente possibile senza impattare l'operatività e/o compromettere la conduzione delle attività che richiedono la fruizione di tali file/documenti, e limitatamente ai casi in cui le informazioni contenute siano considerate dall'azienda "riservate";
- assicurare meccanismi di blocco in automatico dal sistema che impediscono l'installazione di software/ programmi aggiuntivi non autorizzati;
- assicurare l'utilizzo di utenze di dominio profilate;
- assicurare, di regola, meccanismi di single sign-on a copertura dei sistemi aziendali;
- prevedere l'adozione di politiche di sicurezza sulla password che ne prevedono il cambio periodico da parte dell'utente;
- prevedere un processo tracciabile di profilazione degli utenti sui sistemi informatici e sul gestionale aziendale, a seconda del ruolo;
- garantire la tracciabilità, mediante apposita piattaforma informatica, di tutte le dotazioni IT date in uso ai dipendenti, con indicazione del relativo assegnatario;
- incentivare la diffusione della cultura aziendale della legalità anche con riferimento ai rischi legati alla commissione di reati informatici sui sistemi informativi propri di IGS e di terzi.

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

- effettuare autonomamente / in modo non controllato il download di update o upgrade di applicazioni installate dalla Società;
- effettuare il download o installare applicazioni senza le adeguate autorizzazioni o in violazione della normativa interna applicabile;
- installare software/programmi aggiuntivi senza le autorizzazioni o al di fuori della normativa interna della Società.