
CAMPUS X s.r.l.

Modello di Organizzazione, Gestione e Controllo

ex D.Lgs. 231/2001

Protocollo 11

Gestione dei sistemi informativi

INDICE

1. SCOPO	3
2. DESTINATARI E AMBITO DI APPLICAZIONE.....	3
3. RIFERIMENTI	3
4. DEFINIZIONI.....	3
5. PRINCIPI GENERALI DI COMPORTAMENTO	3
6. PRESIDI DI CONTROLLO SPECIFICI PER PROCESSO SENSIBILE	4
6.1. Gestione dei sistemi informativi.....	4
7. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA	6
8. ARCHIVIAZIONE.....	6
9. VALUTAZIONE DEL RISCHIO	6

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 condotte dal personale di Campus X s.r.l. (di seguito anche "Campus X" 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 reati presupposto di cui agli artt. 24-*bis* e 25-*novies* del D.Lgs. 231/2001 (di seguito il "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 nel Processo 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;
- Codice Etico;
- Matrice Processi-Reati-Funzioni;
- Procedure relative ai Processi Sensibili.

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 nonché i principi previsti nella Parte Generale del Modello.

È fatto **divieto** di:

- 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. PRESID DI CONTROLLO SPECIFICI PER PROCESSO SENSIBILE

6.1. Gestione dei sistemi informativi

Con riferimento al Processo Sensibile in oggetto:

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;
- periodicamente viene effettuata un'attività di allineamento tra anagrafica dipendenti e database utenti;
- 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) al fine di evitare accessi non autorizzati;

Gestione degli incidenti e dei problemi di sicurezza informatica

- la gestione degli incidenti di sicurezza informatica è effettuata secondo un iter strutturato, definito e formalizzato in apposita procedura;
- la rete della Società è gestita da dal fornitore esterno SMI Technologies and Consulting S.r.l. (sotto supervisione del Technical Department di Campus X). Sono installati sistemi di sicurezza perimetrale (*firewall*) e *software* di *endpoint security*, le cui definizioni sono rilasciate e distribuite centralmente;

Gestione della sicurezza fisica dei centri di elaborazione dati e locali tecnici IT

- ☐ l'accesso fisico ai locali IT è regolamentato da apposita procedura e monitorato, con accesso riservato al solo personale autorizzato. È garantita la presenza di sistemi di sicurezza quali impianto anti-incendio, sistemi di controllo della temperatura, ecc.;

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

- gli asset IT (*hardware* e *software*) sono assegnati e gestiti secondo un iter definito e formalizzato in apposita procedura;
- sono definite delle regole per l'utilizzo delle apparecchiature informatiche e dei *software* aziendali. È in uso un sistema di *asset management* che consente di rilevare gli *hardware* e i *software* installati;

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

- ☐ sono effettuati, anche con il supporto del sistema di *asset management*, inventari degli *hardware* e dei *software* installati e consegnati; viene verificata la regolarità delle licenze possedute;

Gestione delle comunicazioni e dell'operatività (scambio di informazioni, log management, patch management, politiche di backup, ecc.)

- il fornitore esterno SMI Technologies and Consulting S.r.l. (sotto supervisione del Technical Department di Campus X) gestisce l'operatività dei sistemi tra cui la definizione delle backup policy, ivi comprese le modalità di conservazione delle copie di *backup*;

Gestione del processo di acquisizione, sviluppo e manutenzione di apparecchiature, dispositivi o programmi informatici

- ☐ le *change* applicative sono supervisionate dalil fornitore esterno SMI Technologies and Consulting S.r.l. (sotto supervisione del Technical Department di Campus X) secondo un iter strutturato, definito e formalizzato.

La gestione dei controlli applicati al processo è in capo al fornitore esterno SMI Technologies and Consulting S.r.l. (sotto supervisione del Technical Department di Campus X).

Funzioni coinvolte:

- Presidente
- Amministratori Delegati
- Procuratori

- Direttore Finance
- Responsabile Technical Department
- Direttore HR
- Resident Manager

Presidi e Strumenti di controllo esistenti:

- Codice Etico
- ID SMC 03 Gestione delle risposte sui portali
- Procedura inserimento prenotazioni
- ID FO 20 Procedura stampe PROTEL
- Procedura gestione mail front-office
- Procedura processi booking e front-office
- Procedura gestione e rilevazione delle presenze
- Principi generali di comportamento sub 5
- Segregazione di funzioni
- Sistema di procure e deleghe

7. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Il Responsabile identificato trasmette all'Organismo di Vigilanza i flussi informativi individuati dall'apposita procedura, relativa a tutti i Processi Sensibili, con la periodicità prevista dalla Procedura stessa.

8. 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 Sindaco unico/Collegio Sindacale e dell'Organismo di Vigilanza.

I documenti prodotti nell'ambito delle attività descritte nella presente procedura devono essere conservati per un periodo di almeno cinque anni, salvo diverse previsioni legislative.

9. VALUTAZIONE DEL RISCHIO

PROBABILITÀ DI ACCADIMENTO

- Evento accaduto nel settore = Punteggio 1 (Poco probabile)
- Evento già accaduto nella Società = Punteggio 0
- Possibilità di commissione (da analisi esempi di commissione del reato) = Punteggio 2 (Probabile)

Valore Probabilità: $(1+0) \times 2 = 2$

GRAVITÀ

- Sanzioni pecuniarie = Punteggio 2 (Dannose); Sanzioni interdittive = Punteggio 3 (Molto Dannose).

Valore Gravità complessivo: 5

VALORE RISCHIO BASE: $2 \times 5 = 10$

TOLLERABILE

VALORE RISCHIO RESIDUO: $1 \times 5 = 5$

TOLLERABILE