TITOLO:

REGOLAMENTO SULL'USO DEI SISTEMI INFORMATIVI DELLA FONDAZIONE TEATRO DI SAN CARLO

(approvato con delibera del Sovrintendente n. 176 del 31 ottobre 2019)

Sovrintendente
R. Purchia

Premessa

Il presente Regolamento viene emanato in ottemperanza a quanto indicato:

- Nelle "Linee guida per posta elettronica e internet" adottate dal Garante per la Protezione dei Dati Personali in data 01.03.2007 e nei provvedimenti emanati dalla medesima Autorità in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008);
- Nelle norme in materia di sicurezza del trattamento contenute nell'art. 32 e ss GDPR nonché ai sensi dell'art. 132 ter Codice Privacy così come modificato ex D.Lgs. 101/2018.

Definizioni

"GDPR": Regolamento generale sulla protezione dei dati (Reg. UE n. 2016/679) in inglese General Data Protection Regulation – GDPR (Regulation EU n. 2016/679).

"Dati protetti": Dati personali ricevuti da o per conto della Fondazione oppure ottenuti in altro modo in occasione dello svolgimento dell'attività lavorativa del Responsabile/Direttrice;

"Titolare del trattamento dei dati": "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali [...]" (cfr. art. 4, paragrafo 1, n. 7 GDPR), Egli è la persona fisica o giuridica che decide i mezzi e le finalità del trattamento dei dati protetti. Ai fini della presente nomina a responsabile del trattamento (di seguito "Nomina") il Titolare del trattamento dei dati protetti è la Fondazione Teatro San Carlo, in persona del Sovrintendente pro-tempore Dott.ssa Rosanna Purchia, con sede legale in Napoli, alla via San Carlo n. 16/F, P. IVA 00299840637, inserire P.E.C.: sovrintendenza@pec.teatrosancarlo.it.

"Responsabile per la Protezione dei dati" (RPD o DPO): il DPO è una persona esperta nella protezione dei dati personali, il cui compito è valutare e organizzare la gestione del trattamento dei dati personali, e dunque la loro protezione, da parte del Titolare, affinchè questi siano trattati in modo lecito e pertinente. Egli agisce anche come punto di contatto con gli interessati.

La Fondazione ha nominato un proprio Responsabile della Protezione dei Dati personali, contattabile al seguente indirizzo email: dpo@teatrosancarlo.it.

1. Scopo del documento

Il presente documento si prefigge di tutelare le risorse informatiche ed informative della Fondazione e di fornire indicazioni ai propri dipendenti e collaboratori circa il corretto ed appropriato uso delle stesse. In particolare, l'Ente intende perseguire i seguenti obiettivi:

– ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e confidenzialità dei dati e la continuità dei servizi erogati;

– garantire il rispetto della normativa in materia.

Nello specifico, il presente documento intende tutelare:

- il patrimonio informativo della Fondazione detenuto in formato elettronico;
- i servizi informatici erogati dall'Ente;

- le postazioni di lavoro "fisse" (PC e simili) e "mobili" (PC portatili e simili) se in dotazione;
- i dispositivi cellulari (smartphone) se in dotazione;
- i software di comunicazione (tipo "Messenger", "WhatsApp"e simili);
- i server, le apparecchiature e tutto il materiale hardware in generale.

L'uso nel presente regolamento del termine **"Utente"** si riferisce ad ogni dipendente e collaboratore (per finalità meramente descrittive e non esaustive, collaboratore a progetto, in stage, volontario, tirocinante, consulente, ecc.).

2. I destinatari

Il presente documento si applica ai soggetti di seguito indicati:

a) Dipendenti, a qualsiasi titolo inseriti nell'organizzazione aziendale, senza distinzione di ruolo e/o livello;

b) consulenti e collaboratori della Fondazione, a prescindere dal rapporto contrattuale intrattenuto con la stessa;

c) dipendenti e collaboratori della Fondazione che hanno un contratto in essere con l'Ente e che utilizzano risorse informatiche ed informative della stessa.

Le norme disciplinano sia il comportamento di coloro che sono "meri utilizzatori" (fruitori di PC, smartphone, laptop ecc.), sia il comportamento di coloro che svolgono mansioni tecniche (Amministratori di Sistema, Amministratori di Rete, gestori di banche dati, gestori di servizi, ecc.). Ciascun Utente, in base al proprio profilo "base" o "evoluto", dovrà attuare le norme che sono allo stesso indirizzate e, nel caso di dubbi di applicazione delle stesse, rivolgersi al Titolare o al D.P.O.

3. Le regole

Le regole riguardano tre aspetti dell'organizzazione aziendale: organizzativo, tecnologico-procedurale e comportamentale. Tutti gli interventi sono finalizzati a garantire la confidenzialità, l'integrità e la disponibilità delle informazioni e dei dati della Fondazione.

In particolare:

- La confidenzialità o riservatezza riguarda la conoscibilità e fruibilità delle informazioni ai soli soggetti autorizzati;
- l'integrità è relativa alla completezza ed inalterabilità delle informazioni;
- la disponibilità concerne l'accessibilità ed utilizzabilità delle informazioni nel tempo da parte dei soggetti autorizzati.

4. Gestione degli incidenti e Data Breach.

Ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete) deve essere segnalato dall'Utente in modo tempestivo al Titolare, al Responsabile di settore e al DPO, che avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative. Allo stesso modo, occorrerà procedere nel caso l'incidente di una certa gravità riguardi il patrimonio informativo e di conoscenza detenuto dalla Fondazione oppure le applicazioni informatiche. Per gli incidenti che possono determinare una violazione dei dati personali, cioè la 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 (cd. "data breach"), occorrerà segnalare immediatamente il sinistro al Titolare e/o al D.P.O.

5. Controllo degli accessi alle informazioni detenute in formato elettronico.

Il controllo degli accessi alle informazioni conservate in sistemi informatici è obbligatorio. Per ogni sistema sono stabiliti livelli di autorizzazione all'accesso degli Utenti secondo necessità.
L'accesso è controllato attraverso credenziali (username e password) che identificano in modo univoco l'Utente e proteggono da accessi non autorizzati.
Le password sono personali, ossia è nella responsabilità del dipendente/collaboratore che non ne venga fatto uso illecito. Se si rende necessario conservare la password per iscritto, deve essere custodita in un luogo inaccessibile a persone non autorizzate.

Ogni password deve essere sostituita al massimo ogni 90 giorni (consigliabile).

Le password personali sono a conoscenza solo dei rispettivi dipendenti/ collaboratori autorizzati.

Come password, si assegnerà una "password robusta" caratterizzata da:

- lunghezza uguale o superiore agli 8 caratteri;
- contenente almeno una lettera maiuscola, una minuscola, un numero, ed almeno un segno di punteggiatura;
- non contenente riferimenti agevolmente riconducibili all'ambiente lavorativo o personale (dovrebbero pertanto essere esclusi i propri nomi e devono essere evitati: date di nascita, indirizzi, numeri di telefono propri e di membri della propria famiglia o della cerchia di conoscenze);
- diversa dalle 3 password precedenti.

Quando si abbandona il posto di lavoro, anche per l'intervallo di pranzo, si deve attivare la funzione "blocca computer", (se non automatica, scegliendo l'opzione "blocca" dal menu di avvio).

Alla ripresa del lavoro si inserisce la password.

Solo il Titolare o il Responsabile di settore all'uopo delegato e autorizzato, possono entrare nel server di rete tramite la password di sistema e accedere, mediante una procedura solo a loro nota, ai dati di un dipendente /collaboratore assente, in caso di oggettive necessità di lavoro o sicurezza. In questo caso, il dipendente /collaboratore verrà informato al suo rientro dal Titolare e dovrà inserire nuovamente la propria password.

La persona all'uopo delegata e autorizzata dal Titolare provvederà a disattivare gli account su segnalazione del Titolare stesso in caso di cessazione del rapporto di lavoro di collaborazione o comunque di perdita di diritto dell'Utente.

6. Proprietà e protezione delle informazioni detenute in formato elettronico.

I dati e le informazioni memorizzate, elaborate e/o comunicate attraverso le apparecchiature informatiche in uso presso la Fondazione possono essere oggetto di controllo, per esigenze legate

esclusivamente a ragioni lavorative – come meglio specificato infra – e nei limiti consentiti dalla normativa in materia di tutela dei dati personali e dallo Statuto dei Lavoratori.
La Fondazione è proprietaria degli strumenti messi a disposizione del dipendente/collaboratore e si riserva la possibilità di condurre attività di audit non individualizzate, ossia rivolte all'utilizzo, in generale, degli strumenti da parte del personale: ciò al fine di verificare il rispetto delle regole descritte nel presente documento.
Qualora tali attività di audit dovessero evidenziare fondati elementi di criticità per la sicurezza, per i dati e/o per i beni della Fondazione, quest'ultima si riserva di intraprendere attività individualizzate di monitoraggio finalizzate all'avvio di azioni disciplinari nei confronti dei responsabili.
Tutti i dati personali devono essere archiviati sui server, nel cloud e sulle workstation in apposite partizioni. Solo in questo modo, i dati vengono protetti dalla password di sistema e dalle password personali.

La duplicazione di file o cartelle contenenti dati personali deve essere limitata solo ai quei casi in cui si riveli effettivamente indispensabile e comunque solo all'interno dei gruppi di soggetti individuati e autorizzati dal Titolare del trattamento.

7. Sicurezza delle applicazioni.

Tutte le applicazioni informatiche devono rispettare l'approccio della "privacy by design". Il Regolamento Europeo per la protezione dei dati personali, REG. UE 2016/679 (cd. GDPR), al 78° "considerando" iniziale stabilisce che: "in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici." Le strutture aziendali, qualora affidino ad un fornitore l'incarico di sviluppare applicazioni devono, pertanto, prevedere nei relativi contratti di appalto il rispetto delle stesse prescrizioni di cui al precedente punto. Sarebbe opportuno, inoltre, prestare analoga attenzione anche nel caso di applicazioni acquistate sul mercato.

8. Protezione antivirus.

Il sistema informatico dell'Ente è protetto da software antivirus aggiornato periodicamente. Ogni Utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
L'utilizzo di supporti di dati esterni (dischetti, memorie USB), allegati di e-mail e file trasferiti richiede cautela. Anche l'acquisizione di informazioni da Internet comporta il pericolo di infettarsi con virus.

Pertanto è necessario richiamare l'attenzione di ogni dipendente /collaboratore sulla sua responsabilità.
Nel caso il software antivirus rilevi la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al Titolare o a persona da questi all'uopo delegata ed autorizzata.
Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Titolare o a persona da questi all'uopo delegata ed autorizzata.
I programmi antivirus sono disponibili su tutte le workstation.
L'aggiornamento dell'antivirus deve avvenire periodicamente. Ciascuna workstation è stata impostata affinché effettui l'aggiornamento dell'antivirus, secondo una procedura trasparente al dipendente/collaboratore. Eventuali malfunzionamenti o messaggi dell'antivirus devono essere comunicati tempestivamente da ciascun dipendente/collaboratore al Titolare o alla persona da questi all'uopo delegata ed autorizzata.
In linea generale, ciascun dipendente/collaboratore è tenuto a non utilizzare file o e-mail individuati dall'antivirus come infetti e a dare comunicazione agli altri dipendenti/collaboratori e al Titolare o al Responsabile di settore da questi all'uopo delegata ed autorizzata in caso di comparsa di file o e-mail sospetti e di nuovi virus. Di conseguenza, saranno individuate le misure più opportune per rendere sicuro il sistema, avvalendosi, se necessario, del supporto di consulenti esterni.

9. Utilizzo dei PC.

Le stazioni di lavoro, da tavolo o portatili, sono predisposte con la necessaria dotazione di dispositivi (hardware) e programmi (software) tali da permetterne il corretto funzionamento, in conformità agli standard della Fondazione, Titolare del Trattamento ai sensi del Reg. UE 2016/679 e del D.Lgs. 101/2018, e nel rispetto delle necessarie licenze d'uso.
L'utilizzo dei beni aziendali deve avvenire esclusivamente per lo svolgimento delle mansioni lavorative: non sono ammessi l'appropriazione degli strumenti di lavoro e l'uso per scopi personali.
Il personal computer affidato all'Utente, sia unitariamente considerato, sia come unità di rete, è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
L'Utente è responsabile del PC portatile eventualmente assegnatogli, nell'esercizio della propria attività lavorativa, e deve custodirlo e proteggerlo con diligenza sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.
I personal computer portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni, ovvero la perdita, diffusione non autorizzata e la manomissione delle informazioni e dati trattati tramite l'utilizzo di essi.

La responsabilità della custodia del PC è interamente a carico dell'Utente, fatti salvi i casi di smarrimento, furto o distruzione non riconducibili a dolo o grave negligenza dell'Utente stesso.
Il personal computer dato in affidamento all'Utente permette l'accesso alla rete aziendale solo attraverso le specifiche credenziali di autenticazione.
Non è consentita l'installazione autonoma da parte degli Utenti di programmi provenienti dall'esterno, salvo previa autorizzazione esplicita della Fondazione e sotto la supervisione del Titolare o del Responsabile di settore da questi all'uopo delegato ed autorizzato, in quanto sussiste il concreto ed attuale pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
In ogni caso, l'installazione e l'aggiornamento di dispositivi e programmi sono di esclusiva competenza del personale espressamente autorizzato.
Non è altresì consentito l'uso di programmi diversi da quelli ufficialmente installati dalla Fondazione.
L'inosservanza delle precedenti disposizioni, oltre a determinare il rischio di danneggiamenti al sistema informatico aziendale per incompatibilità con il software esistente, espone la Fondazione a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software (nella qual categoria vanno inclusi anche screensaver, compressori, criptatori etc.) che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.
Ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Titolare o il Responsabile di settore all'uopo da questi delegato, nel caso in cui siano rilevati Virus.
E', quindi, vietato:
Compromettere il funzionamento dei Sistemi Informativi di Rete e delle apparecchiature che li costituiscono con virus o programmi diretti a danneggiare o interrompere il funzionamento del Sistema;
Distruggere, deteriorare o rendere inservibili, in tutto o in parte, programmi, informazioni o dati altrui;
Installare altro software non autorizzato;
Modificare in tutto o in parte il software o le sue configurazioni di funzionamento;
Asportare o copiare in tutto o in parte il software;
Modificare, aggiungere o rimuovere dispositivi hardware e le relative connessioni;
Utilizzare dispositivi di comunicazione diversi da quelli di cui è dotata la postazione di lavoro;
Disattivare, anche temporaneamente, il sistema antivirus;
Aprire sessioni di lavoro tramite modem da stazioni di lavoro connesse alla Rete interna.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi non autorizzati senza che vi sia la possibilità di provarne in seguito l'indebito uso. Per finalità di indirizzo della condotta degli Utenti al riguardo, al fine di evitare di lasciare incustodito il personal computer, in caso di allontanamento

temporaneo dalla postazione di lavoro e mancato spegnimento da parte dell'Utente, si richiede l'adozione della modalità automatica di "screen-saver" a tempo con obbligo di reintrodurre la password per l'accesso.

10. Interventi al sistema informatico

La Fondazione rende noto che il Titolare o la persona da questi all'uopo delegata e autorizzata può compiere interventi sul sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.) in conformità alle esigenze di ordinaria e straordinaria gestione dell'attività aziendale.

Detti interventi potranno comportare anche l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale attività dell'Azienda, si applica anche in caso di assenza od impedimento dell'Utente.

11. Utilizzo e conservazione dei supporti rimovibili.

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili, nonché informazioni costituenti know-how aziendale, devono essere criptati e trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun Utente potrà contattare il Titolare o persona da questi all'uopo delegata e autorizzata e seguire le istruzioni da questo impartite.

I supporti magnetici contenenti dati sensibili potranno essere criptati e dagli Utenti adeguatamente custoditi in archivi chiusi con serratura a chiave e, in caso di elevata criticità, in armadi blindati.

L'Utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

12. Accesso a internet e uso di rete aziendale dalla postazione di lavoro

La navigazione in internet ed il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione.

L'uso di Internet nelle sue numerose funzionalità è consentito esclusivamente per gli scopi attinenti al proprio lavoro e le attività svolte mediante la navigazione in internet o il sistema di posta elettronica sono destinati al conseguimento degli scopi sociali della Fondazione.

I dati che vengono inviati mediante il sistema aziendale di posta elettronica sono di proprietà dell'Ente.

La banda Internet ed il sistema di posta elettronica sono operanti con continuità, 24 ore al giorno per 365 giorni all'anno.

Per l'accesso alla rete ciascun Utente deve essere in possesso degli specifici User-Id e Password.

È assolutamente proibito entrare nella rete e nei programmi con un User-Id / Password diversi da quelli assegnati. Le Password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Superato il sistema di autenticazione l'Utente è collegato alla rete aziendale e ad internet senza ulteriori formalità.
Tutti gli Utenti ai quali è assegnata una postazione di lavoro possono utilizzare internet per motivi attinenti allo svolgimento della propria mansione/incarico.
L'Utente si impegna a:
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;
- salvare i dati al termine della giornata lavorativa in rete, nelle apposite cartelle dedicate. A tale riguardo qualora vi sia la necessità il responsabile di settore può richiedere al sopraintendente la creazione di una cartella lui intestata o in alternativa di una cartella condivisa dal gruppo di lavoro a cui fa riferimento allo specifico progetto
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- conservare la Password nella massima riservatezza e con la massima diligenza;
- non utilizzare credenziali (User-Id, Password e/o Dispositivo di Autenticazione) di altri Utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza.
Di qualsiasi azione o attività svolta utilizzando l' User-Id, Password e/o Dispositivo di Autenticazione assegnati è responsabile l'Utente assegnatario di essi.
Il personal computer assegnato al singolo Utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

13. Comportamenti non consentiti durante la "navigazione" in Internet

Le seguenti condotte non sono consentite:
- navigare in internet e registrarsi su siti i cui contenuti non sono strettamente attinenti all'attività lavorativa svolta, in particolare per effettuare transazioni finanziarie, acquisti online e simili, salvo i casi espressamente autorizzati dal Titolare o da persona da questi all'uopo espressamente delegata ed autorizzata;
- partecipare, per motivi non professionali, a Forum, l'utilizzo di chatline, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames) potendo esporre a rischi di sicurezza la rete aziendale;
- scaricare e/o installare programmi o aggiornamenti dalla Rete (download) per motivi non connessi all'attività lavorativa;
- stante la esclusiva destinazione delle unità di rete alla condivisione di informazioni strettamente professionali, consultare, archiviare o mettere a disposizione materiale inappropriato o che possa urtare la sensibilità altrui (ad es. files di natura pornografica, religiosa, politica, sanitaria, discriminatoria etc.);
- scaricare/scambiare materiale in violazione di diritti d'uso e delle regole del copyright e simili;
- eseguire o favorire pratiche di spamming

- utilizzare risorse informatiche private (PC, periferiche, token ,etc) per scopi non funzionali alle attività del Teatro San Carlo;
- modificare le configurazioni impostate sul proprio PC (es firma diglitale impostata per e-mail).

Utilizzo della posta elettronica.

Il sistema di posta elettronica è di proprietà della Fondazione.

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Qualsiasi uso improprio della posta elettronica sarà perseguito secondo I termini di legge e di contratto.

La casella di posta deve essere mantenuta in ordine, cancellando documenti non più utili. Deve essere controllata regolarmente dall'Utente, il quale deve rimanere nei limiti di dimensione previsti.

L'Utente deve evitare lo scambio di messaggi di posta elettronica con oggetto e contenuto estranei all'attività lavorativa ed indicare sempre nell'oggetto un abstract del contenuto.

All'Utente è vietato intercettare, alterare, impedire o interrompere comunicazioni di altri utilizzatori della Rete ed installare apparecchiature idonee a tale scopo.

È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web non conosciuti).

Parimenti, per motivi di sicurezza, coloro che ricevono messaggi di posta elettronica con allegati di estensioni pericolose o sospette (.exe, .bat, e simili) non devono nè aprirli, nè salvarli, ma immediatamente eliminarli.

A tutela del patrimonio informativo e della sicurezza dei sistemi informativi e di rete, la Fondazione si riserva la possibilità di condurre attività di controllo – atte a verificare il rispetto delle regole di utilizzo della posta elettronica – che potrebbero interessare anche le e-mail in arrivo ed in partenza dalle postazioni degli Utenti per scopi di servizio. Ciò avverrà nel pieno rispetto delle regole imposte dallo Statuto dei Lavoratori e dai provvedimenti emessi in materia dal Garante per la protezione dei dati personali, soltanto a seguito di riscontri su anomalie di rete riscontrate in modo anonimo e previo avviso al personale dipendente sull'avvio di misure ulteriori di verifica sull'utilizzo delle caselle di posta elettronica.

L'accesso alla posta elettronica è personale ed è possibile tramite nome Utente e password di identificazione distinta da quella di accesso al PC.

In fase di configurazione dell'account di posta elettronica l'Utente inserirà la sua password personale.

L'accesso non può essere condiviso o ceduto.

L'accesso alla posta elettronica aziendale è concesso agli utenti solo mediante dispositivi di proprietà della Fondazione dati in dotazione agli utenti (quali ad es.: telefono cellulare o

smartphone, tablet, PC portatile, etc.) o da dispositivi diversi se l'accesso è stato espressamente autorizzato Fondazione per iscritto.

Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato della sicurezza potrà accedere al contenuto del messaggio inviato alla stessa casella.

L'utente dovrà osservare inoltre le seguenti regole:

è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali i dati critici, senza garantirne l'opportuna protezione;

occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare punto e virgola occorre sempre essere consapevoli che posta elettronica e navigazione internet sono veicoli per l'introduzione sulla propria macchina e, quindi, in tutta la struttura internet del teatro di virus ed altri elementi potenzialmente dannosi.

14. Chiusura account aziendali

Nel caso di cessazione per qualsiasi motivo, sia esso concordato o legato al recesso unilaterale di una delle due parti dal rapporto di lavoro e/o collaborazione in essere con la Fondazione, il Titolare del trattamento o il Responsabile di settore provvederà a disattivare il servizio di posta elettronica entro le successive 48 ore, con la rimozione dell'account personale dagli indirizzi attivi gestiti dal sistema di posta elettronica aziendale e adotterà un sistema automatico per informare della chiusura dell'indirizzo e-mail i terzi e fornire a questi ultimi un nuovo referente per quel ruolo e indirizzi alternativi al contatto utilizzato fino a quel momento riferiti all'attività dell'Azienda al quale inviare le comunicazioni di tipo lavorativo/professionale.

15. Cancellazione sicura delle informazioni e dismissione dispositivi elettrici ed elettronici aziendali.

In caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche avviene nel rispetto delle normative di settore (FISMA; HIPPA; SOX; FACT ACT; GLBA; Provvedimento Garante Privacy del 13 ottobre 2008), e comporta la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali.

16. Comportamenti non consentiti nell'utilizzo della posta elettronica.

Le seguenti condotte non sono consentite:

- utilizzare l'indirizzo di posta elettronica aziendale per motivi non attinenti all'attività lavorativa svolta;
- utilizzare l'indirizzo di posta elettronica aziendale per scopi illegali, per inviare e ricevere materiale pornografico, osceno, volgare, diffamatorio, oltraggioso, discriminatorio, abusivo, pericoloso, per inviare dati sensibili, personali e/o commerciali in violazione della normativa vigente in materia di trattamento e protezione dei dati personali;

- utilizzare l'indirizzo di posta elettronica per trasmettere documentazione elettronica che costituisce "know-how" aziendale tecnico o commerciale protetto o non protetto, e che quindi viene contraddistinta da diciture o avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'Azienda, in assenza di autorizzazione del Titolare o di persona da questi all'uopo delegata ed autorizzata;
- utilizzare l'indirizzo di posta elettronica per la partecipazione a dibattiti, Forum o mailing-list, su internet per motivi non professionali;
- effettuare ogni genere di comunicazione finanziaria ivi comprese le operazioni di remote Banking, acquisti online e simili, salvo diversa ed esplicita autorizzazione del Titolare o della persona da questi all'uopo delegata ed autorizzata;
- aprire allegati di posta elettronica ambigui o di incerta provenienza (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati);
- utilizzare sistemi client di posta elettronica non conformi a quelli accettati dall'Azienda.

In caso di violazione o inadempimento di quanto previsto agli articoli 13 e 16 del presente regolamento, il Titolare o la persona da questi all'uopo delegata ed autorizzata procederà al distacco dell'Utente dal collegamento ad internet e si procederà all'eventuale accertamento di responsabilità disciplinari del personale dipendente o inadempimento contrattuale del collaboratore.

17. Uso di altri dispositivi e strumenti aziendali.

La postazione assegnata all'Utente, fax, stampanti, fotocopiatrici, scanner etc. sono strumenti di lavoro, il cui uso dovrà essere strettamente limitato all'espletamento delle mansioni e prestazioni lavorative.

Gli Utenti assegnatari delle singole postazioni sono responsabili del corretto utilizzo delle stesse nello svolgimento dell'attività lavorativa.

Ogni comunicazione scritta in entrata ed in uscita, interna ed esterna, inviata o ricevuta attraverso il fax aziendale che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, dovrà essere visionata dal Titolare o da persona da questi all'uopo delegata ed autorizzata e custodita in appositi armadi chiusi a chiave.

L'Utente è tenuto a limitare la ricezione di telefonate personali sulle linee telefoniche, avendo cura di contenere la durata delle conversazioni al minimo indispensabile.

Per i cellulari aziendali ed i tablet, gli Utenti sono invitati a proteggere sia il dispositivo che la sim card con appositi codici (pin) personalizzati, ovvero altre misure di protezione (impronta digitale, simboli, etc.)

La Fondazione non è responsabile della circolazione e diffusione di documentazione personale che sia avvenuta mediante l'utilizzo improprio degli strumenti aziendali.

All'uso del mezzo telefonico e degli strumenti fax e simili si applicano, ove pertinenti, le prescrizioni e divieti contenute nell'articolo 16 che precede.

18. Compiti e responsabilità.

L'Utente è responsabile della propria postazione informatica e della sua casella di Posta Elettronica.

L'Utente è responsabile della segretezza dei propri User-Id, Password e/o Dispositivo di Autenticazione. È anche responsabile del contenuto dei messaggi inviati dalla propria casella elettronica.

L'Utente si impegna a comunicare al Titolare o a persona da questi all'uopo delegata ed autorizzata, immediatamente, non appena ne venisse a conoscenza, qualsiasi uso non autorizzato da parte di terze persone del proprio User-ID, così come ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.

Gli Utenti sono tenuti a partecipare ai corsi di formazione e ad attenersi alle direttive del Titolare opportunamente comunicate tramite e-mail o circolare.

Ciascun Utente è obbligato a rispettare le disposizioni in materia di Privacy e misure di sicurezza, come specificato nella nomina di autorizzato al trattamento dei dati personali ex art. 29 Reg. UE 679/2016.

La tutela dei dati trattati, di proprietà della Fondazione o dei Clienti di quest'ultima impone l'esclusivo accesso ai sistemi aziendali attraverso dispositivi di proprietà della Fondazione in dotazione agli Utenti o da essa espressamente autorizzati per iscritto.

L'accesso effettuato da dispositivi personali e non autorizzati (quali ad esempio: smartphone, tablets, PC di proprietà dell'Utente) è da considerarsi una violazione del presente regolamento e del contratto di lavoro da cui il rapporto di dipendenza/collaborazione tra l'Azienda e l'Utente scaturisce.

19. Sicurezza archivi cartacei.

Il dipendente/collaboratore, in generale, ha l'obbligo di:

- evitare che persone non autorizzate possano leggere, copiare o comunque impossessarsi dei dati personali in sua custodia;
- restituire o distruggere gli atti e i documenti contenenti dati personali al termine delle operazioni affidategli.

E' fatto obbligo al dipendente di custodire il materiale cartaceo derivante da file affinché nessuno ne prenda visione, possa manipolarlo o riprodurlo.

È fatto divieto lasciare qualsiasi documento incustodito presso la propria postazione qualora sia previsto un allontanamento per un lasso di tempo tale da consentirne eventualmente la visione da parte di terzi.

È fatto divieto lasciare qualsiasi documento in locali estranei alla propria postazione, prestando particolare attenzione a non lasciarli presso la fotocopiatrice

L'archivio relativo ai documenti del personale non più in servizio è collocato in un locale idoneo e ad esso può accedere solo personale autorizzato.

In questo locale, ci si deve attenere in modo rigoroso al divieto di fumare. Deve essere sempre a portata di mano un estintore a CO2, il cui modo d'impiego deve essere noto, secondo le disposizioni impartite ai sensi del D. lgs. 81/08 e succ. modif. e/o integr.

Chiunque abbia la disponibilità di archivi cartacei deve custodirne le chiavi in modo da impedire l'accesso alla documentazione ivi contenuta a soggetti non autorizzati.

20. Distruzione documenti cartacei.

Per procedere alla distruzione dei documenti l'azienda si avvale di trituratori con taglio a croce in grado di creare frammenti di carta con dimensione $\leq 160mm^2$ e larghezza particella 6 mm max – livello di sicurezza P-4 - Classe di protezione 2: Elevata necessità di protezione per dati riservati. La divulgazione non autorizzata comporterebbe enormi conseguenze per l'azienda e potrebbe violare obblighi contrattuali o di legge. La protezione di dati personali deve soddisfare elevati requisiti. Diversamente sussiste il rischio che vengano seriamente compromesse la posizione e le condizioni economiche del soggetto interessato.
Iniziata la procedura, questa non deve essere interrotta fino a quando tutti i documenti non siano stati eliminati. Se la quantità di materiale da smaltire è eccessiva rispetto alla capienza della macchina in uso, svuotare l'apposito cestino prima di proseguire.

21. Riservatezza dei dati.

L'Utente non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto dalla Fondazione, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi.
Tali obblighi non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che l'Utente possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.
Per «Informazioni Riservate» si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento di mansioni per le quali il soggetto è stato assunto dalla Fondazione.
L'Utente si impegna a:
- considerare le Informazioni Riservate come strettamente private e riservate e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni;
- ad utilizzare le Informazioni Riservate unicamente allo scopo di effettuare lo svolgimento dell'attività cui è preposto e di conseguenza a non usare tali informazioni in alcun modo che arrechi danno alla Fondazione, né per alcun altro scopo di qualsiasi natura.

L'obbligo di riservatezza non opera in caso di Informazioni Riservate: a) che al momento in cui vengono rese note siano di pubblico dominio; b) che diventino di pubblico dominio dopo essere state rese note per causa non imputabile all'Utente.

22. Ulteriori misure di sicurezza.

E' compito del Titolare, con l'ausilio del DPO, informare e delucidare regolarmente sul concetto di sicurezza tutti coloro che hanno anche fare con gli strumenti informatici, nonché richiamare l'attenzione sulle conseguenze di una violazione delle norme di sicurezza.

23. Trattamento dei dati affidati all'esterno.

Qualora si renda necessario, previa autorizzazione del Titolare del trattamento o del soggetto autorizzato, trasferire dati personali all'esterno in esecuzione di accordi commerciali e contratti di prestazione, i soggetti esterni (individuali o giuridici) saranno nominati Responsabili Esterni del Trattamento ex art. 28 Reg. UE 2016/679.

Essi dovranno impegnarsi formalmente ad operare nel rispetto della normativa vigente e a garantire la segretezza, l'accurata custodia e la restituzione all'Ente dei dati personali attenendosi scrupolosamente alle istruzioni scritte impartite dalla Fondazione.

24. Disposizioni finali.

La Fondazione non effettua in nessun caso trattamenti di dati personali mediante sistemi hardware e/o software che comportino il controllo a distanza dei lavoratori, come, ad esempio, la riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dai lavoratori o la lettura e/o registrazione sistematica di messaggi di posta elettronica e dei relativi dati esteriori, oltre ciò che sia tecnicamente necessario per svolgere il servizio e-mail.
L'attivazione di controlli, anche individualizzati, avverrà soltanto in presenza di sospetti, che siano gravi, precisi e concordanti, circa la sussistenza di comportamenti illeciti nell'uso dei dispositivi e strumenti aziendali (cd. controlli difensivi).
Il mancato rispetto o la violazione delle norme descritte nel presente Regolamento lede il rapporto di fiducia instaurato con l'Azienda.
Nei casi in cui l'inosservanza delle norme in questione venga valutata come inadempimento alle obbligazioni contrattuali del rapporto di lavoro dipendente o di collaborazione, potranno essere intraprese azioni disciplinari, civili e penali nei limiti previsti dalla legge e dal CCNL di categoria.
Napoli, lì 31.10.2019

Il Titolare del Trattamento
Fondazione Teatro di San Carlo
Rosanna Purchia