Sede legale: Via Magellano, 1 - 10128 TORINO - Tel. +39 011.508.1111 - www.mauriziano.it - P.I./Cod. Fisc. 09059340019

REGOLAMENTO

"Corretto utilizzo della postazione di lavoro, della navigazione Internet e della posta elettronica nel rapporto di lavoro"

Indice generale

Aggiornato Settembre 2019

1 INTRODUZIONE

L'utilizzo delle risorse informatiche ed il libero accesso alla Rete Internet espone l'Azienda a rischi di natura patrimoniale ed a responsabilità penali per violazione di disposizioni di legge, in particolare in materia di diritto di autore e di tutela della riservatezza, con ripercussioni sulla sicurezza e problemi di immagine dell'Azienda.
In particolare, il diffuso uso di tecnologie informatiche fornite dall'Azienda ai suoi collaboratori/dipendenti può dare origine a numerose problematiche, che rendono necessario porre in essere adeguate misure di controllo nel rispetto dei principi espressi dal Garante per la protezione dei dati personali nel Provvedimento n. 13 del 1.03.2007 e valutare eventuali usi scorretti, contrari ai doveri di diligenza e fedeltà di cui agli artt. 2104 e 2105 c.c.,.

Con delibera n. 627 del 8.10.2018 è stato approvato il documento "MISURE TECNICHE DI SICUREZZA ED INTEGRITÀ DEI DATI TRATTATI CON STRUMENTI ELETTRONICI", in ottemperanza al nuovo Regolamento Europeo 2016/679 relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali", pubblicato su Intranet alla pagina https://intranet.mauriziano.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/453

Il GDPR (art. 32), dispone che il titolare del trattamento dei dati personali debba adottare delle misure tecniche e organizzative idonee al fine di assicurare, ed essere poi in grado di dimostrare, che il trattamento dei dati personali è realizzato in modo conforme alla disciplina dettata dal Regolamento stesso. Questa norma è, in particolare, in linea con il principio della responsabilizzazione (c.d. accountability) che sta alla base del nuovo approccio promosso dal Regolamento europeo.

Gli eventi "a rischio" possono essere causati da eventi o comportamenti così classificabili:

- ***comportamenti degli operatori:***
  - *sottrazione di credenziali di autenticazione*
  - *carenza di consapevolezza, disattenzione o incuria*
  - *comportamenti sleali o fraudolenti*
  - *errore materiale*

- ***eventi relativi agli strumenti:***
  - *azione di virus informatici o di programmi suscettibili di recare danno*
  - *spamming o tecniche di sabotaggio*
  - *malfunzionamento, indisponibilità o degrado degli strumenti*
  - *accessi esterni non autorizzati*
  - *intercettazione di informazioni in rete*

- ***eventi relativi al contesto fisico-ambientale:***
  - *ingressi non autorizzati a locali/aree ad accesso ristretto*
  - *sottrazione di strumenti contenenti dati*
  - *eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria*
  - *guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)*
  - *errori umani nella gestione della sicurezza fisica*

L'Azienda adotta il presente Regolamento volto a prevenire comportamenti che, per quanto inconsapevoli, possano creare problemi alla sicurezza nel trattamento dei dati e a disciplinare condizioni e modalità del corretto utilizzo degli strumenti informatici aziendali da parte di dipendenti e collaboratori.

Questo documento è predisposto sulla base delle Linee guida del Garante per posta elettronica e internet pubblicate sul Registro delle deliberazioni Del. n. 13 del 1° marzo 2007, Bollettino del n. 81/marzo 2007, e dei Limiti al controllo sulla posta elettronica del dipendente del 2 aprile 2008, pubblicati sul Bollettino n. 93/aprile 2008, nonché sulla base della Direttiva N.02/09 della Presidenza del Consiglio dei Ministri-Dipartimento della Funzione Pubblica 0024438 del 26/05/2009 e del Trattamento effettuato sulle e-mail di dipendenti ed ex dipendenti - 30 luglio 2015.

Premesse:

- compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
- spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (*artt. 15, 31 ss., 167 e 169 del Codice*);
- emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
- l'utilizzo di Internet da parte dei lavoratori può infatti risultare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di *log file* della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di *log file* di traffico *e-mail* e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
- le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

1.1 Tutela del lavoratore

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà.
Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali

1.2 Principi generali

Nell'impartire le prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia.

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

- il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (*art. 3 del Codice; par. 5.2*);
- il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (*art. 11, comma 1, lett. a), del Codice*). Le tecnologie dell'informazione permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa.
- i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime* (*art. 11, comma 1, lett. b), del Codice: par. 4 e 5*), osservando il principio di *pertinenza* e *non eccedenza*. Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"*.

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore.
Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e in che misura e con quali modalità vengano effettuati controlli.
Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura.

Con riguardo al principio secondo cui occorre perseguire finalità determinate, l'A.O. Ordine Mauriziano si riserva di controllare il corretto utilizzo degli strumenti di lavoro, le cui linee guida vengono riportate nel seguente documento.

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori; in particolare non è da ritenersi consentito:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica;
- la riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- la lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer affidati in uso.

L'A.O. Ordine Mauriziano, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori, di sistemi che consentono indirettamente un controllo a distanza, previo consenso del lavoratore stesso.

In applicazione del principio di necessità l'A.O. Ordine Mauriziano è chiamata a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili ai lavoratori.
Dal punto di vista organizzativo nella stesura del presente Regolamento è stato opportuno:

- valutare attentamente l'impatto sui diritti dei lavoratori;
- individuare preventivamente a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet;
- determinare quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un

loro impiego abusivo.

2 DESCRIZIONE E FINALITA'

Con il presente regolamento l'Amministrazione definisce le modalità di comportamento, monitoraggio e controllo nell'utilizzo delle risorse informatiche aziendali. Il presente regolamento dettaglia:

- I criteri e le modalità di creazione delle utenze utilizzate per l'autenticazione ai servizi informatici dell'Azienda
- Le modalità di accesso alla rete Internet da parte di dipendenti dell'Azienda e personale esterno autorizzato
- La gestione delle caselle di posta elettronica del dominio mauriziano.it
- La gestione delle caselle di posta certificata
- Le prescrizioni minime per garantire la sicurezza della rete aziendale e prevenire utilizzi impropri della rete Internet, che possono essere fonte di responsabilità.
- Le responsabilità relative ai controlli degli accessi.
- L'uso corretto delle postazioni di lavoro

Finalità del presente regolamento, redatto in conformità ai principi di cui al D.Lgs. 196/2003, del GDPR e della L. 300/1970, sono:

- garantire il corretto utilizzo delle risorse informatiche aziendali
- garantire la sicurezza, integrità, disponibilità e confidenzialità dei dati trattati in proporzionalità alla criticità degli stessi

3 DEFINIZIONI

Ai fini del presente regolamento si intende per:

- Amministrazione (anche denominata Azienda o Ente): l'Azienda Ospedaliera Ordine Mauriziano di Torino con sede legale in Via Magellano 1
- "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite una rete di comunicazione elettronica;
- "rete aziendale", l'insieme degli apparati tecnologici, compresi quelli a disposizione dell'utente, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse utilizzate nel perimetro aziendale e verso l'esterno per effettuare qualsiasi tipo di comunicazione informatica;
- "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete di comunicazione elettronica, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente;
- "servizio di posta elettronica", l'insieme delle apparecchiature e delle risorse che consentono all'utente di ricevere, spedire, visualizzare, gestire la posta elettronica, nonché gli eventuali servizi ausiliari al loro funzionamento;
- "utente" o "operatore", qualsiasi persona fisica che utilizza risorse informatiche aziendali nello svolgimento di attività all'interno dell'Ente;
- "responsabile di servizio", il diretto superiore gerarchico dell'utente, come sopra definito, secondo le articolazioni previste dall'Atto Aziendale;
- "dati relativi al traffico", qualsiasi dato sottoposto a trattamento riguardante la trasmissione di

comunicazioni elettroniche e, anche alternativamente, l'uso di servizi di posta elettronica;
- "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- "credenziali di autenticazione", i dati ed i dispositivi, in possesso di un utente, da questo conosciuti o ad esso univocamente correlati, utilizzati per l' autenticazione informatica;
- "parola chiave" o "password", componente di una credenziale di autenticazione associata ad un utente ed a questo nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- "client", dispositivo elettronico configurato o configurabile per consentire la fruizione di servizi di posta elettronica, sia esso fisso, portatile o hand-held.

4 OBIETTIVI

- Uniformare e semplificare, mantenendo elevati standard di sicurezza informatica, i criteri di autenticazione applicativa in uso presso l'Azienda Ospedaliera Ordine Mauriziano di Torino
- Consentire un corretto utilizzo delle risorse Internet, in particolar modo delle risorse scientifiche e delle banche dati, sanitarie e non, presenti sulla rete pubblica
- Definire le regole di assegnazione e di utilizzo delle caselle di posta elettronica e di posta elettronica certificata
- Semplificare e rendere efficienti le comunicazioni aziendali verso l'esterno e tra gli operatori e i Servizi dell'Azienda
- Garantire un'adeguata protezione dei dati e delle infrastrutture di rete interne
- Adempiere agli obblighi informativi nei confronti degli operatori in relazione al Trattamento dei dati effettuato

5 AMBITO DI APPLICAZIONE

Il presente regolamento si applica a tutti i dipendenti senza distinzione di ruolo e/o livello ed a tutti coloro che a vario titolo prestano servizio o svolgono attività per conto e nelle strutture dell'Azienda. Ai fini delle disposizioni regolamentari per "utente" si intende ogni dipendente o collaboratore in possesso di credenziali di autenticazione che può anche essere indicato quale "incaricato del trattamento".
Inoltre, il presente Regolamento si applica, ove tecnicamente possibile, a tutti i processi di autenticazione informatica in uso presso l'Azienda; i Sistemi Informativi Aziendali hanno il compito di adeguare i sistemi di autenticazione delle procedure in uso alla data di emissione del presente regolamento, ove tecnicamente possibile; le acquisizioni di procedure informatiche dovranno esplicitare nelle condizioni di fornitura i vincoli descritti dal presente regolamento ai fini dell'autenticazione applicativa. Per quanto riguarda l'accesso alla rete Internet e all'uso della posta elettronica, il presente regolamento si applica a qualsiasi tipo di collegamento di elaboratori presenti sulla infrastruttura di rete interna verso la rete pubblica Internet, nonché agli accessi tramite dispositivi personali che utilizzano collegamenti WiFi.

6 PRESCRIZIONI DEL REGOLAMENTO

6.1 Sistema di creazione delle utenze

Il requisito per la creazione di una nuova utenza è la presenza del relativo profilo attivo nella banca dati del sistema di gestione del personale, gestita dalla SC Personale, in cui sono presenti i profili anagrafici non solo dei dipendenti strutturati dell'Azienda, ma anche di tutti coloro che a vario titolo

prestano servizio o svolgono attività per conto e nelle strutture dell'Azienda (per esempio, consulenti, stagisti, personale universitario etc…).

I Sistemi Informativi gestiscono la creazione e la gestione delle utenze d'accesso alla rete aziendale e agli applicativi aziendali.

Le utenze di rete ed applicative sono caratterizzate da:

- identificativo utente (parte fissa delle credenziali) costituite dalla lettera iniziale del nome seguita dal cognome, con l'eliminazione di tutti i caratteri non alfabetici: in caso di omonimia, si utilizzano un numero di lettere del nome sufficiente ad eliminare l'omonimia
- univocità dell'identificativo utente anche nei confronti di precedenti identificativi eventualmente scaduti

6.2 Internet: la navigazione web

La rete pubblica Internet è raggiungibile sia dalle postazioni aziendali, sia tramite connettività WiFi nelle aree aziendali coperte dal segnale.
L'utilizzo della rete pubblica è consentito a seguito di autenticazione informatica eseguita utilizzando le credenziali di autenticazione.
Per l'utilizzo della rete Internet da postazioni della LAN Aziendale possono essere utilizzati esclusivamente i browser installati sulle postazioni aziendali dal personale dei Sistemi Informativi.
Non è consentito agli operatori effettuare sulla postazione utilizzata l'installazione di qualsiasi altro applicativo per l'accesso alla rete pubblica, anche quando tale installazione risultasse tecnicamente possibile.
Fatte salve le prescrizioni minime di sicurezza descritte nei paragrafi successivi, i Sistemi Informativi Aziendali valutano situazioni specifiche ed esigenze che non possono essere soddisfatte attraverso l'infrastruttura di accesso standard, ed eventualmente autorizzano modalità di accesso alternative.

I servizi presenti sulla rete pubblica Internet accessibili dalle postazioni aziendali sono:

- HTTP/HTTPS: navigazione Internet tramite programma browser
- WEBMAIL: utilizzo delle caselle di posta elettronica del dominio mauriziano.it tramite navigazione HTTPS

L'A.O. Ordine Mauriziano, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), ha adottato opportune misure che possono, così, prevenire controlli successivi sul lavoratore. In particolare:

- individuazione di categorie di siti considerati non pertinenti all'attività lavorativa, quali: Adult Content; Chat Rooms; Crime/Terrorism; Dating Sites; Gambling; Gaming; Government Blocking List; Malicious; Music Downloads; Spam; Swimsuit/Lingerie/Models; Violence. I filtri applicati vengono continuamente modificati con l'uso di reportistica e degli aggiornamenti del firewall
  a) uso di Blacklist per evitare l'accesso a certi siti, quali: *.facebook.com/*; *.tv.it/*; *.tv.com/*; *.yalp.alice.it/*; *.youtube.*/*
  b) uso di Whitelist per dare l'accesso a siti classificati erroneamente in categorie proibite e/o segnalati dagli utenti

- il *download* di *file* o *software* aventi particolari caratteristiche, quali file musicali, non è consentito; anche il download di programmi che necessitano di installazione sulla postazione di lavoro, non è consentito, se non con il supporto dei tecnici addetti alla manutenzione

c) durante la navigazione Internet vengono memorizzate alcune informazioni, qui elencate, a cui possono accedere solo l'Amministratore e, su richiesta, l'Autorità Giudiziaria:
   1. indirizzi IP del computer che ha navigato
   2. login del navigatore
   3. URL del sito navigato
   4. Data e ora di inizio e fine navigazione

2. i dati suddetti, relativi alla navigazione internet, sono conservati per un periodo non inferiore ai 6 mesi
3. la conservazione dei suddetti dati è strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza secondo le normative vigenti

d) il datore di lavoro, su richiesta dell'Autorità Giudiziaria o su indicazione motivata per iscritto di un Responsabile di Struttura qualora constati che la navigazione Internet è utilizzata indebitamente, informate le Organizzazioni Sindacali, può richiedere all'Amministratore, il controllo a posteriori di accessi avvenuti da una specifica stazione di lavoro in un arco temporale prefissato

e) il datore di lavoro può fare richiesta, motivata da esigenze di servizio, all'Amministratore designato, di attuare delle politiche di restrizione di accesso ad Internet o semplicemente inibire la navigazione Internet da alcune postazioni specifiche situate in posizioni strategiche a cui l'accesso è condiviso da molti dipendenti.

6.3 Posta elettronica

Le caselle di posta elettronica sul dominio mauriziano.it, ancorché contengano il riferimento ai dati anagrafici dei richiedenti, sono di proprietà dell'Azienda, che ne concede l'uso ai richiedenti secondo le norme indicate nel presente Regolamento. L'utilizzo delle caselle di posta deve essere finalizzato esclusivamente a comunicazioni inerenti l'attività lavorativa svolta presso l'Azienda.

Il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i *file* allegati, riguardano forme di corrispondenza assistite da garanzie di segretezza.
Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione o ne faccia un uso personale pur operando in una struttura lavorativa.
É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per ottemperare alle esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.
In questo quadro l'A.O. Ordine Mauriziano ha ritenuto opportuno:

a) rendere disponibili indirizzi di posta elettronica solo ai lavoratori per cui il Responsabile del Servizio ne abbia fatto richiesta motivata da esigenze di servizio;
b) mettere a disposizione di ciascun lavoratore possessore di casella postale apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad 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 della struttura. Ha inoltre prescritto come opportuno ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica, da parte di

altro personale. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (amministratore di sistema), l'attivazione di un analogo accorgimento, avvertendo gli interessati;

c) mettere in grado l'interessato di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa, in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;

d) disporre per tutti i possessori di casella postale dell'A.O. Mauriziano:

- che l'invio di dati personali e/o sensibili propri o relativi a pazienti, attraverso la posta elettronica, è proibito per motivi di sicurezza e che l'Ente non può quindi ritenersi responsabile della perdita di tali dati o del recapito non corretto di tali dati
- che, osservando il principio di *pertinenza* e *non eccedenza*, l'uso prevalente della casella postale Mauriziano deve essere relativo a scopi lavorativi e che lo scambio di corrispondenza tra l'interessato e i propri familiari, amici e conoscenti, che esuli dagli scopi lavorativi, deve essere assolutamente limitato nel tempo e nella quantità
- l'inserimento automatico della seguente informativa, in calce a tutti i messaggi di posta elettronica che vengono inviati dal Mauriziano:

==========

§§§ Le informazioni contenute nella presente comunicazione e relativi allegati possono essere riservate e sono, comunque, destinate esclusivamente alle persone o all'ente sopraindicati. La diffusione, distribuzione e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita ai sensi dell'art. 616 c.p. sia ai sensi del Regolamento UE 2016/679 e all'ulteriore normativa applicabile in materia di protezione dei dati personali. Se avete ricevuto questo messaggio per errore, vi preghiamo di distruggerlo e di informarci immediatamente inviandoci un messaggio all'indirizzo: privacy@mauriziano.it §§§

==========

- sanzioni, anche di tipo disciplinare, qualora constati che la posta elettronica è stata utilizzata indebitamente, decise di volta in volta, sulla base della gravità del fatto e/o adottando le sanzioni previste dal Garante

Sulla base delle indicazioni sopra riportate, gli operatori che hanno accesso ad una casella di posta del dominio mauriziano.it devono pertanto attenersi, nell'utilizzo delle stesse, alle seguenti regole:

- consultare la propria casella con frequenza giornaliera, salvo casi di assenza dal lavoro; tale casella può comunque essere consultabile dal dipendente titolare della stessa tramite accesso al di fuori della rete aziendale;
- prevedere, in caso di assenza prolungata e programmata, l'attivazione di un sistema di risposta automatica ai messaggi di posta elettronica ricevuti indicando, nel messaggio di accompagnamento, ogni riferimento utile per contattare la struttura organizzativa competente;
- delegare altro dipendente dell'ufficio (fiduciario) a verificare i contenuti dei messaggi e ad inoltrare al Direttore della S.C. quelli rilevanti per l'attività lavorativa, anche in previsione che, in caso di assenza improvvisa o prolungata, e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi stessi;
- provvedere a conservare, anche utilizzando le apposite aree dei server aziendali messe a disposizione dei singoli servizi, e ad effettuare la memorizzazione dei messaggi di posta ricevuti/inviati in relazione alle varie tipologie di comunicazione e ai tempi di conservazioni

richiesti e/o prescritti;

- non utilizzare l'indirizzo mail aziendale per l'iscrizione a qualsiasi servizio on line (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale etc.) che non siano strettamente correlati alla propria attività istituzionale;
- non utilizzare l'indirizzo mail aziendale per comunicazioni personali;
- 'firmare' le comunicazioni in uscita inserendo sempre il proprio nome e cognome, servizio di appartenenza, nome dell'Azienda, recapito telefonico, indirizzo e-mail ed eventuale numero di fax
- rispondere all'eventuale richiesta del mittente di conferma di lettura del messaggio;
- non inviare messaggi "a tutti" o a gruppi con elevato numero di indirizzi, al fine di preservare l'efficacia dei sistemi, quando non assolutamente necessario;
- non inviare messaggi che possano danneggiare la reputazione e l'immagine dell'Azienda;
- non inviare comunicazioni che siano diffamatorie, oscene, pornografiche, offensive, tali da recare danno o che possano essere considerate da altri fonti di molestie o discriminazione religiosa, sessuale, razziale, politica o sindacale;
- non inviare comunicazioni che possano infrangere la legislazione vigente, in particolare quella sui diritti d'autore, che diffondano virus nell'infrastruttura aziendale, che costituiscano e-mail 'spazzatura' o siano 'catene di Sant'Antonio' informatiche;
- Verificare periodicamente lo spazio a disposizione sulla casella di posta, mettendo in atto le attività necessarie al fine di evitare il non ricevimento di messaggi di posta per mancanza di spazio.

6.3.1 Soluzione tecnica adottata

Da circa 6 anni il mail server non è più gestito internamente al Mauriziano, bensì è in service presso un datacenter esterno, pertanto nessuno del personale del CED ha accesso come amministratore di sistema al server della posta elettronica mauriziano.it. L'amministratore del sistema pertanto è rappresentato dalla Società che gestisce il server.

6.4 Caselle di posta certificata

L'Azienda si è dotata delle seguenti caselle di posta certificata:

Servizio	Funzione	PEC
Direzione Generale	Azienda Ospedaliera Ordine Mauriziano di Torino	aso.ordinemauriziano@postemailcertificata.it
Direzione Sanitaria d'Azienda	Informazioni sanitarie ed organizzative sui servizi all'utente	direzionesanitaria.mauriziano@pcert.postecert.it
	Ufficio Stato Civile	statocivile.mauriziano@postecert.it
	Ufficio Relazioni con il Pubblico	urp.mauriziano@pcert.postecert.it
S.C. Gestione e Organizzazione delle Risorse Umane	Ricezione ed invio certificati di malattia	personale.mauriziano@pcert.postecert.it
	Ufficio Concorsi	concorsi.mauriziano@pcert.postecert.it
	Organizzazione Sviluppo Risorse Umane	osru.mauriziano@pcert.postecert.it
	Invio informazioni sulle malattie all'INPS	malattie.mauriziano@postecert.it
	Trattamento Economico	trattamentoeconomico.mauriziano@postecert.it

Servizio	Funzione	PEC
S.S. Affari Generali,	Affari Generali	affarigenerali.mauriziano@pcert.postecert.it

Servizio	Funzione	PEC
Legali, Assicurazioni	PROTOCOLLO gestione corrispondenza certificata	protocollo.mauriziano@pcert.postecert.it
S.C. Tecnico	Servizio Tecnico	tecnico.mauriziano@pcert.postecert.it
S.S. Contabilità Generale e Bilancio	Economico Finanziario	economicofinanziario.mauriziano@pcert.postecert.it
	Fatturazione Elettronica	fatture.mauriziano@postecert.it
S.C. ICT & Sistemi Informativi	Sistemi Informativi	ssi.mauriziano@pcert.postecert.it
S.C. Provveditorato	Provveditorato	provveditorato.mauriziano@pcert.postecert.it
	Economato	economato.mauriziano@pcert.postecert.it
S.C. Direzione Professioni Sanitarie	Servizio Infermieristico Tecnico Riabilitativo Ostetrico	sitro.mauriziano@pcert.postecert.it
S.S. Contabilità Analitica e Controllo di Gestione	Controllo di Gestione	controllogestione.mauriziano@pcert.postecert.it
S.S. Prevenzione, Protezione dai rischi	Prevenzione e Protezione	prevenzione.mauriziano@pcert.postecert.it
S.S. Ingegneria Clinica	Ingegneria Clinica	ingclinica.mauriziano@postecert.it
S.C. Farmacia Ospedaliera	Farmacia	farmacia.mauriziano@pcert.postecert.it
	Invio ordini	ordinifarmacia.mauriziano@postecert.it
S.C. Laboratorio Analisi-Chimico Cliniche e Microbiologia	Laboratorio Analisi	labanalisi.mauriziano@postecert.it
S.C. Fisica Sanitaria	Fisica Sanitaria	fisicasan.mauriziano@postecert.it
S.C. Nefrologia e Dialisi	Invio referti per Centro Trapianti	nefrologia.mauriziano@postecert.it
S.C.D.U. Ematologia	Invio referti per Centro Trapianti	ematologia.mauriziano@postecert.it
S.C. Pneumologia	Invio referti per Centro Trapianti	pneumologia.mauriziano@postecert.it
S.S. Dietologia e Nutrizione Clinica	Dietologia e Nutrizione Clinica	dietetica.mauriziano@postecert.it
Nucleo Ospedaliero per la Continuità delle Cure (NOCC)	Continuità delle Cure	nocc.mauriziano@postecert.it

Le Strutture aziendali, non ancora dotate di caselle di posta certificata, che intendono avvalersi di detta casella per l'inoltro di e-mail registrate a protocollo, saranno abilitate in tal senso a fronte di motivata richiesta.

6.5 Modalità di utilizzo di identificativo utente (user) e password

L'accesso alla rete aziendale è consentito previa digitazione delle credenziali. L'uso della password è strettamente personale.

La password deve essere custodita e digitata segretamente. La password deve essere modificata in autonomia con frequenza di almeno una volta ogni 90 giorni. In caso di sostituzione il criterio di scelta della password deve essere tale da non facilitarne l'individuazione.

Se si ritiene opportuno cambiare la password con periodicità inferiore ai 90 giorni, basta utilizzare i tasti CTRL-ALT-DEL della tastiera della postazione di lavoro e scegliere l'opzione "Cambia password..."

In caso di sospetto di conoscenza della password da parte di terzi, l'operatore deve immediatamente utilizzare le procedure di cambio password presenti sul portale intranet, anche precedentemente la data di scadenza.
L'utilizzatore deve operare con diligenza per mantenere riservate le proprie credenziali di autenticazione, compresa la scelta di password non banali e non riconducibili alla propria persona.
Tutte le attività informatiche effettuate a seguito di autenticazione sono ricondotte alla persona fisica a cui sono state rilasciate le credenziali.
La legge non punisce chi abusa ma la responsabilità è sempre in capo a chi non ha cura di mantenere "segreta" la password.

6.6 Protezione Antivirus

Le postazioni aziendali sono dotate di software antivirus, installato dal personale dei Sistemi Informativi, che ne configura la modalità di aggiornamento automatico.
L'operatore che verifica che la postazione dalla quale utilizza la rete pubblica Internet non è dotata di programma antivirus, o che questo non è aggiornato, deve segnalare ai Sistemi Informativi tale situazione tramite l'Help Desk del servizio.

7 CORRETTO UTILIZZO DEGLI STRUMENTI

Nel seguito si riportano alcune indicazioni per il corretto utilizzo degli strumenti in uso presso l'Azienda Ordine Mauriziano di Torino:

Strumento	Corretto Utilizzo
Postazione di lavoro	• L'accesso in rete avviene tramite l'uso della propria login e password • Deve essere utilizzata esclusivamente come strumento aziendale, ne consegue che è vietato ogni utilizzo personale dello stesso, o non inerente l'attività lavorativa o comunque per finalità estranee al rapporto di lavoro • L'utente si impegna a mantenere la configurazione originaria (come impostata dalla SC ICT & Sistemi Informativi) degli strumenti che si utilizzano • I dati lavorativi NON devono essere memorizzati nel disco fisso (es. sul desktop del computer o in una qualunque altra area locale). • La postazione di lavoro deve essere spenta (o comunque resa inaccessibile) al termine del proprio orario di lavoro e/o comunque non deve essere lasciata incustodita senza disconnettersi dalla rete • Qualora sorgesse l'esigenza di assentarsi dalla propria postazione, anche per brevi periodi, ciascun autorizzato dovrà attivare in ogni caso lo screen saver e la relativa password, ovvero porre il device in modalità stand-by. • Eventuale furto dovrà essere denunciato al Commissariato di Polizia e segnalato all'Azienda, secondo quanto previsto al n. 3 della Procedura Data Breach adottata con Delibera n. 533 del 10.08.2018 • L'eventuale controllo a distanza, per motivi di manutenzione, deve sempre essere effettuato previo consenso del lavoratore
Password di rete	• Scadenza trimestrale • Lunghezza minima di 8 caratteri • Deve contenere almeno 3 delle seguenti condizioni: [lettera maiuscola]; [lettera minuscola]; [numero]; [carattere speciale]

Strumento	Corretto Utilizzo
	• Non può essere uguale alle precedenti 4 password • La sua segretezza è responsabilità del lavoratore
Software applicativi	• Tutti i programmi di Office Automation, quali Microsoft Office o LibreOffice, non sono strumenti "sicuri" per la registrazione di dati relativi alla salute. • Sulla base della legge regionale n. 9 del 26 marzo 2009, contenente disposizioni circa l'utilizzo di soluzioni open source, è stata installata, in sostituzione del software Microsoft Office, la piattaforma LibreOffice, che non richiede licenza in quanto gratuita ed è compatibile a Microsoft Office. • Qualsiasi nuovo software applicativo di cui si renda necessaria e/o opportuna l'installazione deve essere autorizzato dalla SC ICT & Sistemi Informativi facendone richiesta via email a manutenzione@mauriziano.it • L'accesso ai software applicativi aziendali, quali AURIGA, EUSIS ecc, avviene attraverso login e password, richiesti alla SC ICT & Sistemi Informativi
Software BABELE	• È il solo software sanitario aziendale riconosciuto come "sicuro" per la registrazione di dati personali e relativi alla salute dei pazienti
Aree condivise di rete	• Sono l'unico strumento ammesso per memorizzare tutti i dati di interesse lavorativo • Giornalmente vengono effettuati backup a cura della SC ICT & Sistemi Informativi
Dispositivi rimovibili (CD/DVD; Pen Drive; ecc)	• NON devono contenere né dati personali né dati relativi alla salute dei pazienti • Devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere recuperato da terzi non autorizzati. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la cancellazione, ed, addirittura, anche dopo la formattazione del supporto stesso. • Nel caso in cui sia assolutamente necessario memorizzare dati personali (anche relativi alla salute), il supporto deve essere protetto da password.
Internet	• La navigazione avviene attraverso l'utilizzo di un proxy o server che è preposto ad evitare: la visione di siti non pertinenti all'attività lavorativa; la visione di siti pericolosi o non permessi dalle politiche aziendali; di scaricare files o programmi non permessi dalle politiche aziendali • Durante la navigazione Internet vengono memorizzate alcune informazioni, relative alla postazione di lavoro da cui si è navigato, il login del dipendente, l'URL del sito e la data e ora di inizio e fine navigazione. Tali dati, conservati per legge per un periodo non inferiore a 6 mesi, possono essere richiesti solo all'Amministratore di sistema, dall'Autorità Giudiziaria o da un responsabile del servizio, su richiesta motivata e informando le Organizzazioni Sindacali • Su alcune postazioni, situate in posizioni strategiche, quali la sala operatoria, la rianimazione o l'emergenza, è possibile all'Azienda richiedere di inibire la navigazione Internet per rendere tali postazioni maggiormente fruibili

Strumento	Corretto Utilizzo
	• Si invitano inoltre gli utenti a rispettare, in generale, i principi di c.d. "Netiquette" (https://it.wikipedia.org/wiki/Netiquette).
Posta elettronica (PEO)	• Il contenuto dei messaggi di posta elettronica, come pure i dati delle comunicazioni e i *file* allegati, riguardano forme di corrispondenza assistite da garanzie di segretezza. • Elenchiamo alcune delle funzionalità specifiche attuate e/o attuabili autonomamente dal dipendente: ◦ Invio di messaggi di risposta automatica in caso di assenza del dipendente. ◦ Inoltro automatico ad altro indirizzo di posta elettronica. • In calce ad ogni email è stato inserito automaticamente un avviso riguardante la privacy • L'invio di dati personali e/o relativi alla salute propri o di pazienti, attraverso la posta elettronica, è proibito per motivi di sicurezza e l'Azienda non può ritenersi responsabile della perdita di tali dati o del recapito non corretto di tali dati. • Osservando il principio di *pertinenza* e *non eccedenza*, l'uso prevalente della casella postale Mauriziano deve essere relativo a scopi lavorativi e lo scambio di corrispondenza tra l'interessato e i propri familiari, amici e conoscenti, che esuli dagli scopi lavorativi, deve essere assolutamente limitato nel tempo e nella quantità.
Posta elettronica (PEO)...continua	• Nelle risposte alle e-mail, è necessario provvedere ad eliminare le parti di testo sovrabbondanti rispetto alle finalità della comunicazione da inviare (c.d. "overquoting" - cfr. https://it.wikipedia.org/wiki/Citazione_(Internet)): quella di lasciare grandi quantità di testo citato in calce alle email è una cattiva pratica che deve essere scoraggiata. • Sono previste sanzioni, anche di tipo disciplinare, qualora si constati che la posta elettronica è stata utilizzata indebitamente, decise di volta in volta, sulla base della gravità del fatto e/o con riferimento alle sanzioni previste dall'ordinamento nazionale e dell'Unione Europea.
Posta Elettronica Certificata (PEC)	• Ad alcuni servizi è stata attivata una casella di Posta Elettronica Certificata per l'interscambio di posta con altre strutture pubbliche analoghe, locali, regionali e nazionali. • A differenza della posta elettronica ordinaria (PEO), la PEC equivale ad una raccomandata con avviso di ricevimento e contiene un riferimento temporale opponibile ai terzi (la ricevuta di avvenuta consegna dà certezza giuridica di recapito nonché "data certa").

8 MONITORAGGIO E CONTROLLI

L'A.O. Ordine Mauriziano di Torino può avvalersi di sistemi di controllo del corretto utilizzo degli strumenti di lavoro, che determinano un trattamento dei dati personali riferiti o riferibili ai lavoratori, nel rispetto di quanto previsto dal Provvedimento del Garante della Privacy del 1/3/2007 n. 13;
Le attività sull'uso del servizio di accesso a internet sono automaticamente registrate in forma elettronica attraverso i LOG del sistema firewall.
Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima e/o aggregata, in modo tale da precludere l'identificazione degli utenti e/o delle loro attività;

I dati anonimi e/o aggregati, riferibili all'intera Azienda, sono a disposizione del Titolare per le valutazioni di competenza e riguardano:

- per ciascun sito/dominio visitato le seguenti informazioni: il numero di indirizzi IP che lo visitano, il numero delle relative pagine richieste e della quantità di dati scaricati;
- per ciascun indirizzo IP le seguenti informazioni: il numero di siti visitati, la quantità totale di dati scaricati e le postazioni di lavoro utilizzate per la navigazione.

I dati personali contenuti nei log possono essere trattati esclusivamente nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
- su richiesta della Direzione Aziendale quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
- su richiesta della Direzione Aziendale limitatamente al caso di utilizzo anomalo degli strumenti da parte degli utenti di una specifica struttura;
- qualora vi sia l'evidenza o comunque il fondato sospetto che sia in corso o sia stato posto in essere un illecito

In particolare i controlli si svolgeranno in maniera graduata:

- In via preliminare l'Azienda provvederà ad eseguire dei controlli su dati aggregati, (c.d. ‘controllo anonimo’) riferiti all'intera Azienda.
- Nel caso in cui vengano rilevate anomalie o irregolarità, potrà essere inviato un avviso generalizzato ai dipendenti che richiami questi ultimi all’utilizzo corretto degli strumenti elettronici aziendali, nel rispetto della normativa vigente e dei diritti di terzi, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite. Qualora le anomalie o le irregolarità dovessero persistere, si procederà circoscrivendo l’invito al personale per cui è stata rilevata l’anomalia.
- In caso di ripetute anomalie e di reiterate irregolarità si procederà a controlli su base individuale o per postazione di lavoro indicando le ragioni legittime, specifiche e non generiche, per cui i controlli verrebbero effettuati – anche per verifiche sulla funzionalità e sicurezza del sistema – inoltrando preventivi avvisi agli interessati.
- Nel caso in cui la posta elettronica e la rete intranet e internet siano utilizzate indebitamente o di riscontro reiterato uso non conforme delle risorse informatiche, l’Amministratore di sistema che effettua i controlli, segnalerà il comportamento alla Direzione Generale, per le valutazioni del caso e gli eventuali ulteriori provvedimenti