SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Modena

Disciplinare sull'Utilizzo delle Postazioni di Lavoro

dell'Azienda Ospedaliero – Universitaria di Modena

Riferimento documentale	
Titolo del documento	Disciplinare sull'Utilizzo delle Postazioni di Lavoro dell'Azienda Ospedaliero – Universitaria di Modena
Numero di versione	1.0
Data Pubblicazione	25/11/2020
Stato del documento	
Redatto da	Ing. Roberto Savigni
Autorizzato da	Ing. Mario Lugli 
Verificato da	Ing. Mario Lugli 

Sommario

Premessa

Nel pieno rispetto dei diritti e delle libertà fondamentali dei cittadini, della dignità delle persone con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati personali, l'Azienda Ospedaliero – Universitaria di Modena adotta il presente "Disciplinare sull'utilizzo delle postazioni di lavoro".
La normativa e gli atti di riferimento del presente Regolamento sono i seguenti:

- D.Lgs n°196 del 2003 e successive modificazioni e integrazioni (Codice in materia di Protezione dei dati personali);
- Regolamento europeo in materia di protezione dei dati personali GDPR (**UE 2016/679)**
- Codice per la amministrazione digitale (D.Lgs n° 82/2005 e s.m.i);
- Circolare Agid 18 aprile 2017, n. 2/2017 in materia di Misure minime di sicurezza ICT per le pubbliche amministrazioni
- Documento Programmatico sulla Sicurezza dell'Azienda Ospedaliero – Universitaria di Modena (vigente);
- Provvedimento a carattere generale del Garante per la protezione dei dati personali dell'1/03/2007 ad oggetto: **"**Lavoro: le linee guida del Garante per posta elettronica e internet", pubblicato in G.U. n° 58 del 10/03/2007;
- Statuto dei lavoratori (L. n° 300/1970);
- Direttiva n° 2 DD 26/05/2009, c.d. "Direttiva Brunetta", del Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri.
- Cloud Computing - La guida del Garante della Privacy per imprese e pubblica amministrazione (anno 2012)

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate. Le proposte verranno esaminate dal Servizio Tecnologie dell'Informazione.
Il presente "Disciplinare" è soggetto a revisione con frequenza almeno annuale da parte del Servizio Tecnologie dell'Informazione.

Art. 1 - oggetto

Il "Disciplinare" ha per finalità di stabilire le norme per l'accesso e l'utilizzo dei seguenti servizi dell'Azienda Ospedaliero - Universitaria di Modena, di seguito denominata "Azienda":

1) Posta elettronica;
2) Rete internet;
3) Computer aziendali; di seguito indicati nel loro complesso come "Servizi Informatici Aziendali" (d'ora in poi S.I.A.).

L'Azienda garantisce che i dati informatizzati da essa gestiti, nonché i sistemi di elaborazione dati e gli strumenti di telecomunicazioni, non saranno utilizzati per il controllo a distanza dei lavoratori (artt. 4 e 8, L. 20 maggio 1970, n.300 – Statuto dei Lavoratori), se non nei limiti consentiti dallo Statuto dei Lavoratori, così come modificato dal D. Lgs. 151/2015 [Jobs Act] e comunque previa informativa ai dipendenti interessati.
Il presente "Disciplinare" è rivolto esclusivamente ai dipendenti dell'Azienda e loro equiparati. Nel seguito del presente documento, per semplicità espositiva, si farà riferimento genericamente all'operatore. Tutte le altre figure (ad es. collaboratori esterni, fornitori, ospiti, ecc…), eventualmente autorizzate, saranno oggetto di un separato disciplinare a cura del Servizio Tecnologie dell'Informazione (di seguito S.T.I.).
I S.I.A. sono regolamentati, oltre che dalle presenti norme, anche da eventuali altri regolamenti per l'accesso a servizi particolari.

Art. 2 - Definizioni e Abbreviazioni

Definizioni

Nel presente "Disciplinare" i termini di seguito elencati hanno le correlate definizioni:

- BLACK-LIST: elenco dei siti non accessibili agli utenti;
- CATENA DI S. ANTONIO: invio di messaggi di posta elettronica che istighino il destinatario a propagare i messaggi ricevuti ad una pluralità di destinatari, senza attinenza con l'attività lavorativa;
- HOSTING: ospitare sui propri server web le pagine di un sito web esclusivamente di soggetti terzi, rendendolo così accessibile da Internet;
- HOUSING: concessione in locazione ad un utente della possibilità di inserire un suo server all'interno dell'infrastruttura IT aziendale;
- INDIRIZZO IP: numero che identifica univocamente un dispositivo collegato ad una rete informatica;
- INTERNET PROVIDER: azienda che fornisce all'Azienda Ospedaliero - Universitaria di Modena il canale di accesso alla rete Internet;
- LOG: registrazione elettronica automatica generata da applicazioni o dispositivi, riguardante informazioni sulle attività eseguite all'interno degli impianti aziendali;
- MAIL SPAMMING o SPAM: invio massivo di messaggi di posta elettronica non desiderati e diretti ad una pluralità di destinatari, aventi generalmente contenuto commerciale o comunque non attinente l'attività lavorativa;
- POSTAZIONE DI LAVORO: personal computer (PC), o altro idoneo dispositivo, collegabile alla rete aziendale tramite il quale l'utente accede ai servizi;
- SUPPORTO INFORMATICO: qualsiasi componente in grado di conservare stabilmente dati informatici;
- UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica;
- UTENTE INTERNET: persona autorizzata ad accedere al servizio "Internet" con l'esclusione dei siti previsti nella "black-list";
- MALWARE: Programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico, rubare informazioni sensibili o mostrare pubblicità indesiderata.

Abbreviazioni

Nel presente "Disciplinare" verranno utilizzate le seguenti abbreviazioni e acronimi:

- AOUMO: Azienda Ospedaliero Universitaria di Modena
- AZIENDA: Azienda Ospedaliero Universitaria di Modena
- S.T.I. : Servizio Tecnologie dell'Informazione
- S.I.A.: Servizi Informatici Aziendali

Art. 3 - Incaricati al trattamento dei dati personali

I S.I.A. sono strumenti di lavoro forniti dall'Azienda, che ne fissa le modalità di utilizzo: gli utenti sono tenuti ad osservarle scrupolosamente.
Gli utenti sono nominati, ai sensi del Testo Unico u.v., "incaricati al trattamento dei dati personali" a cui hanno accesso o che sono trattati mediante i S.I.A..
I dati devono essere trattati limitatamente alle operazioni indispensabili per le finalità per i quali sono stati raccolti e nei limiti delle funzioni degli incaricati, e comunque nel rispetto dei principi di pertinenza e non eccedenza stabiliti dalle norme vigenti.

Art. 4 - Identificazione dell'utente per l'accesso ai servizi e loro utilizzo

L'utilizzo dei S.I.A. richiede, da parte di tutti gli utenti, un codice di identificazione personale (userid) ed una parola chiave segreta (password).

L'Azienda si riserva, a seguito di evoluzione delle tecnologie, di introdurre, anche solo in particolari contesti, sistemi di autenticazione "forte", basati, ad esempio, su smart card o caratteristiche biometriche, nel rispetto delle normative vigenti.
Per accedere ai S.I.A., un nuovo utente dovrà fornire i propri dati identificativi, prendere visione del presente regolamento e compilare e sottoscrivere in forma completa in ogni sua parte la modulistica web presente all'indirizzo http://richiesteict.aou.mo.it.
La richiesta dovrà essere inviata all'indirizzo di posta del responsabile della struttura o della procedura che potrà a sua volta validarla o respingerla. Una volta validata la richiesta verrà presa in carico dal servizio S.T.I. che provvederà alle abilitazioni richieste se giudicate consone o a respingerle motivandole.

La password non potrà essere ceduta a terzi neppure temporaneamente e dovrà essere mantenuta segreta e dovrà essere obbligatoriamente modificata dall'utente in ogni caso in cui egli abbia fondati sospetti che la segretezza della password sia venuta meno.
Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi. L'utente non deve lasciare incustodita o facilmente accessibile la postazione di lavoro una volta collegata al sistema, e deve disattivare la connessione qualora si debba allontanare. Inoltre non deve rendere accessibili in alcun modo le informazioni concernenti la propria password.
La userid identificativa dell'utente alla cessazione del rapporto di lavoro viene archiviata e potrà essere riassegnata ad altro utente dopo due anni dalla sua cessazione.
Non sono previsti codici di accesso anonimi, salvo nei casi in cui sia prevista una successiva procedura di identificazione personale per l'accesso alle procedure e/o ai dati veri e propri.
L'utente deve conservare la password con la massima riservatezza e con la massima diligenza.
La password:

- non deve essere banale né contenere riferimenti facilmente riconducibili all'utente;
- dovrà essere lunga almeno 8 caratteri tra i quali: lettere minuscole, lettere maiuscole, numeri, caratteri speciali;
- dovrà essere modificata da quest'ultimo al primo utilizzo e successivamente almeno ogni tre mesi.

Alla scadenza dei tre mesi, nel caso in cui l'utente non avesse provveduto a modificare la propria password, l'abilitazione dell'utente verrà sospesa.
L'utente avrà ancora due mesi per riattivare il proprio profilo semplicemente cambiando la password con le modalità opportune e in modo autonomo.
Alla scadenza di questi ulteriori due mesi, il codice di identificazione personale (userid) verrà disattivato.
Qualora si utilizzino sistemi che non siano in grado di richiedere automaticamente il cambio di password è indispensabile che l'utente – autonomamente - provveda a cambiarla ogni tre mesi.
Nel caso in cui l'utente si dimentichi la propria password, o nel caso in cui l'account venga bloccato a causa di un numero elevato di tentativi d'accesso con una password sbagliata, per riottenere l'accesso ai servizi l'utente dovrà inviare una richiesta di reimpostazione della password al Servizio Tecnologie dell'Informazione (d'ora in poi S.T.I.), firmata e con in allegato una fotocopia del tesserino di riconoscimento aziendale o di un documento di identità valido o, in alternativa, collegarsi al sito https://changepassword.aou.mo.it e seguire le istruzioni per il reset della password. Nel caso di disattivazione della userid per riottenere l'accesso ai servizi l'utente dovrà eseguire nuovamente la richiesta informatizzata di abilitazione ai servizi informatici aziendali elencata precedentemente.
Dopo sei mesi di non utilizzo dei servizi la userid e la password verranno automaticamente disattivati.
Nel caso in cui l'utente perda la qualità che gli consentiva di accedere ai servizi informatici aziendali, lo S.T.I. a seguito di segnalazione provvederà alla disattivazione di userid e della password.
Nel caso in cui l'utente a seguito di variazione di Servizio o di funzione debba accedere a servizi e/o risorse diverse da quelle previste inizialmente lo S.T.I. a seguito di segnalazione provvederà all'aggiornamento dei privilegi dell'utente.
L'utente si impegna a comunicare immediatamente allo S.T.I. il furto, lo smarrimento, la perdita ovvero l'appropriazione a qualsivoglia titolo da parte di terzi della password.

Nel caso di prolungata assenza dell'utente, egli dovrà utilizzare, qualora siano tecnicamente disponibili, funzioni che consentano di inviare messaggi automatici di risposta per "fuori sede" e che contengano le coordinate per un contatto alternativo con la struttura.
È facoltà del dirigente responsabile dell'utente richiedere allo S.T.I., nel caso di assenze prolungate o improvvise di questi e in condizioni di urgenza e necessità, l'accesso ai suoi dati e messaggi di posta elettronica e consultare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale fatto deve rimanere traccia su apposito verbale informando il lavoratore alla prima occasione utile.
Tenuto conto del provvedimento generale del Garante per la protezione dei dati personali del 01/03/2007 "Lavoro: le linee guida del Garante per la posta elettronica e Internet", relativamente al punto 5.2/b, ove si definisce la figura del fiduciario, si ritiene che i suggerimenti ivi contenuti non siano funzionalmente adottabili dall'Azienda.
Gli strumenti di comunicazione aziendali e gli strumenti di produttività personale in genere – telefono fisso, telefono cellulare, stazioni informatizzate di lavoro, fax, stampanti, ecc… - concessi in uso dovranno essere utilizzati per fini esclusivamente istituzionali e connessi alla propria mansione e attività di servizio. Nessun altro uso di tali strumenti è consentito se non espressamente autorizzato anche se nelle potenzialità della strumentazione concessa in uso ed eventualmente abilitata. A questo proposito è bene precisare che talvolta non è possibile disabilitare determinate funzionalità da alcuni apparati tecnologici, o che questo, anche se tecnicamente possibile, può essere organizzativamente oneroso per l'Azienda; comunque la disponibilità di una determinata funzionalità non autorizza il consegnatario di un bene all'utilizzo della stessa se non espressamente autorizzato e comunque se non necessario all'espletamento delle proprie mansioni e riconducibile ad attività istituzionali.
Nessun dispositivo personale potrà essere collegato alla rete dell'Azienda e/o utilizzato per trattare dati istituzionali aziendali. Qualora l'Azienda, per l'espletamento della propria attività istituzionale si avvalga di attrezzature la cui gestione in sicurezza ricada sotto la responsabilità di personale non dipendente o a questi assimilabile, dovrà essere formalmente definito un Responsabile esterno che si faccia garante degli aspetti di sicurezza e di rispondenza alla normativa vigente in tema di trattamento dei dati personali per tutti i trattamenti che avvengono su tali attrezzature.
L'Azienda si riserva di verificare l'utilizzo degli strumenti aziendali concessi in uso – ad esempio il telefono, le stazioni di lavoro informatizzate, i palmari, ecc… - qualora si evidenzino volumi anomali di traffico o vi siano altri elementi che indichino un uso non conforme alle presenti indicazioni.
L'Azienda vieta di memorizzare e/o trattare dati a fini personali di qualsiasi tipo per mezzo o all'interno degli strumenti aziendali concessi in uso. Il personale tecnico dell'Azienda, o il personale delle aziende che in nome e per conto dell'Azienda effettuano attività di manutenzione sugli strumenti aziendali - attrezzature di produttività personale, sistemi di comunicazione, ecc… - potranno accedere a detti strumenti per compiti connessi alla rispettiva funzione e mansione. Non potrà essere addotto come impedimento all'accesso il fatto che siano presenti dati utilizzati a fini personali in forza del suddetto divieto di gestire dati non connessi alla propria mansione e/o attività istituzionale.

Art. 5 - Finalità e limitazioni d'uso

Tenuto conto del provvedimento generale del Garante per la protezione dei dati personali del 01/03/2007 "Lavoro: le linee guida del Garante per la posta elettronica e Internet", l'accesso ai S.I.A. è da intendersi quale "strumento di lavoro".
È pertanto vietato l'uso dei S.I.A. nei seguenti casi:

- per l'utilizzo di procedure aziendali con modalità e finalità non attinenti ai propri doveri d'ufficio;
- per ricerche e/o consultazioni di siti il cui contenuto informativo appaia osceno, offensivo alla morale nonché alla pubblica decenza, a contenuto discriminatorio di taluni o razzista, a sfondo politico e/o religioso;
- per trasferire sulla postazione dell'utente programmi e/o file di dati relativi a progetti od obiettivi estranei all'utente o per finalità personali (come ad esempio file il cui contenuto sia protetto da diritto d'autore);
- per ricerche e/o consultazioni, all'interno dell'orario di lavoro, in maniera ripetuta e unicamente per scopi personali, di siti il cui contenuto informativo non sia attinente con l'attività lavorativa dell'utilizzatore;

- per ricerche e/o consultazioni palesemente incompatibili con i fini istituzionali dell'Azienda. È comunque vietato l'uso dello strumento nei casi configurati dalla normativa vigente come reato, in particolare:
  diffusione di virus, "cavalli di troia" o altri programmi la cui azione consista nel sabotaggio, distruzione, alterazione o visione del contenuto informativo delle postazioni degli altri utenti, degli elaboratori aziendali e dei dati in essi contenuti, anche qualora l'obiettivo sia all'esterno della rete aziendale;
- per attività di furto di dati aziendali o di altri utenti, organismi e/o aziende;
- per attività di hackeraggio e pirateria informatica in generale.

I servizi aziendali potranno richiedere l'accesso a particolari siti istituzionali in "modalità privilegiata", ovvero senza disporre delle credenziali per la generica navigazione Internet oppure con una disponibilità di banda superiore al normale.
Lo S.T.I. provvederà ad evadere queste richieste compatibilmente con le risorse tecniche a disposizione.

Art. 6 - Rilevazione statistica delle attività

Accesso ad Internet
Le operazioni di accesso ad Internet potranno essere memorizzate per finalità di sicurezza del sistema con la gradualità prevista dalla normativa vigente.
La rilevazione statistica delle attività avviene attraverso i file di "log" generati dai sistemi.
I log non sono accessibili per la consultazione e la loro tenuta avviene a cura degli Amministratori di Sistema nominati secondo le modalità previste dalla normativa vigente e dai regolamenti aziendali in merito. Questi log non sono oggetto di operazioni di backup.
Nell'ambito dell'attività autorizzata alla navigazione in Internet, lo S.T.I. provvede ad effettuare elaborazioni statistiche utilizzando i dati di "log" dell'uso del servizio, che contengono:

- data e ora dell'accesso;
- nome del sito richiamato per la consultazione;
- esito della consultazione;
- tipologia di operazione richiesta e informazioni sugli eventuali file scaricati;
- numero di byte trasferiti dall'elaboratore remoto e viceversa.

Qualora lo S.T.I. riscontri le seguenti anomalie:

- traffico superiore del 20% rispetto alla media dell'ultimo semestre;
- utilizzo di porte e/o protocolli non utilizzati dai programmi aziendali;
- contemporanea presenza di sessioni parallele dirette al medesimo sito remoto;
- traffico dati diretto a siti presenti nella black-list;

agli utenti verrà inviato un avviso generalizzato che informa della sospensione, per un periodo limitato e definito nella stessa informativa, dei controlli anonimi e del fatto che i log di sistema verranno utilizzati per l'individuazione di tali anomalie. Durante questo periodo, in aggiunta alle informazioni enunciate in precedenza, verrà rilevato anche l'indirizzo IP di partenza della navigazione. Al termine del periodo di osservazione questi log saranno distrutti a cura dello S.T.I..
In ogni caso non verranno estratte statistiche a livello individuale, bensì su base aggregata per area, settore o ufficio. In nessun caso i log del sistema generati sono usati come strumento di controllo dell'operato dell'utente. Da essi non è ricavabile alcuna informazione relativa al tempo trascorso nelle varie navigazioni dai singoli utenti.
L'Azienda utilizzerà le risultanze dell'elaborazione statistica dei log per aggiornare una black-list finalizzata ad impedire la navigazione verso siti vietati o non attinenti agli scopi istituzionali dell'Azienda.
Qualora un sito bloccato venga segnalato, attraverso l'apposita pagina di richiesta di sblocco, di interesse aziendale e riconosciuto come tale dallo S.T.I., lo stesso sarà rimosso dalla black-list e la rimozione avrà efficacia nei confronti di tutti gli utenti.
I log potranno essere oggetto di provvedimenti dell'Autorità Giudiziaria e Amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo. A seguito di specifica richiesta da parte delle Autorità preposte essi verranno memorizzati in forma non anonima, conservati e consegnati secondo le istruzioni ricevute da parte delle Autorità stesse.

Posta elettronica

Non viene tenuto alcun log relativo all'attività svolta dagli utenti con il servizio di posta elettronica. L'unico log generato dal sistema è di tipo diagnostico con la finalità di individuare eventuali problemi in invio e ricezione della posta e la sua conservazione è limitata nel tempo a 28 giorni solari da un sistema automatico di cancellazione. Questo log non è oggetto di operazioni di backup.

I messaggi inviati e ricevuti rimangono memorizzati sul server di posta fino al raggiungimento dello spazio disponibile per il singolo utente. Regolarmente l'utente dovrà provvedere a cancellare i messaggi più vecchi oppure a memorizzarli in locale sulle stazioni di lavoro tramite il software client installato sul PC assegnato.

Il server di posta viene regolarmente salvato permettendo così un recupero delle mail inavvertitamente cancellate, entro 30 giorni.

Accesso remoto alle postazioni utente

Gli strumenti di accesso remoto utilizzati dallo S.T.I. non costituiscono in alcun modo controllo a distanza dell'attività del lavoratore.

Ogni accesso remoto da parte di personale tecnico autorizzato ad una stazione di lavoro avviene solo per finalità di assistenza tecnica al fine di aggiornare/ripristinare le condizioni di funzionamento ottimali e/o di installarne delle nuove.

Ogni accesso avviene dietro consenso dell'utente espresso mediante la pressione di un tasto (o mediante altre azioni che denotino volontarietà e consapevolezza degli utenti); ciò quindi implica la presenza dell'utente davanti al monitor che ha piena visione delle operazioni svolte dall'addetto all'assistenza remota e ha facoltà di interromperle in ogni istante.

L'accesso remoto alle postazioni è ammesso senza consenso dell'utente se esse si trovano in modalità disconnessa ("logout"), e in tal caso l'utente remoto accede al sistema con le proprie credenziali senza accedere ai contenuti dei profili personali degli utenti del PC.

Nel caso in cui, per problematiche tecniche urgenti ed improcrastinabili, si renda necessario accedere con le credenziali di uno specifico utente, e questi non sia disponibile, verrà resettata la sua password e lo stesso dovrà provvedere alla sostituzione della password al primo collegamento. In questi particolarissimi casi lo S.T.I. documenterà dettagliatamente ogni operazione effettuata con le credenziali dell'utente, ed informerà lo stesso con la massima tempestività.

In nessun caso lo S.T.I. chiede la password di accesso degli utenti, che comunque non è conosciuta dal personale tecnico.

Art. 7 - Configurazioni hardware e software

Le postazioni di lavoro utente vengono predisposte e configurate per il corretto uso dei S.I.A. dallo S.T.I..

L'utente si impegna a mantenere la corretta configurazione della postazione di lavoro che utilizza. Le politiche relative ai software di gestione della sicurezza sono gestite centralmente e non è richiesta all'utilizzatore alcuna operazione manuale in merito.

A tal fine le postazioni di lavoro sono normalmente configurate per consentire l'accesso dell'utente solamente in modalità non privilegiata. Nel caso in cui a causa di particolari requisiti tecnici si renda necessario elevare i privilegi informatici dell'utente, quest'ultimo è maggiormente tenuto a preservare la configurazione della propria macchina così come impostata dallo S.T.I..

Qualora durante un intervento di manutenzione, i tecnici S.T.I. rilevino postazioni utente non conformi agli standard aziendali autorizzati, in mancanza di una specifica precedente deroga, gli stessi procederanno d'ufficio a ripristinare tali postazioni secondo gli standard definiti.

Nel caso in cui l'utente ritenga siano necessarie modifiche alla configurazione, ivi compresa l'installazione di nuovi programmi, dovrà formulare una richiesta allo S.T.I. che provvederà ad autorizzare o meno la richiesta, in quanto ogni modifica implica potenziali ricadute sulle corrette funzionalità delle procedure aziendali.

L'utente è responsabile delle attrezzature informatiche a lui assegnate, anche temporaneamente, e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, soprattutto nel caso di attrezzature portabili.
L'Azienda persegue una politica di centralizzazione nella gestione dei dati aziendali, per cui progressivamente le gestioni locali di dati scompariranno sostituite da gestioni centralizzate su server, qualora ciò sia tecnicamente possibile. Fino a che questo processo non sarà stato portato a compimento potranno esistere gestioni locali di dati su stazioni di lavoro personali (personal computer non connessi in rete o connessi in rete, ma con la possibilità di gestire localmente documenti e/o dati) la cui tutela è demandata a all'utente finale.
L'effettuazione dei salvataggi con frequenza opportuna – almeno comunque settimanale – su supporti magnetici e la conservazione degli stessi in luogo idoneo - possibilmente sotto chiave e in contenitori ignifughi - è compito del singolo dipendente che usa la stazione (nel caso di stazioni di lavoro usate da un solo utilizzatore) o da un incaricato opportunamente individuato dal delegato al trattamento nel caso di stazioni di lavoro condivise.
Ove è già presente un file server è fatto divieto di memorizzare in locale sulle stazioni di lavoro dati sensibili, che vanno salvati sui file servers. Nel caso in cui l'utente sotto la propria responsabilità memorizzi anche solo per brevi periodi dati in locale sulla stazione di lavoro, dovrà gestire i requisiti minimi di sicurezza della stessa.
Tutti i pc devono avere il programma antivirus installato e configurato per l'aggiornamento automatico; nel caso in cui si verifichi la non rispondenza della stazione di lavoro a tale requisito si è pregati di rivolgersi allo S.T.I. Aziendale

Art. 8 - Utilizzo dei supporti di memorizzazione

È vietato l'uso di supporti di memorizzazione removibili per la memorizzazione di dati personali o sensibili. Deroghe a tale regola sono possibili solo nei casi in cui sia possibile dimostrare il corretto uso dei supporti di memorizzazione ai sensi della circolare AGID del 18 aprile 2017 n.2/2017:

- è possibile il reimpiego del supporto solo nel caso non siano più recuperabili le informazioni precedentemente memorizzate;
- nel caso non sia possibile garantire il requisito di cui al punto (1), il supporto removibile dopo l'uso andrà distrutto.

In generale i supporti di memorizzazione, anche non removibili, che contengono dati personali o sensibili, nel caso in cui non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dismessi (per es. per obsolescenza o per guasto) dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile.

Art. 9 - Dismissione o cessione di supporti informatici

I supporti informatici non più necessari e contenenti dati devono essere resi inutilizzabili prima di dismetterli.
Questa operazione può essere effettuata distruggendo i supporti o sottoponendoli a cancellazioni logiche definitive con appositi software.
I supporti che dovessero essere ceduti a terzi vanno puliti sottoponendoli a cancellazioni logiche definitive con appositi software.
Lo S.T.I. è a disposizione per ogni informazione di dettaglio al riguardo.

Art. 10 - Modalità di prestazione dei servizi

L'Azienda si impegna a fornire continuità ai servizi erogati, riservandosi la possibilità d'interromperli per le manutenzioni ordinarie o in caso di situazioni straordinarie (ad es. attacco informatico) che possano compromettere integrità, disponibilità e riservatezza dei dati aziendali. Qualora possibile le interruzioni saranno preventivamente comunicate agli utenti.

Per migliorare la qualità o la sicurezza dei servizi e dei sistemi informatici attualmente predisposti, l'Azienda valuterà con attenzione eventuali osservazioni, suggerimenti ed indicazioni che gli utenti faranno pervenire allo S.T.I..
L'operatività specifica del personale S.T.I., per la peculiare attività che svolge, in particolare per quanto riguarda la sperimentazione di nuove tecnologie da introdurre eventualmente in Azienda, è disciplinata in apposito documento di incarico.

Art. 11 - Backup e protezione dati sensibili

Lo S.T.I. provvede al salvataggio periodico delle banche dati prodotte dai Sistemi Informatici Centralizzati. La periodicità è indicata nel Documento Programmatico sulla Sicurezza (D.P.S.).
Gli utenti possono richiedere allo S.T.I. la creazione di cartelle condivise tra più utenti. Lo S.T.I., dopo una breve istruttoria, valuta se procedere e, in caso affermativo, provvede alla creazione sui propri server di tale cartella ed alle configurazioni sui PC degli utenti interessati. Tale cartella viene altresì inserita nei backup automatici.
Costituiscono dati di rilevanza aziendale soltanto quelli memorizzati sui server in proprietà gestiti dallo S.T.I.. Gli utenti non devono avere dati personali o sensibili memorizzati sui PC aziendali. Se ciò avviene, l'Azienda non è responsabile di tali dati e non ne garantisce il periodico salvataggio né tantomeno il ripristino in caso di necessità.
Rimane comunque responsabilità dell'utente la cura e la protezione di eventuali file contenenti dati riservati e/o sensibili memorizzati sul proprio PC.

Art. 12 - Buon uso della rete e delle attrezzature aziendali di comunicazione

La rete di trasmissione dati e fonia è un prezioso bene aziendale condiviso e pertanto va gestita nel rispetto delle esigenze complessive di azienda. In funzione di ciò viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione dello S.T.I.. È' altresì vietato alterare in qualsiasi modo la configurazione software della stazione di lavoro - o di altri dispositivi direttamente connessi alla rete, dati o fonia - per quanto attiene all'accesso alla rete. È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale per fini non espressamente autorizzati. In particolare, tali divieti si possono tradurre, anche se non esaurire, nelle seguenti esplicite proibizioni:

- divieto di condividere cartelle in rete (né dotate di password, né sprovviste di password) se non espressamente autorizzate dallo S.T.I. Aziendale;
- divieto di alterare la configurazione di rete di stazioni di lavoro e altri dispositivi in rete (stampanti condivise, ecc…), comprendendo in ciò anche il divieto di aggiungere protocolli di rete o servizi in rete (per es. condivisione di stampanti in rete, browsing di risorse di rete, ecc…);
- è vietato intercettare/monitorare/ascoltare/leggere dati sulla rete di trasmissione dati o sulla rete di comunicazione in fonia;
- è vietata l'installazione non autorizzata di modem per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia per l'accesso a banche dati esterne o interne all'azienda;
- è vietata l'installazione non autorizzata di apparati di rete di qualsiasi tipo – hub, switch, router, access point WI-FI, access server, ecc… -;
- è vietata l'installazione di qualsiasi attrezzatura informatica o di comunicazione non espressamente autorizzata dallo S.T.I. Aziendale;
- è vietata l'installazione di hardware o software di qualsiasi tipo che consenta o faciliti il by-pass delle misure di presidio del confine aziendale - per es. software di comunicazione che garantiscano accessi che non passino dai Firewall Aziendali o dagli altri accessi autorizzati e presidiati.

L'utente è inoltre tenuto a conservare con la massima cura eventuali dispositivi per l'accesso ai sistemi aziendali e ad usarli conformemente alle specifiche indicazioni d'uso. La perdita o danneggiamento degli stessi sarà sanzionata.

I responsabili delle varie macro-articolazioni organizzative, di concerto con i delegati al trattamento e con il Servizio S.T.I., sono responsabili della adozione degli atti e delle misure organizzative necessarie a garantire un adeguato controllo relativamente alle norme di buon uso dei sistemi informatici e di telecomunicazione dell'Azienda.

Art. 13 - Virus e altro Malware

Si invitano gli utenti:

- alla massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione removibile sia stato utilizzato su un computer diverso dal proprio (supponendo che il proprio PC sia immune da infezioni) occorrerà verificare l'assenza di virus mediante un programma antivirale aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato non sarà possibile utilizzare il supporto di memorizzazione, in quanto potenzialmente infetto;
- in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è vietato utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte;
- è bene sempre evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure. Nel caso pervenga un messaggio di tale natura procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato, avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri. Nel caso si abbia notizia di un nuovo tipo di virus, comunicare tale informazione all'ufficio CARP del Servizio S.T.I. Aziendale (**cedareareteppc@aou.mo.it**) e non inviare indiscriminati messaggi a tutti i propri conoscenti: questo evita l'ingenerarsi di falsi allarmi e di inutili catene di Sant'Antonio.

Art. 14 - Internet

È permesso l'uso con moderazione della rete internet da parte degli utenti limitatamente ai siti web autorizzati e non bloccati dall'Azienda. L'apertura per motivi personali di siti bloccati non è autorizzata.
Tutti gli accessi ad Internet vengono registrati sul sistema di sicurezza aziendale in appositi file di log, come specificato all'Art. 6 del presente documento.
Tali log sono indispensabili all'Azienda per poter costantemente monitorare il corretto funzionamento del sistema nella sua globalità e per poter effettuare statistiche periodiche sull'uso del sistema, entrambi su base anonima. I log saranno trattati in maniera tale da fornire informazioni in maniera aggregata in modo da precludere l'immediata identificazione degli utenti, a meno che non vi siano specifiche ragioni per accedere al dettaglio massimo, cioè alle informazioni di tipo nominativo.

l'Azienda si riserva di filtrare l'accesso a siti che risultino non in relazione con le attività istituzionali; il filtraggio verrà attuato mediante l'inserimento del sito in una cosiddetta "Black list" ovvero nell'inserimento del sito in una categorizzazione, eventualmente predisposta anche da fornitori esterni specializzati; la lista dei siti inaccessibili o delle categorie potrà essere chiesta alla direzione del Servizio ICT Aziendale da chiunque e, in caso di motivate ragioni, potrà essere autorizzata la navigazione sul sito mediante rimozione dalla lista di esclusione; l'esclusione dei siti verrà operata periodicamente in base all'analisi di dati aggregati. A tal proposito, a partire dal 2015 è stata effettuata una modifica delle impostazioni del server proxy, al fine di limitare il numero dei siti a cui gli operatori possono accedere liberamente e prevenire così casi di navigazione indebita: rimane salva la possibilità di richiedere alla direzione del Servizio ICT Aziendale, di accedere ad uno o più siti bloccati, motivandone la necessità.

A titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:

- Servirsi o dar modo ad altri di servirsi della stazione di accesso a Internet per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;

- Scaricare software dalla rete; eventuali necessità dovranno essere appositamente richieste allo S.T.I. che provvederà a eseguire fisicamente lo scarico da stazione protetta, applicare le misure antivirus relative e consegnare il software al richiedente;
- Utilizzare Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem o chiavette GSM) da quello centralizzato;
- Usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete;

Non è consentito all'utente di produrre, pubblicare o manutenere siti web diversi da quello ufficiale aziendale mediante la rete aziendale e/o i S.I.A., salvo specifica autorizzazione scritta da parte della Direzione Aziendale o di Ufficio da questa espressamente delegato.
È altresì vietato utilizzare il sito aziendale, sia mediante la pubblicazione che l'inserimento di link a siti esterni, per pubblicizzare e/o promuovere attività non confacenti o addirittura in concorrenza con le attività erogate dall'Azienda Ospedaliero - Universitaria di Modena.
È diritto di ogni servizio chiedere di inserire uno spazio informativo (tecnicamente consistente in una o più "pagine", collegate tra loro ed alla "home page" aziendale) sul sito aziendale, di cui è direttamente responsabile anche per il contenuto e la correttezza delle informazioni.
A tale proposito i servizi dovranno fare richiesta all'Ufficio Comunicazione segnalando gli identificativi delle persone che potranno inserire informazioni sul sito e chi sarà il responsabile che ne autorizzerà la pubblicazione.
A tal fine lo S.T.I. provvederà a creare uno spazio web sul sito interno e/o sul sito pubblico, collegandolo alla pagina iniziale, o nella sottopagina eventualmente di riferimento.
Lo S.T.I. mette a disposizione il proprio supporto tecnico per la soluzione di eventuali problemi relativi all'applicazione delle procedure previste dal presente articolo, fatto salvo il fatto che l'inserimento e l'aggiornamento delle informazioni sono sempre a carico dei singoli servizi.
È' fatto divieto agli utenti di utilizzare il logo aziendale nei siti personali senza espressa autorizzazione del responsabile dell'Ufficio Comunicazione.
Si applicano in ogni caso le norme dei Codici deontologici professionali.
È' di norma vietato realizzare funzioni di hosting e/o housing, salvo specifica autorizzazione scritta da parte della Direzione Aziendale o di Ufficio da questa espressamente delegato.

Art. 15 - Servizio di Posta Elettronica

Il Servizio Informatico fornisce due distinte tipologie di indirizzi di e-mail:

- indirizzo di servizio o di gruppo, il cui nome richiama il servizio/gruppo in cui lavora l'utente;
- indirizzo legati al nominativo dell'utente richiedente.

L'indirizzo di servizio/gruppo deve comunque essere associato ad almeno un altro account nominativo di utente e non può essere utilizzato per l'invio di messaggi, ma solo in ricezione. Sarà compito dello S.T.I. fare in modo che i messaggi inviati a detto indirizzo siano smistati a tutti gli appartenenti al gruppo a cui è associato questo indirizzo.
Ogni account nominativo di posta ha uno spazio dedicato a disposizione di 1000MB. Il raggiungimento di tale limite implica l'impossibilità di utilizzare, in tutto o in parte, il servizio. Al raggiungimento del 80% dell'occupazione dello spazio disponibile viene segnalato all'utente mediante un messaggio di posta elettronica.
Gli utenti possono richiedere allo S.T.I. l'estensione dello spazio dedicato. Lo S.T.I., dopo una breve istruttoria, valuta se procedere e, in caso affermativo, provvede all'assegnazione di una diversa dimensione dello spazio dedicato alla posta.
Tutti i possessori di una casella di posta elettronica nominativa sono tenuti, quando possibile, a consultare quotidianamente la propria corrispondenza ed a provvedere tempestivamente allo scarico della stessa. Si ricorda che la consultazione via web non comporta lo scaricamento della posta dal server aziendale, operazione possibile soltanto con un client appositamente configurato sulla propria stazione di lavoro.
Per ottenere un account di posta elettronica è necessario seguire le indicazioni previste all'art. 4 del presente "Disciplinare".

È' possibile consultare la posta elettronica non ancora scaricata o inviare nuovi messaggi collegandosi direttamente al sito internet aziendale, per consentire agli utenti fuori sede di continuare ad utilizzare il servizio.
Per inviare e ricevere e-mail relative ad argomenti inerenti l'attività lavorativa è obbligatorio utilizzare l'account aziendale.
È' vietato l'utilizzo dell'account di posta elettronica aziendale per comunicazioni estranee all'attività lavorativa, per un uso personale e non istituzionale
E' vietato l'inoltro delle mail ricevute sulla casella di posta aziendale verso caselle di posta personali.
E' vietato l'utilizzo della posta elettronica per l'invio di dati sensibili, se non all'interno dello stesso dominio di posta istituzionale. In particolare è vietato un uso di tale strumento dal quale possa derivare la possibilità, anche indiretta o preterintenzionale, di rilevare le opinioni politiche, religiose o sindacali dell'operatore, le sue inclinazioni sessuali, il suo stato di salute.
È' consentito un moderato utilizzo di provider esterni di posta elettronica per comunicazioni personali, esclusivamente in modalità web, con l'avvertenza che l'Azienda non può fornire supporto in caso di impossibilità di raggiungere i siti web di tali provider a causa delle particolari configurazioni della rete finalizzate a massimizzare la sicurezza. Inoltre la modalità di consultazione di tali informazioni deve essere compatibile con i vincoli di sicurezza del sistema aziendale e deve avvenire in maniera non eccessiva e pregiudizievole degli obblighi del lavoratore nei confronti dell'Azienda
Tutta la posta in transito sul sistema aziendale viene controllata da un sistema antivirus che, oltre a bloccare le e-mail con virus, effettua i seguenti controlli:

- blocco delle e-mail con allegati potenzialmente pericolosi (file con estensioni EXE, .COM, VBS, .PIF, .SCR, .SYS, .BIN, .OVL, .DRV, .OVY, .LNK)
- blocco delle e-mail con dimensioni complessive (messaggio di posta + allegati) superiori a 30 Mb
- blocco delle e-mail con più di 30 allegati e/o più di 50 destinatari
- in particolari situazioni, ad esempio massicce ricezioni di e-mail infette, il Servizio S.T.I. Aziendale si riserva di bloccare e cancellare le e-mail che contengano particolari allegati o che abbiano nell'oggetto o nel corpo del messaggio particolari parole e/o frasi riconducili alla violazione di sicurezza o a codice pericoloso.

Al fine di garantire il corretto funzionamento della posta elettronica aziendale e di evitare la proliferazione del traffico indebito – che in termine tecnico viene chiamato SPAM – l'Azienda ha in uso un sistema AntiSPAM che filtra tutta la posta gestita. Il sistema AntiSPAM utilizza regole euristiche per decidere l'inoltro o meno di un messaggio. Le regole di filtraggio possono causare:

- il passaggio di SPAM qualora non sufficientemente selettive;
- il mancato inoltro di posta elettronica erroneamente giudicata dal sistema come SPAM.

Per le ragioni sopra indicate si vieta l'utilizzo della posta elettronica di materiali in copie uniche o comunque per l'invio di comunicazioni di cui debba essere garantito l'inoltro al destinatario.

Il sistema di posta elettronica in uso, e concesso in utilizzo, non è un sistema di posta certificata, non vi è pertanto la garanzia della consegna o della ricezione dei messaggi di posta, né fornisce garanzia di riservatezza relativamente ai messaggi inviati in quanto non usa alcuna tecnica di crittografia dei contenuti o di protezione delle autenticazioni. È pertanto fatto divieto di inviare materiali che non siano compatibili con tali caratteristiche del servizio.

L'Azienda mette a disposizione funzionalità di avviso in caso di assenza prolungata dell'operatore, che sfruttano le peculiarità del sistema di posta elettronica e possono fornire coordinate di altri riferimenti all'interno dell'Azienda tali da garantire il corretto funzionamento dei servizi.
L'attivazione di tali misure sarà a cura dell'utente che potrà attuarla in autonomia o che potrà avvisare il Servizio S.T.I. Aziendale di attuare la misura se tecnicamente non in grado; qualora l'utente non abbia adottato tale misura e l'assenza si protragga per più di una settimana, il delegato al trattamento potrà richiedere al Servizio S.T.I. Aziendale l'adozione di tale misura.
Ogni assegnatario di indirizzo di posta elettronica aziendale potrà, in caso di necessità, dirottare la propria posta elettronica su un diverso indirizzo di posta elettronica aziendale; nel caso non sia in grado di attuare detta misura in autonomia, potrà chiedere al Servizio S.T.I. Aziendale la messa in atto della misura; della attuazione di tale misura verrà tenuta traccia e verrà data notizia al lavoratore interessato alla prima occasione utile.

Qualora vengano inviati messaggi di posta elettronica che prevedano che l'eventuale risposta possa essere conosciuta da più persone nell'ambito dell'Azienda, occorrerà rendere edotto di ciò il destinatario.
Fatte salve le limitazioni di cui ai punti precedenti l'Azienda favorisce l'utilizzo della posta elettronica come strumento per la rapida comunicazione fra i dipendenti, fra dipendenti e cittadini, fra pubbliche amministrazioni, purché queste comunicazioni siano parte delle attività istituzionalmente previste e compatibili con le mansioni proprie di ogni operatore. Fatte salve le limitazioni precedentemente esposte, alla trasmissione telematica di atti e documenti all'interno dell'Azienda per posta elettronica è riconosciuta la stessa validità della trasmissione per via cartacea; in particolare potranno essere trasmessi atti deliberativi, disposizioni dirigenziali e documenti in genere che non contengano dati sensibili e il cui mancato recapito non ingeneri danni per l'azienda, per i dipendenti o per altri. L'utilizzo della posta elettronica, in questi casi, potrà sostituire completamente l'invio di carta. Atti o documenti aventi valenza generale possono essere comunicati a tutti o a grande parte dei dipendenti dell'Azienda; ciò può avvenire tramite l'utilizzo di apposite liste di distribuzione che sono messe a disposizione in posta elettronica; esigenze particolari od occasionali di comunicazione ad un numero di utenti il cui volume o la cui qualità non sia già stata prevista dovranno essere inoltrate dal Servizio S.T.I. Aziendale.
Alla cessazione del rapporto di lavoro, la casella di posta verrà chiusa e il suo contenuto salvato, in quanto potenzialmente contenente dati di cui la proprietà è aziendale. L'indirizzo di posta verrà quindi messo in condizione di non ricevere più mail ed eventualmente, su richiesta del capo servizio, di segnalare al mittente, tramite messaggio automatico e per un periodo limitato di massimo mesi 6, che l'indirizzo in questione non è più valido e che le comunicazioni potranno essere inoltrate a un indirizzo aziendale diverso.
L'utente non è autorizzato a scaricarsi su supporto esterno l'intero contenuto della casella di posta, né a cancellarla completamente.
Passati due anni dalla chiusura della casella di posta, il contenuto della stessa verrà rimosso dal server di posta e l'indirizzo potrà essere riassegnato

Art. 16 – Cloud Aziendale

La necessità di una sempre maggior disponibilità di accesso ai propri dati da parte dei professionisti, su sistemi diversi e con tecnologie diverse, ha portato all'evoluzione del concetto di portabilità dei dati, passando dagli oramai 'storici' floppy disk, ai supporti di memorizzazione rimovibili USB (quali chiavette o hard disk), ai servizi cloud pubblici (come Dropbox o Google Drive per citare solo i più diffusi)
La peculiarità dei dati tipicamente trattati dai professionisti aziendali è spesso riconducibile alla categoria definita come dati sensibili, secondo le normative vigenti (il nuovo regolamento europeo in materia di trattamento dei dati GDPR).
D'altro canto, l'uso di un servizio di cloud pubblico gratuito, ha spesso come rovescio della medaglia le seguenti criticità, che spesso vengono accettate senza nemmeno rendersene conto della portata potenziale (vedi ad esempio: https://www.google.com/intl/it/policies/terms/), quali, ad esempio:

- nessuna responsabilità da parte del fornitore del servizio su eventuale diffusione o perdita dei dati memorizzati nel cloud
- Il fornitore del servizio viene autorizzato ad usare i dati presenti nel cloud gratuito per i propri scopi commerciali, quali profilazione utente, marketing, cessione a terzi, …
- Nessuna sicurezza dell'eliminazione effettiva dei dati in caso di cancellazione e/o spostamento degli stessi in un altro ambiente o fornitore

Per questi motivi è stato installato sui server dell'Azienda Ospedaliero – Universitaria di Modena un servizio di memorizzazione cloud simile a quelli sopracitati ma che, essendo fisicamente sui server aziendali, è più rispondente alle regole di privacy (Cloud Computing - La guida del Garante della Privacy per imprese e pubblica amministrazione)

L'utilizzo di questo sistema di memorizzazione su cloud privato, ancorché innovativo per l'azienda, è tuttavia sottoposto in toto e senza alcuna eccezione al presente disciplinare ed in particolare agli art. 4 e art. 5 in esso contenuti

Art. 17 - Comunicazioni di massa

È' fatto obbligo agli utenti segnalare allo S.T.I. l'eventuale ricevimento di messaggi, sia da utenti interni che esterni, appartenenti ad una delle seguenti categorie:

- "mail spamming" e "catene di S. Antonio";
- aventi contenuto diffamatorio per l'Azienda od i suoi dipendenti;
- aventi contenuto moralmente deplorevole, scandaloso, propagandistico per correnti politiche o fazioni religiose;
- aventi contenuto non attinente l'attività lavorativa ed il cui ricevimento sia "non gradito" all'utente;
- aventi il fine di "intasare" le caselle di posta elettronica.

La segnalazione va indirizzata esclusivamente via e-mail all'indirizzo **cedarearetepc@aou.mo.it**, inoltrando la e-mail sospetta.
Gli utenti interni che attuano uno dei comportamenti vietati verranno segnalati al Dipartimento Risorse Umane per le eventuali sanzioni disciplinari.
Per quanto riguarda comunicazioni da inviare in maniera massiva a tutte le caselle di posta aziendali, in genere per comunicazioni che rivestono particolare importanza per un congruo numero di utenti, l'autorizzazione deve essere ottenuta dall'Ufficio Comunicazione, che valuterà e approverà il testo proposto per l'invio.

Art. 18 - Data breach

Dal mese di agosto 2015, in ottemperanza ad un obbligo sancito dal Garante Privacy è stata introdotta e diffusa tra tutti i dipendenti una procedura per la comunicazione obbligatoria e tempestiva al Garante (entro le 72 ore dalla conoscenza del fatto) di eventuali violazioni dei dati o incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle banche dati dell'Azienda – c.d. data breach[1].
Pertanto, chiunque in Azienda sospetti sia avvenuto un data breach deve immediatamente comunicarlo allo S.T.I., utilizzando l'indirizzo email: **security@aou.mo.it**, nonché adottare la procedura aziendale PO 160 per la gestione di data breach ai sensi del GDPR (Regolamento europeo 679/2016)

Art. 19 - Cessazione della disponibilità dei servizi informatici aziendali

Ai sensi del presente "Disciplinare", la disponibilità dei servizi informatici aziendali cesserà per l'utente nei seguenti casi:

1) qualora non sussistesse più la condizione di dipendente o di collaboratore esterno. Questo evento dovrà essere comunicato tempestivamente da parte del responsabile del servizio cessante allo S.T.I., in modo da poter eliminare dai S.I.A. tutte le abilitazioni;
2) qualora non fosse confermata o venisse revocata l'autorizzazione all'uso fornita dal Responsabile; il quale dovrà comunicare l'evento come al punto precedente;
3) qualora avvenisse il trasferimento di un utente da un servizio ad un altro. Il Responsabile del servizio cessante dovrà comunicare tempestivamente la cessazione del rapporto, mentre il

[1] Fra gli eventi che possono essere ascritti ad un data breach, pur essendo l'elenco non esaustivo, vi sono: l'accesso abusivo a dati personali, sensibili o giudiziari contenuti nelle banche dati aziendali; la copia abusiva per immagine su supporto informatico di documenti analogici contenenti dati personali, sensibili o giudiziari; la perdita o il furto di attrezzature aziendali – PC portatili, PC fissi, dispositivi di memorizzazione, ecc… che contengano dati personali, sensibili o giudiziari; attacchi condotti da persone o software – malware - che ottengano l'accesso alle banche dati aziendali o più in generale eventi che possano portare ad accessi indebiti o alla cattura di dati di accesso e di identificazione - user name e password.

Responsabile del servizio subentrante dovrà autorizzare le nuove abilitazioni con le procedure descritte all'art. 4 del presente "Disciplinare";

Art. 20 - Altri strumenti di comunicazione aziendale: Telefoni fissi, telefoni mobili, ecc…

L'utilizzo personale e non istituzionale del telefono è autorizzato per motivi di urgenza e/o necessità indifferibili, quando cioè non è possibile usare il telefono personale cellulare.
L'azienda, mediante configurazioni sugli apparati tecnologici, impedisce l'effettuazione di chiamate dalla rete aziendale verso determinate categorie di numeri: ad esempio numeri a pagamento per servizi particolari che si giudicano non interessanti dal punto di vista istituzionale, ecc….
Ogni operatore che abbia la necessità di utilizzare, per fini istituzionali, una classe di numeri non abilitata potrà richiedere una specifica abilitazione.
Per fini di controllo della spesa telefonica l'Azienda tiene traccia delle telefonate effettuate, qualora queste inducano un onere economico per l'Azienda; vengono altresì tracciate le telefonate in ingresso in quanto può essere richiesto dai servizi aziendali l'avvenuta ricezione o meno di una chiamata ad un determinato numero interno.
Viene registrato:

- il numero del chiamante;
- il numero chiamato;
- la data e ora di inizio della telefonata e la data e ora di fine della stessa

Tutti i log sopra citati vengono conservati dall'Azienda un anno solare in maniera disaggregata per poter confrontare gli andamenti di costo con i dati aggregati degli anni precedenti. I dati disaggregati dal primo gennaio dell'anno al trentuno dicembre dell'anno potranno essere tenuti fino alla fine di marzo dell'anno successivo per i controlli istituzionali, dopo di che dovranno essere aggregati in maniera tale che possano essere utilizzati per i confronti con i periodi successivi. I controlli verranno effettuati in maniera non nominativa e aggregata – ad esempio aggregando i dati per edificio o per unità erogante; qualora i dati evidenzino anomalie tali da giustificare controlli aggiuntivi, potranno essere ulteriormente approfonditi. Normalmente sarà necessario adottare una gradualità nei controlli che preveda prima il controllo del dato aggregato e la notifica di eventuali anomalie e solo successivamente, qualora il problema persista, un controllo sui dati disaggregati.
Qualora l'integrità del sistema tecnologico dell'azienda o la gravità del fatto lo rendano necessario sarà possibile accedere immediatamente al dato disaggregato; qualora possibile, gli approfondimenti sui dati che si rendessero necessari saranno condotti con verifiche a campione.
In generale tutte le verifiche dovranno rispettare i criteri della pertinenza e non eccedenza rispetto al fine di controllo amministrativo proprio dell'Azienda; qualora le verifiche portino all'accertamento della violazione delle presenti regole o più in generale all'accertamento di utilizzi impropri, l'Azienda si riserva di adottare le opportune misure disciplinari e amministrative.

Art. 21 - Tutela del diritto d'autore

Vista la legge 248 del 18/08/2000 relativa alla tutela del diritto d'autore:

- è vietata la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici e dei manuali a corredo dei programmi, si ricorda infatti che anche i manuali sono coperti dalla legge sul diritto di autore e possono essere riprodotti solo dietro autorizzazione del titolare dei diritti esclusivi;
- è fatto divieto ad ogni utilizzatore del sistema informativo aziendale scaricare, gestire in qualsiasi modo e trattare dati o informazioni che violino la normativa sulla tutela del diritto d'autore;
- qualora l'operatore nonostante tale divieto infranga tale normativa sarà penalmente e civilmente responsabile del proprio operato sollevando l'azienda da ogni responsabilità.

Art. 22 - Ulteriori istruzioni per la tutela delle informazioni gestite dagli operatori

Documentazione cartacea

- L'operatore, per tutto il periodo in cui effettua le operazioni di trattamento dei dati, non deve mai perdere di vista i documenti, adempiendo ad un preciso obbligo di custodia dei medesimi.
- L'operatore deve controllare che i documenti siano sempre completi ed integri.
- In caso di abbandono, anche temporaneo, dell'ufficio, l'operatore non deve mai lasciare incustoditi i documenti (sulla scrivania o su tavolini di reparto); è infatti necessario identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.); ove si utilizzi un contenitore/locale chiuso a chiave occorre accertarsi che non esistano duplicati abusivi delle chiavi e che le stesse siano in possesso solo di operatori autorizzati.
- Occorre in particolare accertarsi che nessun visitatore o terzo estraneo possa venire a conoscenza (anche per cause accidentali) del contenuto dei documenti.
- Al momento della consegna di documenti contenenti dati personali o sensibili ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate.
- La distruzione dei documenti contenenti dati personali o sensibili deve avvenire con modalità che rendano impossibile l'individuazione dell'interessato da parte di terzi non autorizzati (mediante apposita macchinetta tritatutto o distruzione manuale in piccoli pezzi).

Comunicazioni telefoniche e via fax

- Nel caso in cui sia necessario effettuare comunicazioni telefoniche agli interessati, occorre aver chiesto preliminarmente all'interessato medesimo l'autorizzazione a conferire con chi risponda all'apparecchio. In caso di risposta negativa l'operatore deve chiedere in alternativa un numero riservato.
- Occorre fare attenzione a discutere, comunicare o comunque trattare dati personali/sensibili per telefono in presenza di terzi non autorizzati che potrebbero inavvertitamente venire a conoscenza di tali dati.
- In caso di invio di documentazione a mezzo fax, bisogna prestare attenzione alla corretta digitazione del numero cui inviare il documento e verificarne l'esattezza; qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è opportuno anticipare l'invio del fax avvertendo il destinatario, assicurarsi che il ricevimento avvenga nelle mani del medesimo ed evitare che soggetti estranei o non autorizzati possano conoscere il contenuto della documentazione inviata.
- L'apparecchio fax (se esistente) deve essere sempre collocato in luogo non accessibile a terzi non autorizzati.
- E' sempre da preferire l'utilizzo del servizio del faxserver aziendale (**mailfax**), con inoltro dei fax in ingresso ad un account di mail aziendale.

Utilizzo della fotocopiatrice e della stampante

- In caso di stampa o duplicazione non riuscite di documentazione contenente dati personali/sensibili, occorre evitare di gettare i fogli nel cestino senza aver provveduto a rendere illeggibile il contenuto dei dati.
- Qualora si utilizzi carta riciclata per fotocopie e stampe, occorre sempre accertarsi che non siano accidentalmente riportati dati personali e/o sensibili.
- Occorre utilizzare con attenzione le macchine fotocopiatrici di ultima generazione che possono scannerizzare e memorizzare il documento, talvolta conservando il file elettronico dello stesso.

Rapporti di front office

- **Rispetto della distanza di cortesia**: l'operatore di sportello deve prestare attenzione al rispetto dello spazio di cortesia e, se del caso, invitare gli utenti a sostare dietro le apposite linee/barriere delimitanti lo spazio di riservatezza.
- **Controllo dell'identità del richiedente**: nel caso di richieste di comunicazioni di dati (presentate per telefono o via fax) occorre verificare l'identità del soggetto richiedente (ad esempio formulando una serie di quesiti al fine di un accertamento sommario) e la sua legittimazione a ricevere le informazioni su quanto richiesto.

- **Identificazione dell'interessato e controllo dell'esattezza dei dati**: nel momento della raccolta di dati anagrafici (in particolar modo nel caso di cittadini stranieri) occorre fare attenzione alla digitazione ed all'inserimento corretto dei dati identificativi dell'interessato.
- **E' vietata la chiamata nominativa dell'utente**: nelle sale e negli spazi di attesa i nomi dei pazienti non devono essere divulgati ad alta voce; occorre utilizzare un sistema che prescinda dai dati anagrafici (es. codice alfanumerico, orario della prenotazione, ecc.). Eventuali deroghe ed eccezioni devono essere discusse con l'Ufficio Privacy.

Corretta comunicazione dei dati

- La richiesta di comunicazione o documentazione di dati personali e sensibili può essere evasa nei confronti dell'interessato o di un terzo a ciò delegato (per iscritto) o legittimato per legge (in casi dubbi rivolgere sempre richiesta di chiarimenti al responsabile del trattamento). In tal senso assoluta attenzione deve essere in particolare prestata nelle operazioni di consegna di referti diagnostici, cartelle cliniche, risultati di analisi e certificati.
- Devono comunque essere rispettate le modalità del controllo dell'identità del richiedente (vd. paragrafo "rapporti di front office").
- La comunicazione di dati idonei a rivelare lo stato di salute deve essere sempre effettuata da un medico o da personale sanitario a ciò delegato (art. 84 D.Lgs. 196/03).
- L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi nonché essere contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.
- L'invio di documentazione sanitaria per via elettronica (e-mail, condivisione cloud, ecc..) deve sempre avvenire crittografando i file e inviando la password per decrittografare tramite mezzo trasmissivo diverso (es. con un messaggio SMS)

Rispetto della privacy in corsia

- Devono essere adottate soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza, da parte di terzi, di informazioni idonee a rivelare lo stato di salute (ad es. utilizzo, laddove possibile, di spazi riservati).
- Devono altresì essere adottate soluzioni tali da garantire il rispetto della dignità dell'interessato, in occasione di prestazione mediche particolarmente delicate (ad es. utilizzo di paraventi).
- L'interessato ricoverato, se cosciente e capace, deve essere preventivamente informato e poter decidere a chi possa essere data comunicazione della propria presenza in ospedale. Qualora l'interessato non possa essere interpellato in proposito, potranno essere fornite informazioni, anche telefoniche, sul passaggio o sulla presenza dello stesso al Pronto Soccorso o in altri reparti solo ai terzi legittimati come familiari e congiunti, previo accertamento sommario dell'identità del richiedente (es. mamma che contatti il Pronto Soccorso per avere notizie circa l'eventuale presenza del figlio nella struttura).
- Occorre porre in essere procedure dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparto o strutture indicativa dell'esistenza di un particolare stato di salute (sono vietate ad es. le carrozzine che riportano per esteso il nome dell'unità operativa di appartenenza).
- E' vietata, in locali aperti al pubblico o di passaggio, l'affissione di liste di pazienti in attesa di intervento; in tali luoghi è vietata altresì l'affissione della turnistica degli operatori riportante la causa di assenza (es. malattia).
- Non devono essere visibili ad estranei documenti sulle condizioni cliniche del malato (es. cartelle cliniche/infermieristiche poste vicino al letto di degenza). Qualora fosse necessario mantenere la grafica ai piedi del letto, essa dovrà essere girata o comunque posizionata in modo tale da non poter essere immediatamente visibile da terzi estranei.

Art. 23 - Servizio deputato ai controlli

L'Azienda delega al Servizio Tecnologie dell'Informazione i controlli tecnici sui sistemi informatici previsti dalla presente linea guida e alle macro articolazioni gestionali la responsabilità complessiva del controllo del personale afferente alle unità organizzative di competenza.

Art. 24 - Comportamenti che danno luogo a segnalazione

Ai sensi del presente "Disciplinare", potranno essere segnalati al Dipartimento Risorse Umane, che valuterà le eventuali sanzioni disciplinari, gli assegnatari dei S.I.A. che porranno in essere uno o più dei seguenti comportamenti in aggiunta a quelli già indicati nell'art. 13:

a) installazione non autorizzata di hardware o software;
b) alterazione non autorizzata della configurazione hardware o software della stazione di lavoro;
c) comunicazione o diffusione di credenziali di accesso a sistemi e procedure informatiche, nonché altre informazioni tecniche riservate;
d) scarico non autorizzato di materiale informatico estraneo all'attività lavorativa;
e) violazione in genere di norme del Codice Penale, nella parte in cui tratta dei reati informatici;
f) violazione di quant'altro stabilito nel presente "Disciplinare".

Art. 25 - Informativa

Il Titolare del trattamento dei dati è l'Azienda Ospedaliero - Universitaria di Modena.
I Responsabili del trattamento dei dati personali, a mezzo di strumenti informatici dell'Azienda, sono:

- Lo S.T.I. (nella persona del Direttore del Servizio) per quanto attiene alla gestione dei dati effettuata mediante i sistemi informativi aziendali, circa le modalità tecnologiche e gli strumenti utilizzati per l'erogazione del servizio, ivi compreso il profilo della sicurezza;
- I delegati al trattamento dei dati designati dal Titolare del trattamento con apposito provvedimento, per quanto attiene alle decisioni riguardo alla finalità ed alle modalità organizzative di utilizzo dei sistemi o servizi di competenza;
- i terzi che, in relazione ai servizi chiamati ad espletare per conto dell'Azienda, siano dalla stessa autorizzati all'utilizzo di sistemi informatici aziendali.

I diritti dell'interessato previsti dal Regolamento europeo in materia di protezione dei dati personali (GDPR), in particolare il diritto di conoscere i dati che lo riguardano (art. 15), il diritto di aggiornarli (art. 16), il diritto di cancellare (art. 17), il diritto di limitazione al trattamento (art. 18), il diritto alla portabilità dei dati (art 20) nonchè i dati eventualmente trattati in violazione di legge potranno essere esercitati rivolgendosi ai delegati al trattamento dei dati designati dal Titolare del trattamento con apposito provvedimento.
Il presente "Disciplinare" inizierà ad essere applicato dalla data dall'adozione del relativo provvedimento di approvazione e potrà essere soggetto in qualsiasi momento a modifiche ed aggiornamenti, dovuti ad innovazione tecnologica e/o a modifiche organizzative aziendali, nonché per il mutato quadro normativo di riferimento.
Tali variazioni saranno rese note a tutti i dipendenti tramite l'emanazione di nuovi provvedimenti deliberativi.