Fondazione Torino Musei

Modello di organizzazione, gestione e controllo

(adottato ai sensi del D.Lgs. 231/2001)

Parte Speciale F

Sistemi informativi

Documento approvato con delibera del Consiglio Direttivo del 22/12/2020

INDICE

1 FINALITA'

La presente Parte Speciale del Modello ha la finalità di definire le regole che tutti i soggetti coinvolti nell'ambito delle attività "sensibili", elencate nel successivo paragrafo 2, dovranno osservare al fine di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001 e assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

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

- indicare i principi di comportamento e i presidi di controllo che i soggetti coinvolti devono osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza ed alle altre strutture di controllo gli strumenti per esercitare le attività di monitoraggio, controllo, verifica.

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

- Parte Generale del Modello;
- Parti Speciali del Modello;
- Codice Etico di Fondazione Torino Musei;
- corpo normativo e procedurale di Fondazione Torino Musei;
- ogni altro documento aziendale che regoli attività rientranti nell'ambito di applicazione del Decreto.

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di legge.

2 LE ATTIVITA' SENSIBILI

Le attività che Fondazione Torino Musei (di seguito la Fondazione), a seguito dell'attività di *risk assessment*, ha considerato sensibili ai sensi del D.Lgs. 231/2001 nell'ambito del processo di gestione dei sistemi informativi sono:

- gestione degli accessi logici a dati e sistemi;
- gestione dei *back-up*;
- gestione di *software*, apparecchiature, dispositivi o programmi informatici;
- gestione della sicurezza della rete;
- gestione della sicurezza fisica.

3 GESTIONE SISTEMI INFORMATIVI

3.1 I reati e gli illeciti amministrativi potenzialmente rilevanti

I reati e gli illeciti amministrativi che la Fondazione ritiene potenzialmente applicabili nell'ambito dell'attività sensibile in oggetto (si rimanda all'*Allegato 1* del Modello "*I reati e gli illeciti amministrativi del Decreto Legislativo 231/2001*" per una descrizione di dettaglio di ciascuna fattispecie richiamata) sono:

-

- i reati in materia di Violazione del diritto d'autore (richiamati dall'art. 25-*novies* del D.Lgs. 231/2001).
- i reati informatici e di trattamento illecito dei dati (richiamati dall'art. 24-*bis* del D.Lgs. 231/2001), in particolare:
  - art. 615-*ter* c.p. - Accesso abusivo ad un sistema informatico o telematico;
  - art. 617-*quinquies* c.p. - Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche;
  - art. 635-*bis* c.p. - Danneggiamento di informazioni, dati e programmi informatici;
  - art. 635-*ter* c.p. - Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
  - art. 635-*quater* c.p. - Danneggiamento di sistemi informatici o telematici;
  - art. 635-*quinquies* c.p. - Danneggiamento di sistemi informatici o telematici di pubblica utilità.

3.2 Ambito di applicazione

I successivi principi di comportamento e presidi di controllo si applicano a tutti i Destinatari che, in ragione del proprio incarico o della propria funzione, sono coinvolti nella gestione dei sistemi informativi e, in particolare, a:

- Responsabile Settore Tecnico.

3.3 Principi di comportamento

I Destinatari che, in ragione del proprio incarico o della propria funzione, siano coinvolti nell'ambito dell'attività in oggetto, devono:

- valutare la corretta implementazione tecnica delle abilitazioni / profilazioni utente ai principali sistemi aziendali, verificandone la corrispondenza con le relative mansioni e il rispetto del principio generale di segregazione dei compiti;
- monitorare il corretto utilizzo degli accessi (*user-id*, *password*) ai sistemi informativi aziendali e di terze parti;
- monitorare gli accessi tramite VPN;
- effettuare le attività di *back-up*;
- verificare la sicurezza fisica, della rete e dei sistemi informativi aziendali e tutelare la sicurezza dei dati;
- identificare le potenziali vulnerabilità nel sistema dei controlli IT;
- provvedere al corretto mantenimento dei file di *log* generati dai sistemi;
- gestire la manutenzione *software* e *hardware* dei sistemi secondo le prassi esistenti;
- identificare le persone dotate di accessi particolari (internet, VPN, siti esterni privati o pubblici, sistemi informativi esterni privati o pubblici) e credenziali specifiche;
- monitorare il corretto utilizzo degli accessi fisici ai sistemi informativi di dipendenti e terze parti;

- vigilare sulla corretta applicazione di tutti gli accorgimenti ritenuti necessari al fine di fronteggiare, nello specifico, i delitti informatici e il trattamento illecito dei dati, suggerendo ogni più opportuno adeguamento;
- monitorare le attività di fornitori terzi in materia di *networking*, gestione degli applicativi e gestione dei sistemi *hardware*;
- garantire che non sia consentito l'accesso alle aree riservate (quali *server rooms*, locali tecnici, ecc.) alle persone che non dispongono di idonea autorizzazione, temporanea o permanente e, in ogni caso, nel rispetto della normativa (interna ed esterna) vigente in materia di tutela dei dati personali.

In particolare, tutti i dipendenti della Fondazione devono:

- custodire accuratamente le risorse informatiche aziendali o di terze parti (es. *personal computer* fissi o portatili) utilizzate per l'espletamento delle attività lavorative;
- utilizzare gli strumenti informatici aziendali e assegnati nel rispetto delle procedure aziendali in vigore ed esclusivamente per l'espletamento della propria attività lavorativa;
- utilizzare la navigazione in internet e la posta elettronica esclusivamente per le attività lavorative;
- custodire accuratamente le proprie credenziali di accesso ai sistemi informativi utilizzati, evitando che soggetti terzi possano venirne a conoscenza, e aggiornare periodicamente le *password*;
- rispettare le *policy* di sicurezza concordate e definite con le terze parti per l'accesso a sistemi o infrastrutture di queste ultime.

È infine espressamente vietato:

- detenere, diffondere o utilizzare abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- distruggere o alterare documenti informatici archiviati sulle *directory* di rete o sugli applicativi aziendali e, in particolare, i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario;
- lasciare documenti incustoditi contenenti informazioni riservate o codici di accesso ai sistemi;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di acquisire abusivamente, danneggiare o distruggere informazioni o dati contenuti nei suddetti sistemi informativi;
- danneggiare, distruggere gli archivi o i supporti relativi all'esecuzione delle attività di *back-up*;
- lasciare incustodito il proprio personal computer sbloccato;
- utilizzare i sistemi informativi a disposizione per attività non autorizzate nell'ambito dell'espletamento delle attività lavorative;
- acquisire abusivamente, danneggiare o distruggere informazioni o dati contenuti nei sistemi informativi aziendali o di terze parti;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;

- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- rivelare ad altri (se non a seguito di delega formale) o utilizzare in modo improprio gli strumenti di firma digitale assegnati;
- aggirare o tentare di eludere i meccanismi di sicurezza aziendali (antivirus, *firewall*, *proxy server*, ecc.) di terze parti;
- porre in essere condotte miranti alla distruzione o all'alterazione di sistemi informativi aziendali o di terze parti;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- salvare sulle unità di memoria aziendali contenuti o file non autorizzati o in violazione del diritto d'autore;
- utilizzare o installare programmi diversi da quelli autorizzati e privi di licenza;
- installare, duplicare o diffondere a terzi programmi (*software*) senza essere in possesso di idonea licenza o superando i diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze);
- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione, al fine di procurare un vantaggio per la Fondazione;
- accedere ad aree riservate (quali *server rooms*, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente.

3.4 Presidi di controllo

Si elencano di seguito i presidi di controllo che devono essere posti in essere nell'ambito della gestione della gestione dei sistemi informativi.

3.4.1 *Gestione degli accessi logici a dati e sistemi*

- L'accesso alle informazioni che risiedono sui *server* e sulle banche dati aziendali e di terze parti è consentito solo al personale autorizzato e deve essere limitato da idonei strumenti di autenticazione tramite *User ID* e *password* e profilazione d'accesso alle cartelle di rete.
- Al momento dell'assunzione di nuovo personale, deve essere aggiornato l'elenco del materiale informatico oggetto di assegnazione e deve essere data adeguata comunicazione allo stesso circa le relative regole di utilizzo. In caso di interruzione del rapporto di lavoro, deve essere restituito tutto il materiale informatico assegnato in sede di assunzione.
- La creazione / disabilitazione degli account utente deve essere formalizzata tramite richiesta via e-mail al Settore Tecnico da parte del Settore Risorse Umane ovvero dal Responsabile del Settore / Museo presso la quale sarà / è impiegato il neo assunto / dimissionario.
- Il Settore Tecnico deve creare / disabilitare l'utenza e i relativi diritti di accesso in funzione della posizione ricoperta dal dipendente e in base alle licenze disponibili. In caso di esaurimento delle licenze il Settore Tecnico deve avviare la richiesta di acquisto delle stesse,

(secondo le modalità definite dalla Parte Speciale C "*Approvvigionamento di lavori, beni, servizi, consulenze e incarichi professionali*" del presente Modello).

- Con specifico riferimento al sistema gestionale di contabilità, le abilitazioni di accesso e la relativa profilazione, così come ogni operazione di cancellazione o modifica delle utenze, possono essere richieste esclusivamente dal Responsabile del Settore Contabilità, Bilancio e Controllo di Gestione.
- Il riconoscimento dell'utente deve avvenire attraverso *User ID* e *password*. Al dipendente neo assunto deve essere attribuita una *password* provvisoria da modificarsi al primo *log-on*.
- La comunicazione delle *password* di accesso agli applicativi aziendali deve avvenire in modalità confidenziale e ogni dipendente deve provvedere alla custodia, non divulgazione della stessa e al suo periodico aggiornamento.
- Il Settore Tecnico deve effettuare attività periodiche di monitoraggio degli accessi agli applicativi aziendali e di revisione delle utenze attive al fine di garantire la corretta profilazione e concessione dei privilegi a sistema.
- Gli indirizzi di posta elettronica nominativi sui domini della Fondazione possono essere assegnati esclusivamente a soggetti dipendenti e devono essere ad esclusivo uso lavorativo.
- Le connessioni al sistema da remoto devono avvenire esclusivamente tramite canali di comunicazione sicuri (VPN) e sono consentite al solo personale autorizzato.

3.4.2 Gestione dei back-up

- Devono essere definiti piani di *back-up* periodici dei dati, file, programmi e sistemi operativi (su aree di memoria e su server della Fondazione o su server esterni), al fine di garantire la salvaguardia del patrimonio informativo aziendale.

3.4.3 Gestione di software, apparecchiature, dispositivi o programmi informatici

- Gli utenti non possiedono i privilegi necessari per effettuare alcuna installazioni di software sulla propria postazione di lavoro. Le richieste di installazione devono essere inoltrate al Settore Tecnico che le consentirà solo dopo avere verificato il possedimento della relativa licenza.

3.4.4 Gestione della sicurezza della rete

- La rete interna deve essere confinata e protetta tramite adeguati strumenti di limitazione degli accessi (*firewall* e *proxy*), supervisionati dal Settore Tecnico.
- I *server*, le postazioni fisse e portatili devono essere protetti contro potenziali attacchi esterni attraverso l'utilizzo di specifici *software* antivirus, che effettuino controlli in entrata, costantemente aggiornati sotto la supervisione da parte del Settore Tecnico.
- Il Settore Tecnico, con l'eventuale supporto di fornitori esterni, è responsabile di effettuare un'attività periodica di manutenzione sulle macchine e di verifica su *firewall* e *software*, nonché sul corretto aggiornamento dell'antivirus.

- L'accesso a internet di tutti gli utenti della Fondazione deve essere regolamentato e filtrato attraverso un sistema di *web filtering*, supervisionato dal Settore Tecnico.

3.4.5 Gestione della sicurezza fisica

- L'accesso alla sala CED o ai vani tecniciè consentito esclusivamente al Settore Tecnico e al personale opportunamente autorizzato da quest'ultimo.