DS TECH S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

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

sulla "Responsabilità Amministrativa delle Imprese"

PARTE SPECIALE V
REATI INFORMATICI

INDICE

1. FINALITÀ

La presente Parte Speciale ha la finalità di definire linee e principi di comportamento che i Destinatari del Modello - come declinati nella Parte Generale - dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività svolte in DS Tech e considerate "a rischio", la commissione dei reati previsti dal Decreto all'art. 24-*bis*, ossia i delitti informatici.

Nello specifico, la presente Parte Speciale del Modello ha lo scopo di:

- indicare le regole che i Destinatari del Modello sono chiamati ad osservare ai fini della corretta applicazione nella gestione delle attività di cui al paragrafo 3 – "*Le attività sensibili rilevanti ai fini del D. Lgs. 231/2001*";
- fornire all'Organismo di Vigilanza e alle altre funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo, verifica.

Nei paragrafi seguenti sono dettagliati:

- le singole fattispecie di reato rilevanti nel contesto aziendale di DS Teche le attività sensibili ai fini del D.lgs. 231/01 - ossia le attività aziendali in cui è teoricamente possibile la commissione degli illeciti previsti dall'art. 24 *bis* del Decreto;
- i principi generali di comportamento, i protocolli di prevenzione e il sistema dei controlli di cui DS Techsi è dotata in riferimento alle attività sensibili rilevate.

2. FATTISPECIE DI REATO RILEVANTI

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente rilevanti per il contesto aziendale della Società i seguenti reati richiamati dall'art. 24 *bis* del D.lgs. 231/01:

A) Delitti informatici (art. 24-bis D.lgs. 231/2001)
   a) Documenti informatici (art. 491-bis c.p.)
   b) Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
   c) Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.)

d) *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-bis c.p.)*
e) *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)*
f) *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)*
g) *Falsificazione. alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617-sexies c.p.)*
h) *Circostanze attenuanti (art. 623-quater c.p.)*
i) *Estorsione (art. 629, comma 3, c.p.)*
j) *Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)*
k) *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.)*
l) *Danneggiamento di sistemi informatici e telematici (art. 635-quater c.p.)*
m) *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1 c.p.)*
n) *Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635-quinquies c.p.)*
o) *Circostanze attenuanti (art. 639-ter c.p.)*
p) *Frode informatica (art. 640-ter c.p.)*
q) *Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)*
r) *Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1 comma 11 D.L. 21 settembre 2019, n. 105 "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica")*

3. LE "ATTIVITÀ SENSIBILI" RILEVANTI AI FINI DEL D.LGS 231/2001

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal Decreto, l'individuazione delle cosiddette "attività sensibili", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

3.1. Le attività sensibili

Le analisi svolte hanno permesso di individuare, con riferimento al rischio di commissione dei reati della presente Parte Speciale, le attività sensibili della Società di seguito elencate:

INF01. Gestione della sicurezza informatica interna

Attività relativa alla gestione dell'infrastruttura ICT aziendale e dell'accesso ai sistemi informativi della Società nonché alle modalità operative seguite per la gestione di banche dati aziendali e documenti elettronici aziendali, pubblici o privati, in modo che siano monitorati gli stati di utilizzo, modifica ed archiviazione dei documenti.

INF02. Gestione e utilizzo delle e-mail e degli strumenti informatici aziendali

Attività relativa alla gestione dell'e-mail e degli altri strumenti informatici.

INF03. Accesso ai sistemi informatici dei clienti

Attività relativa all'accesso ai sistemi informatici dei clienti.

3.2. Il sistema dei controlli

Il sistema dei controlli, adottato da DS Tech, anche sulla base delle indicazioni fornite dalle Linee Guida di Confindustria, prevede con riferimento alle attività sensibili individuate:

a) Principi generali di comportamento, validi per le attività sensibili;
b) Principi di controllo, applicati in maniera specifica ai singoli processi sensibili;

Oltre ai principi di controllo sopra enunciati, la Società può prevedere per un singolo processo sensibile ulteriori presìdi di controllo che garantiscono un monitoraggio più stringente delle attività aziendali svolte.

3.2.1. Principi generali di comportamento

Nello svolgimento delle attività sensibili sopra riportate, è previsto l'espresso obbligo a carico dei Destinatari – in via diretta per gli esponenti aziendali e tramite specifiche clausole contrattuali per i collaboratori esterni ed i *partners* – di osservare i seguenti principi generali di comportamento, definiti in conformità alle previsioni contenute nel Codice Etico.

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello di Organizzazione, Gestione e Controllo;
- Codice Etico;
- procure e deleghe;
- ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto.

La Società richiede:

a) astensione da qualsiasi condotta che possa compromettere la riservatezza e l'integrità delle informazioni e dei dati aziendali e dei terzi;
b) astensione da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informatico aziendale o altrui;
c) di custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
d) di attivare ogni misura ritenuta necessaria per la protezione del sistema, evitando che terzi possano avere accesso allo stesso in caso di allontanamento dalla postazione;
e) l'utilizzo delle risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
f) di utilizzare la rete aziendale in maniera responsabile, evitando l'accesso a siti web non correlati al lavoro e rispettando le politiche aziendali sulla sicurezza informatica;
g) il controllo dell'autenticità del mittente prima di procedere all'apertura dei link e degli allegati ricevuti via e-mail;
h) di segnalare immediatamente al Team IT qualunque attività sospetta relativa a tentativi di attacchi informatici nonché qualunque violazione della presente Parte Speciale del Modello della quale vengano a conoscenza nello svolgimento della propria attività lavorativa.

È responsabilità dei singoli soggetti interessati segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche/integrazioni che si ritenga opportuno apportare alla presente Parte Speciale.

3.2.2. Principi di controllo

I principi di controllo – così come definiti nella Parte Generale – sono l'insieme delle misure di prevenzione e degli strumenti di verificabilità *ex post* adottati dalla Società al fine di presidiare lo svolgimento delle singole attività sensibili e sono descritti in corrispondenza di ciascuna di esse.

In particolare, si tratta di:

- segregazione dei compiti: indicazione dei soggetti aziendali coinvolti nel singolo processo, al fine di garantire indipendenza ed obiettività dello stesso;
- tracciabilità dell'attività: previsione di modalità di archiviazione della documentazione rilevante ai fini della verificabilità *ex post* del processo di svolgimento dell'attività sensibile considerata;
- formalizzazione di deleghe/procure: implementazione di un sistema di poteri di firma e di rappresentanza che sia coerente con le responsabilità organizzative e gestionali assegnate e chiaramente definito e conosciuto all'interno della Società;

- esistenza di procedure/linee guida/prassi operative specifiche: disposizioni aziendali formalizzate o prassi operative idonee a fornire principi di comportamento e modalità operative per lo svolgimento delle attività sensibili;
- ulteriori presìdi che la Società adotta specificamente ad integrazione ed implementazione di quelli sopra elencati.

4. ANALISI DELLE SINGOLE ATTIVITÀ SENSIBILI

INF01. Gestione della sicurezza informatica interna

Principi di controllo:

a) la segregazione delle attività è garantita dal coinvolgimento di più funzioni e soggetti aziendali, tra le quali:
- *CTO*
- *Help Desk*
- *HR*

TENUTA E ARCHIVIAZIONE DELLA DOCUMENTAZIONE AZIENDALE:

b) tutta la documentazione riguardante la Società è in cloud;
c) il CTO ha la funzione di coordinamento e controllo sull'uso degli strumenti informatici;
d) la Società ha adottato un sistema informatico per cui le password relative agli account dei dipendenti e necessarie per accedere ai dati aziendali sono cifrate e accessibili unicamente tramite connessioni sicure.

SICUREZZA DEI DISPOSITIVI INFORMATICI:

e) l'ufficio della Società di Roma è dotato di allarme e il sensore è connesso a una centrale operativa che permette di ottenere un immediato contatto con le Forze dell'Ordine;
f) l'accesso agli uffici della Società avviene attraverso un lettore QR code e ai dipendenti viene comunicato un numero di matricola con chiave asimmetrica per cui il server è in grado di decifrare il numero e così monitorare le entrate e le uscite.

CONTROLLI E TEST:

g) la Società effettua test di phishing nei confronti dei propri dipendenti al fine di migliorare la consapevolezza della sicurezza informatica ed effettua periodicamente sessioni formative;
h) la Società effettua periodicamente controlli sulla sicurezza sui propri server e sta implementando un sistema di controllo centralizzato sui pc dei dipendenti;

i) per l'installazione di nuovi software sui pc aziendali in uso ai dipendenti è necessaria l'autorizzazione dei superiori gerarchici o dell'Help Desk.

INF02. Gestione e utilizzo delle e-mail e degli strumenti informatici aziendali

a) la segregazione delle attività è garantita dal coinvolgimento di più funzioni e soggetti aziendali, tra le quali:
- *Help Desk*
- *Responsabile di Area*

ASSUNZIONE

b) in sede di assunzione la Società valuta la competenza informatica dei candidati. In particolare, agli "sviluppatori" viene sottoposto un questionario apposito e per alcune funzioni aziendali viene chiesta l'elaborazione di un progetto;
c) al momento dell'assunzione, al nuovo dipendente viene consegnato il pc aziendale, un modulo di consegna contenente le prescrizioni relative alle modalità di utilizzo del pc e degli strumenti informatici aziendali con espresso obbligo di utilizzo degli stessi solamente per attività lavorative;
d) al momento dell'ingresso in Società, al nuovo dipendente viene creato un account con una password che deve essere periodicamente aggiornata;
e) l'accesso all'intranet della Società avviene da parte del dipendente con apposite credenziali e limitatamente alla propria area di competenza.

CESSAZIONE DEL RAPPORTO DI LAVORO

f) i dipendenti in smartworking si collegano ai sistemi aziendali attraverso la VPN.
g) nel caso di cessazione di un rapporto di lavoro, la Società provvede a chiudere l'account del dipendente e a chiedere la restituzione della dotazione aziendale;
h) si procede con l'effettuazione di controlli dello stato della dotazione aziendale riconsegnata al momento della cessazione del rapporto di lavoro.

SOFTWARE

i) la Società vieta l'utilizzo di software senza licenza.
j) per l'installazione di nuovi software sui pc aziendali in uso ai dipendenti è necessaria l'autorizzazione dei superiori gerarchici o dell'Help Desk.
k) quando il dipendente ottiene la conferma dell'attivazione della nuova licenza, viene informato altresì delle specifiche regole di comportamento;
l) vi è l'obbligo di disinstallare eventuali software scaricati senza licenza da parte dei dipendenti.

INF03. Accesso ai sistemi informatici dei clienti

a) la segregazione delle attività è garantita dal coinvolgimento di più funzioni e soggetti aziendali, tra le quali:
   - *CTO*
   - *Help Desk*

b) Ds Tech, nello svolgimento della propria attività, sia di sviluppo, sia manutentiva, opera anche sui server dei propri clienti;

c) alcuni clienti della Società prevedono sui propri server appositi sistemi in grado di garantire che l'attività di sviluppo o manutentiva esercitata da parte dei dipendenti di DS tech avvenga su macchine virtuali isolate che impediscano agli stessi di estrapolare o scaricare ulteriori dati dei clienti accedendo così ai sistemi aziendali dello stesso;

d) la Società, quando opera su server di clienti che non prevedono alcun meccanismo di controllo, inserisce nel conferimento dell'incarico al dipendente, apposite prescrizioni circa le modalità e i limiti di accesso ai server dei clienti.

5. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza ha il potere di attivarsi con specifici controlli a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), ma comunque effettua periodicamente controlli a campione sulle attività sociali potenzialmente a rischio di reati al fine di verificare se le suddette attività vengano svolte secondo le regole del Modello e, in particolare, alle procedure interne in essere.

Per il corretto espletamento dei propri compiti, l'OdV ha accesso a tutta la documentazione aziendale rilevante e può convocare per chiarimenti e/o approfondimenti tutti soggetti preposti alle varie attività che riterrà opportuni.