Azienda Ospedaliera 'S. Maria' – Terni

AZIENDA OSPEDALIERA SANTA MARIA TERNI

Deliberazione del Commissario Straordinario n. 882 del 30/12/2019

Oggetto: Regolamento utilizzo dei sistemi informatici aziendali e Regolamento sull'utilizzo di Internet - posta elettronica- telefono-fax. Approvazione.

Ufficio proponente: Ufficio Affari Legali

Esercizio	**assente**
Centro di Risorsa	**assente**
Posizione Finanziaria	**assente**
Importo	**assente**
Prenotazione Fondi	**assente**

IL COMMISSARIO STRAORDINARIO

Vista la proposta di delibera di pari oggetto dell'Ufficio Proponente di cui al num. Provv. 2333 del 20/12/2019 contenente:

- Attestazione del Dirigente della Direzione Economico Finanziaria in ordine alla regolarità contabile - Dott. Riccardo BRUGNETTA;
- il Parere del Direttore Amministrativo - Dott.ssa Sabrina SOCCI;
- il Parere del Direttore Sanitario - Dr. Massimo DE FINO.

DELIBERA

Di fare integralmente propria la menzionata proposta di delibera che allegata al presente atto ne costituisce parte integrante e sostanziale e di disporre quindi così come in essa indicato.

IL COMMISSARIO STRAORDINARIO
(Dott. Andrea CASCIARI)*

* La presente copia è conforme al documento originale ai sensi del D.Lgs. n. 82/2005. Il corrispondente documento digitalmente firmato è conservato negli Archivi del Azienda Ospedaliera "S.Maria" di Terni.

Richiamate :

-la deliberazione del D.G. n.422 del 22.05.2018 con la quale è stato nominato il Responsabile della Protezione dei Dati (RDP) dell'Azienda Ospedaliera " S. Maria" di Terni, in ottemperanza a quanto previsto dall'art. 37 del Regolamento Europeo, individuato nella persona della responsabile dell'Ufficio Affari legali dott.ssa Giuseppina Ferraro ;

-la deliberazione del Commissario Straordinario n. 212 del 29.05.2019 avente ad oggetto " Processo di attuazione del Regolamento Europeo sulla Protezione dei dati Personali 2016/679.primi adempmenti";

-la Deliberazione del D. G. n. 720 del 2018 avente ad oggetto *Costituzione Team multidisciplinare per l'adeguamento al GDPR e a supporto del responsabile del Trattamento dei dati (DPO);*

Atteso che il GDPR dichiara che "la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale" e che esso "protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali";

Che questa Azienda ha inteso di adottare un nuovo approccio nel trattamento dei dati personali, sia degli **utenti** che accedono alle strutture aziendali, sia degli **operatori** che vi lavorano. In particolare, sono previsti in capo all'Azienda/Titolare del trattamento nuovi adempimenti e un'intensa attività di adeguamento alla normativa comunitaria, obiettivi non semplici in una realtà sanitaria di grandi dimensioni, in cui quotidianamente vengono trattati migliaia di dati estremamente delicati come quelli riguardanti la salute delle persone;

Che la gestione di un sistema complesso come quello della Azienda Ospedaliera " S.Maria" di Terni, che tratta dati particolari e, per la maggior parte, relativi alla salute, ha fatto sì che questa Direzione Aziendale abbia ritenuto indispensabile redigere il Regolamento Aziendale concernente l'utilizzo dei sistemi informatici Aziendali ed il Regolamento sul Corretto Uso di Internet - Posta Elettronica –Telefono /Fax;

Visti i Regolamenti concernenti l'utilizzo dei sistemi informatici Aziendali ed il Corretto Uso di Internet-Posta Elettronica-Telefono /Fax , redatti dal Responsabile dell'Ufficio legale che sono parte integrante e sostanziale del presente atto;

Preso atto della nota email del 28.10.2019 con la quale il Responsabile dell'Ufficio informatico ha espresso parere positivo in merito alle misure contenute nei menzionati Regolamenti;

Ritenuto che i menzionati Regolamenti si applicano a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (a titolo esemplificativo lavoratori somministrati, collaboratori a progetto, in stage, specializzandi, personale universitario, altro) oltre che ai dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'Azienda;

SI PROPONE DI DELIBERARE

* La presente copia è conforme al documento originale ai sensi del D.Lgs. n. 82/2005. Il corrispondente documento digitalmente firmato è conservato negli Archivi del Azienda Ospedaliera "S.Maria" di Terni.

-di approvare, per le motivazioni di cui alle premesse, il Regolamento Aziendale concernente l'utilizzo dei sistemi informatici aziendali ed il Regolamento sul Corretto Uso di Internet - Posta Elettronica –Telefono /Fax, da intendersi parte integrante e sostanziale del presente provvedimento;
-di trasmettere i menzionati Regolamenti, al fine di darne la massima pubblicità, all'ufficio preposto che ne garantirà la pubblicazione e la consultazione sul sito web aziendale, nonché a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (a titolo esemplificativo lavoratori somministrati, collaboratori a progetto, in stage, specializzandi, personale universitario, altro) oltre che ai dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'Azienda per consentirne la più idonea diffusione ;

-di trasmettere il presente provvedimento all'Ufficio Relazioni Sindacali per darne informativa alle OO.SS. delle varie aree contrattuali;

-di disporre che il presente atto venga pubblicato nell'albo pretorio on line aziendale ai sensi dell'art. 32, comma 1, della legge 18.09.2009, n. 69 e del D.Lgs 14.03.2013 n. 33;

- **di individuare** quale responsabile del procedimento amministrativo ai sensi della L. 241/90 la Dott.ssa Giuseppina Ferraro , Collaboratore Amministrativo Professionale Esperto.

Responsabile del Procedimento
Dott.ssa Giuseppina Ferraro

Responsabile Ufficio Affari Legali
Dott.ssa Giuseppina Ferraro

* La presente copia è conforme al documento originale ai sensi del D.Lgs. n. 82/2005. Il corrispondente documento digitalmente firmato è conservato negli Archivi del Azienda Ospedaliera "S.Maria" di Terni.

AZIENDA OSPEDALIERA SANTA MARIA TERNI

REGOLAMENTO
SUL CORRETTO USO DI INTERNET - DELLA POSTA ELETTRONICA – DEL TELEFONO /FAX

approvato con deliberazione n. ..... del .....

UTILIZZO DELLA POSTA ELETTRONICA

Il dipendente è tenuto ad un corretto uso dei servizi informatici che l'A.O. gli mette a disposizione per svolgere la propria attività lavorativa. Tra essi v'è anche la casella di posta elettronica (cd. mailbox).
Essa, seppur contraddistinta da diversi username di identificazione e password di accesso, è da ritenersi equiparata ai normali strumenti di lavoro dell'ente e viene quindi messa a disposizione dei singoli dipendenti o collaboratori per lo svolgimento dell'attività lavorativa agli stessi demandata.
L'uso improprio della posta elettronica costituisce violazione dell'obblighi di diligenza e fedeltà di cui agli artt. 2104 e 2105 del codice civile con conseguente possibilità per l'A.O. di irrogare sanzioni disciplinari al lavoratore che per l'appunto la utilizzi indebitamente.
La casella di posta elettronica è dunque di proprietà dell'A.O., considerando anche che in genere l'account è così contraddistinto: nome (o semplice iniziale).cognome dell'incaricato@ente.it (es. m.rossi@aospterni.it).
L'account è pur sempre riservato, ma in tali casi personalità dell'indirizzo non significa "privatezza" del medesimo poiché l'indirizzo aziendale – al di là dell'uso di intestazioni apparentemente personali del lavoratore quale principale utilizzatore – proprio in quanto tale, per sua intrinseca natura, può sempre essere nella disponibilità di accesso e lettura da parte di soggetti diversi, sempre appartenenti alla struttura aziendale, rispetto al suo consuetudinario utilizzatore al fine, per esempio, di consentire la regolare continuità della attività dell'ente nelle frequenti ipotesi di sostituzioni di colleghi per ferie, malattia, gravidanza etc. Pertanto, così come non può configurarsi un diritto del lavoratore ad accedere in via esclusiva al computer aziendale, parimenti non appare astrattamente prospettabile un suo diritto all'utilizzo esclusivo e riservato di una casella di posta elettronica aziendale.
Ciò implica che su richiesta dell'A.O. il personale addetto ai Sistemi Informativi possa accedere alla mailbox, eventualmente modificando le credenziali di accesso. L'A.O. provvederà ad informare ex post (cioè ad intervento effettuato) la persona, stendendo apposito verbale, in cui verranno spiegate modalità e motivazioni dell'intervento stesso.
Sarà cura dell'A.O. mettere a disposizione dell'incaricato anche apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente in caso di assenze (per es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto dell'incaricato assente o della struttura. Preferibilmente dovrebbero essere indicati account generici, es. info@ente.it oppure urp@ente.it oppure ufficioreclami@azienda.it (account cc.dd. condivisi), senza che sia indicato un account specifico né un numero interno. Non deve essere indicato il motivo dell'assenza.

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

AZIENDA OSPEDALIERA SANTA MARIA TERNI

Allo stesso modo non deve essere indicata la propria mailbox privata (non aziendale) o il proprio numero di cellulare.
È opportuno indicare il numero del centralino generale o di reparto, ove il mittente possa far presente le proprie esigenze.
I messaggi di posta elettronica dovranno contenere un disclaimer o avvertimento, rivolto ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute anche da altri membri dell'organizzazione di appartenenza del mittente, con eventuale rinvio alla policy adottata dalla stessa.
Stanti i principi di necessità, proporzionalità (pertinenza e non eccedenza), finalità, liceità, correttezza e trasparenza del trattamento dei dati personali, il controllo o il monitoraggio delle mail non potrà che essere graduale, dovendosi così escludere l'ammissibilità di controlli prolungati, costanti o indiscriminati e sono comunque vietate la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail. Trattandosi poi di controlli a distanza sarà certamente applicabile la disciplina di cui all'art. 4 della legge 300/1970, in modo che la policy sia trasparente e condivisa tra ente e lavoratori.

Ogni forma di controllo occulto è vietata e comunque l'A.O. non utilizza "sniffer" o altri dispositivi hardware o software finalizzati all'intercettazione e/o all'interruzione e/o all'impedimento di comunicazioni telematiche, come quelle che avvengono tramite e-mail.

- La casella di posta interna deve essere utilizzata esclusivamente per le comunicazioni inerenti la propria funzione lavorativa e le mansioni assegnate. È generalmente vietato l'uso a carattere personale (messaggi ad amici, corrispondenza sentimentale, appuntamenti extra-lavorativi, ordinazioni via mail a imprese commerciali etc.), ma è tollerato un uso minimo e per comunicazioni urgenti a familiari o parenti. Sarà cura dell'A.O. predisporre eventuali macchine di contenimento per l'uso privato della posta elettronica da parte dei lavoratori.

- Le e-mail non provenienti dagli organi apicali o dagli organi di management dell'A.O. ovvero provenienti da mittenti sconosciuti o con oggetto in lingua straniera o allusivo o non facente riferimento all'attività dell'ente, devono essere cestinate senza essere lette e immediatamente cancellate dal cestino.

- È assolutamente vietato eseguire o estrarre gli allegati delle e-mail, del cui contenuto o della cui provenienza non si è sicuri (si pensi a messaggi con oggetto in lingua straniera o in apparenza accattivante e stimolante la curiosità): gli allegati possono, infatti, contenere virus o altri codici maligni, nascosti nell'allegato (tecnica "troiana"), che possono avere come scopo o effetto l'indebita appropriazione e divulgazione di password o di altri codici d'accesso ovvero il danneggiamento di dati dell'A.O. ovvero l'interruzione, anche solo temporanea o parziale, del funzionamento dei sistemi informatici o la compromissione della loro sicurezza. Tuttavia è possibile configurare il firewall per bloccare preventivamente mail con allegati infetti o per effettuare lo screening preventivo degli stessi. Nel caso comunque

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

che mail con allegato provengano da persone note, è buona prassi chiedere prima conferma per telefono.

- È vietato cliccare sui link presenti nel corpo delle mail di incerto contenuto o provenienza (ut supra): anche il click su tali link potrebbe attivare virus e altri codici maliziosi, come sopra visto per gli allegati o potrebbe comunque attivare procedure di download (o comunque consentire l'intrusione) di codice arbitrario o malizioso (cross site scripting o XSS).

- Non è consentito utilizzare l'indirizzo di posta elettronica lavorativo per inviare o memorizzare messaggi (interni o esterni) di natura minatoria, ingiuriosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, così come più in generale è assolutamente vietato utilizzare la mail per commettere reati di ogni sorta (es. trasmissione, in HTML o in allegato, a una o più persone, di immagini o file pedopornografici ovvero archiviazione dei medesimi in cartelle di posta appositamente create; rivelazione di password o di codici d'accesso, indebitamente ottenuti, a terze persone, con o senza compenso; tentativi di estorcere danaro dietro minaccia; istigazione a delinquere o a violare le leggi dello Stato; propaganda sovversiva o a scopo terroristico; istigazione all'odio razziale...).

- Non è consentito utilizzare l'indirizzo di posta elettronica lavorativo per la partecipazione, in Internet, a dibattiti, forum, newsgroup o mailing-list non attinenti all'attività istituzionale dell'ente o estranei all'attività lavorativa.

- Non è consentito aderire o rispondere a messaggi che invitano ad inoltrare e perpetuare (verso ulteriori indirizzi e-mail) contenuti o documenti oggetto delle cosiddette "catene di S. Antonio", così come è vietato inoltrare falsi allarmi, false richieste di aiuto etc. (joke, hoax etc.).

- È vietato trasmettere materiale commerciale e/o pubblicitario non richiesto.

- È vietato utilizzare la posta elettronica per comunicare ad altri utenti informazioni di qualsiasi tipo relativamente ai virus. Questa misura serve ad evitare l'invio di un elevato numero di messaggi del tipo "c'è un virus in circolazione". In caso di sospetta presenza di virus informatico, bisogna invece avvisare telefonicamente l'Help Desk che fornirà le indicazioni su come operare.

- È assolutamente vietato inviare messaggi di posta elettronica in caso di accertata presenza nel sistema di virus informatici o di altri malware (codici maligni): la posta elettronica potrà essere riutilizzata solo dopo la rimozione del virus.

- Bisogna porre particolare attenzione ai messaggi con i quali si richiedano al lavoratore la comunicazione di password o di altri codici identificativi che devono restare riservati: in

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

genere essi non vengono richiesti via mail, ma per la comunicazione vengono utilizzati canali più sicuri e comunque ufficiali e autorizzati dall'A.O.. Potrebbe infatti trattarsi di attività fraudolente di social engineering (ingegneria sociale o "arte dell'inganno"), quali lo scam (truffa alla nigeriana), il phishing o altri tentativi di furto di identità ("identity theft").

- In caso di spamming (comunicazioni pubblicitarie non sollecitate o pubblicità indesiderata), è consigliabile non rispondere, soprattutto a fronte di messaggi che invitano a cancellarsi con un click su una determinata area della mail contraddistinta da un link. Infatti il click non serve ad altro che a far sapere allo spammer che l'account è attivo.

- Non è consentito effettuare comunicazioni di tipo finanziario, ivi comprese le operazioni di remote banking, né possono essere poste in essere attività di e-commerce, acquisti on-line e simili, salvo diversa ed esplicita autorizzazione e sempre per finalità istituzionali.

- Non è consentito simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta, non proprie, per l'invio di messaggi (c.d. mailspoofing).

- L'utente non può esprimere via mail posizioni che facciano ritenere che egli stia parlando in nome e per conto dell'A.O., a meno che non sia stato appositamente delegato o autorizzato per farlo.

- Non è consentito prendere visione della posta altrui, se non a fronte di apposita delega da parte del proprietario della casella postale (vedi la procedura di cui al paragrafo precedente).

- Il lavoratore non utilizzerà sistemi client di posta elettronica che non siano stati previamente testati e autorizzati dal personale addetto ai Sistemi Informativi dell'A.O.: infatti in seguito alla semplice visualizzazione della posta scaricata nell'anteprima di molti client, quando il formato utilizzato è quello "HTML", è possibile contrarre virus o altri codici maliziosi. Onde evitare inutili rischi, sempre che si voglia utilizzare un client di posta elettronica, risulterà molto utile disattivare la cd. "anteprima", come per es. quella di "Outlook Express".

- Non è consentito l'utilizzo di programmi di crittografia e steganografia non previsti esplicitamente dal security management dell'A.O..

- Per quanto possibile, non dovrebbe consentirsi la comunicazione di dati delicati come quelli sensibili o giudiziari attraverso la mail, salve eventuali cautele stabilite dall'A.O. (per es. posta elettronica certificata, protocollo S/Mime, utilizzo di allegati compressi e protetti con password robuste o cifrati tramite l'uso di crittografia simmetrica DES, 3DES o meglio AES, etc.). E in tal senso va incentivato e favorito l'uso della posta elettronica certificata o P.E.C. (v. D.P.R. 68/2005 e art. 48 del D.Lgs. 82/2005 e succ. modif.), almeno per le comunicazioni di carattere ufficiale (per es. contatti con enti pubblici o con aziende fornitrici) e per la trasmissione di dati particolarmente delicati (es. dati sensibili, soprattutto quelli

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

sulla salute e sulla vita sessuale) in modo che possa esserne garantita l'inalterabilità, l'integrità e l'autenticità per tutto il corso della trasmissione del file da una mailbox all'altra, dal momento dell'invio/inoltro a quello di arrivo (momenti entrambi che la tecnologia della P.E.C. è in grado di certificare e di rendere certo e opponibile a terzi).

- La mail deve essere firmata (basta la semplice indicazione del nome e cognome del mittente), ma non va assolutamente usato lo specimen, ossia l'immagine scannerizzata della propria firma fisica. Semmai si possono utilizzare software per la generazione di firme digitali o comunque, per le comunicazioni ufficiali (v. punto precedente) è sempre preferibile l'uso della posta elettronica certificata.
- Qualsiasi utilizzo non conforme alla presente policy e/o alle leggi vigenti resterà esclusivamente a carico dell'utilizzatore, che se ne accollerà le rispettive responsabilità e conseguenze sul piano civile, penale, disciplinare. A tal proposito l'A.O. si riserva il diritto di verificare l'attuazione della policy e di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituenti reato, mentre si riserva di agire comunque sotto il profilo civilistico e disciplinare in caso di ogni tipo di violazione o di illecito, anche se non rivesta rilevanza penale.

REGOLE PER UNA SICURA LEGITTIMA NAVIGAZIONE IN INTERNET (Codice Etico)

La navigazione in Internet deve avvenire esclusivamente a fini lavorativi.

- È vietato svolgere attività di e-commerce, shopping virtuale o trading online.

- È vietato scaricare software da siti web; dove ciò sia assolutamente necessario a fini lavorativi, gli utenti devono accertarsi che siano state adottate le opportune precauzioni per proteggere le risorse di A.O., informatiche e di rete, quando si scaricano programmi, file o dati da Internet. È richiesta la conformità totale alle regole della policy AV, con particolare riferimento al divieto di download di immagini (.jpg, .gif etc.) o di file di testo cc.dd. a rischio (es. i formati word con estensione .doc o altri formati come excel, che potrebbero contenere macro) o file audio o video o audio-video (quale che ne sia l'estensione: .mp3, .avi, .mpg, .wmv etc.), salvo autorizzazione e salvo lo screening preventivo. Gli utenti non devono intenzionalmente sviluppare, scaricare o in qualche modo installare programmi o altri software che possano insidiare risorse informatiche o di rete dell'A.O. e/o danneggiare o modificare il software, l'hardware o le informazioni in tali risorse contenute. I file cc.dd. eseguibili (con estensioni .exe) e in genere i file con estensioni a rischio (.cab, .com, .pif etc.) non devono mai essere aperti, salvo screening preventivo e autorizzazione del personale addetto ai Sistemi Informativi.

- In generale è proibito svolgere sulla rete ogni attività vietata dalla legge dello Stato, dalle normative vigenti nei Paesi ospitanti i servizi di rete che vengono acceduti e dalla normativa internazionale, nonché dai regolamenti e dalle consuetudini di utilizzo delle reti e dei servizi di rete acceduti (netiquette). Sono dunque consentite solo le attività che non arrechino

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

danno ad altri utenti o all'A.O. e che comunque non siano in contrasto con il presente documento e con le norme legislative vigenti.

- È assolutamente vietato accedere abusivamente a sistemi informatici altrui o intrattenervisi senza il consenso dell'avente diritto, ovvero diffondere virus, worm, trojan, bot o altri programmi la cui presenza danneggia la rete e/o le risorse ad essa collegate, così come è vietato intercettare abusivamente comunicazioni telematiche altrui, pubblicare su siti web password o altri codici d'accesso (atti di criminalità informatica - legge 547/1993).
- È assolutamente vietato compromettere l'integrità dei sistemi o dei servizi o delle risorse di rete attraverso attacchi DoS o DDoS (diniego di servizio, syn-flooding, net-straking, mail-bombing), avvalendosi o meno di programmi maliziosi, come worm o bot o backdoor o rootkit.

- È assolutamente vietato violare la privacy di altri utenti e più in generale l'integrità e la riservatezza di dati personali altrui, così come è vietato utilizzare servizi o risorse di rete in modo da danneggiare o molestare altre persone o da attentare alla dignità umana (es. realizzazione di servizi di internet relay chat o blog o forum o newsgroup o siti a sfondo terroristico, razzista, diffamatorio, pedopornografico o inneggianti all'odio religioso etc.).

- È assolutamente vietato creare o trasmettere qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno o indecente, specialmente se riguardante il sesso, la razza o il credo.

- È vietato creare o trasmettere materiale finalizzato allo scopo di arrecare disturbi o produrre ingiustificate preoccupazioni (es. falsi allarmi, catene di Sant'Antonio, joke, hoax etc.).

- È assolutamente vietato il consumo di risorse in misura tale da compromettere l'efficienza di altri servizi di rete, per es. occupando indebitamente la banda di trasmissione tramite servizi di peer-to-peer o di file-sharing, sia in upload, sia in download, sia in condivisione, condotte tra l'altro sanzionate, a seconda dei casi, in via civile, amministrativa e penale dalla legge sul diritto d'autore (legge 633/1941 e successive modifiche.

- È vietato usare sistemi cc.dd. "rogue", quali notebook, cellulari non aziendali, laptop, I-Pod, lettori mp3 in particolare per effettuare il download dalla rete, se non sono stati preventivamente autorizzati.

- È assolutamente vietato impedire l'uso della rete ad altri utenti legittimi, per esempio sovraccaricando le linee di accesso o gli apparati di commutazione, ovvero accedere alla rete con apparecchiature o software che interferiscono con il corretto funzionamento della rete stessa o di altre reti ad essa collegate.

- È assolutamente vietato permettere il transito di dati e/o informazioni sulla rete tra due soggetti entrambi non ammessi all'accesso sulla rete intranet (third party routing).

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

- Possono essere visitati solo siti a carattere istituzionale e per scopi strettamente legati all'espletamento delle proprie mansioni lavorative o comunque per necessità professionali, di aggiornamento professionale, normativo etc. È assolutamente vietato visitare siti illegali (es. siti di cracking o diffamatori o pedopornografici etc.) e a rischio (siti commerciali, siti pornografici, BBS clandestini etc.). Per la navigazione non istituzionale l'A.O. si riserva di mettere a disposizione dei lavoratori macchine di contenimento per gli orari di pausa, sempre che la navigazione non avvenga per scopi illeciti o comunque su siti illegali e a rischio. In alternativa l'A.O. si riserva di istallare strumenti necessari al filtraggio dei contenuti (URL filtering o content filtering), per mezzo dei quali in via preventiva è inibito l'accesso a determinati siti che presentino un determinato indirizzo IP o URL o particolari stringhe di testo, tag, directory etc..

- È assolutamente vietato collegarsi, con computer dell'A.O., alla rete Internet utilizzando chiavette USB e/o interfacce PCMCIA che sfruttano la connessione via cellulare (GSM, UMTS, GPRS).

In caso di mancato rispetto o violazione delle suddette regole o comunque nel caso di comportamenti non consentiti o non conformi al presente regolamento, l'amministratore di rete ovvero il responsabile del trattamento dei dati personali può sospendere temporaneamente l'accesso ai servizi informando gli organi di management.
Ogni unità operativa, congiuntamente all'ufficio Risorse Umane e all'ufficio Legale, deve sviluppare ed implementare una pratica disciplinare formale per i casi di non conformità alle policy e alle pratiche interne.
Restano salve le eventuali responsabilità civili, amministrative e penali di chiunque abbia commesso illeciti e la cui responsabilità sia stata accertata.

USO DEL TELEFONO

L'uso di telefoni aziendali è consentito esclusivamente per motivi aziendali.

In deroga a quanto sopra è concesso agli utenti di usare il telefono per comunicazioni personali solo in caso di necessità quali ad esempio:

- Avvisare membri della famiglia di ritardi o imprevisti;
- Per motivi di sicurezza della famiglia;
- Per necessità impreviste.

In ogni caso le conversazioni dovranno essere limitate in durata alla effettiva necessità.
Non possono essere utilizzati né telefoni né fax per comunicare informazioni riservate.
Nell'invio di telefax occorre utilizzare il frontespizio dell'Azienda.

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

AZIENDA OSPEDALIERA SANTA MARIA TERNI

Redatto a cura del DPO
Ferraro Giuseppina

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

AZIENDA OSPEDALIERA SANTA MARIA TERNI

REGOLAMENTO
CONCERNENTE L'UTILIZZO
DEI SISTEMI INFORMATICI AZIENDALI

approvato con deliberazione n. ..... del .....

CAPO I – DISPOSIZIONI GENERALI
Art. 1 – Oggetto e principi generali
Art. 2 – Campo di applicazione
Art. 3 – Definizioni
Art. 4 – Gestione assegnazione delle credenziali di autenticazione

CAPO II – DISPOSIZIONI PER L'UTILIZZO DEI SISTEMI INFORMATICI
Art. 5 – Utilizzo della rete informatica aziendale
Art. 6 – Utilizzo del personal computer / dispositivo postazione
Art. 7 – Utilizzo di telefoni, scanner, fotocopiatrici, stampanti
Art. 8 – Utilizzo di Notebook, Smartphone, Tablet e relative applicazioni mobili (APP)
Art. 9 – Utilizzo delle memorie esterne (chiavi UUSB, Hard Disk, Memory Card, CD Rom, DVD Rom, ecc.)
Art. 10 – Utilizzo di infrastruttura di rete e File System
Art. 11 – Protezione Antivirus
Art. 12 – Modifiche delle risorse ICT
Art. 13 – Smarrimento e furto delle risorse ICT
Art. 14 - Sanzioni

CAPO III – NORME FINALI
Art. 15 – Norma di rinvio
Art. 16 – Entrata in vigore

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

AZIENDA OSPEDALIERA SANTA MARIA TERNI

CAPO I – DISPOSIZIONI GENERALI

Art. 1/2 - OGGETTO E PRINCIPI GENERALI

Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (a titolo esemplificativo lavoratori somministrati, collaboratori a progetto, in stage, specializzandi, personale universitario, altro) oltre che ai dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'Azienda.

Poiché attraverso il Sistema informativo Aziendale sono trattati dati personali e sensibili le disposizioni in materia di sicurezza approvate ed adottate soddisfano anche lo scopo di rispettare la normativa vigente in materia di privacy e di protezione dei dati personali.

Art. 3 - DEFINIZIONI

Ai fini del presente regolamento si intende per:

- **Utente:** è la persona autorizzata ad accedere alla rete informatica aziendale, ad internet e alla posta elettronica, agli applicativi aziendali e alle altre risorse informatiche e telematiche a ciò autorizzato;
- **Autorizzato al trattamento:** è la persona fisica autorizzata a compiere operazioni di trattamento dal titolare;
- **E-mail:** indica la funzione di posta elettronica per lo scambio di messaggio e di documenti;
- **Download (in italiano scaricamento)**: è l'azione di ricevere o prelevare dalla rete informatica un file trasferendolo sul disco rigido del computer o su altra periferica dell'utente;
- **Upload (in italiano, caricamento):** è il processo di invio di un file (o più genericamente di un flusso finito di dati o informazioni) ad un sistema remoto attraverso una rete informatica;
- **Freeware:** è un software che viene distribuito in modo gratuito;
- **Shareware:** è un software che può essere liberamente ridistribuito, e può essere utilizzato per un periodo di tempo di prova variabile scaduto il quale per continuare ad utilizzare il software è necessario registrarlo presso la casa produttrice, pagandone l'importo;
- **Ransomware:** è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione.

Art. 4 - GESTIONE E ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

L'abilitazione attraverso le credenziali di autenticazione per l'accesso alla rete informatica viene eseguita dal personale del servizio di assistenza ai Sistemi Informativi o da altro personale all'uopo deputato e deve essere preceduta da regolare richiesta del responsabile di funzione/unità organizzativa, nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente, attraverso il "modulo o procedura informatizzata (se attivata) di abilitazione utente".

Lo stesso responsabile è tenuto a dare repentina comunicazione nel caso di revoca e/o trasferimento degli utenti della propria funzione/unità organizzativa.

Nel caso di collaboratori la preventiva richiesta, se necessario, verrà inoltrata direttamente dal responsabile del servizio con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (User ID), assegnato dal servizio di assistenza ai Sistemi Informativi o da altro personale all'uopo deputato, associato ad una parola chiave (password) riservata, che dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione, senza preventiva autorizzazione da parte del servizio di assistenza ai Sistemi Informativi.

La parola chiave deve rispettare le regole di complessità previste dai singoli applicativi e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

Al primo utilizzo della rete informatica aziendale verrà chiesto obbligatoriamente di sostituire la parola chiave rilasciata dal servizio per l'informatica o da altro personale all'uopo deputato, sarà poi il sistema a chiedere la sostituzione della stessa ogni tre mesi.

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, il responsabile di funzione/unità operativa dovrà richiedere una nuova password di accesso al personale dei Sistemi Informativi o da altro personale all'uopo deputato.

Soggetto preposto alla custodia delle credenziali di autenticazione alla rete informatica è il personale incaricato del servizio di assistenza ai Sistemi Informativi dell'Azienda.

CAPO II – DISPOSIZIONE PER L'UTILIZZO DEI SISTEMI INFORMATICI

Art. 5 - UTILIZZO DELLA RETE INFORMATICA AZIENDALE

Tutti gli Utenti devono utilizzare le risorse ICT, fornite dall'Azienda, in maniera diligente, in modo appropriato, efficiente, rispettoso e per motivi lavorativi.

Gli Utenti devono utilizzare le risorse ICT solamente per fini professionali (in relazione alle mansioni assegnate) e per conto dell'Azienda, evitando l'uso per attività non pertinenti (ad esempio esecuzione di programmi di intrattenimento, giochi on line, etc.).

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

AZIENDA OSPEDALIERA SANTA MARIA TERNI

Al fine di scongiurare i rischi derivanti dall'effetto "bridge" (ponte) tra la rete Intranet aziendale ed altre reti, gli Utenti devono evitare di accedere dall'esterno della rete Intranet ai servizi di posta elettronica aziendali e/o al servizio web aziendale e contemporaneamente ad altri siti Internet potenzialmente pericolosi.

Particolare cautela deve essere posta, inoltre, nell'utilizzo di reti Wi-Fi gratuite per accedere alla rete Intranet e ai servizi di posta elettronica aziendale dal momento che nell'accedere a tali servizi devono essere inserite le credenziali e che queste ultime potrebbero essere facilmente carpite da malintenzionati/hacker.

Gli Utenti non devono eseguire copie (anche parziali) di software protetto da leggi sul diritto d'autore che non sia già installato sui dispositivi forniti in uso dall'Azienda.

Gli utenti, in generale, sono tenuti a:

- Sottoporre a scansione antivirus preventiva gli eventuali supporti mobili utilizzati (pendrive USB, CDROM/DVD, hard disk esterni, ecc.) prima di utilizzare le risorse negli stessi contenuti;
- Modificare periodicamente le password, di cui al precedente art.2 c.2.4 del presente Regolamento;
- Presidiare le risorse ICT al fine di evitare l'accesso a soggetti terzi non autorizzati;
- Bloccare i dispositivi connessi alla rete nel caso in cui non si possano presidiare i dispositivi medesimi;
- Non trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Organizzazione, salvo specifica autorizzazione;

Evidenziando, ulteriormente, che il sistema informatico aziendale è composto da un insieme di unità server centrali e dispositivi/postazioni informatiche connessi o meno alla rete aziendale, comunque messi a disposizione dall'Organizzazione agli Utenti per lo svolgimento dei compiti affidati e che utilizzano diversi sistemi operativi e applicativi, si avverte che l'Azienda non effettua il backup dei dati memorizzati localmente.

I file creati, elaborati o modificati sul dispositivo/postazione locale assegnato e di cui risulta necessario assicurare l'integrità dei dati in caso di rottura del device stesso, devono essere salvati nei server/Nas o comunque in una struttura centrale, comunicati e messi a disposizione dall'Azienda.

Le cartelle utenti presenti nei server/Nas o comunque in una struttura centrale dell'Azienda 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. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio.

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

Tutti i documenti per cui si renda necessaria la garanzia della conservazione devono essere posizionati nei server/Nas, comunque in una struttura centrale, o copiati sugli stessi periodicamente.

Il personale addetto ai Sistemi Informativi potrà in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui personal computer degli incaricati sia sulle unità di rete.

Risulta opportuno che, con regolare periodicità (almeno ogni mese), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante in ossequio al principio della minimizzazione del trattamento dei dati.

Art. 6 - UTILIZZO DEL PERSONAL COMPUTER / DISPOSITIVO / POSTAZIONE

Il personal computer/dispositivo/postazione affidato all'utente, si ribadisce ancora una volta, essere 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 dispositivo/postazione deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

Il personal computer dispositivo/postazione dato in affidamento all'utente permette l'accesso alla rete dell'Azienda solo attraverso specifiche credenziali di autenticazione come meglio descritto precedentemente.

L'Azienda rende noto che il personale addetto ai Sistemi Informativi o altro personale esterno a ciò incaricato è autorizzato a compiere interventi nel 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.).

La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata o impedimento dell'utente.

Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC/dispositivo/postazione, il personale addetto ai Sistemi Informativi o altro personale esterno a ciò incaricato ne darà comunicazione agli utenti interessati preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

Il personale addetto ai Sistemi Informativi o altro personale esterno a ciò incaricato ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro Virus, Spyware, Malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico.

In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale addetto ai Sistemi Informativi o da altro personale esterno a ciò incaricato per conto dell'Organizzazione né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la stessa Azienda a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico dell'Organizzazione), come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

Salvo preventiva espressa autorizzazione del personale tecnico incaricato, non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer dispositivo/postazione né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale addetto ai Sistemi Informativi o altro personale esterno a ciò incaricato nel caso in cui siano rilevati virus e adottando quanto previsto dal presente Regolamento.

Il personal computer dispositivo/postazione 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 senza che vi sia la possibilità di provarne in seguito l'indebito uso.

Art. 7 - UTILIZZO DI TELEFONI, SCANNER, FOTOCOPIATRICI, STAMPANTI

Tutti i dispositivi elettronici dati in dotazione al personale dell'Organizzazione devono considerarsi strumenti di lavoro: ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative. Fra i dispositivi in questione vanno annoverati i telefoni aziendali, PC portatili, Tablet, telefoni cellulari, Smartphone, etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete dell'Azienda o di condividere documenti, dati e materiali ivi conservati e/o trattati.

Il telefono aziendale affidato all'utente è quindi uno strumento di lavoro.

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di necessità ed urgenza evidente, mediante il telefono fisso aziendale a disposizione.

È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salvo diversa autorizzazione.

È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva autorizzazione.

È vietato l'utilizzo di scanner aziendali per fini personali, salvo preventiva autorizzazione da parte del Responsabile dell'unità operativa. Solo in caso di necessità e urgenza, gli Utenti possono utilizzare tali beni per motivi non attinenti all'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati.

Per quanto concerne l'uso delle stampanti gli Utenti sono tenuti a:

- Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
- Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
- Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi.
- Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate.

Il controllo sul corretto utilizzo degli strumenti in parola è affidato ai Responsabili delle Strutture/P.O. a cui detti strumenti sono stati assegnati.

Art. 8 - UTILIZZO DI NOTEBOOK, SMARTPHONE, TABLET E RELATIVE APPLICAZIONI MOBILI (APP)

Fatto salvo il fatto che ai dispositivi mobili si applicano le regole di utilizzo previste per i personal computer/dispositivi/postazione connessi in rete e comunque tutte le policy di sicurezza previste dall'Azienda, l'utilizzo di dispositivi cellulari, Tablet e computer portatili all'esterno dei locali dell'Organizzazione, deve essere oggetto di particolare cura ed attenzione da parte degli Utenti perché tale utilizzo rappresenta una fonte di rischi particolarmente rilevante in termini di sicurezza, sia delle risorse in sé sia dei dati nelle stesse contenuti.

Tali dispositivi, infatti, possono essere soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "infettati" da virus o codice malevole.

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

Per altro un'eventuale contaminazione da virus informatici potrebbe diffondersi e ripercuotersi all'intera rete informatica dell'Azienda, una volta che tali dispositivi siano collegati direttamente alla rete interna.

È necessario, pertanto, adottare ulteriori norme comportamentali nonché specifiche procedure, di seguito descritte, che gli Utenti sono chiamati ad applicare in modo scrupoloso:

- Cifrare i dati (laddove possibile e previa analisi dei rischi/costi-benefici);
- Fare periodicamente delle copie di back-up dei dati e verificarle regolarmente;
- Attestarsi, con frequenza almeno settimanale, alla rete intranet dell'Organizzazione per scaricare gli aggiornamenti forniti dall'Organizzazione (patch, hotfix ed elenchi dei virus);
- Mantenere abilitato l'antivirus;
- Non disabilitare le impostazioni di sicurezza originariamente impostate dall'Organizzazione;
- Evitare di accedere e navigare in siti web "pericolosi" per la sicurezza informatica, a prescindere dal fatto che ciò avvenga al di fuori dell'orario di lavoro;
- Non mantenere abilitati protocolli insicuri di comunicazione, come ad es. il Bluetooth, oltre il tempo strettamente necessario;

Per Notebook e Tablet è fatto divieto abilitare l'utilizzo di configurazioni con cartelle locali di servizi di condivisione file (es. DropBox, OneDrive, Google Drive, etc.) per evitare di memorizzare localmente file aziendali condivisi. L'utilizzo di detti servizi di File Sharing è consentito su questo tipo di dispositivi mobili solamente in modalità "on-line"

Premesso che i terminali di nuova generazione applicati alla telefonia mobile (Smartphone e Tablet) e le relative applicazioni mobili software (note comunemente con l'abbreviazione "App"), sono in fase di evoluzione costante e consentono, con crescente facilità, di utilizzare, registrare e trasmettere dati sensibili tramite diverse tecnologie di rete, comunicando e diffondendo in rete dati e immagini in tempo reale, si fa presente che si tratta di apparecchiature che, per le loro potenzialità, possono essere utilizzate violando, anche involontariamente, i diritti delle persone interessate alla comunicazione, come pure di terzi inconsapevoli.

Per gli Smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "App") diverse da quelle già istallate, salvo specifica autorizzazione.

Ulteriori attenzioni vanno riposte sui dispositivi mobili come computer portatili, Tablet e Smartphone che possono venire concessi in uso dall'Organizzazione agli Utenti "in movimento" ovvero spesso operanti fuori sede e che necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete. Questi particolari Utenti saranno responsabili del loro utilizzo e della loro custodia con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, senza lasciarli incustoditi o a vista all'interno del mezzo di trasporto utilizzato.

Gli strumenti elettronici, di cui al presente punto, che permettono l'attivazione di una procedura di protezione (es. PIN) devono sempre essere abilitabili solo con la digitazione del codice previsto stesso e non possono essere lasciati privi di codice di accesso.

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

AZIENDA OSPEDALIERA SANTA MARIA TERNI

L'Utente dovrà provvedere a trasferire tutti i files creati o modificati sui dispositivi mobili nei supporti locali (Server/Nas) messi a disposizione dell'Organizzazione al rientro in ufficio e cancellarli in modo definitivo dagli strumenti elettronici mobili. In caso di smarrimento o furto dei dispositivi mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'Organizzazione che provvederà - se del caso - ad occuparsi delle procedure connesse alla tutela dei dati.

L'Utente è tenuto comunque alla rimozione di eventuali file elaborati sui dispositivi mobili prima della riconsegna del bene.

Qualora venisse assegnato un Cellulare/Smartphone aziendale all'Utente, anche a questo strumento di lavoro si applicano le medesime regole sopra previste per l'utilizzo del telefono fisso aziendale: in particolare è vietato l'utilizzo dello Smartphone messo a disposizione per inviare o ricevere SMS o altro tipo di messaggi (Whatsapp, Messanger, Twitter, etc.) di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.

Art. 9 - UTILIZZO DELLE MEMORIE ESTERNE (CHIAVI USB, HARD DISK, MEMORY CARD, CD ROM, DVD ROM, ECC.)

Di norma non devono essere utilizzate memorie esterne. Agli Utenti può essere assegnata una memoria esterna solo in casi di effettiva e motivata necessità.

Questi dispositivi devono essere gestiti con le stesse accortezze di cui, in generale, quanto già evidenziato per l'utilizzo delle risorse ICT e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

- I supporti di memorizzazione rimovibili contenenti dati particolari e giudiziari, se non più utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri utenti, solo se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

- I supporti di memorizzazione rimovibili contenenti dati particolari e giudiziari devono essere custoditi in idonei archivi chiusi a chiave, a cura dell'utente che li gestisce abitualmente, e sotto sua diretta ed esclusiva responsabilità.

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

Qualora le memorie esterne contengano dati particolari e giudiziari e tali memorie esterne vengano portate all'esterno dell'Organizzazione è responsabilità dell'Utente cifrare il contenuto della memoria stessa in maniera tale che lo smarrimento accidentale della memoria non comporti la perdita dei dati in essa contenuti.

Art. 10 - UTILIZZO INFRASTRUTTURA DI RETE E FILE SYSTEM

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

AZIENDA OSPEDALIERA SANTA MARIA TERNI

Per l'accesso alle risorse informatiche dell'Organizzazione attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione. È assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone.

L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (es. cartelle su server/Nas) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro.

I dispositivi/postazioni informatiche e tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server/Nas dell'Organizzazione, ovvero sui dispositivi/postazioni, di documenti non inerenti all'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dal personale addetto ai Sistemi Informativi, a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche sulle altre risorse informatiche viene rimosso secondo le regole previste dal presente Regolamento, fermo restando ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare del personale addetto ai Sistemi Informativi e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C: o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse, poiché non sono garantite la sicurezza e la protezione contro l'eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

È vietato trasferire documenti elettronici dai sistemi informativi e device/postazioni dell'Organizzazione a device esterni (hard disk, chiavette, CD, DVD e altri supporti).

È vietato salvare documenti elettronici dell'Azienda (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, Google Drive, OneDrive, WeTransfer, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi. In caso di necessità l'Azienda dovrà mettere a disposizione modalità in linea con le presenti direttive.

Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

L'Organizzazione mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno. Tale accesso potrà avvenire mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna o altre modalità congrue allo stesso scopo L'accesso mediante VPN, o altra modalità, viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Organizzazione necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

dell'Organizzazione che necessitino di svolgere compiti specifici, pur non essendo presenti in sede.

Le richieste di abilitazione all'accesso mediante VPN, o altra modalità congrua, dovranno seguire le regole già descritte per il rilascio di credenziali ed autenticazione ai sistemi.

All'interno delle sedi lavorative è resa disponibile anche una rete senza fili, c.d. "WiFi". Tali reti consentono l'accesso alle risorse e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete WiFi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Organizzazione necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Organizzazione che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse.

Si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

Art. 11 - PROTEZIONE ANTIVIRUS

Il sistema informatico dell'Organizzazione è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software di tipo malware.

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 personale addetto ai Sistemi Informativi.

Ogni dispositivo di supporto di memorizzazione elettronico di provenienza esterna all'Organizzazione, come già ribadito, dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale addetto ai Sistemi Informativi.

L'utente utilizzatore del dispositivo/postazione verifica periodicamente lo stato di aggiornamento dell'antivirus aziendale installato. A fronte di eventuali anomalie contattare il personale addetto ai Sistemi Informativi.

Art. 12 - MODIFICHE DELLE RISORSE ICT

Per quanto riguarda le modifiche si devono distinguere:

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

- **Modifiche hardware degli strumenti dell'Organizzazione:** gli Utenti non devono intervenire sui dispositivi, togliendo, sostituendo od installando componenti hardware (ad esempio masterizzatori CDROM/DVD, schede LAN, ecc.) senza previa autorizzazione;
- **Modifiche software:** gli Utenti non devono modificare i parametri di configurazione dei dispositivi assegnati.

Gli Utenti, inoltre, non devono alterare la configurazione originaria del dispositivo ricevuto in uso (ad es. disinstallando, eseguendo o installando applicazioni che interferiscano sul funzionamento del dispositivo medesimo) senza previa autorizzazione.

Art. 13 - SMARRIMENTO E FURTO DELLE RISORSE ICT

Nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del loro contenuto, gli Utenti devono segnalare tempestivamente l'accaduto ai soggetti di seguito indicati:

- Autorità Giudiziaria (sporgendo denuncia);
- Call Center dell'assistenza informatica, per l'eventuale blocco dell'uso delle risorse ICT.

Art. 14 - SANZIONI

È fatto obbligo a tutti gli utenti di osservare le disposizioni del presente Regolamento.

Il mancato rispetto o la violazione delle disposizioni regolamentari è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari e risarcitori previsti dalla contrattazione collettiva e dalla legge, nonché con tutte le azioni civili e penali consentite (a titolo esemplificativo codice penale: art. 595, artt. 600-ter e segg., art. 615-ter, art. 615-quarter, art. 615-quinques, art. 617-quarter, art. 617-quinquies, art. 617-sexies, art. 635-bis, art. 635-ter, art. 635- quarter, art. 635-quinquies, art. 640 ed art. 640 ter).

L'inosservanza di tali disposizioni, delle direttive in material di sicurezza delle informazioni, costituiscono inadempimento oltre a costituire violazione di norme.

CAPO III - NORME FINALI

Art. 15 – NORMA DI RINVIO

Per tutto quanto non previsto dal presente Regolamento si rinvia alla normativa statale e regionale di riferimento.

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it

AZIENDA OSPEDALIERA SANTA MARIA TERNI

Art. 16 – ENTRATA IN VIGORE

Il presente Regolamento entra in vigore nel quindicesimo giorno successivo a quello della pubblicazione della relativa deliberazione di approvazione nell'Albo on-line istituzionale.

Redatto a
cura del DPO
Ferraro Giuseppina

Via Tristano di Joannuccio, 1 - 05100 Terni (TR)
C.F.- P.I.: 00679270553 - Centralino: 0744/2051
www.aospterni.it