MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D. LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE B REV.02

REATI INFORMATICI (ART. 24 BIS)

APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE IL 26/03/2020

ISSELNORD S.R.L.

SEDE LEGALE IN VIA TRIESTE, 4 19020 FOLLO (SP)

ISCRIZIONE AL REGISTRO DELLE IMPRESE DI LA SPEZIA

P.IVA 00861600112

Data e firma di redazione DGE	Data e firma di approvazione ADE
18/02/2020	25/02/2020

LE FATTISPECIE DI REATO RILEVANTI

La presente Parte Speciale si riferisce ai reati informatici, richiamati dall'art. 24 bis del D. Lgs.231/2001, ed in particolare riporta le singole fattispecie di reato considerate rilevanti per la responsabilità amministrativa di ISSELNORD S.r.l. Individua inoltre le cosiddette attività "sensibili" (quelle dove è teoricamente possibile la commissione del reato e che sono state individuate nell'ambito dell'attività di *risk assessment*) specificando i principi comportamentali ed i presidi di controllo operativi per l'organizzazione, lo svolgimento e la gestione delle operazioni svolte nell'ambito delle sopracitate attività "sensibili".

In considerazione dell'analisi dei rischi effettuata, è risultato potenzialmente realizzabile nel contesto aziendale di ISSELNORD S.r.l. il seguente reato:

Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491 bis c.p.)

L'articolo in oggetto stabilisce che se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

La norma conferisce valenza penale alla commissione di reati di falso attraverso l'utilizzo di documenti informatici.

IDENTIFICAZIONE DELLE ATTIVITA' A RISCHIO REATO

Le attività che la Società ha individuato come sensibili, nell'ambito dei delitti informatici, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato.

Tali attività sono di seguito riepilogate:

1. Gestione accesso ai sistemi informatici aziendali (Attività inserita in via prudenziale);

2. Gestione credenziali d'accesso (Attività inserita in via prudenziale);

3. Gestione della sicurezza fisica e logica dei dati (Attività inserita in via prudenziale)

Data e firma di redazione DGE	Data e firma di approvazione ADE
18/02/2020	25/02/2020

PRINCIPI GENERALI DI COMPORTAMENTO

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D. Lgs.231/2001 e al Codice Etico, tutti i Destinatari del Modello che, a qualunque titolo, siano stati designati o incaricati a svolgere le attività d'azienda (progettazione, vendita, realizzazione, manutenzione, riciclaggio, riparazione di apparecchiature, impianti e sistemi; realizzazione e commercializzazione di applicazioni *software*), sono tenuti ad osservare i seguenti principi di comportamento e controllo:

- Il personale non può utilizzare i sistemi informatici (come attrezzature, dispositivi e strutture aziendali) per necessità personali o per scopi contrari a norme di legge, all'ordine pubblico, buon costume e deve astenersi da qualsiasi condotta che possa compromettere la riservatezza e l'integrità delle informazioni e dei dati aziendali e dei terzi ed in particolare si premura di non lasciare incustoditi i propri sistemi informatici e bloccarli, qualora si allontani dalla postazione di lavoro, con i propri codici di accesso ovvero di spegnere il computer e tutte le periferiche al termine del turno di lavoro;
- Il personale è tenuto a conservare, custodire e salvaguardare i beni aziendali, impedendo l'utilizzo degli stessi in modo non conforme all'interesse sociale;
- Il personale non può assumere comportamenti che possano danneggiare, alterare, deteriorare o distruggere i sistemi informatici o telematici, i dati informatici delle Società e/o di terzi, nonché interrompere o intercettare comunicazioni informatiche o telematiche anche tra terzi in modo illecito, installando, ad esempio, programmi senza aver preventivamente informato la funzione aziendale preposta alla gestione della sicurezza informatica;
- tutti coloro a cui sono state assegnate *password* e chiavi di accesso alla rete aziendale e alle diverse applicazioni sono tenuti a custodirle in modo idoneo con l'obiettivo di impedirne una facile identificazione ed un uso improprio.
- il personale non può utilizzare connessioni alternative rispetto a quelle fornite dalla Società nell'espletamento dell'attività lavorativa resa in suo favore.

PROCEDURE DI CONTROLLO

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati informatici, con particolare riferimento al processo strumentale alla commissione dei reati quale la gestione della dell'infrastruttura tecnologica.

In particolare tali principi trovano specifica attuazione nelle procedure adottate dalla Società.

Procedura ICT

- il personale accede al sistema informativo aziendale unicamente attraverso il profilo identificativo assegnato, attraverso user ID e password strutturate sulle base di un adeguato livello di complessità;
- sono predisposti idonei controlli/monitoraggi sulla rete informatica aziendale al fine di individuare comportamenti anomali o attività eccezionali dei server al di fuori degli orari di operatività sociale e predisposizione di adeguate difese/protezioni fisiche dei server stessi al fine di prevenire l'ingresso e l'uscita di materiale o di personale non autorizzati;
- è previsto un regolamento interno che regoli l'utilizzo della strumentazione tecnologica (e.g. laptop, telefoni) concessa in dotazione al personale della Società;
- è garantita la protezione dei sistemi informatici aziendali, al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare, impedire, interrompere o danneggiare le comunicazioni e/o i dati relativi ad un sistema informatico o telematico di terzi;
- sono definiti controlli di individuazione, prevenzione e ripristino al fine di proteggere da software dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema;
- sono definiti formalmente i requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;
- sono definiti i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- la funzione aziendale preposta alla gestione della sicurezza informatica deve definire i criteri e le modalità per la gestione del processo di dismissione delle utenze cessate;
- sono definiti e regolamentati gli accessi fisici alle sale server aziendali;
- gli amministratori di sistema sono muniti di proprie credenziali di autenticazione e gli accessi sugli applicativi aziendali sono adeguatamente tracciati su log, nel rispetto delle disposizioni del Garante;
- le applicazioni tengono traccia delle modifiche, compiute dagli utenti, ai dati ed ai sistemi;
- il server e i laptop aziendali sono aggiornati periodicamente sulla base delle specifiche necessità; il server e i laptop aziendali sono inoltre protetti da programmi antivirus, aggiornati in modo automatico, contro il rischio di intrusione;
- la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (*firewall* e *proxy*);
- i dispositivi telematici di instradamento sono collocati in aree dedicate e protetti al fine di renderli accessibili al solo personale autorizzato;
- sono previste regole per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi;

- sono definite regole per la navigazione in Internet che includono tra le altre l'utilizzo della rete al solo fine lavorativo, il divieto di scarico di software nelle strutture informative aziendali;
- sono definite regole di utilizzo della posta elettronica, che si riassumono nel divieto d'uso della casella di posta personale per finalità estranee alle esigenze di servizio;
- sono previste soluzioni di *content filtering* a difesa dell'integrità del sistema informatico da potenziali attacchi veicolati in modalità vietata (*malware* tipo *botnet*) e presenza nella postazione lavoro di software antivirus aggiornato.

Data e firma di redazione DGE	Data e firma di approvazione ADE
18/02/2020	25/02/2020