Modello di organizzazione, gestione e controllo

ai sensi del Decreto Legislativo 8 Giugno 2001, n. 231

PROTOCOLLO 06

GESTIONE SISTEMI INFORMATIVI

INDICE

1. SCOPO

Il presente protocollo ha lo scopo di presidiare le aree di attività aziendali a rischio-reato nell'ambito della gestione dei sistemi informativi di Vetrerie Meridionali S.p.a. (di seguito anche "Ve.Me" o la "Società").
Coerentemente con la Parte Generale del Modello organizzativo ai sensi del D.Lgs. 231/2001, il documento definisce le linee guida comportamentali nonché i presidi operativi di controllo cui tutti i Destinatari, quali amministratori, dipendenti e/o collaboratori (ivi inclusi eventuali *partner* e/o consulenti esterni incaricati) della Società, si attengono nello svolgimento della propria attività al fine di prevenire o mitigare il rischio di commissione dei seguenti reati presupposto:

- i reati informatici di cui all'art. 24-*bis* del D.Lgs. 231/2001 (di seguito anche il "Decreto");
- i reati in violazione del diritto d'autore di cui all'art. 25-*novies* del Decreto;

Il protocollo, redatto in conformità alle previsioni del D.Lgs. 231/2001, costituisce, pertanto, parte integrante del Modello previsto dal Decreto medesimo.

2. DESTINATARI E AMBITO DI APPLICAZIONE

Il presente protocollo si applica ai responsabili delle Funzioni, ai loro diretti riporti gerarchici, nonché a qualsiasi soggetto che risulti a vario titolo coinvolto nella seguente Attività sensibile:

- *Gestione dei sistemi informativi.*

3. RIFERIMENTI

- D.Lgs. 231/2001 "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*";
- Modello organizzativo ai sensi del D.Lgs. 231/2001 – Parte Generale;
- Codice Etico di Vetrerie Meridionali S.p.A.;
- Procedura per il conferimento di procure e deleghe;
- Mansionari;
- Contratto intercompany con la Società del Gruppo O-I Italy S.p.A. relativo alla messa a disposizione di licenze software, di strumentazione informatica e di assistenza informatica.

4. DEFINIZIONI

- **Modello 231 o Modello**: modello organizzativo adottato dalla Società ai sensi del D.Lgs. 231/2001.
- **Organismo di Vigilanza o OdV**: l'organismo, interno all'ente, dotato di autonomi poteri di iniziativa e di controllo, che, ai sensi dell'art. 6 del Decreto, ha il compito di vigilare sul funzionamento e l'osservanza del modello di organizzazione, gestione e controllo e di curarne l'aggiornamento.

5. PRINCIPI GENERALI DI COMPORTAMENTO

I Destinatari a qualsiasi titolo coinvolti nella gestione dei sistemi informativi in ordine agli ambiti di applicazione sopra richiamati sono tenuti a osservare, oltre alle previsioni del presente protocollo, le norme di legge applicabili, i principi di condotta previsti nel Codice Etico di Ve.Me., nonché i principi previsti nella Parte Generale del Modello e nei relativi regolamenti aziendali sull'utilizzo degli strumenti informatici.

È fatto **divieto** di:

- porre in essere comportamenti tali da integrare le fattispecie delittuose di cui agli artt. 24-*bis* (Delitti informatici e trattamento illecito dei dati) e 25-*novies* (delitti in materia di violazione del diritto d'autore) del Decreto;
- porre in essere comportamenti che, sebbene non integranti le fattispecie delittuose di cui sopra o non diretti alla commissione delle stesse, potrebbero potenzialmente diventarlo;
- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza;
- accedere a un sistema informatico o telematico non possedendo le credenziali d'accesso o utilizzando le credenziali di altri colleghi abilitati;
- detenere, procurarsi o diffondere abusivamente codici di accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- utilizzare dispositivi tecnici o *software* non autorizzati e/o atti a impedire o interrompere le comunicazioni relative a un sistema informatico o telematico;
- distruggere, danneggiare, cancellare, alterare informazioni, dati o programmi informatici altrui e di pubblica utilità;
- utilizzare *software* non fornito sul proprio supporto originale o comunque dal soggetto detentore dei diritti d'autore relativi allo stesso, nonché in numero superiore alle licenze acquistate dalla Società;
- riprodurre, diffondere o comunque mettere a disposizione di altri *software* senza il consenso del soggetto detentore dei diritti d'autore relativi allo stesso;
- lasciare incustodito e/o accessibile ad altri il PC assegnato dalla Società.

È fatto **obbligo** ai Destinatari di attenersi alle seguenti prescrizioni:

- informare tempestivamente il responsabile dell'ufficio di appartenenza in caso di smarrimento o furto delle attrezzature informatiche aziendali;
- attenersi alle *policy* adottate dalla Società che disciplinano l'utilizzo dei sistemi e degli applicativi informatici della Società stessa.

6. PRESIDI DI CONTROLLO SPECIFICI PER ATTIVITÀ SENSIBILE

6.1. Gestione dei sistemi informativi

Vengono illustrati di seguito i principi specifici delineati con riferimento all'Attività sensibile in oggetto e relative sotto-attività:

Gestione degli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni

- la concessione, variazione e rimozione degli accessi, interni ed esterni, ai sistemi informativi della Società è gestita secondo un iter definito e formalizzato ed è eseguita dal reparto IT della Società del Gruppo O-I Italy S.p.A., su indicazione di VE.ME, e in virtù di un contratto; il processo prevede l'utilizzo di appositi tool di *onboarding/offboarding*/modifica.
- ogni richiesta di accesso ai sistemi informativi della Società e/o modifica dei permessi di accesso deve essere trasmessa via mail dal Responsabile della funzione competente e viene autorizzata dal Direttore di Stabilimento o dal Responsabile Amministrativo o dal Responsabile dell'Ufficio del Personale per le aree di propria competenza.
- Il processo di *onboarding* ed *offboarding* è coordinato dal Responsabile dell'Ufficio del Personale.

Gestione e protezione logica e fisica della postazione di lavoro

- l'accesso alle postazioni di lavoro è regolato da un sistema di password impostate secondo precise regole di gestione e complessità;
- le postazioni di lavoro sono dotate di meccanismi di controllo (ad es. meccanismi di log out automatico, standby per inattività) al fine di evitare accessi non autorizzati;
- l'infrastruttura è situata in un locale chiuso, all'interno di un'area ad accesso controllato a mezzo password.

Gestione del processo di assegnazione e dismissione degli asset IT, siano essi software (ad es. licenze) o hardware

- ogni richiesta di dismissione degli asset viene autorizzata dal Direttore di Stabilimento
- ogni richiesta di assegnazione degli asset viene autorizzata dal Direttore di Stabilimento o dal Responsabile Amministrativo o dal Responsabile dell'Ufficio del Personale per le aree di propria competenza, fermo restando che la prima assegnazione (in occasione di assunzione), rientrante nel processo di onboarding, è coordinata dal Responsabile dell'Ufficio del Personale

Gestione del processo di classificazione e controllo dei beni (sia hardware sia software)

- gli asset IT sono assegnati su richiesta dei Responsabili delle funzioni aziendali competenti di Ve.Me., che segnalano il fabbisogno a O-I Italy S.p.A.;

- la messa a disposizione e manutenzione degli asset IT è a cura di O-I Italy S.p.A., in virtù di un contratto;
- O-I Italy S.p.A. aggiorna annualmente un elenco delle apparecchiature e delle licenze software fornite, predisponendo un apposito documento.

Gestione delle comunicazioni e dell'operatività (scambio di informazioni, log management, patch management, politiche di backup, ecc.), Gestione e protezione delle reti, Gestione degli incidenti e dei problemi di sicurezza informatica, Gestione del processo di acquisizione, sviluppo e manutenzione di apparecchiature, dispositivi o programmi informatici

- Il reparto IT di O-I Italy S.p.A. gestisce l'operatività dei sistemi tra cui la definizione delle backup policy, ivi comprese le modalità di conservazione delle copie di backup;
- sono installati sistemi di sicurezza perimetrale (firewall) e software antivirus, rilasciate e distribuite centralmente dal reparto IT di O-I Italy S.p.A.;
- la gestione degli incidenti di sicurezza informatica è effettuata secondo un iter strutturato, gestito dal reparto IT di O-I Italy S.p.A.;
- il processo di acquisizione, sviluppo e manutenzione di apparecchiature, dispositivi o programmi informatici è a cura di O-I Italy S.p.A., che, su richiesta di VE.ME, seleziona il fornitore, stipula i contratti e monitora la corretta esecuzione del contratto;
- le ulteriori procedure di sicurezza vengono definite ed espletate dal reparto IT di O-I Italy S.p.A., in virtù di un contratto intercompany.

7. ARCHIVIAZIONE

Tutta la documentazione prodotta nell'ambito delle attività disciplinate nel presente Protocollo, comprese eventuali comunicazioni a mezzo posta elettronica, è conservata a cura della funzione competente e messa a disposizione, su richiesta, del Consiglio di Amministrazione, del Collegio Sindacale e dell'Organismo di Vigilanza.