FILM COMMISSION TORINO PIEMONTE

FILM COMMISSION TORINO PIEMONTE

REGOLAMENTO INFORMATICO

PER IL TRATTAMENTO E

LA SICUREZZA DEI DATI PERSONALI

– ISTRUZIONI PER L'UTILIZZO DEI SISTEMI INFORMATICI E TELEMATICI AZIENDALI –

Ai sensi del Regolamento UE 2016/679 e D.L. 101 del 10 agosto 2018

Data	Oggetto
16/09/2025	Emissione/Aggiornamento

1. Premessa

Premesso che l'utilizzo delle infrastrutture e degli strumenti informatici aziendali deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare ulteriori regole interne dirette ad evitare comportamenti inconsapevoli e/o scorretti.

Questo regolamento si ispira al Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 1° marzo 2007 ed è consegnato agli utenti, in una logica di trasparenza, al fine di dare adeguata informazione anche circa i trattamenti dei dati personali che FILM COMMISSION TORINO PIEMONTE effettua con sistemi e impianti aziendali (quali sistemi software e simili) e circa la presenza di sistemi che consentono controlli indiretti ovvero a distanza sui medesimi, nonché sulle modalità d'uso degli strumenti aziendali e di effettuazione di tali controlli. Ciò anche a valere, quanto ai lavoratori dipendenti, quale informativa ai sensi delle disposizioni applicabili (art. 4, comma 3, della legge 300/1970). I dati e le informazioni dell'utente (quali, esemplificativamente, dati anagrafici, relativi alla attività lavorativa, indirizzi email, indirizzi IP, numeri di telefono, log, metadati del traffico telematico, contenuti delle comunicazioni, etc.), che sono trattati in connessione con l'utilizzo da parte dell'utente di strumenti e risorse informatiche di FILM COMMISSION TORINO PIEMONTE(compresi il filesystem e gli strumenti di comunicazione email e collaborativi mediante chiamate audio/video), potranno essere utilizzati a tutti i fini connessi al rapporto di lavoro o al diverso rapporto in essere fra FILM COMMISSION TORINO PIEMONTE e l'utente, anche con riferimento a valutazioni ed erogazione di corrispettivi, verifica circa eventuali inadempimenti, procedimenti disciplinari (quanto ai dipendenti).

Per questo aspetto, questo regolamento integra l'informativa già resa ai sensi degli artt. 13 e 14 del reg. UE 2016/679.

La riservatezza delle persone attraverso la corretta acquisizione, gestione e circolazione dei dati personali e mediante l'adozione di adeguate misure di sicurezza per la loro protezione è tutelata dal Regolamento UE 2016/679.

2. Il Regolamento Informatico

Il Regolamento Informatico (da qui in avanti anche "**Regolamento**") viene redatto da FILM COMMISSION TORINO PIEMONTE (in qualità di Titolare del trattamento), in collaborazione con l'Amministratore di Sistema (da qui in avanti anche "**ADS**")e/o l'Ufficio/Area ICT (da qui in avanti anche "**Ufficio ICT**") preposto alla gestione (controllo, manutenzione, ecc.) degli strumenti informatici, e richiede la sottoscrizione ai lavoratori all'atto di assunzione o successivamente con atto separato, che disciplina l'utilizzo della strumentazione informatica aziendale.

Tale documento è idoneo sia a sollevare il Titolare del trattamento da eventuali responsabilità civili o penali relative ad un illecito utilizzo della strumentazione informatica da parte del personale, sia per i dipendenti, al fine di distinguere gli atti concernenti l'attività aziendale da quelli estranei alla

stessa in relazione alla strumentazione informatica, fornendo garanzie circa il trattamento dei loro dati personali.

Il Regolamento può pertanto definirsi come strumento di prevenzione in grado innanzi tutto di dimostrare l'attenzione e la volontà di evitare eventi estranei all'attività lavorativa, dall'altra come strumento di indicazione per gli utenti su come utilizzare le risorse informatiche aziendali senza per questo incorrere, anche in buona fede, in illeciti.

Inoltre, il Regolamento rappresenta un momento evolutivo, laddove intervenendo in modo puntuale, consente di individuare quali limiti e quali diritti sono vigenti all'interno dell'ambiente lavorativo.

3. Oggetto e Finalità

In un'ottica di prevenzione, con il presente Regolamento si intende promuovere nei Dipendenti una "*cultura informatica*", affinché l'utilizzo degli strumenti informatici messi a disposizione ed utilizzati sia conforme alle finalità societarie ed avvenga nel pieno rispetto della legge.

Inoltre, con l'entrata in vigore del Regolamento UE 2016/679, si rende necessario impartire istruzioni, agli utilizzatori, circa le modalità e le precauzioni da adottare in occasione del trattamento dei dati: dalla segretezza, alla riservatezza di taluni, alle modalità di salvataggio. Centrale è inoltre l'indicazione relativamente alla custodia, conservazione e controllo dei dati informatici, o all'uso di credenziali di autenticazione, o del divieto relativo all'utilizzo di supporti informatici estranei all'ambito aziendale.

Il Regolamento Informatico individua in modo specifico l'esatta destinazione della strumentazione informatica, evitando a priori che possano nascere equivoci relativamente al duplice utilizzo della stessa (aziendale e personale) e ne informa in maniera precisa e chiara gli utilizzatori.

Il presente Regolamento fornisce le linee guida principali e le regole per un corretto uso delle infrastrutture e degli strumenti informatici (nel complesso, **Risorse Informatiche**) di FILM COMMISSION TORINO PIEMONTE, impartisce istruzioni per il trattamento dei dati personali ai soggetti autorizzati ai sensi dell'art. 29 Regolamento UE 2016/679, introduce misure di sicurezza volte a garantire una adeguata protezione dei dati personali.

4. Definizioni

- **"Strumento Informatico o risorsa informatica"**: device (dispositivi quali elaboratori, rete informatica, stampanti, smartphone, tablet, dispositivi di archiviazione, ecc.), software e/o service (servizio) concessi al lavoratore (dipendente, collaboratore, amministratore, etc.) al fine di rendere la prestazione lavorativa e da questi utilizzato per scopi prettamente aziendali.
- **"Dati personali"**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Formano oggetto del presente regolamento i dati

personali dell'utente o di cui l'utente venga a conoscenza in occasione o in ragione del suo rapporto con FILM COMMISSION TORINO PIEMONTE.

- **"Dati particolari"**, dati personali che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. L'articolo 9 del Regolamento (UE) 2016/679 ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- **"Ufficio/Area ITC"**: la funzione aziendale preposta a sovraintendere gli strumenti informatici aziendali garantendo efficacia, efficienza e sicurezza degli stessi per assolvere i compiti e i progetti dell'Azienda. Ne fanno parte il Responsabile ITC e gli Amministratori di Sistema (ADS).
- **"Rete Internet":** la rete di reti, principalmente basata sul protocollo di comunicazione TCP/IP.
- **"Abuso":** qualsivoglia violazione del presente regolamento o di altre disposizioni civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete.
- **"Autorizzazione":** ai sensi dell'art. 29 del Reg. (UE) 2016/679 e dell'art. 2 quaterdecies e s.m.i. del D.lgs. n. 196/2003, ogni incaricato del trattamento, a cui sia stato dato accesso al sistema informativo aziendale mediante credenziali di autenticazione, è autorizzato all'utilizzo della strumentazione elettronica in dotazione (computer, stampanti, fax, scanner, fotocopiatori, dispositivi di rete, etc.) e all'utilizzo della strumentazione telefonica (telefoni a filo, telefoni cordless, telefoni cellulari, compresi smartphone e tablet, etc.) e del sistema di telefonia in dotazione per lo svolgimento dei compiti assegnati e in particolare al trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute (lettera di nomina ad autorizzato, codesto Regolamento, etc.).
- **"Credenziali di autenticazione":** le informazioni e/o i dispositivi, in possesso di una persona, solo da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
- **"Data Breach":** Una violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
- **"Utente o Utilizzatore":** qualsiasi persona fisica che utilizza una o più risorse informatiche.

5. Ambito ed Applicabilità del Regolamento

Le norme di seguito riportate all'interno del Regolamento hanno valore di ordine di servizio.

Il presente Regolamento si applica a tutti i soggetti che, a prescindere dalla forma giuridica contrattuale (dipendenti, stagisti e collaboratori a vario titolo, etc.), svolgono attività in presenza o in remoto, per FILM COMMISSION TORINO PIEMONTE e che utilizzano le risorse informatiche di FILM COMMISSION TORINO PIEMONTE, sia in modo esclusivo sia condiviso.

Pertanto, tutti i soggetti (incaricati e non) che operano nell'ambito del Titolare del trattamento, sono tenuti al rispetto scrupoloso del Regolamento, nell'ambito delle proprie competenze e attività.

L'inosservanza di tali norme potrà essere suscettibile di provvedimenti, commisurati alla gravità della violazione.

6. Autorizzazione all'utilizzo della strumentazione elettronica

Con il presente Regolamento, ai sensi del Regolamento UE 2016/679, si Autorizzano gli incaricati del trattamento all'utilizzo della strumentazione elettronica in dotazione (computer, stampanti, fax, scanner, fotocopiatori, dispositivi di rete, ecc.) per lo svolgimento dei compiti assegnati ed in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzioni ricevute nell'incarico e mansionario di assunzione e/o nel contratto di collaborazione.

7. Norme di comportamento

Gli strumenti e le risorse informatici sono messi a disposizione degli utenti perché li utilizzino per finalità professionali e, pertanto, il loro uso è previsto per lo svolgimento di compiti lavorativi e attività a favore di FILM COMMISSION TORINO PIEMONTE. Gli utenti nell'utilizzare gli strumenti informatici di FILM COMMISSION TORINO PIEMONTE devono curarne l'integrità e il funzionamento, e segnalare a FILM COMMISSION TORINO PIEMONTE le esigenze di manutenzione e di interventi finalizzati ad assicurarne la funzionalità.

Pertanto, è vietato l'uso illegale degli strumenti informatici da parte dei destinatari del presente Regolamento, nonché qualsiasi uso che possa interrompere il funzionamento dell'infrastruttura aziendale e di terzi.

Si ribadisce e si sollecita l'adozione dei corretti comportamenti per l'utilizzo degli elaboratori elettronici, delle credenziali di autenticazione, della posta elettronica, della navigazione in Internet e della memorizzazione di dati e documenti elettronici, secondo quanto stabilito dal Titolare del trattamento in accordo e sotto la supervisione dell'Amministratore di Sistema e del Responsabile della gestione e manutenzione della strumentazione elettronica. Tutti gli incaricati devono essere a conoscenza delle modalità e procedure in vigore (c.d. Regolamento Informatico) nell'utilizzo del sistema informativo interno.

8. Indicazioni e regole

8.1. Integrità delle risorse informatiche

Come per tutte le altre proprietà di FILM COMMISSION TORINO PIEMONTE, gli utenti devono utilizzare le risorse informatiche con la massima diligenza, nell'interesse di FILM COMMISSION TORINO PIEMONTE e nel rispetto delle disposizioni contenute nel presente Regolamento.

Le risorse informatiche in dotazione sono strumenti di lavoro, adeguate alle necessità, ai compiti ed agli incarichi di competenza di ciascun incaricato.

È fatto tassativo **divieto** dell'utilizzo degli strumenti informatici per scopi differenti e/o personali.

Gli utenti devono rispettare l'integrità delle risorse informatiche, secondo quanto di seguito precisato:

a. Gli utenti non devono inserire, modificare o rimuovere apparati in rete senza preventiva autorizzazione degli amministratori di rete.

b. Non è consentito modificare le caratteristiche hardware e software impostate sulle risorse informatiche in uso o installare ulteriori dispositivi hardware e/o applicativi software rispetto a quelli in dotazione.

c. Non è consentito l'uso di qualsiasi dispositivo esterno rimovibile (ad es. USB pendrive), se non quelli aziendali o quelli autorizzati per l'uso all'interno della rete aziendale per motivi attinenti esclusivamente alla propria attività.

d. Gli utenti non devono abusare delle risorse informatiche, alterandole o facendone cattivo uso. Ciò include, a mero titolo esemplificativo:

- tentativi intenzionali di accedere o apportare modifiche a informazioni personali, individuali o ogni altra informazione per cui l'utente non possieda idonea autorizzazione;
- tentativi intenzionali di apportare modifiche a sistemi o altre risorse informatiche per cui l'utente non possieda idonea autorizzazione;
- invio intensivo di posta elettronica indesiderata o invasiva (spam);
- stampa di copie cartacee per fini non istituzionali di documenti, file, dati o programmi;
- riproduzione, duplicazione, salvataggio o scarico (download o file sharing) di programmi informatici o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore (cfr. Art. 8.6);
- modifiche di configurazioni di sistemi di uso collettivo che non siano state autorizzate dagli amministratori di sistema o che violino copyright esistenti (cfr. Art. 8.6);
- tentativi intenzionali di bloccare o mandare fuori servizio computer, reti, servizi od altre risorse informatiche di FILM COMMISSION TORINO PIEMONTE o di terzi;
- più in generale, attività intenzionali che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli utenti;
- danneggiamento o vandalismo nei confronti di device, apparati, software, file o altre risorse informatiche.

e. gli utenti devono assicurarsi e garantire di non sviluppare o usare programmi o utilità che interferiscano con l'attività di altri utenti, o che modifichino parti del sistema o che accedano a informazioni private o riservate. L'uso di ogni programma nocivo espone ad azioni legali di carattere civile o penale da parte dei danneggiati e a richieste di risarcimento anche da parte di FILM COMMISSION TORINO PIEMONTE; si ricomprende tra i programmi nocivi software applicativi:

- scaricati da fonti illecite e ad alto rischio Virus/Malware;
- con finalità illecite.

f. Gli utenti sono tenuti ad applicare ai dispositivi di elaborazione personalmente assegnati, di cui hanno disponibilità, le cure necessarie per una corretta manutenzione e funzionamento, garantire che i dispositivi siano custoditi sotto la loro supervisione o quando impossibilitati, riposti in idonei contenitori o ambienti dotati di serratura accessibili solo all'incaricato stesso, per evitare il furto o la manomissione. Gli utenti devono inoltre verificare che le seguenti dotazioni di sicurezza siano in uso e non vengano disattivate neanche temporaneamente:

- attivazione del controllo d'accesso al dispositivo mediante autenticazione (username e password) secondo le caratteristiche e modalità specificate al

capitolo 8.2 paragrafo "Gestione delle credenziali di accesso ai servizi informatici";

- installazione e manutenzione in efficienza dei sistemi antivirus e di protezione personali.

L'ADS e/o il Responsabile dell'Ufficio ICT, può disporre di tali beni secondo necessità, sostituendo, aggiornando, rimuovendo adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore, fatto salvo eventuali specifiche e documentate esigenze lavorative.

L'utilizzatore che abbia necessità di apportare modifiche software o hardware agli strumenti informatici in dotazione, deve farne preventiva richiesta al gestore/amministratore di sistema.

Quanto memorizzato sui supporti magnetici, ottici ed elettronici potrebbe essere oggetto di analisi, controllo e duplicazione da parte del personale tecnico autorizzato, per migliorare l'affidabilità del sistema informativo e la disponibilità dei dati.

Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, ecc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dal Responsabile dell'Ufficio ICT o non esplicitamente autorizzati, tali componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso.

L'amministratore di sistema o gestore della strumentazione elettronica e/o suoi incaricati sono gli unici che possono provvedere o autorizzare l'installazione, l'aggiornamento e la configurazione di dispositivi hardware e/o software sui programmi in uso, sugli elaboratori elettronici, sulla rete informatica e più in generale sull'intero sistema informativo.

8.2.Sistema di autenticazione e di autorizzazione

Gli utenti non devono accedere a device, software, servizi, dati, informazioni o reti senza appropriata autorizzazione, o abilitare intenzionalmente altri all'accesso non autorizzato, indipendentemente dal fatto che le risorse citate appartengano o meno a FILM COMMISSION TORINO PIEMONTE. Un utente che sia stato autorizzato ad utilizzare un account protetto tramite password o altra tecnologia è tenuto a custodire con cura e a mantenere riservate le chiavi d'accesso relative all'account.

L'utente è personalmente soggetto a responsabilità civili e penali, in caso di abusi o incidenti di sicurezza, nel caso divulghi la password o renda accessibile ad altri l'account senza il permesso dell'amministratore di sistema.

Gli incaricati che operano sotto il controllo del sistema di autorizzazione sono soggetti alla verifica periodica di sussistenza delle condizioni che danno loro diritto all'accesso ai dati ed alle risorse informatiche aziendali.

Ogni anomalia scoperta in account di sistema o relativa alla sicurezza di sistemi o reti deve essere segnalata tempestivamente all'amministratore di sistema preposto e/o Responsabile dell'Ufficio ICT, in modo che possano essere attuati gli opportuni passi per investigare sui problemi e risolverli.

8.2.1. Credenziali di autenticazione per programmi e siti web ad accesso riservato

Alcuni programmi o siti web necessari per svolgere l'attività lavorativa forniscono un ulteriore livello di autenticazione.
Tali programmi prevedono la consegna di credenziali e/o dispositivi di autenticazione agli incaricati autorizzati ad operazioni di consultazione e/o trattamento dei dati ivi contenuti.
Talvolta, mediante la consultazione e/o il trattamento, si acquisiscono informazioni coperte da "riservatezza": per tale ragione si richiedono specifiche garanzie in termini di competenza e privacy.

Alcuni siti web sono concessi in uso al Titolare del trattamento, il quale, a sua volta, mette a disposizione ciascun sito, a seconda delle necessità, agli incaricati autorizzati che vi accedono con profilo di autorizzazione univoco previa autenticazione mediante codice identificativo e parola chiave condivisa da tutti gli incaricati autorizzati e assegnata dall'amministratore del sito.

Qualora l'applicazione richieda l'autenticazione OTP con token temporaneo l'azienda mette a disposizione tale supporto allo scopo di vietare l'uso di strumenti personali (ricezione sms e/o applicazioni su device mobile personali)

Il rilascio dell'accesso allo strumento di autenticazione a due fattori richiederà apposita concessione autorizzativa da parte del Titolare del trattamento.

8.2.2. Policy Gestione delle Credenziali di Accesso ai Servizi Informatici

All'attivazione di un account le credenziali vengono fornite dall'ADS o dal personale autorizzato dell'Ufficio ITC direttamente al dipendente/collaboratore. Una volta che il dipendente/collaboratore è in grado di accedere alla posta elettronica, ulteriori credenziali, ad esempio per piattaforme applicative gestionali, vengono inviate via mail.

Al primo accesso i sistemi sono configurati per richiedere all'utente un cambio password.

Le credenziali su sistemi non amministrati direttamente da FILM COMMISSION TORINO PIEMONTE possono essere rilasciate secondo modalità differenti.

CARATTERISTICHE DELLE PASSWORD

Le password devono essere definite secondo queste regole:

- Lunghezza minima 8 caratteri alfa/numerici, qualora il sistema non consenta di raggiungere la suddetta lunghezza di password, questa dovrà contenere il numero massimo di caratteri consentito da sistema.
- Si deve utilizzare almeno una lettera minuscola, una lettera maiuscola e un segno alfanumerico.
- Non possono essere uguali a una password già presente nell'elenco di password già utilizzate dall'utente entro un periodo di 48 mesi.
- Non deve essere facilmente riconducibile all'utente, ad esempio il nome di battesimo con anno di nascita.

I requisisti di complessità che le password devono soddisfare dovranno essere valutati in maniera commisura al rischio.
Il personale dell'Ufficio ICT, gli ADS non possono risalire alle password in chiaro dei singoli utenti. Le password dovranno essere memorizzate solo in modalità cifrata.
Le credenziali su sistemi non amministrati da FILM COMMISSION TORINO PIEMONTE possono non richiedere le presenti prescrizioni in termini di complessità della password, tuttavia, si richiede agli

utenti di seguire comunque le presenti indicazioni di buona pratica per la definizione delle proprie password.

RESET DELLE CREDENZIALI

Nel caso si presenti la necessità di un reset della password è necessario contattare l'ADS o il personale autorizzato dell'Ufficio ITC.

GESTIONE DELLE CREDENZIALI DA PARTE DEGLI UTENTI

L'utente è tenuto a conservare le credenziali a sua disposizione con la massima cura e riservatezza. Non devono essere comunicate a terzi o colleghi ne riportate dove facilmente visibili da terzi.

L'utente deve prendere tutti gli accorgimenti necessari per evitare che a fronte dello smarrimento di agende, cellulari o altri dispositivi, credenziali di sistemi di FILM COMMISSION TORINO PIEMONTE siano esposti ad un uso fraudolento.

Nel caso in cui l'utente abbia coscienza che le proprie credenziali siano state ottenute da terzi è tenuto a informare immediatamente l'ADS e/o il Responsabile dell'Ufficio ITC.

RISORSE AD USO CONDIVISO

L'utente che deve condividere una risorsa informatica con un collega sprovvisto di credenziali di autenticazione deve avvisare l'ADS e/o il Responsabile dell'Ufficio ITC che valuta se attivare un altro account dedicato o se inserire l'account dell'utente per tale risorsa nell'elenco degli accessi in deroga, chiedendo a utente e collega di compilare manualmente e a loro cura un registro di accesso che riporti il loro nominativo e il momento del collegamento e se possibile della disconnessione.

8.3. Utilizzo della Posta Elettronica

Tenuto conto che la posta elettronica è uno strumento di lavoro, qualora ad un incaricato del trattamento, per l'adempimento delle proprie mansioni, sia affidata una casella di posta elettronica, valgono le seguenti indicazioni:

- l'utilizzo della posta elettronica è strettamente limitato all'uso lavorativo;
- è fatto divieto di utilizzare le caselle di posta elettronica aziendale assegnate ai dipendenti e ai collaboratori (caselle del tipo nome.cognome@) per inviare e ricevere messaggi di carattere personale non attinenti al lavoro anche se l'indirizzo identificativo può contenere parti che richiamano al nominativo dell'utente; infatti FILM COMMISSION TORINO PIEMONTE non si assume alcuna responsabilità al riguardo di tali messaggi personali, trasmessi infrangendo il divieto, compresa la riservatezza dei loro contenuti;
- la natura della corrispondenza effettuata con le caselle di posta elettronica istituzionali (caselle del tipo 'nome ufficio o funzione@ragione_sociale_azienda.it) non è privata e non è consentito utilizzare tali caselle per motivi non attinenti allo svolgimento delle mansioni assegnate; non è possibile garantire la riservatezza dei messaggi inviati e ricevuti, essendo tutte le comunicazioni entranti o uscenti, passibili di analisi, controllo, duplicazione e archiviazione da parte del personale tecnico autorizzato, al fine di migliorare l'affidabilità del sistema informativo e la disponibilità dei dati e di tutelare l'organizzazione nei rapporti con terzi;
- non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- le caselle di posta elettronica possono essere oggetto di salvataggio automatico sia per le comunicazioni in ingresso che in uscita.

8.3.1. Risposta automatica in caso di assenza

L'utente, in caso di assenze pianificate o prolungate (ad esempio per ferie o attività di lavoro fuori sede) qualora non sia in grado di consultare la casella di posta assegnata, deve attivare l'apposita funzionalità di sistema (cd. *Regola fuori sede*) che consente di inviare automaticamente un messaggio di risposta indicando, se del caso, i recapiti (anche e-mail o telefonici) di un altro utente.

In caso di assenze non programmate (ad esempio malattia) di durata superiore a 2/3 giorni la procedura sopra descritta, ove possibile, sarà attività dall'utente avvalendosi del servizio di casella di posta elettronica via web.

8.3.2. Accesso straordinario e individuazione fiduciario

In caso di assenza improvvisa e prolungata dell'utente che non ha possibilità di accedere alla casella autonomamente, ove ricorrano specifici motivi di sicurezza o si manifestassero improrogabili necessità legate all'attività lavorativa, FILM COMMISSION TORINO PIEMONTE si riserva di accedere alla casella di posta elettronica assegnata all'utente e, di conseguenza, al contenuto dei messaggi ivi presenti, per il tramite dell'ADS e/o il Responsabile dell'Ufficio ICT, su richiesta esplicita e documentata del Responsabile dell'Ufficio di appartenenza ed a seguito di autorizzazione da parte del Delegato Privacy - e di utilizzare quei messaggi o funzioni della casella ritenuti rilevanti per lo svolgimento di attività lavorativa o per garantirne la sicurezza. Di tale attività è redatto apposito verbale da parte del Responsabile dell'Ufficio che deve, altresì, informare l'utente alla prima occasione utile e consegnare copia del verbale.

L'utente può, in aggiunta, indicare con apposita delega un fiduciario, nell'ambito della unità organizzativa di appartenenza, nella persona del Responsabile dell'Ufficio o altro addetto. Il fiduciario, controfirmata la delega per accettazione, in caso di necessità avrà il compito di verificare il contenuto dei messaggi e curare l'inoltro alle competenti funzioni aziendali di quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Anche in questo caso il fiduciario deve redigere apposito verbale e consegnarlo alla prima occasione utile all'utente interessato.

8.3.3. Accesso dopo la cessazione del rapporto di lavoro

In caso di cessazione del rapporto di lavoro di un incaricato, affidatario di una casella di posta elettronica, il personale tecnico autorizzato provvederà ad assegnare tale casella all'amministratore di sistema o ad eventuale delegato assegnato prima della cessazione del rapporto di lavoro.

L'archivio dei messaggi inviati e ricevuti per tramite della casella sarà mantenuto secondo le politiche delle caselle attive.

Eventuali messaggi di carattere personale che non abbiano contenuti afferenti all'ambito lavorativo, indirizzati all'ex-incaricato saranno tempestivamente rimossi dall'archivio della posta elettronica e, per quanto possibile, resi irrecuperabili.

Inoltre, l'azienda procederà all'eliminazione dell'account allo scopo di consentire all'azienda il passaggio di consegne ad altri incaricati e le conclusioni di eventuali attività intraprese con clienti e fornitori. L'azienda si impegna a terminare i processi di gestione della e-mail riferita al lavoratore entro 90 giorni dalla cessazione del rapporto lavorativo.

8.3.4. Ulteriori indicazioni

In ogni comunicazione elettronica inviata all'esterno, è consigliabile apporre in calce la seguente dicitura:

"La presente e-mail è riservata ed è rivolta unicamente al destinatario sopra evidenziato. I dati sono trattati dal mittente, dai collaboratori del gruppo di lavoro, dagli incaricati autorizzati, nel rispetto del Regolamento UE 2016/679; qualora persone non evidenziate quali destinatari ricevessero codesta e-mail sono pregati di informare tempestivamente la nostra struttura e di rimuovere il messaggio. Tutte le comunicazioni, sia in uscita che in ingresso, potrebbero essere conosciute ed archiviate da parte dell'organizzazione di appartenenza del mittente."

Si ritiene utile portare a conoscenza alcune norme di comportamento che salvaguardano gli elaboratori dall'infezione di virus informatici ed evitano un sovraccarico del servizio di posta elettronica:

- Nel caso di mittenti sconosciuti, di messaggi insoliti oppure di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti è opportuno cancellare i messaggi senza aprirli.
- Controllare gli allegati di posta elettronica prima del loro utilizzo: non eseguire download di file eseguibili o documenti da siti web o ftp non conosciuti.
- Evitare la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata).
- Utilizzare formati compressi (*.zip, *.jpg) per l'invio di allegati pesanti.
- Nel caso in cui si debba inviare un documento all'esterno è preferibile utilizzare un formato protetto da scrittura (*.pdf).
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali. Prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
- La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili.

8.4. Utilizzo dei dispositivi personali (BYOD - Bring your own device)

Senza esplicita autorizzazione è severamente vietato utilizzare mezzi propri (es. tablet notebook, smartphone, etc.) per collegarsi alla rete aziendale, sia mediante collegamenti diretti (es. cavo di rete LAN, wi-fi, etc.), sia mediante collegamenti remoti (es. VPN, desktop remoto, RDP, TeamViewer, VNC, etc.). L'autorizzazione deve essere data dal Delegato Privacy consultati il Responsabile dell'Ufficio ICT e gli ADS.

L'autorizzazione ad utilizzare i dispositivi non aziendali per rendere la prestazione lavorativa comporta l'impegno, per il soggetto che viene autorizzato, ad utilizzare tali dispositivi:

- correttamente configurati dal punto di vista della sicurezza informatica;
- dotati di antivirus/anti-malware aggiornati;
- di avere messo in atto tutti i comportamenti, predisposizioni e configurazioni necessarie in termini di sicurezza informatica analogamente a quanto previsto per i dispositivi aziendali;
- è fatto divieto di archiviare localmente qualsiasi dato su strumenti informatici privati e/o ad uso promiscuo;
- a semplice richiesta da parte dell'ADS e/o il Responsabile dell'Ufficio ICT devono essere rimossi dal dispositivo di proprietà dell'incaricato tutti i file e i programmi attinenti all'attività lavorativa;
- l'uso di memorie rimovibili personali deve essere autorizzato. A semplice richiesta la memoria deve essere svuotata;

- la configurazione dell'account di posta aziendale su propri dispositivi personali deve essere autorizzata. A semplice richiesta l'account deve essere rimosso;
- è facoltà dell'utente, che utilizza un proprio dispositivo, richiedere l'assistenza tecnica da parte dell'Ufficio ICT.

Salvo diversi accordi derivanti da esigenze di servizio, durante l'utilizzo di mezzi propri (es. tablet notebook, smartphone, etc.), l'utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli strumenti in uso, consapevole che in caso contrario la scrivente Fondazione potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e dell'utente.

Inoltre, è da considerarsi autorizzato, senza specifica autorizzazione, l'accesso da dispositivi personali alle risorse in Cloud (es. tramite Office 365), ferme restando le responsabilità di cui sopra.

La gestione dei dispositivi mobili (Mobile Device Management o MDM), è a cura dell'Ufficio ICT, il quale procede alla configurazione e alla gestione dei dispositivi mobili, al fine di garantirne la sicurezza.

8.5. Navigazione in Internet

La navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

Premesso che Internet è da intendersi prioritariamente come fonte di informazione per finalità di ricerca, studio e documentazione per lo svolgimento delle proprie mansioni nonché strumento di lavoro per raggiungere le risorse remote (cloud) si precisa che:

- È assolutamente proibita la navigazione in Internet, sia durante che al di fuori dell'orario di lavoro, per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
- Non possono essere utilizzati modem/router privati per il collegamento alla rete.
- È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato.
- È vietato, in particolare, scaricare o effettuare streaming di contenuti multimediali (musicali, video, fotografici, ecc.) che non siano attinenti all'attività lavorativa.
- È vietata la partecipazione a social network e forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati) e di bacheche elettroniche, la registrazione in guest books anche utilizzando pseudonimi (o nicknames).
- È proibita l'effettuazione di ogni genere di transazione finanziaria, di remote-banking, di e-commerce, salvo i casi autorizzati e/o per attività aziendali attinenti alla propria funzione e incarico.
- È vietata la consultazione di siti con contenuti pornografici o comunque illegali, non leciti e lesivi del decoro e della morale.

Il Responsabile e personale tecnico autorizzato possono adottare politiche adattative, restrittive e di verifica sulla navigazione, monitorando statisticamente il traffico in base a criteri su sorgente, destinazione, tipologia, durata, fascia oraria, ecc.

Utilizzando sistemi informativi per esigenze produttive, organizzative o di sicurezza sul lavoro (ad es., per rilevare anomalie, per manutenzioni, per garantire le comunicazioni elettroniche, ecc.), è

indispensabile l'uso di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, nel rispetto dello Statuto dei lavoratori (art. 4 comma 2 della l. n. 300/1970). Tali sistemi registrano le connessioni, ovvero tengono traccia dell'ora, dell'elaboratore richiedente e della risorsa richiesta e potrebbero eventualmente memorizzare il contenuto della risposta. A meno di particolari esigenze tecniche o di sicurezza, circoscritte comunque a periodi di tempo limitati, tali sistemi sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra scrittura come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico.

8.6. Diritto d'autore, copyright e licenze d'uso

Gli utenti devono rispettare diritti d'autore, copyright e licenze d'uso di software, materiali audiovisivi, documenti ed ogni altra informazione digitale protetta a norma di legge.

Ogni materiale protetto da diritto d'autore o copyright **non deve essere copiato** al di fuori di quanto specificato dal proprietario dei diritti o del copyright o di quanto previsto dalle leggi sul diritto d'autore. Il materiale protetto non può essere copiato per mezzo di attrezzature o sistemi di FILM COMMISSION TORINO PIEMONTE, fatto salvo quanto conseguente alla disponibilità di una licenza d'uso valida, o permesso dalle leggi sul diritto d'autore e sul copyright.

Tutte le informazioni soggette a diritto d'autore o copyright (testi, immagini, icone, programmi, video, audio, etc.) ottenute da strumenti informatici o risorse di rete **devono essere usate in conformità con le leggi vigenti**. L'origine del materiale copiato deve essere correttamente attribuita ed evidenziata. Il plagio di informazioni digitali è soggetto alle stesse sanzioni che si applicano al plagio di altre opere o tipologie di dati.

Tutti i documenti e informazioni relative all'attività lavorativa presso FILM COMMISSION TORINO PIEMONTE devono essere opportunamente protette e non diffuse senza autorizzazione. Il loro utilizzo deve essere rispettoso del livello di riservatezza delle informazioni stesse.

8.7. Uso delle unità condivise di rete

Le unità condivise di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Eventuali file non strettamente legati all'attività lavorativa potranno essere eventualmente salvati sul device assegnato all'utente e in nessun caso sulle cartelle personali del server aziendale.

FILM COMMISSION TORINO PIEMONTE, in ogni caso, si riserva, per il tramite degli ADS e/o del Responsabile dell'Ufficio ICT, la facoltà di procedere a propria discrezione alla rimozione di ogni file o applicazione che riterrà essere pericolosa per la sicurezza del sistema ovvero acquisita o installata in violazione del presente regolamento.

8.8. Memorizzazione di dati e documenti elettronici

L'accesso ai dati memorizzati in locale sui singoli elaboratori risulta sempre protetto dalla procedura di controllo degli accessi che, come descritto ai paragrafi precedenti, richiede l'utilizzo delle credenziali di autenticazione per ottenere l'accesso ai dati e la verifica dei privilegi di accesso gestiti dal sistema di autorizzazione.

Il salvataggio di dati, documenti e file rilevanti per l'attività lavorativa, utilizzabili da altri utenti o comunque da salvaguardare, deve essere effettuato utilizzando le cartelle condivise del server di rete.

Nel caso di trattamento di dati personali appartenenti a categorie particolari, l'archiviazione dei dati dovrà inoltre attenersi alle seguenti misure di sicurezza:

- È vietato l'uso di supporti di archiviazione removibili non autorizzati per la memorizzazione dei dati.
- È vietato il salvataggio dei documenti aziendali su supporti diversi da quelli forniti ed autorizzati.
- Eventuali supporti di memorizzazione removibili contenenti dati particolari, possono essere riutilizzati solo se i dati precedentemente contenuti non sono più in alcun modo recuperabili (i dischi, quindi, devono essere formattati ed i nastri riscritti).

8.9. Protezione da Virus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus, spyware, trojan, malware o mediante ogni altro software aggressivo.

Per la protezione contro i rischi di intrusione e l'azione di programmi pericolosi, su tutti gli elaboratori è installato uno specifico software antivirus.

L'aggiornamento del software antivirus è effettuato in automatico mediante l'apposita funzione del prodotto utilizzato.

Il modulo "Autoprotezione" del software antivirus è installato con modalità residente in memoria e risulta perciò sempre attivo, assicurando una costante protezione automatica contro l'ingresso o la propagazione all'esterno di virus od altri programmi pericolosi attraverso le normali attività del posto di lavoro.

La funzione di autoprotezione non deve essere disabilitata da parte dell'utente; qualora particolari esigenze ne rendessero necessaria la temporanea disattivazione, l'interessato dovrà farne richiesta al Responsabile dell'Ufficio ICT, che in tal caso disporrà il costante monitoraggio del posto di lavoro per tutto il periodo in cui esso opera privo di protezione.

8.10. Protezione dalle truffe: il fenomeno "Phishing"

8.10.1. Che cos'è?

Il phishing è una frode informatica, realizzata attraverso l'invio di e-mail contraffatte, finalizzata all'acquisizione, per scopi illegali, di dati riservati oppure a far compiere alla vittima determinate operazioni/azioni. I malintenzionati che si avvalgono delle tecniche di phishing non utilizzano virus, spyware, malware o altre tipologie di software malevolo, ma si limitano, piuttosto, ad usare tecniche di social engineering1, attraverso le quali vengono studiate ed analizzate le abitudini delle persone, cioè delle potenziali vittime, al fine di carpirne potenziali informazioni utili. Il phishing è quindi un tipico attacco di social engineering che sfrutta l'interazione umana e in cui è richiesta la partecipazione attiva della vittima.

[1] Il social engineering rappresenta un insieme di tecniche utilizzate dai cybercriminali per attirare gli ignari utenti ad inviare loro i loro dati riservati, infettare i loro computer tramite malware o aprire collegamenti a siti infetti.

8.10.2. Cos'è tecnicamente?

Il phishing fa riferimento al tentativo di furto tramite dispositivi connessi. L'azione può essere manuale o eseguita attraverso uno strumento che automatizza il processo, può anche trattarsi di una combinazione dei due approcci.

Chi vuole sferrare un attacco di phishing generalmente ricorre ad una metodologia standard che di solito si articola in diverse fasi.

La prima di queste, consiste nell'inviare alle potenziali vittime dei messaggi di posta elettronica contenenti delle informazioni il più possibile veritiere, familiari e/o allettanti. Il messaggio fraudolento, per essere il più credibile possibile, simula delle situazioni che in realtà possono verificarsi. A titolo di esempio un tipico messaggio di phishing potrebbe riguardare:

- la scadenza di una determinata password di un servizio on-line;
- l'accettazione dei cambiamenti delle condizioni contrattuali;
- il potenziale rinnovo della carta prepagata o della carta di credito;
- dei potenziali problemi inerenti accrediti, addebiti o trasferimenti di denaro su determinati conti online;
- la mancata, incompleta o errata presenza di informazioni, che magari riguardano determinati servizi bancari on-line;
- la presenza di offerte di lavoro particolarmente allettanti, che magari invitano ad inserire le coordinate bancarie per far sì di esser tra i primi a beneficiarne;

Una volta quindi catturata l'attenzione dell'ignaro utente, il messaggio fraudolento, contenente un apposito allegato o un semplice collegamento ipertestuale, permetterà di effettuare l'accesso al sito Internet in questione. Il sito "fake" assomiglierà il più possibile a quello "ufficiale", con la speranza che il malcapitato utente inserisca username, password e/o altre potenziali informazioni utili.

Se a questo punto l'utente di turno "abbocca all'amo", il phisher, potrà disporre e utilizzare a suo piacimento i dati ottenuti con tutte le spiacevoli conseguenze del caso.

Gli attacchi di phishing possono essere condotti anche mediante l'invio di SMS, telefonate e altre applicazioni web fraudolente progettati per indurre le persone a scaricare malware, condividere informazioni sensibili (ad esempio, numeri di carta di credito e di conti bancari, credenziali di accesso) o intraprendere altre azioni che espongono sé o le proprie organizzazioni alla criminalità informatica.

8.10.3. Perché è rilevante?

Gli attacchi di phishing riusciti spesso portano a furto d'identità, frodi con carta di credito, attacchi ransomware, violazioni dei dati e ingenti perdite finanziarie per individui e per aziende.

Il phishing è la forma più comune di ingegneria sociale: per ottenere risultati positivi, gli attacchi di ingegneria sociale si basano sull'errore umano e su tattiche di pressione. Generalmente, l'aggressore finge di essere una persona o un'organizzazione di cui la vittima si fida - ad esempio, un collega, un capo, un'azienda con cui la vittima o il datore di lavoro della vittima ha relazioni commerciali - e crea un senso di urgenza che spinge la vittima ad agire in modo avventato. Gli hacker utilizzano queste tattiche perché è più facile e meno costoso ingannare le persone piuttosto che violare un computer o una rete.

8.10.4. Riconoscere un tentativo di phishing

Riconoscere un tentativo di phishing non è sempre semplice, ma alcuni consigli, un po' di disciplina e una certa dose di buon senso possono essere di grande aiuto. Gli attacchi di phishing fanno spesso leva sulla paura per offuscare la lucidità dell'utente.

Il phishing può interessare computer fissi, portatili, tablet e smartphone. La maggior parte dei browser Internet è dotata di metodi per verificare la sicurezza dei link, ma la prima linea di difesa contro il phishing è il giudizio degli utenti.

La regola principale per difendersi è solo una: **nessuno può tutelare le nostre informazioni meglio di noi stessi**. Per questo è necessario allenarsi a riconoscere i segnali di phishing e cercare di agire responsabilmente.

Di seguito alcuni importanti consigli per salvaguardarsi dal phishing:

- Non condividere mai i propri dati sensibili con una terza parte.
- Non aprire allegati del messaggio se non si è sicuri dell'identità del mittente.
- Non cliccare su alcun link presente nel corpo del messaggio se non si è sicuri dell'identità del mittente.
- Se si ricevono mail che sembrano provenire, ad esempio dalla tua banca che ti chiedono di inserire dati personali (login e password o numero di carta di credito) verifica sempre la veridicità della mail chiamando telefonicamente la banca.
- Per una maggiore protezione, quando si riceve un'e-mail da una fonte che si ritiene non sicura, è consigliato navigare manualmente al link fornito digitando nel browser l'indirizzo del sito web legittimo.
- Prestare attenzione al certificato digitale del sito web.
- controllare che la connessione sia HTTPS, la "S" indica infatti il termine "sicuro": non è una garanzia di legittimità, ma la maggior parte dei siti legittimi utilizza HTTPS proprio per una maggiore sicurezza. I siti HTTP, anche quelli legittimi, sono vulnerabili agli attacchi hacker.
- verificare che all'apertura della pagina web, il dominio sia effettivamente quello "ufficiale".
- Se si nutrono sospetti sulla legittimità di un'e-mail, è consigliato estrapolare un nome o parte del testo del messaggio e inserirlo in un motore di ricerca per verificare l'esistenza di attacchi di phishing noti che si avvalgono degli stessi metodi.
- Scorrere il cursore sopra il link per verificare se sia legittimo.
- Si consiglia sempre di utilizzare dei software di sicurezza anti-malware. La maggior parte degli strumenti di sicurezza informatica è in grado di rilevare allegati o link ingannevoli, quindi, anche se si cade in un tentativo di phishing ben formulato, lo strumento di sicurezza impedirà la condivisione delle informazioni con le persone sbagliate.
- Utilizzare password robuste e cambiarle con frequenza.
- NON utilizzare mai la stessa password per i vari servizi on-line.

Si tenga presente che, anche se ci sono diversi attacchi di phishing, il phishing tramite e-mail è il più diffuso e riconoscibile. Questo attacco è diventato sempre più sofisticato trasformandosi in spear phishing, whaling e attacco mirato. Gli attacchi di phishing si sono anche estesi dai programmi di e-mail alle piattaforme di comunicazione, compresi i messaggi di testo e i social media.

Gli attacchi di phishing includono:

- Phishing tramite e-mail – Un hacker invia un messaggio e-mail contenente un collegamento con l'intenzione di generare interesse, preoccupazione o curiosità. Lo scopo dell'e-mail è convincere il destinatario a cliccare sul collegamento.
- Vishing – Un malintenzionato chiama un telefono fisso, mobile o VoIP per coinvolgere l'utente in una conversazione.
- Smishing – Un criminale invia un messaggio di testo chiedendo all'utente di cliccare su un collegamento o di telefonare al mittente.
- Pharming – Poiché sempre più persone sono diventate consapevoli dei pericoli di cliccare su collegamenti contenuti in e-mail non richiesti, i malintenzionati hanno creato il pharming. Un attacco di pharming include un URL dannoso con la speranza che il destinatario lo copi e lo incolli all'interno del browser e acceda direttamente al sito web. Il pharming compromette la cache locale delle informazioni del DNS (Domain Name System) che le vittime utilizzano per raggiungere la destinazione corretta. Il collegamento malevolo conduce l'utente verso un sito web contraffatto.
- Spear phishing – Un hacker invia un'e-mail mirata e creata su misura a un'organizzazione o a un individuo. Le e-mail di spear phishing prendono solitamente di mira i manager o coloro che operano nei reparti finanziari.
- Whaling – Il whaling è simile allo spear phishing, ma prende generalmente di mira i top manager di un'organizzazione.

8.10.5. Cosa fare in caso di phishing

1. Qualora si sia subito un attacco di phishing o si ha il dubbio sull'attendibilità di una comunicazione è necessario:
   a) segnalare tempestivamente agli amministratori di sistema/rete e al Responsabile dell'Ufficio ICT l'accaduto;
   b) informare, se necessario, direttamente in modo verbale o telefonico il Delegato Privacy, la Direzione e il Responsabile dell'Ufficio ICT.

Il Responsabile dell'Ufficio ICT, dal momento in cui viene a conoscenza dell'evento, procede alla fase successiva di verifica della comunicazione.

2. Qualora si siano comunicati dati è necessario:
   a) contattare tempestivamente gli amministratori di sistema/rete e il Responsabile dell'Ufficio ICT dell'accaduto per avvertirli e, successivamente
   b) va effettuato un cambio password ricordando di non utilizzare mai la stessa password.

9. Assegnazione degli Strumenti Informatici

L'assegnazione degli strumenti aziendali mobili avviene mediante specifica lettera da controfirmare da parte del dipendente o collaboratore, contenente il dettaglio delle apparecchiature consegnate al dipendente/collaboratore, che da quel momento se ne assume la responsabilità e l'obbligo a conservare e a custodire i beni in oggetto con cura e massima diligenza, e a non destinarli ad altri usi che non siano quelli sopra previsti, a non cedere neppure temporaneamente l'uso dei beni sopra individuati a terzi, né a titolo gratuito, né a titolo oneroso, e di restituire gli stessi entro il termine nello stato attuale, salvo il normale deterioramento d'uso.

Tali beni restano comunque nella piena disponibilità di FILM COMMISSION TORINO PIEMONTE e l'Ufficio ICT possono:

- disporre di tali beni secondo necessità, sostituendo, aggiornando, rimuovendo adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore, fatto salvo eventuali specifiche e documentate esigenze lavorative;
- provvedere o autorizzare l'installazione, l'aggiornamento e la configurazione di dispositivi hardware e/o software sui programmi in uso.

10. Smartworking e Telelavoro

L'azienda contempla la possibilità, per gli incaricati autorizzati, di operare attraverso propria strumentazione elettronica e/o fornita dall'azienda, in modalità smartworking e telelavoro, con specifica autorizzazione e regolamento rilasciato in funzione dell'attività da svolgere definendo modalità, tempistiche, periodo e obiettivi. L'Ufficio ICT provvederà al rilascio della documentazione autorizzativa e della strumentazione necessaria (ove prevista).

11. Formazione e aggiornamenti del comparto I.T.

L'Ufficio ITC provvederà ad informare i lavoratori su eventuali aggiornamenti normativi o di natura tecnica (introduzione di nuovi programmi o strumentazione elettronica). Tali informazioni vengono pubblicate mediante sistemi di comunicazione in uso all'azienda.

La formazione è gestita a distanza o in modo diretto, da parte del responsabile dell'Ufficio ICT o da soggetti terzi incaricati, appartenenti alla struttura e/o fornitori di soluzioni hardware/software esterni.

12. Sicurezza dei Dati - Guasto, furto e altre situazioni pregiudizievoli

1. Qualora venga smarrito o rubato un dispositivo proprietà di FILM COMMISSION TORINO PIEMONTE o in uso tramite FILM COMMISSION TORINO PIEMONTE, è necessario:
   a) segnalare tempestivamente alla Direzione, agli amministratori di sistema/rete e il Responsabile dell'Ufficio ICT l'accaduto;
   b) fornire documento di specifica denuncia del furto alle Autorità Competenti;
   c) fornire il Modulo di furto/smarrimento sottoscritto, nel quale l'utente dichiara la configurazione e le condizioni di protezione dei dati presenti sul dispositivo, quali:
      - la tipologia di dati conservati sul suo dispositivo.
      - se è disponibile un backup e a quando risale.
      - la configurazione di sicurezza del dispositivo (credenziali, cifratura, controllo remoto, localizzazione, etc.).
2. Data Breach. In ogni caso, il soggetto che prende coscienza di un incidente di sicurezza è tenuto a:
   a) informare tempestivamente il Delegato Privacy inviando opportuna segnalazione mediante messaggio di posta elettronica al punto di contatto privacy manera@fctp.it presidiato mettendo in copia anche la Direzione di FILM COMMISSION TORINO PIEMONTE e il Responsabile dell'Ufficio ICT;
   b) informare, direttamente in modo verbale o telefonico il Delegato Privacy, la Direzione e il Responsabile dell'Ufficio ICT.

Il Delegato Privacy, dal momento in cui viene a conoscenza dell'evento, procede alla fase successiva di qualificazione dell'incidente.

13. Cessazione del Rapporto di Lavoro o di Collaborazione

Nel caso in cui cessi il rapporto di lavoro o di collaborazione, l'utente incaricato del trattamento deve:

- consegnare i beni aziendali in dotazione (telefono e computer portatili, chiavette USB, etc.);
- copiare i files e documenti elettronici di rilevanza aziendale sul server;
- cancellare e rimuovere file e programmi attinenti all'attività lavorativa da ogni dispositivo o servizio informatico di tipo personale (l'utente non deve trattenere per sé nessuna copia di file o documenti).

È compito dell'Ufficio ICT in seguito alla cessazione di un incarico:

- effettuare il ripristino alla configurazione iniziale (reset) dei beni aziendali dotati di sistema operativo;
- attivare un risponditore automatico che avvisi il mittente del fatto che la casella postale non è più attiva e comunichi riferimenti e-mail alternativi; la casella postale verrà disattivata senza ritardo e, comunque, al più tardi entro due mesi dalla data di cessazione, mentre rimarranno conservati i back-up storici;
- disattivare le credenziali di autenticazione sui server;
- in caso di sospensione prolungata del rapporto di lavoro per malattia, aspettativa etc. dell'incaricato, verrà attivato un risponditore automatico che comunicherà riferimenti e-mail alternativi, fatte salve eventuali deroghe ed accorgimenti da adottarsi caso per caso tenuto conto della ripresa delle attività lavorative.

14. Aspetti Legali

Ai sensi degli artt. 244-246 c.p.p., a seguito di indagini giudiziarie o azioni legali, FILM COMMISSION TORINO PIEMONTE può essere tenuta, dietro formale richiesta delle competenti Autorità, a fornire tracciati relativi all'uso di risorse informative o a consentire l'ispezione di files, nastri, dvd ed altri dispositivi di archiviazione dell'utente localizzati su apparati posseduti ed utilizzati da FILM COMMISSION TORINO PIEMONTE.

15. LOG

Tutti gli strumenti informatici registrano informazioni, dette LOG, riguardanti accessi/connessioni/operazioni, che possono comprendere dati personali relativi agli utenti.

I log tengono traccia dell'ora, dell'identificativo richiedente (es. indirizzo IP, numero di telefono), eventualmente del riferimento all'utente assegnatario e della risorsa richiesta e potrebbero eventualmente memorizzare il contenuto della comunicazione o il tipo di operazione.

A meno di particolari esigenze tecniche o di sicurezza, circoscritte, in ogni caso, a periodi di tempo limitati, tali sistemi sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati (attraverso procedure di sovra registrazione come, ad esempio, la cd.

rotazione dei log file). I log contenenti le registrazioni della navigazione sul web, degli accessi ai sistemi di elaborazione e degli accessi a Microsoft Office 365, sono conservati il tempo necessario per perseguire gli interessi legittimi, in genere per almeno sei mesi.

16. Osservanza delle disposizioni e controlli

È obbligatorio attenersi alle disposizioni di cui sopra, a quelle contenute nelle altre policy e nei regolamenti aziendali, comprese quelle in materia di Privacy per quanto concerne il trattamento di dati personali mediante strumenti elettronici e non.

Il mancato rispetto o la violazione del regolamento potrebbe comportare provvedimenti disciplinari, anche gravi, mentre l'inosservanza delle misure di sicurezza per i dati personali, sanzioni amministrative o addirittura azioni civili e penali.

Si rammenta che la violazione di taluni divieti può rappresentare un illecito penale e determinare l'integrazione dei presupposti per una responsabilità amministrativa dell'ente da reato, ai sensi del d.lgs. n. 231/2001.

Nel rispetto dei principi di pertinenza e di non eccedenza, le verifiche sugli strumenti informatici saranno realizzate nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e dei regolamenti aziendali. Il tecnico preposto effettua verifiche periodiche su ciascuno strumento informatico in dotazione agli utenti al fine di garantire il funzionamento ottimale degli strumenti e di verificare il rispetto del presente Regolamento e delle disposizioni vigenti.

Trattamenti ulteriori di dati personali dei destinatari, anche appartenenti a categorie particolari, possono essere effettuati per esigenze connesse all'esecuzione del contratto in essere con il medesimo (anche in relazione al suo adempimento ovvero inadempimento); ad obblighi di legge (anche in presenza di ordini di autorità pubbliche, inclusa l'autorità giudiziaria, a ciò legittimate); a necessità di salvaguardia di interessi vitali del Destinatario o di terzi; alla finalità di accertare, esercitare o difendere diritti, e comunque tutelare, anche in sede giurisdizionale, posizioni soggettive della Fondazione e di terzi; al perseguimento di legittimi interessi della Fondazione, come proteggere i propri interessi commerciali, economici e finanziari ovvero assumere iniziative, anche in prevenzione, rispetto a fatti illeciti o diffamatori, ovvero che possono causare danni ovvero pregiudizio alla Fondazione, al destinatario, ad altri destinatari, a fornitori, clienti e in generale a terzi.

I controlli, qualora ve ne siano, sono effettuati dagli ADS o dalla struttura aziendale autorizzata, e avvengono con gradualità per reparto, ufficio, gruppo di lavoro, etc. in modo da individuare l'area da richiamare all'osservanza delle regole, ove occorrente.

In caso di successive e perduranti anomalie, ovvero ravvisandone la necessità per finalità legittime, FILM COMMISSION TORINO PIEMONTEsi riserva di effettuare verifiche anche su base individuale, in ogni caso finalizzate alla verifica del rispetto delle disposizioni applicabili. In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi di FILM COMMISSION TORINO PIEMONTE e le finalità legittime.

Potranno altresì essere svolte attività di Vulnerability Assessment e di Penetration Test anche all'insaputa degli utenti, degli ADS e dell'ufficio ICT, al fine di testare, in sicurezza, la robustezza dei sistemi contro tentativi malevoli di causare incidenti di sicurezza e/o violazioni di dati.

17. Informativa

Ai sensi degli artt. 13-14 del Reg.to UE 2016/679, in conformità a quanto disposto dal Provvedimento n. 13 del 1° marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che:

- il soggetto giuridico scrivente, attraverso l'Ufficio ICT e i propri fornitori informatici, può effettuare un monitoraggio periodico dell'hardware e del software installato negli elaboratori aziendali. Tale operazione viene effettuata, in modo completamente automatico per le macchine in rete ed in modo semiautomatico per le macchine stand-alone, mediante l'utilizzo di apposito software installato o da installare in ogni computer aziendale. Il monitoraggio, necessario per finalità organizzative (inventario del parco macchine e contabilità delle licenze d'uso del software), non coinvolge in alcun modo i dati personali ed i documenti presenti sui computer, ma permette la rilevazione di software installato in violazione di questo regolamento;
- al fine di prevenire, per quanto ed ove possibile, comportamenti scorretti durante la navigazione in Internet, l'azienda si avvale di appositi filtri che impediscono l'accesso a siti non ritenuti idonei ed il download di files multimediali non attinenti all'attività lavorativa;
- i sistemi informatici utilizzati internamente alla rete registrano le connessioni, ovvero tengono traccia dell'ora, dell'identificativo della risorsa richiedente (es. indirizzo IP, numero di telefono), eventualmente dell'nominativo dell'utente assegnatario, della risorsa richiesta e potrebbero eventualmente memorizzare il contenuto della comunicazione. A meno di particolari esigenze tecniche o di sicurezza, circoscritte comunque a periodi di tempo limitati, tali sistemi sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi al traffico ingenerato.
- i files contenenti le registrazioni della navigazione sul web sono conservati per sei mesi come previsto dalle norme in vigore e da esigenze di sicurezza;
- i log contenenti le registrazioni degli accessi ai sistemi sono conservati per sei mesi come previsto dalle norme in vigore e da esigenze di sicurezza;
- dati di traffico e tabulati telefonici: i sistemi in uso (centralino e telefoni mobili) consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori.
- I dati di traffico acquisiti dal sistema di telefonia sono utili per la validazione dei prospetti di consumo che le compagnie telefoniche addebitano, sulla base dei tabulati telefonici da esse riscontrati; pertanto, l'operazione di trattamento dei dati di traffico mira principalmente a verificare la sussistenza e la veridicità dei conti telefonici. Potrebbe emergere dall'analisi primaria un interesse ad approfondire la genesi dei costi ed eventualmente a verificare il corretto utilizzo dei telefoni aziendali. Pertanto, è facoltà del Titolare effettuare controlli mirati all'individuazione di condotte illecite o vietate, ricorrendo sia ai tabulati telefonici, sia ai dati di traffico registrati dal sistema di telefonia interno, mediante operazioni di analisi, selezione e raffronto.
- ulteriori dati possono essere raccolti ai sensi dell'art. 4 dello Statuto dei lavoratori (l. n. 300/1970) relativamente a strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa (es. computer, tablet, autovetture, telefono, software, ecc.), strumenti di registrazione degli accessi e delle presenze, per tutti i fini connessi al rapporto

di lavoro sulla base di codesto regolamento e di eventuale ulteriore informazioni circa le specifiche modalità d'uso e di effettuazione dei controlli;

- Il trattamento dei dati degli utenti, utilizzatori degli strumenti informatici, così come descritto, è obbligatorio, pena l'impossibilità di utilizzare qualunque elaboratore informatico.
- I dati personali saranno trattati nel rispetto in conformità alle misure e agli obblighi imposti dal Regolamento UE 679/2016 (GDPR) e dal D.lgs. 196/2003 (Codice in materia di protezione dei dati personali), come modificato dal D.lgs. 101/2018, in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, esatti, e se necessario aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità del trattamento.
- I dati potranno essere comunicati in Italia e all'Estero all'interno degli enti collegati con FILM COMMISSION TORINO PIEMONTE, a soggetti terzi per incarichi specifici e rispondenti alle finalità del trattamento e nei casi previsti dalla legge.
- Gli utenti possono esercitare i propri diritti quando previsto, nei confronti del titolare del trattamento, ai sensi degli artt. dal 15 al 22 del GDPR scrivendo all'ufficio/area ICT ai seguenti recapiti: info@fctp.it

Ricevuta

La preghiamo di restituirci copia della presente RICEVUTA firmata per ricevuta ed accettazione del REGOLAMENTO INFORMATICO PER IL TRATTAMENTO E LA SICUREZZA DEI DATI PERSONALI

Distinti saluti.

Il Titolare del trattamento

FILM COMMISSION TORINO PIEMONTE

Luogo e Data: TORINO 16/9/2025

Io sottoscritto (nome e cognome) _____dichiaro di aver ricevuto copia del REGOLAMENTO INFORMATICO PER IL TRATTAMENTO E LA SICUREZZA DEI DATI PERSONALI e di averne preso visione e di averlo compreso ed accettato integralmente.

In fede

MODULISTICA

Allegato A - ASPETTI ORGANIZZATIVI E GESTIONALI

I Soggetti individuati dalla Fondazione per la gestione delle attrezzature informatiche sono:

Riferimento	Funzione
M2 Informatica	Amministratore del Sistema Informatico
Alfonso Papa	Responsabile Ufficio/Area ICT
M2 Informatica	Gestione backup
It Gate / Vodafone	Gestione Sistema Telefonico e connettività rete dati
M2 Informatica / It Gate	Responsabile della gestione e manutenzione della strumentazione elettronica

Allegato B - VERBALE DI ACCESSO STRAORDINARIO

Presso _____ _____in data _____
dalle _____ alle _____ si è reso necessario eseguire un accesso straordinario su:

- ☐ Archivio/casella di posta elettronica _____ assegnata all'utente _____
- ☐ cartella [ ] di rete / [ ] locale _____assegnata all'utente _____
- ☐ servizio cloud _____assegnato all'utente _____
- ☐ altro _____

per i seguenti motivi (specifici e non generici):

- ☐ assenza prolungata o impedimento dell'assegnatario che rende indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, quali _____
- ☐ modifica del profilo di autorizzazione per l'accesso ai dati
- ☐ copia di salvataggio dei dati
- ☐ controllo di sicurezza in merito alla presenza di minacce per i dati ed i sistemi di elaborazione
- ☐ controllo in merito al rispetto dei regolamenti interni
- ☐ altro _____

L'intervento è avvenuto a cura di _____ (tecnico), su richiesta di _____ (responsabile) che ha eseguito le seguenti operazioni:

1. _____
2. _____
3. _____
4. _____
5. _____

Si rilascia copia all'utente assegnatario interessato; l'utente [ ] può / [ ] deve reimpostare la propria parola chiave.

_____, lì _____

Il tecnico

_____

Il Responsabile

_____

L'utente assegnatario per ricevuta

_____

Allegato C - MODULO ASSEGNAZIONE DISPOSITIVI AZIENDALI

NUMERO [_____] /anno [___2025_____]

DATA	16/09/2025	NOMINATIVO ADDETTO ICT:	Alfonso Papa

In data odierna viene assegnato al/alla dipendente _____

la seguente strumentazione informatica, di proprietà della FILM COMMISSION TORINO PIEMONTE:

- Computer aziendale marca _____modello_____ seriale _____ comprensivo di caricabatterie
- Mouse aziendale marca _____
- Tastiera aziendale marca _____
- Auricolari aziendali marca _____
- Stampante aziendale marca _____
- Webcam aziendale marca _____
- USB pen drive aziendale marca _____
- Monitor marca_____ modello___ _____ seriale _____ comprensivo di cavi video e di alimentazione
- Smartphone aziendale marca _____ modello _____ seriale IMEI_____ con sim [fornitore telefonia] numero di telefono_____
- Unità di archiviazione esterna USB modello _____ da n. _____Gb/Tb
- Altro_____

Si ricorda che, in accordo al Regolamento informatico, l'utilizzo della strumentazione è strettamente correlata allo svolgimento delle mansioni e compiti aziendali, e che pertanto **non è possibile utilizzare tali strumenti per fini personali**.

La strumentazione aziendale assegnata deve essere conservata e custodita con diligenza, e riconsegnata al proprio responsabile o all'Ufficio ICT in maso di malfunzionamento e/o cessazione del rapporto di lavoro.

In accordo a quanto previsto dal Regolamento informatico, **in caso di furto o smarrimento** sarà suo dovere sporgere immediata denuncia alle Autorità, indicando tra l'altro la configurazione e le condizioni di protezione dei dati presenti sul dispositivo, quali:

- la tipologia di dati conservati sul suo dispositivo.
- se è disponibile un backup e a quando risale.
- la configurazione di sicurezza del dispositivo (credenziali, cifratura, controllo remoto, localizzazione, etc.), e

segnalare tempestivamente l'accaduto al Delegato Privacy, inviando opportuna segnalazione mediante messaggio di posta elettronica al punto di contatto privacy presidiato mettendo in copia anche la Direzione e il Responsabile dell'Ufficio ICT.

Per accettazione

FIRMA DEL DIPENDENTE

_____

Allegato D - MODULO RITIRO DISPOSITIVI AZIENDALI

NUMERO [_____]/anno [_____]

DATA		NOMINATIVO ADDETTO ICT:	

In data odierna viene assegnato al/alla dipendente _____

la seguente strumentazione informatica, di proprietà della FILM COMMISSION TORINO PIEMONTE:

- ○ Computer aziendale marca _____modello_____ seriale _____ comprensivo di caricabatterie
- ○ Mouse aziendale marca _____
- ○ Tastiera aziendale marca _____
- ○ Auricolari aziendali marca _____
- ○ Stampante aziendale marca _____
- ○ Webcam aziendale marca _____
- ○ USB pen drive aziendale marca _____
- ○ Monitor marca_____ modello___ _____ seriale _____ comprensivo di cavi video e di alimentazione
- ○ Smartphone aziendale marca _____ modello _____ seriale IMEI_____ con sim [fornitore telefonia] numero di telefono_____
- ○ Unità di archiviazione esterna USB modello _____ da n. _____Gb/Tb
- ○ Altro_____

In accordo al Regolamento informatico, l'Ufficio ICT si occuperà di procedere alla cancellazione dei dati presenti sulle unità di archiviazione, **e si riserva di effettuare un successivo controllo per verificare che non risulti attrezzatura assegnata non restituita, nonché di accertare eventuali danni derivanti da incuria non attribuibile alla normale usura** (es: danni da caduta, presenza di liquidi all'interno dei dispositivi, riparazioni "artigianali", ecc.)

Per RICEVUTA (rilasciare una copia al dipendente)

FIRMA DEL DIPENDENTE

_____

FIRMA DELL' ADDETTO ICT

_____