TEATRONAZIONALE
TEATRO STABILE TORINO

Regolamento per l'utilizzo delle Risorse Informatiche

1. Oggetto e ambito di applicazione.
Il presente regolamento disciplina le modalità di accesso e di utilizzo della rete, dei servizi IT e delle risorse informatiche della Fondazione Teatro Stabile di Torino con sede in Via Rossini, 12 – 10124 Torino.
Il lpresente documento fa riferimento al quadro normativo delineatosi a partire dall'entrata in vigore del Regolamento UE 2016/679 (di seguito GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali loro afferenti, e del successivo decreto legislativo n. 101/2018, recante disposizioni per l'adeguamento dell'ordinamento nazionale alla normativa europea, il quale ha apportato svariate modifiche al D.Lgs. n. 196/2003, cd. Codice privacy.
La rete informatica della Fondazione si compone di varie parti.
Le risorse infrastrutturali costituiscono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica.
Il patrimonio informativo è l'insieme delle banche dati in formato digitale e, in generale, di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati da parte dei vari Uffici e Servizi. I dati personali contenuti all'interno del patrimonio informativo devono essere trattati secondo i principi e le prescrizioni del GDPR.
Il presente regolamento si applica a tutti gli utenti, sia interni che esterni, autorizzati ad accedere alla rete informatica della Fondazione TST.
Per utenti interni si intendono tutti i dipendenti e i collaboratori della Fondazione.
Per utenti esterni si intendono i consulenti, le ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, e qualsiasi altro ospite esterno, che necessitino di accesso alla rete informatica. Agli stessi verrà fornita – se richiesta e con la debita documentazione di rilascio – una password di accesso temporanea alla rete informatica, la quale verrà prontamente modificata, al termine dell'utilizzo richiesto, da parte dell'Amministratore di Sistema. Ai

medesimi utenti esterni verrà fatta sottoscrivere una liberatoria sulle modalità di utilizzo della rete della Fondazione.

2. Responsabilità dei dipendenti.
Al fine di garantire la tutela della riservatezza dei dati e delle informazioni relative ai lavoratori, il trattamento dei dati mediante l'uso di tecnologie telematiche viene effettuato nel pieno rispetto dei diritti, delle libertà fondamentali, nonché della dignità degli interessati, ed in ossequio ai divieti posti dallo Statuto dei lavoratori sul controllo a distanza e dei principi di necessità, correttezza e finalità determinate, esplicite e legittime. Ogni utente è responsabile, sotto il profilo sia civile sia penale, del corretto uso delle risorse informatiche, dei Servizi e dei programmi ai quali ha accesso e dei dati che tratta nell'ambito degli incarichi attribuiti dalla Fondazione TST in qualità di Titolare del Trattamento.
Spetta al Titolare del Trattamento, anche tramite il Responsabile del Trattamento e i suoi delegati, illustrare agli interessati i contenuti del presente regolamento e vigilare affinché tutti lo rispettino.

3. Doveri di comportamento dei dipendenti.
Le strumentazioni informatiche, la rete Internet e la posta elettronica devono essere utilizzati dal personale della Fondazione TST unicamente come strumenti di lavoro.
È vietato qualsiasi utilizzo delle strumentazioni sopra citate per scopi non inerenti l'attività lavorativa, e ciò in quanto tale erroneo utilizzo può comportare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza della Fondazione stessa.
In particolare, non può essere dislocato, nelle aree di condivisione della rete, alcun file che non sia legato all'attività lavorativa, nemmeno per brevi periodi.
Agli utenti è assolutamente vietato effettuare la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinioni o appartenenza sindacale o politica.
Non è parimenti consentito scaricare, scambiare o utilizzare materiale protetto dal diritto d'autore.

4. Utilizzo dei personal computer o altri device.
Il personale, per lo svolgimento della propria prestazione lavorativa, utilizza soltanto computer o device di proprietà della Fondazione Teatro Stabile di Torino
In riferimento ad ogni computer o device in uso, il personale è tenuto a:

- attivare sul PC lo screensaver e la relativa password;
- conservare la password nella massima riservatezza e con la massima diligenza;
- non inserire password locali che non rendano accessibile il computer se non esplicitamente autorizzati dall'Amministratore di Sistema;
- non modificare la configurazione hardware e software del PC in uso, di proprietà della Fondazione, se non a seguito di esplicita autorizzazione scritta;
- non rimuovere, danneggiare o asportare componenti hardware;
- non installare sul PC dispositivi hardware personali (modem, schede audio, masterizzatori, pendrive, dischi esterni, telefoni, ecc.), salvo specifica autorizzazione scritta da parte dell'Amministratore di Sistema;
- non installare autonomamente programmi informatici, se non esplicitamente autorizzati dall'Amministratore di Sistema;
- non utilizzare programmi non autorizzati, che sono spesso utilizzati per veicolare virus;
- mantenere sempre attivi sulla propria postazione di lavoro i software antivirus preinstallati ed attenersi alle disposizioni tecniche impartite dall'Amministratore di Sistema;

- prestare la massima attenzione ai supporti di origine esterna (es. pendrive), verificando precauzionalmente tramite il programma di antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti;
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- non cedere, una volta superata la fase di autenticazione, l'uso della propria postazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso al server, ad Internet e ai servizi di posta elettronica;
- spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione;
- procedere, dopo la sessione di lavoro, al salvataggio di quanto prodotto nelle aree indicate dall'Amministratore di Sistema;
- non eccedere nella raccolta e nella conservazione dei dati, secondo le prescrizioni del GDPR;
- segnalare all'Amministratore di Sistema i dati non più utili o non più pertinenti, al fine di avviarli alla loro cancellazione sicura.

5. Utilizzo di pc portatili.
L'utente è responsabile del PC portatile assegnatogli e deve:

- applicare al PC portatile le regole di utilizzo previste per i PC connessi alla rete;
- custodirlo con diligenza e in luogo protetto durante gli spostamenti;
- rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna.

6. Utilizzo della rete informatica.
Gli utenti della rete informatica sono tenuti a utilizzare la rete in modo conforme a quanto stabilito dal presente regolamento. Essi, pertanto, devono:

- mantenere segrete e non comunicare a terzi, inclusi gli Amministratori di Sistema, le password d'ingresso alla rete e ai programmi e non permettere ad alcuno di utilizzare il proprio accesso;
- provvedere periodicamente alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili, al fine di evitare un'archiviazione eccessiva;
- verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pendrive), prima di trasferirlo su aree comuni della rete.

Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della rete, interferire con la connettività altrui o con il funzionamento del sistema e, quindi, di:

- utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare file e software di altri utenti, utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
- sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate;
- modificare le configurazioni impostate dall'Amministratore di Sistema;
- limitare o negare l'accesso al sistema a utenti legittimi;
- effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc.);
- distruggere o alterare dati personali altrui.

7. Utilizzo di Internet.

L'accesso alla navigazione in Internet deve essere effettuato esclusivamente a mezzo della rete della Fondazione TST e solo ed esclusivamente per scopi lavorativi. È tassativamente vietato l'utilizzo di modem personali.

Gli utenti sono tenuti a utilizzare l'accesso ad Internet in modo conforme a quanto stabilito dal presente regolamento e, quindi, devono:

- navigare in Internet in siti attinenti allo svolgimento delle funzioni e mansioni assegnate;
- registrarsi solo a siti con contenuti legati all'attività lavorativa;
- partecipare a forum o utilizzare chat esclusivamente per motivi strettamente attinenti l'attività lavorativa.

Agli utenti è fatto espresso divieto di utilizzare Internet con modalità che possano recare danno alla Fondazione o a terzi e, quindi, è fatto espresso divieto di:

- far conoscere ad altri la password del proprio accesso;
- usare Internet per motivi personali;
- servirsi dell'accesso ad Internet per svolgere attività in violazione del diritto d'autore o di altri diritti tutelati dalla normativa vigente;
- scaricare software gratuiti dalla rete, salvo casi di comprovata utilità e previa autorizzazione in tal senso da parte dall'Amministratore di Sistema;
- guardare video o filmati utilizzando la rete Internet, se non per motivi attinenti il lavoro;
- effettuare transazioni finanziarie, operazioni di remote banking, acquisti online e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal Titolare del trattamento;
- inviare fotografie, dati personali propri o altrui dalle postazioni Internet in uso.

La navigazione in internet per motivi di sicurezza è monitorata tramite il server in Cloud Cisco Umbrella ed alcuni siti e categorie di siti non sono visitabili a meno di autorizzazione.

8. Utilizzo della posta elettronica.

Gli utenti assegnatari di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e sono tenuti a utilizzarle in modo conforme a quanto stabilito dal presente regolamento.

In particolare, costoro devono:

- conservare la password nella massima riservatezza e con assoluta diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura e, dove possibile, preferire l'utilizzo di cartelle di rete condivise;
- inviare preferibilmente file in formato PDF protetti mediante password;
- accertarsi dell'identità del mittente e controllare, a mezzo di software antivirus, i file allegati di posta elettronica prima del loro utilizzo;
- rispondere a e-mail pervenute solo da mittenti conosciuti e cancellare preventivamente le altre;
- premere sui link contenuti all'interno di messaggi SOLO quando vi sia la comprovata sicurezza sul contenuto dei siti richiamati o sull'identità del mittente.

Agli utenti è fatto espresso divieto di utilizzare la posta elettronica in modo tale che possa recare danno alla Fondazione o a terzi e, quindi, è fatto divieto di:

- prendere visione della posta elettronica altrui;
- simulare l'identità di un altro utente, ovvero utilizzare, per l'invio di messaggi, credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;

- utilizzare strumenti software o hardware atti a visionare il contenuto delle comunicazioni informatiche all'interno dell'Amministrazione;
- trasmettere a mezzo posta elettronica dati personali, anche particolari, o informazioni di alcun genere, se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati e con le opportune cautele (quali password, crittografia, ecc.);
- inviare, tramite posta elettronica, user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici;
- utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o chat, salvo diversa ed esplicita autorizzazione del Titolare.

9. Utilizzo delle password.

Le password di ingresso alla rete sono previste ed attribuite dall'Amministratore di Sistema.
È necessario procedere alla modifica della password a cura dello stesso utente al primo utilizzo e, successivamente, a scadenza semestrale, con contestuale comunicazione della medesima all'Amministratore di Sistema.
Qualora la password non venga autonomamente variata dall'incaricato entro i termini previsti, l'utente verrà automaticamente disabilitato. Sarà quindi necessario rivolgersi all'Amministratore di Sistema, il quale provvederà a riabilitare l'utente ed assegnargli una password provvisoria che l'utente dovrà cambiare al primo acceso.
Le password possono essere formate da lettere (maiuscole o minuscole), devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'utente.
La password deve essere immediatamente sostituita, dandone comunicazione all'Amministratore di Sistema, nel caso si sospetti che la stessa abbia perso il carattere di segretezza, con contestuale comunicazione all'Amministratore di Sistema della nuova password.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Titolare del Trattamento e/o all'Amministratore di Sistema.

10. Utilizzo dei supporti magnetici.

Gli utenti devono trattare con particolare cura i supporti magnetici (chiavette USB, CD riscrivibili,..), in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti.
In particolare, gli utenti devono:

- evitare di utilizzare supporti rimovibili personali per il trasferimento dei dati personali particolari;
- custodire i supporti magnetici contenenti dati particolari e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto;
- consegnare i supporti magnetici obsoleti al Titolare del Trattamento e/o all'Amministratore di Sistema, ai fini della loro opportuna distruzione documentata, onde evitare che il loro contenuto possa essere recuperato successivamente alla cancellazione.

11. Utilizzo delle stampanti e dei materiali di consumo.

Stampanti e materiali di consumo in genere possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi o utilizzi eccessivi. Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dalle stampanti i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati. Si dovranno distruggere personalmente e sistematicamente le stampe non più utili e/o necessarie a fini lavorativi.

12. Utilizzo di telefonini e di altre apparecchiature di registrazione di immagini e suoni.
È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo:

- diversa ed esplicita disposizione del Titolare del Trattamento, da concordarsi di volta in volta e comunque sempre prima di effettuare tale trattamento;
- informazione preventiva degli interessati (informativa privacy da fornire loro);
- acquisizione del loro libero consenso, preventivo ed informato.

13. Linee guida per l'utilizzo dei profili social network.
L'avvento e la crescente diffusione dei servizi di social network segnalano un cambiamento radicale nell'accessibilità pubblica a dati ed informazioni, secondo modalità e misure sinora sconosciute. Assimilando i mezzi di diffusione del pensiero dei social network (Facebook, Twitter, Linkedin, WhatsApp, Blog, Chat ed altro), alle dichiarazioni rese dall'incaricato a mezzo degli strumenti tradizionali di comunicazione pubblica (giornali, radio, televisione), si ricorda che il diritto di manifestazione del pensiero e di critica in costanza del rapporto di lavoro soggiace a determinati limiti, esplicitazioni dei doveri di fedeltà, di riservatezza ed adesione ai valori della Fondazione TST, che incombono sull'incaricato in quanto deducibili nella prestazione lavorativa medesima, in particolare attinenti a:

a) continenza verbale;
b) continenza sostanziale: verità dei fatti e del ruolo ricoperto all'interno della Fondazione;
c) divulgazione di qualsiasi tipo di dato o informazione relativo e attinente l'attività del dipendente o collaboratore all'interno della Fondazione

Allorchè il "profilo privacy" scelto e adottato dal dipendente o collaboratore consente la visualizzazione dei suoi "post", commenti, video e foto, anche ad una cerchia di utenti aperta e sostanzialmente indeterminabile, l'incaricato soggiace a valutazioni e a possibili azioni di responsabilità disciplinare quando integri una lesione del rapporto fiduciario che lega il dipendente o il collaboratore alla Fondazione, con evidenti profili di violazione della riservatezza e danno dell'immagine della Fondazione, alla continuità e alla regolarità dell'attività.

13. Amministratore di Sistema.
L'Amministratore di Sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse informatiche dell'Ente e al quale sono consentite in maniera esclusiva le seguenti attività:

- gestire la manutenzione delle componenti hardware e software di tutte le strutture informatiche di appartenenza del Titolare, collegate in rete o meno;
- gestire (mediante creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della rete informatica, secondo le direttive impartite dal Titolare del Trattamento;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto in materia di diritti dei lavoratori e secondo la vigente normativa sulla privacy;
- creare, modificare, rimuovere o utilizzare qualunque account o privilegio, attesa l'autorizzazione del Titolare, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto in materia di diritti dei lavoratori e secondo la vigente normativa sulla privacy;
- rimuovere programmi software dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei

dati e nel pieno rispetto di quanto previsto in materia di diritti dei lavoratori e secondo la vigente normativa sulla privacy;

- rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto in materia di diritti dei lavoratori e secondo la vigente normativa sulla privacy;
- utilizzare le credenziali di accesso di amministrazione del sistema, o l'account di un utente tramite re-inizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, non tracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Titolare del Trattamento per l'utente assente o impedito, e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

14. Inosservanza del regolamento.

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite. La contravvenzione alle regole contenute nel presente regolamento da parte di un utente comporta l'immediata revoca delle autorizzazioni ad accedere alla rete informatica del Comune ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigenti. Se gli utenti interni perseverassero nell'uso ed abuso degli strumenti elettronici a loro disposizione, il Comune datore di lavoro è autorizzato a procedere con controlli prima sull'ufficio e, infine, sul gruppo di lavoro: solo a questo punto, ripetendosi l'anomalia, sarà lecito il controllo su base individuale.

15. Avviso di possibilità di controllo degli strumenti lavorativi ex art. 4 comma 3 L. 300/1970 (c.d. Statuto dei Lavoratori).

Ai sensi e per gli effetti dell'art. 4 comma 3 della L. 300/1970 (c.d. Statuto dei Lavoratori), i dipendenti della Fondazione TST vengono espressamente avvisati di quanto segue.

Come indicato nell'art. 2 dell'accordo sindacale siglato il 04-19.03.2019 ai sensi dell'art. 4, comma 1 L. n. 300/1970, In deroga al generale divieto di controllo di cui all'art. 4 comma 1 dello Statuto dei Lavoratori, gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi da cui derivi una possibilità di controllo del dipendente non richiedono l'adozione di una procedura sindacale per la loro implementazione e i dati raccolti attraverso i medesimi strumenti sono utilizzabili a tutti i fini connessi al rapporto di lavoro.

A tal fine, si avvisa che:

- le modalità d'utilizzazione degli strumenti medesimi, e in particolare dei computer in uso ai dipendenti della Fondazione e di uso comune, sono quelle precisate nel presente regolamento;
- le modalità di effettuazione dei controlli sui pc possono variare in funzione delle esigenze e delle possibilità operative: possono avvenire da remoto o in loco, mediante copia integrale del contenuto di un pc o mediante copia parziale. I controlli avvengono solo ad opera di Amministratori di Sistema con privilegi di accesso previamente autorizzati o direttamente dal Titolare del trattamento.

Della copia di volta in volta effettuata sarà garantita l'integrità e la non modificabilità, secondo i principi dell'analisi forense, in modo da permettere al dipendente l'eventuale contro-controllo della stessa nella sua forma e nei suoi contenuti originali.

Torino, 28 ottobre 2022