SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Modena

REGOLAMENTO AZIENDALE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E DEGLI STRUMENTI DI COMUNICAZIONE

dell'Azienda USL di Modena

Sommario

1 Principali riferimenti normativi

- Regolamento (UE) 2016/679 in materia di protezione dei dati personali - GDPR
- D. Lgs. 196/2003 e s.m.i. “Codice in materia di protezione dei dati personali” – Codice Privacy
- Autorità Garante per la protezione dei dati personali, Deliberazione 13/2007 “Lavoro: le linee guida del Garante per posta elettronica e internet”
- Autorità Garante per la protezione dei dati personali, Provvedimento del 13 ottobre 2008 “Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali”.
- Legge 300/1970 e s.m.i cd “Statuto dei lavoratori”
- Legge 547/1993 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"
- D. Lgs. 82/2005 e s.m.i. “Codice dell’amministrazione digitale”
- D.P.R. 68/2005 “Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3”
- Presidenza del Consiglio dei Ministri, Dipartimento per le innovazioni e la tecnologia, Direttiva 27 novembre 2003 “Impiego della posta elettronica nelle pubbliche amministrazioni”.
- Presidenza del Consiglio dei Ministri, Dipartimento per le innovazioni e la tecnologia, Direttiva del 18 novembre 2005 “Linee guida per la Pubblica amministrazione digitale”
- Presidenza del Consiglio dei Ministri, Dipartimento della funzione pubblica, Direttiva n. 2/2009 "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro"
- DPCM 8 agosto 2013 “Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali [...]”
- Circolari AgID nn. 1 e 2/2017[1]
- Piano triennale AgID per l’informatica[2]

2 Oggetto e campo di applicazione

Il presente documento, redatto a cura del Servizio Information & Communication Technology Aziendale (di seguito “SICT”) e dell’Ufficio Privacy Aziendale regolamenta l’accesso e l’uso delle risorse informatiche della Azienda USL di Modena (nel seguito AUSL), secondo i principi e le disposizioni della normativa citata in premessa e le indicazioni in materia di corretto uso delle risorse informatiche, nel rispetto delle politiche e disposizioni definite in accordo con la Direzione Aziendale.

In particolare, le istruzioni riportate si rifanno alla normativa in materia di protezione dei dati personali, alla normativa sul crimine informatico e più in generale al corpo normativo che disciplina il processo di digitalizzazione delle pubbliche amministrazioni.

Scopo del documento è quello di agevolare la lettura e l’interpretazione della normativa, fornendo agli utilizzatori le necessarie prescrizioni e istruzioni operative.

Il documento opera nei confronti di ogni dipendente dell’Azienda e di tutti coloro che a vario titolo si trovino ad utilizzare il sistema informativo aziendale. Nel seguito del presente documento, per semplicità espositiva si farà riferimento genericamente all’utilizzatore.

Gli estensori si impegnano ad adeguare questo Regolamento in funzione di eventuali mutamenti legislativi, di aggiornamenti degli strumenti informatici aziendali o in ragione di particolari necessità tecniche. L'ultima versione sarà sempre consultabile sul sito Intranet Aziendale.

[1] http://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg
[2] https://www.agid.gov.it/it/agenzia/piano-triennale

Sarà cura di ciascun utilizzatore verificare che siano state pubblicate nuove versioni del presente Regolamento e adottare comportamenti congrui a quanto prescritto relativamente ai propri ambiti specifici di competenza e di attività.

Si sottolinea che l'uso improprio o illecito degli strumenti di informazione e comunicazione determina un danno all'Azienda, reale o potenziale, sia in termini di perdita di risorse (per esempio la disponibilità e l'efficienza del sistema complessivo, ma anche di tempo lavorativo del dipendente), sia in termini di effetti dannosi diretti, quali l'introduzione di virus, la trasmissione illecita di dati riservati, la commissione di reati eventualmente attribuibili all'Azienda ecc.

Le attività di controllo e vigilanza sono fondate sul principio della "proporzionalità" che si concretizza nella pertinenza e non eccedenza del controllo; pertanto, i mezzi e l'ampiezza del controllo sono proporzionati agli scopi che, nello specifico, sono quelli di garantire la sicurezza del sistema informatico e l'appropriato utilizzo delle risorse.

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. 113, 114, 171 Codice Privacy; 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.

3 Definizioni

Risorse Informatiche

Qualsiasi mezzo di comunicazione e elaborazione elettronica, hardware, software, rete, servizio e informazione in formato elettronico di proprietà dell'Azienda o in disponibilità o a essa concesso in licenza d'uso.

Le risorse informatiche includono a titolo di esempio:

- sistemi informatici a uso sanitario, amministrativo o tecnico (es. posta elettronica, accesso a Internet, applicativi aziendali quali Gestione di Reparto/Specialistica SIO, Auriga, Onconet, Diapason, Archiflow ecc.);
- ogni sistema di elaborazione elettronica delle informazioni: server, personal computer fissi o portatili, tablet e similari (inclusi smartphone);
- software di base e di ambiente: sistemi operativi, software di rete, sistemi per il controllo degli accessi, package, utility e similari;
- software di produttività individuale (Office, LibreOffice, OpenOffice, Project, Visio ecc.);
- ogni informazione elettronica registrata o conservata in file e banche dati;
- ogni periferica: stampanti, scanner, plotter, apparecchiature per l'archiviazione elettronica dei dati, supporti di memorizzazione, videoterminali;
- ogni dispositivo di rete: concentratori, ripetitori, modem, switch, router, gateway, firewall, apparati VoIP e similari, access point, chiavette Internet;
- ogni mezzo trasmissivo di cablaggio strutturato per reti locali, metropolitane e geografiche: cavi in fibra e in rame per dorsali e cablaggio orizzontale, permutazioni, attestazioni, patch e similari.

Utilizzatori

Persone fisiche dipendenti o collaboratori a vario titolo, frequentatori, universitari, volontari che hanno accesso a strumenti informatici o telematici collegati alla rete o ai sistemi dell'Azienda USL di Modena e che sono nella potenzialità di utilizzarli o che hanno in qualsiasi modo accesso ai dati di cui l'AUSL sia Titolare.

Trattamento

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Interessato
La persona fisica cui si riferiscono i dati personali.

Dato
In merito al tipo di dati si distinguono:

- *Dato personale*
  Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- *Particolari categorie di dati*
  Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Soggetti attivi del trattamento
In merito ai soggetti che possono effettuare operazioni di trattamento si distinguono:

- *Titolare*
  La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; nel nostro caso Titolare del trattamento è l'Azienda USL di Modena
- *Delegati*
  Personale dipendente della Azienda, individuato in virtù delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati, al quale, avvalendosi dello strumento della delega di funzioni, il Titolare attribuisce i compiti e le funzioni connessi al trattamento di dati personali. In particolare i Delegati 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.
- *Responsabile*
  La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
- *Soggetti designati/autorizzati*
  Le persone fisiche espressamente designate, a cui il Titolare del trattamento, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, attribuisce specifici compiti e funzioni connessi al trattamento di dati personali.

Comunicazione
Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dell'Unione Europea, dal Responsabile o dal suo rappresentante nel territorio dell'Unione Europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies del Codice Privacy, al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione.

Diffusione
Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Per soggetti indeterminati si intendono soggetti non identificabili a priori.

Archivio
Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Misure di sicurezza

Le misure tecniche e organizzative definite dal Titolare del trattamento e adeguate al rischio insito nel trattamento effettuato.

Spetta infatti al Titolare eseguire una valutazione dei rischi connessi al trattamento: la probabilità e la gravità del rischio per i diritti e le libertà degli interessati sono determinate tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

Le misure di sicurezza possono essere di tre tipologie:

- Tecniche, cioè volte a proteggere le architetture di rete, gli applicativi e le banche dati e la trasmissione dei dati stessi (ad esempio autenticazione informatica, uso delle password, sistema di autorizzazione e configurazione dei profili di accesso, antivirus e antispam, back up, pseudonimizzazione/anonimizzazione dei dati);
- Fisiche, cioè volte a proteggere le aree, i locali e gli archivi da accessi non autorizzati (ad esempio armadi chiusi a chiave, controllo degli accessi con badge o sistemi di registrazione dei visitatori, vigilanza);
- Organizzative, cioè individuate dal titolare per l'assegnazione di compiti e responsabilità, per la costituzione di una cultura aziendale sulla tematica di protezione dati, per garantire che i trattamenti avvengano per finalità autorizzate e consentite (ad esempio informativa e consenso, deleghe di funzioni, autorizzazioni a trattare i dati, definizione dei termini di conservazione dei dati, gestione data breach, formazione dei dipendenti).

Credenziali di autenticazione

Misura di sicurezza tecnica: I dati e i dispositivi in possesso di una persona, da questa conosciuti o a essa univocamente correlati, utilizzati per l'autenticazione informatica, ovvero il processo che garantisce l'accesso a un sistema informatico.

La parola chiave (password) è la componente di una credenziale di autenticazione associata a una persona e solo a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica, da mantenere riservata.

4 Principi generali

Le risorse informatiche:

- Sono parte integrante del patrimonio dell'Azienda USL di Modena;
- Devono essere utilizzate per gestire le attività aziendali, secondo le finalità autorizzate e definite dalla Direzione Aziendale e inerenti alla propria mansione, nel rispetto dei principi di integrità e riservatezza, minimizzazione, esattezza, limitazione della conservazione;
- Devono essere rese disponibili solo alle persone autorizzate e nei limiti di quanto necessario allo svolgimento dell'attività istituzionale;
- Devono essere protette mediante misure tecniche e organizzative adeguate, in modo da garantire la sicurezza dei dati personali dal rischio di trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Le regole stabilite si riferiscono a tutte le risorse informatiche dell'Azienda, incluso l'accesso a Internet e l'utilizzo della posta elettronica, sono applicate da tutti i soggetti che le utilizzano e hanno valenza per tutte le tipologie di dati.

L'Azienda fornisce gli strumenti informatici e telematici agli utilizzatori, confidando sul comune impegno affinché siano sempre garantiti sia il loro corretto ed equilibrato utilizzo, sia la sicurezza e l'integrità del sistema informatico/informativo e affinché non vengano pregiudicate o ostacolate le attività dei singoli o della collettività a causa di un uso inappropriato delle risorse disponibili da parte del singolo e non vengano perseguiti interessi privati in contrasto con quelli pubblici.

Tutti coloro che per ragioni di servizio devono avere accesso ai servizi informatici aziendali devono previamente essere stati autorizzati al trattamento dei dati da parte del titolare o di un suo delegato.

I dati possono essere trattati limitatamente alle operazioni indispensabili per l'esercizio delle rispettive funzioni.

Autorizzare le abilitazioni agli applicativi per il personale di propria afferenza è un atto che impone la preventiva valutazione in merito alla effettiva esigenza del personale di accedere ai dati per lo svolgimento della propria attività lavorativa.

La mancanza di tale valutazione costituisce una grave violazione della normativa sulla protezione dei dati personali, potendo determinare conseguenze (quali accessi illegittimi o trattamenti non autorizzati dei dati) pesantemente sanzionate.

Oltre a quanto definito nel presente Regolamento, che ha comunque sempre valore, si precisa che, con riferimento alle risorse informatiche messe a disposizione o date in uso all'Azienda da altre organizzazioni, hanno valore anche gli accordi e le condizioni contrattuali stipulate fra le parti.

5 Divieti

Di seguito si richiamano i principali divieti da rispettare nell'utilizzo delle risorse informatiche dell'Azienda. In particolare è fatto divieto di:

- Introdursi abusivamente nei sistemi informatici aziendali;
- Procurare a sé, o ad altri, profitto, o arrecare danni all'Azienda, procurandosi, riproducendo, diffondendo, o consegnando codici, parole chiave o altri mezzi idonei all'accesso ai sistemi informatici.
- Riprodurre, duplicare e/o asportare, comunicare a terzi, diffondere i dati di cui l'Azienda è titolare del trattamento.
- Riprodurre e asportare documentazione di qualsiasi tipo classificata riservata, compresi progetti, schede, prospetti, se non, per fini particolari, dietro esplicita autorizzazione del titolare dei relativi diritti (o di persona delegata).
- Intercettare, impedire, interrompere le comunicazioni inerenti ai sistemi informatici.
- Distruggere, deteriorare, rendere inservibili, del tutto o in parte, i sistemi informatici ovvero i programmi e le informazioni o i dati esistenti nei sistemi.
- Riprodurre, duplicare e/o asportare programmi installati di cui l'Azienda è licenziataria o proprietaria.
- Introdurre, installare, utilizzare programmi che non siano stati regolarmente acquistati, distribuiti e installati dalle preposte funzioni aziendali.
- Adottare comportamenti che mettano a rischio la sicurezza del sistema informatico/informativo, inclusi i dati ivi contenuti, o che pregiudichino o ostacolino le attività della collettività degli utilizzatori.

La violazione di tali divieti è punita, a seconda della gravità, sotto il profilo della responsabilità penale, civile, amministrativa e disciplinare.

A titolo di esempio, si elencano di seguito alcune figure di reato di natura informatica previste dal Codice Penale:

- Attentato a impianti informatici di pubblica utilità (art. 420);
- Falsificazione di documenti informatici (art. 491bis);
- Accesso abusivo ad un sistema informativo o telematico (art. 615ter);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615quater);
- Diffusione di programmi diretti a danneggiare o interrompere un sistema informativo (art. 615quinquies);
- Violazione di corrispondenza telematica (artt. 616-617sexies);
- Intercettazione di e-mail (art. 617quater);
- Danneggiamento di sistemi informatici e telematici (art. 635bis);
- Frode informatica (alterazione dell'integrità di dati allo scopo di procurarsi un ingiusto profitto) (art. 640ter).

A sua volta il Codice Privacy prevede le seguenti autonome fattispecie di reati:

- Trattamento illecito di dati (art. 167)
- Comunicazione o diffusione illecita di dati personali oggetto di trattamento su larga scala (art. 167bis);
- Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art. 167ter)
- Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (art. 168)
- Inosservanza di provvedimenti del Garante (art. 170)
- Violazioni sui controlli a distanza dei lavoratori e indagini sulle opinioni (art. 171).

6 Responsabilità

6.1 Procedure informatizzate autorizzate

Le procedure informatiche distribuite e gestite dal SICT sono tutte e sole quelle individuate definite dal Servizio stesso ed inserite nell'elenco presente nella relativa pagina della Intranet Aziendale.

Relativamente a tali procedure, sono a carico del SICT la definizione delle misure di sicurezza e più in generale il rispetto della normativa e delle disposizioni aziendali, per quanto riguarda i server, i software di base, le procedure applicative, le infrastrutture, i dispositivi della rete aziendale.

Sono invece a carico degli utilizzatori, ciascuno per i rispettivi ambiti di competenza, la adozione delle misure di sicurezza, e più in generale, il rispetto della normativa e delle disposizioni aziendali, in particolare di questo Regolamento, per quanto riguarda le postazioni di lavoro (personal computer) e le attività svolte con esse.

6.2 Data breach

In ottemperanza all'obbligo sancito dal GDPR, è stata introdotta e diffusa tra tutti i dipendenti e collaboratori aziendali una procedura per la gestione degli episodi di violazione di dati personali – c.d. data breach - e la relativa comunicazione alla Autorità Garante per la protezione dei dati personali.

Pertanto tutti gli utilizzatori dei sistemi informatici e telematici aziendali che abbiano notizia o sospetto di una possibile violazione di dati sono tenuti ad attivare la procedura aziendale – DG.PO.013 - per la segnalazione di data breach, reperibile, insieme alla apposita modulistica, sul sito intranet Aziendale – sezione privacy.

6.3 Procedure informatizzate non gestite dal SICT

Fermo restando il divieto di installare e utilizzare programmi non autorizzati, se per qualsiasi ragione, in particolare la necessità di garantire la continuità gestionale, dovessero essere in uso presso le Unità Operative procedure informatizzate NON distribuite dal SICT, fintanto che esse rimangono operative l'organizzazione e la gestione delle misure di sicurezza e più in generale il rispetto della normativa e delle disposizioni Aziendali, sono a carico del singolo delegato del trattamento, che deve rivolgersi al SICT per verificarne la corretta applicazione.

7 Sistemi di autenticazione e di autorizzazione

Il delegato al trattamento dovrà richiedere l'attivazione delle credenziali di autenticazione informatica per ciascun operatore previamente autorizzato al trattamento, specificando a quali dati e tipi di operazioni può accedere in relazione ai compiti impartiti.

Il trattamento di dati personali con strumenti elettronici è consentito infatti ai soli utilizzatori autorizzati come sopra e dotati di credenziali di autenticazione, in genere costituite da NomeUtente (username) e password.

7.1 Credenziali di autenticazione (coppia username e password)

Le credenziali di autenticazione sono il presupposto necessario per l'utilizzo dei sistemi informatici messi a disposizione dall'Azienda USL di Modena.

Tutti coloro che per ragioni di servizio devono avere accesso al sistema informatico aziendale devono essere intestatari di un nome utente all'interno del dominio di sicurezza aziendale e di un utente di posta elettronica.

Le credenziali consentono il superamento di una procedura d'autenticazione che permette l'accesso all'infrastruttura informatica, a uno specifico trattamento o a un insieme di trattamenti.

7.2 Accesso agli applicativi aziendali

Tutte le informazioni relative alle modalità di abilitazione agli applicativi aziendali sono riportate nella relativa sezione della Intranet Aziendale.

7.3 Gestione delle credenziali aziendali

Le credenziali aziendali consistono in un codice per l'identificazione dell'incaricato, associato ad una parola chiave riservata conosciuta solamente dal medesimo (username e password).

Esistono altre tipologie di credenziali (biometriche, smartcard, ecc) non in uso presso l'Azienda USL di Modena: potrebbero essere fornite da altri enti per programmi/sistemi non aziendali, in tal caso i riferimenti per l'abilitazione, l'utilizzo e l'assistenza con queste credenziali non aziendali sono a carico dell'ente che le ha fornite.

Lo username, o nome utente, è di norma costituito dal cognome seguito dall'iniziale del nome dell'utilizzatore (es. rossim). I casi di omonimia sono gestiti con l'introduzione di caratteri distintivi (di norma le lettere seguenti nel nome, in caso di ulteriore omonima si inseriscono numeri in sequenza).

Lo stesso username non potrà, neppure in tempi diversi, essere assegnato ad utilizzatori diversi.

La password è una parola segreta, conosciuta solo dall'utilizzatore che, in coppia con lo username, permette di accedere alla procedura informatizzata scelta dal dipendente. La prima password viene fornita dal SICT per consentire il primo accesso al sistema informatico aziendale, ma subito dopo deve essere modificata dall'utente. Inoltre a tutti gli utenti del dominio di sicurezza aziendale viene chiesto automaticamente ogni tre mesi il cambio della parola chiave; tuttavia, qualora si ritenga che la stessa non sia più sicura, è possibile sostituirla anche prima. La parola chiave non deve contenere riferimenti facilmente riconducibili all'utilizzatore.

La password è strettamente personale e per nessun motivo deve essere resa nota ad altri. La sua conoscenza da parte di estranei consentirebbe il trattamento dei dati in nome e per conto del titolare effettivo delle credenziali, con imputazione allo stesso di eventuale uso improprio di apparecchiature, strumenti o servizi, salvo che tale utente titolare dia prova di illecito utilizzo delle sue credenziali da parte di terzi.

A ogni utilizzatore è assegnata individualmente una credenziale di dominio (username e password), il dominio dell'Azienda USL di Modena è denominato "SIADOM". Con tali credenziali si può accedere a tutti i PC aziendali e a tutti i programmi/sistemi a cui si è stati abilitati (concessione fatta su richiesta esplicita da parte del proprio responsabile/delegato al trattamento). Esistono anche altre credenziali per l'autenticazione, vengono fornite per l'utilizzo di programmi/sistemi aziendali che non permettono l'accesso tramite le credenziali di dominio.

Le credenziali vengono disattivate nel caso di non utilizzo per oltre 6 mesi.

Le abilitazioni specifiche collegate alle proprie credenziali vengono disattivate anche in caso di perdita della qualifica o della mansione in funzione della quale l'utilizzatore era stato autorizzato ad accedere ai dati personali.

Sono esplicitamente vietate credenziali di accesso anonime o generiche, ovvero non corrispondenti a una persona fisica.

La scelta sicura della password si realizza attraverso le seguenti regole di buon senso:

- Deve essere facilmente memorizzabile in modo tale che si possa evitare di scriverla (per es. sulla postazione di lavoro o in prossimità), ma non banale e di facile individuazione (per es. con riferimenti chiari al possessore).
- La sua lunghezza deve essere di almeno otto caratteri e deve contenere almeno un numero e una lettera maiuscola.
- Non deve contenere lo username assegnato alla persona.
- Deve essere modificata al primo utilizzo e successivamente ogni tre mesi
- Deve essere modificata ogni volta che si ritenga che possa essere conosciuta, intenzionalmente o accidentalmente, da altri.
- In caso di modifica, la nuova password non può essere uguale ad una delle ultime tre password precedenti.

Il cambio password può essere eseguito agevolmente (da qualunque PC premere CTRL+ALT+CANC e scegliere "CAMBIO PASSWORD").

7.4 Sistema d'autorizzazione per le procedure informatizzate distribuite dal SICT

L'assegnazione di credenziali di autenticazione abilita l'assegnatario a una serie di "servizi informatici di base" quali a esempio:

- Accesso a una casella di posta elettronica (assegnazione d'ufficio);
- Accesso ad internet (assegnazione d'ufficio);
- Visualizzazione del Portale del dipendente (assegnazione d'ufficio);
- Accesso a una cartella di rete personale (assegnazione su richiesta);
- Accesso potenziale a gran parte degli applicativi aziendali (richiede separata autorizzazione).

Le abilitazioni all'uso dei servizi informatici di base (quelli indicati con "assegnazione d'ufficio") sono fornite al momento dell'assunzione. La maggior parte dei servizi e procedure informatiche distribuite dal SICT prevedono differenti profili di autorizzazione, definibili per ciascun utilizzatore o per classi omogenee di utilizzatori.

Per l'abilitazione all'accesso a servizi informatici e procedure non comprese nei servizi di base, la relativa autorizzazione dovrà essere richiesta dal delegato al trattamento cui afferisce l'utilizzatore.

È dovere del suddetto delegato al trattamento, che approva la richiesta, dare immediata comunicazione al SICT circa la modifica o revoca di funzioni che avevano giustificato l'accesso da parte di un proprio collaboratore a procedure/banche dati/servizi.

In ogni caso, periodicamente e comunque almeno annualmente, il delegato al trattamento deve verificare la sussistenza delle condizioni per la conservazione dei profili d'autorizzazione attribuiti ai singoli utilizzatori.

Dopo un limitato numero di tentativi d'accesso falliti, alcuni sistemi di sicurezza disattivano lo username, che sarà riattivabile solo a seguito di richiesta scritta del singolo designato al trattamento.

Nel caso di prolungata assenza o impedimento di un operatore le cui credenziali consentano in modo esclusivo l'accesso ad alcuni dati o strumenti elettronici, tale da rendere indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, l'operatore potrà individuare per iscritto un altro lavoratore (fiduciario) a cui affidare il compito di accedere in sua vece, o, alternativamente, il proprio delegato al trattamento il quale potrà richiedere per iscritto al SICT di autorizzare un altro operatore all'accesso ai dati o strumenti interessati. Tale attività dovrà essere riportata in apposito verbale dal delegato che deve informare l'operatore assente alla prima occasione utile.

8 Norme generali per l'utilizzo delle apparecchiature informatiche

L'utente deve utilizzare in modo corretto e lecito le risorse che gli sono state messe a disposizione.

Si riportano di seguito alcune tra le principali indicazioni che tutti gli utilizzatori devono rispettare: sulla Intranet è presente una pagina con le "domande frequentemente richieste" (sigla dall'inglese "FAQ") che dettagliano maggiormente procedure informatiche inerenti PC ed applicativi; inoltre si possono richiedere

informazioni maggiori (nel caso ancora permangano dubbi dopo l'approfondimento nelle FAQ) tramite l'aiuto del programma di richieste di intervento/manutenzione informatica (link HELPDESK sempre sulla Intranet aziendale).

8.1 Computer aziendali

Il personal computer aziendale in dotazione è uno strumento di lavoro. L'utilizzo personale o improprio dello stesso può comportare inefficienze, problemi di sicurezza e costi di manutenzione imprevedibili ed è pertanto non consentito, salvo casi particolari espliciti.

- Il computer deve essere usato in condizioni di sicurezza e stabilità che lo preservino da pericoli di danneggiamento.
- Possono essere utilizzati unicamente programmi/applicazioni installati o autorizzati dal SICT e per i quali siano stati regolarmente assolti gli oneri relativi alla concessione delle licenze d'uso, ove richieste. In caso di necessità di ulteriori applicazioni il dipendente dovrà farne richiesta al SICT.
- È vietato disinstallare o disattivare i software presenti sul PC, in particolare i sistemi di protezione e sicurezza aziendali (tra cui l'antivirus), e i prodotti software di inventariazione e controllo remoto. Eventuali eccezioni devono essere concordate con il SICT ed esplicitamente autorizzate.
- Il personale tecnico potrà effettuare verifiche automatizzate o puntuali sui software presenti nelle postazioni, rimuovendo o bloccando l'esecuzione dei software non autorizzati, richiedendo eventualmente giustificazioni agli utenti utilizzatori relativamente alle anomalie riscontrate.
- L'utilizzatore è personalmente responsabile del computer assegnatogli; egli ha pertanto l'obbligo, per quanto nelle sue possibilità, di impedire ad altri indebiti utilizzi dell'apparecchiatura informatica.
- In caso di assenze brevi (es. pausa mensa, riunione ecc.) durante le quali l'apparecchiatura rimane incustodita è obbligatoria l'attivazione dello screensaver (salvaschermo) protetto da password o l'impostazione della funzione automatica di standby.
- È obbligatorio segnalare tempestivamente casi di furti o incidenti relativi alla sicurezza, anche al fine di dare seguito a eventuali segnalazioni obbligatorie di data breach alla Autorità Garante per la protezione dei dati e all'interessato.
- Per finalità di sicurezza e risparmio energetico, computer e monitor devono sempre essere spenti al termine del loro utilizzo. Le apparecchiature devono essere disattivate anche nel caso di prolungate assenze dal servizio, pur nell'ambito dell'orario di lavoro.
- Nessuna periferica o dispositivo componente la stazione di lavoro può essere rimossa, salvo specifica autorizzazione.
- Al computer possono essere connesse solamente periferiche o dispositivi forniti o autorizzati dall'Azienda, da utilizzarsi esclusivamente se necessari per le attività Aziendali.

Si sottolinea che il furto o l'indebito utilizzo di un computer rilevano, oltre che sotto il profilo patrimoniale, anche in relazione a un possibile improprio utilizzo dei dati in esso contenuti e/o alla perdita degli stessi.

Il personale tecnico del SICT (o personale di ditte esterne a ciò autorizzato) potrà effettuare verifiche automatizzate o puntuali sulle periferiche presenti nelle postazioni, disabilitando o rimuovendo le periferiche non autorizzate, eventualmente chiedendo motivazioni e giustificazioni agli utilizzatori relativamente alle anomalie riscontrate.

8.2 Computer portatili aziendali

Oltre a quanto indicato nel paragrafo precedente, gli utilizzatori dei computer portatili aziendali (includendo anche tablet, mini PC ecc.) devono conservare con cura il portatile, sia durante gli spostamenti sia sul luogo di utilizzo aziendale o extra aziendale, adottando idonee precauzioni per preservarlo da furti e custodendolo in luogo sicuro in caso di allontanamento, anche temporaneo.

Il SICT provvederà a dotare i portatili di ulteriori sistemi di sicurezza (es. crittografia dei contenuti, sistemi antifurto ecc.).

8.3 Utilizzo di attrezzature informatiche personali

Le attrezzature personali di qualsiasi tipologia (PC, tablet, smartphone ecc.) non possono essere collegate alla rete aziendale, salvo diversa esplicita autorizzazione in forma scritta rilasciata dal SICT.

In alcuni casi i dispositivi personali potranno collegarsi, previa richiesta al SICT, a sottoreti appositamente predisposte nel rispetto della sicurezza della rete aziendale e pertanto destinate a funzioni limitate (es. rete EmiliaRomagnaWiFi).

8.4 Stampanti e scanner

Salvo eccezioni particolari e giustificate (es. ambulatori, guardiole, sportelli), sono installate stampanti di rete o fotocopiatrici multifunzione (con funzione stampante e scanner) in modo da consentirne l'uso condiviso tra più uffici, settori, strutture, anche al fine di un razionale utilizzo delle risorse assegnate.

Sono distribuite esclusivamente stampanti bianco/nero, generalmente laser. Nel caso si ritenga indispensabile l'acquisto di una stampante a colori, per es. per uso clinico, la richiesta dovrà essere motivata e autorizzata dal Responsabile del Servizio richiedente.

È consentita la stampa solo di documenti strettamente necessari, mentre dovrà essere sempre privilegiato l'utilizzo di documenti informatici. In caso di stampa è importante ritirarla prontamente dai vassoi delle stampanti condivise per evitare accesso indesiderato a dati personali. Si raccomanda in particolare di indirizzare verso una stampante dedicata, collocata in un'area controllata, le stampe di documenti contenenti dati di salute o giudiziari.

È buona regola, inoltre, privilegiare la stampa di documenti in fronte/retro e bianco/nero e in modalità risparmio.

In caso di necessità di stampa di documenti particolarmente lunghi o di un numero significativo di copie, si consiglia di rivolgersi al fornitore del servizio "fornitura a somministrazione di stampati" attraverso i canali e le procedure stabilite dai contratti attivati per l'Azienda (di tale contratto è titolare il Servizio Acquisti).

È vietato alterare la configurazione di rete delle stampanti condivise; per ogni necessità è necessario rivolgersi all'Help Desk secondo i canali indicati sulla Intranet Aziendale.

Si ricorda che nel caso di utilizzo di scanner deve essere rispettata la normativa sul diritto d'autore, analogamente a quanto avviene per la riproduzione di documenti attraverso fotocopiatrici.

È vietato inviare tramite stampanti di rete messaggi di posta elettronica contenenti dati di natura particolare, quali i dati di salute, anche in considerazione del mittente non identificabile (fotocopiatrici@ausl.mo.it). È opportuno pertanto, una volta effettuata la scansione del documento che si intende spedire con la posta elettronica, inviarlo previamente alla cartella di rete del servizio di appartenenza/personale ed effettuare l'invio della mail dalla propria postazione e dal proprio account di posta, scegliendo il documento da tale cartella, Il documento dovrà essere protetto da password come da relative indicazioni (v. § 12.4.1).

È altresì vietato effettuare la scansione e la relativa trasmissione di documenti aventi contenuto oltraggioso e/o discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

8.5 Supporti di memorizzazione: CD, DVD, hard disk esterni, memory card, pen drive

È vietato l'uso di periferiche e supporti rimovibili per il salvataggio e la memorizzazione di dati personali. Infatti l'eventuale perdita accidentale del supporto, il cui contenuto non sia crittografato, consentirebbe a chiunque di accedere ai medesimi dati, configurando una ipotesi di data breach da segnalare all'Autorità Garante per la protezione dei dati ed eventualmente all'interessato/agli interessati, nel caso in cui l'accesso indebito o la perdita riguardino dati personali.

Nel caso fosse strettamente necessario deve essere inviata opportuna richiesta motivata al SICT.

8.6 Norme generali per l'utilizzo del software distribuito dal SICT

L'utilizzatore autorizzato al trattamento mediante software applicativi aziendali:

- Deve utilizzare il software solo per attività aziendali.
- Deve trattare i dati personali contenuti nel software nel rispetto delle istruzioni fornite con la nomina ad autorizzato al trattamento.
- Non deve cedere il software e/o le proprie credenziali di accesso ai software a cui è abilitato a colleghi o a terzi.
- Deve utilizzare solo software aziendali assegnati e per cui sia stata concessa l'abilitazione.

Inoltre si ribadisce che:

- È vietata qualsiasi riproduzione (permanente, temporanea, parziale o totale), traduzione, distribuzione di software di terzi, che non sia autorizzata in base alla licenza a esso applicabile.
- Salvo specifiche autorizzazioni, non è consentito l'uso in azienda di software acquisito privatamente o disponibile gratuitamente, né l'uso all'esterno dell'azienda di software aziendale.
- È vietato all'utente che disponga dei diritti per farlo, alterare le impostazioni del sistema operativo o degli applicativi in senso contrario ai criteri minimi di sicurezza (in particolare a quanto indicato dalle circolari agid del 2017 es. Attivazione dell'esecuzione automatica di macro nei file di office, visualizzazione automatica del contenuto dei file ecc.).

8.7 Software antivirus e di protezione dei dati

Il SICT, mediante l'utilizzo di firewall e prodotti antivirus gestiti e aggiornati centralmente, assicura la protezione dell'infrastruttura, dei sistemi informatici e delle postazioni di cui effettua la manutenzione.

L'aggiornamento dell'antivirus avviene giornalmente, quello delle patch critiche e di sicurezza di Windows avviene mensilmente, previa verifica in ambienti di test.

È vietato il collegamento alla rete aziendale di qualsiasi personal computer non adeguatamente protetto mediante software antivirus (aggiornamento almeno settimanale) e patch di sicurezza del sistema operativo (aggiornamento almeno mensile).

In applicazione delle indicazioni AgID, i sistemi aziendali saranno gradualmente impostati in modo tale che sia impedita la visualizzazione automatica del contenuto (per es. di una mail), in particolare dei file allegati (per es. la visualizzazione di un pdf in una mail); così come continua a essere inibita l'esecuzione automatica da qualsiasi supporto (chiavette USB, CD, DVD ecc.).

8.8 Dischi di rete, cartelle personali e cartelle condivise

L'Azienda mette a disposizione degli utilizzatori che ne facciano richiesta spazio su dischi di rete (cartelle che possono essere personali o condivise tra più utilizzatori) per l'archiviazione di informazioni di carattere professionale. Non possono essere collocati sulle unità di rete - nemmeno per periodi brevi - file personali o comunque aventi contenuto diverso da quello strettamente connesso all'attività lavorativa. Le cartelle di rete possono essere protette da password. L'accesso a cartelle di rete può essere concesso anche solo per la visualizzazione dei contenuti e non per la modifica.

La richiesta di concessione di spazio su disco di rete va fatta tramite form di richiesta e in caso di quota elevata possono essere richieste ulteriori dettagli e/o autorizzazione del proprio responsabile.

Il servizio SICT svolge periodici controlli a campione sulle unità di rete e può procedere autonomamente alla rimozione di dati non connessi alle attività proprie dell'Azienda.

Il SICT provvede al backup dei dati collocati su unità di rete (completo mensile con retention di un anno, incrementale giornaliero con retention di 30 giorni). Nel caso di perdita di dati in rete, pertanto, sarà possibile richiedere il recupero del file così come salvato nell'ultima versione di backup. Per questi motivi è obbligatorio l'utilizzo delle unità di rete per il salvataggio di dati/file di particolare importanza e rilevanza.

Le unità di rete devono essere mantenute con diligenza a cura degli utilizzatori mediante la periodica – almeno semestrale – revisione dei dati salvati e l'eliminazione di quelli obsoleti o, comunque, non più utilizzati o necessari. È opportuno evitare la duplicazione di dati onde consentire uno sfruttamento razionale delle unità di rete.

È possibile che, per ragioni di razionalizzazione delle risorse, il SICT introduca la limitazione degli spazi concessi a ciascun utilizzatore o gruppi di utilizzatori in quote (es 1GB, 5 GB, 10 GB) secondo la reale necessità di utilizzo delle risorse condivise.

I server aziendali centralizzati sono le uniche entità predisposte alla condivisione di risorse. È vietato condividere localmente (sul proprio PC) e direttamente dischi, cartelle o risorse ad eccezione delle stampanti comuni.

Per ogni cartella condivisa è individuato un referente, avente la responsabilità di definire l'elenco degli utilizzatori e dei profili di abilitazione, nonché di verificare il corretto utilizzo della cartella da parte degli utilizzatori stessi.

Al referente spetta verificare periodicamente e comunque almeno annualmente, le abilitazioni assegnate agli utilizzatori, segnalando tempestivamente al SICT la necessità di assegnare, modificare o cancellare l'accesso alla cartella da parte degli utilizzatori.

Lo spazio assegnato può essere concordato di volta in volta secondo le reali necessità.

9 Collegamento di attrezzature alla rete dati

La rete dati aziendale su cavo o wireless (wi-fi) è gestita dal SICT.

L'accesso di computer o altre attrezzature alla rete aziendale deve essere autorizzato dal SICT, che definisce la connettività da assegnare in base alle caratteristiche dell'attrezzatura e alle esigenze dell'utilizzatore.

9.1 Rete AUSL

La rete interna permette l'accesso a tutti i principali applicativi aziendali e pertanto è destinata all'uso da parte dell'utente aziendale esclusivamente mediante dispositivi dell'Azienda.

Il collegamento alla rete di attrezzature informatiche personali, se ammesso, è regolato mediante accesso a sottoreti predisposte ad-hoc (per es. la rete pubblica regionale EmiliaRomagnaWiFi per l'eccesso a internet).

Pertanto sono vietati:

- Il collegamento alla rete aziendale di computer e server se non forniti o autorizzati dal SICT.
- Il collegamento alla rete aziendale di personal computer non adeguatamente protetti mediante software antivirus (aggiornamento almeno settimanale) e patch di sicurezza del sistema operativo (aggiornamento almeno mensile).
- Il collegamento alla rete, non autorizzato dal SICT, di apparati di rete quali switch, router (anche USB o wifi) e attrezzature per reti wireless (es. access point).
- Qualsivoglia forma di collegamento ad altre reti laddove la stazione di lavoro sia connessa alla rete dell'Azienda. Sono pertanto vietate, per le stazioni di lavoro connesse alla rete aziendale, le connessioni tramite modem o chiavette Internet e l'utilizzo di una doppia scheda di rete; per i PC portatili dotati sia di scheda di rete tradizionale che di scheda di rete wireless, entrambe le schede possono essere abilitate al collegamento alla rete aziendale purché non vengano utilizzate contemporaneamente.

Le regole valgono anche per le attrezzature collegate o ospitanti strumentazioni medicali e analitiche.

9.2 Altre reti wi-fi in Azienda

Oltre alla rete dati aziendale, sia cablata che wi-fi, è disponibile anche la rete pubblica regionale EmiliaRomagnaWiFi, accessibili da parte di chiunque senza credenziali e veicolata sull'infrastruttura aziendale.

10 Uso e salvataggio dei dati aziendali

Il SICT provvede al salvataggio dei dati registrati tramite i sistemi informativi aziendali centralizzati.

La politica di backup (creazione di copie di sicurezza), che definisce la frequenza di salvataggio e il tempo di tenuta dei backup, viene adottata dal SICT in linea con indicazioni normative, raccomandazioni e best practice.

Al fine di salvaguardare tutti i documenti aziendali ritenuti di interesse e utilità per l'Azienda (es. documenti doc, xls, pdf ecc.) gli stessi dovranno essere salvati su dischi di rete e server gestiti dal SICT (v. § 8.8) in quanto il salvataggio sul PC non garantisce adeguati livelli di sicurezza.

11 Utilizzo della posta elettronica

11.1 Definizioni e strumenti

11.1.1 Casella di Posta e account

Spazio dedicato ad accogliere i messaggi di posta in transito tra un qualsiasi inviante e il ricevente proprietario della casella stessa. Si definisce "account" di posta l'identificativo dell'utente necessario per essere riconosciuto come utente unico dal servizio di posta elettronica. A ogni account è associata una parola chiave (password) nota soltanto all'utente.

La password e l'account associati costituiscono la credenziale di autenticazione con la quale l'utilizzatore può accedere alla propria casella di posta.

Le caselle di posta si intendono sempre di tipo personale, ovvero l'indirizzo della casella è associato ad una persona precisa (nel formato indicato sotto): non si possono creare caselle di posta impersonali, il cui indirizzo non sia associato in maniera diretta ad una persona specifica. Se si rileva la necessità per motivi specifici e particolari di una casella di posta impersonale (denominata anche casella di gruppo) se ne può fare richiesta al SICT che valuterà il caso ed eventualmente proporrà soluzioni alternative.

11.1.2 Casella di Posta PEC

La posta elettronica certificata o PEC è un tipo particolare di posta elettronica che consente di attribuire a un messaggio di posta elettronica lo stesso valore legale di una tradizionale raccomandata con avviso di ricevimento, garantendone la prova dell'invio e della consegna. Ogni ente pubblico è dotato di una casella PEC istituzionale, chiamata PEI. Essa è inserita in un elenco pubblico (chiamato IPA – Indice delle Pubbliche Amministrazioni, gestito da AgID) e può essere utilizzata da un qualsiasi soggetto, pubblico o privato, che intenda inviare una comunicazione informatica valida agli effetti di legge all'ente intestatario della casella.

Per l'Azienda USL di Modena il dominio è pec.ausl.mo.it, l'indirizzo della PEI è auslmo@pec.ausl.mo.it. Questa casella è sempre presidiata e integrata con il sistema di protocollo aziendale.

Sono inoltre state attivate caselle PEC per vari Servizi Aziendali, il cui elenco aggiornato è sempre riportato nell'IPA.

11.1.3 Casella di Posta individuale

Casella di posta elettronica associata a ciascun dipendente o collaboratore fornita d'ufficio o in seguito a sua richiesta (mediante compilazione di apposita modulistica online). L'utilizzo della casella di posta elettronica costituisce un diritto e un dovere per ogni dipendente, pertanto essa gli viene assegnata d'ufficio, salvo esplicita richiesta contraria e motivata da parte del suo Responsabile.

La mail aziendale può essere fornita anche a soggetti non dipendenti, ma con altri rapporti di collaborazione con l'Azienda, mediante apposita modulistica o su sistema informatizzato. In ogni caso è sempre possibile effettuare la richiesta di account.

L'intestatario della casella è responsabile della lettura e dell'invio dei messaggi, ed è responsabile della custodia e dell'aggiornamento della password di accesso esclusiva.

La casella di posta ordinaria è genericamente nel formato "n.cognome@ausl.mo.it" mentre il tipico account di dominio SIADOM è nella forma "cognomen". I casi di omonimia sono gestiti con l'introduzione di caratteri distintivi o altre modalità secondo i casi.

Per i soggetti esterni legati da relazioni commerciali (es. i fornitori di servizi) si utilizza un suffisso identificativo "-ext", in modo tale da rendere sempre nota la circostanza. L'indirizzo di posta apparirà nella forma n.cognome-ext@ausl.mo.it[3] .

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 vietato inviare materiali che non siano compatibili con tali caratteristiche del servizio, come indicato più avanti nel documento.

11.1.4 Mailing-List

La mailing-list è un account fittizio che maschera, con un contenuto semantico più appropriato, uno o più account e-mail diversi. Per es. alla mailing-list "msg-sia@ausl.mo.it" corrisponde l'elenco delle mail di tutti i componenti del Servizio ICT Aziendale. Se ne intuisce immediatamente, pertanto, l'estrema utilità e praticità nel lavoro quotidiano.

Tuttavia per evitare il proliferare di mailing-list senza regole e per non appesantire il sistema, esse sono sottoposte ai seguenti vincoli:

- Una mailing-list è rilasciata previa formale richiesta inviata al SICT utilizzando l'apposita modulistica o il sistema di richieste online dei servizi informatici.
- Ogni mailing-list deve avere un referente che ne è responsabile, che va definito al momento della richiesta stessa, e che potrà richiedere le modifiche (aggiunte di nuovi account mail nella mailing-list, rimozione di account mail ecc.).
- Una mailing-list non può riferirsi a gruppi con più di 30 elementi.
- Non possono appartenere a una mailing-list account di soggetti esterni all'Azienda. Fanno eccezione i casi in cui tale circostanza sia desumibile dal nome della mailing-list (es. da una mailing-list denominata "assistenza.xxx" si può desumere che esso possa contenere l'indirizzo di qualche tecnico del fornitore xxx, quindi esterno all'azienda); sono ammesse inoltre eccezioni in casi particolari che devono essere autorizzati dal SICT.
- Le mailing-list devono essere funzionali all'organizzazione aziendale: possono essere utilizzate per non fornire all'esterno riferimenti personali in ricezione (es: referente.urp invece del nome esplicito delle persone), per creare liste di distribuzione, per semplificare le operazioni di invio e ricezione di messaggi ecc.
- Una mailing-list può essere configurata in 3 modalità (da specificare nel momento della richiesta stessa):
    - Aperta: tutti possono inviare mail alla mailing-list.
    - Chiusa: solo gli account mail contenuti nella mailing-list possono inviare mail alla mailing-list stessa; chi non ne fa parte, non potrà inviare mail.
    - Con Moderatori: solo alcuni account mail (interni o esterni alla mailing-list stessa) - definiti come "moderatori" – potranno inviare mail alla mailing-list; solitamente non si impostano più di 3 moderatori.

La mailing-list va gestita con particolare attenzione soprattutto nel caso di invio di informazioni riservate. Occorre infatti essere sempre consapevoli dei reali destinatari contenuti nella mailing-list, tenendo conto peraltro che la composizione della stessa può cambiare nel tempo a insaputa del mittente.

11.1.5 Webmail e altri programmi client di posta

L'accesso a una casella di posta aziendale e alla corrispondente gestione delle proprie e-mail (ricezione, invio, modifica, inoltro ecc.) può avvenire attraverso l'uso di differenti strumenti:

[3] Salvo eccezioni presenti per ragioni storiche che saranno nel tempo eliminate

Webmail:
Sistema che consente la gestione della casella di posta agendo direttamente sui dati conservati sul server di posta, senza che questi debbano essere trasferiti sul proprio PC. Il vantaggio principale del suo utilizzo è quello di poter accedere da qualsiasi punto interno o esterno all'Azienda alla propria casella di posta. Inoltre, con l'utilizzo della Webmail il problema dell'integrità dei dati è a carico del gestore del sistema. Il sistema Webmail in uso ha tutte le gestioni di base delle e-mail (invio, ricezione, modifica, eliminazione, archiviazione ecc.); permette anche la gestione di alcune impostazioni utili come il risponditore automatico (ad es. in caso di assenza) e la gestione della password della propria casella di posta elettronica aziendale.

Client di posta elettronica: Mozilla Thunderbird e Microsoft Outlook
Programmi di gestione della casella di posta elettronica. Il programma Thunderbird è quello installato ed utilizzato come standard (perché gratuito e non necessita di una licenza a pagamento). Il programma Outlook viene fornito con licenza a pagamento (pertanto deve esserne fatta richiesta motivata e validata dal proprio direttore di servizio, deve essere acquistato il pacchetto Microsoft Office). Entrambi i programmi sono configurati in modo da consentire l'accesso diretto al mail server e alle mail ivi contenute (con una gestione compatibile con la WebMail).

Per ragioni di efficienza nell'assistenza e nella manutenzione dei sistemi informatici l'utilizzo di programmi diversi da Webmail, Mozilla Thunderbird o da Microsoft Outlook è vietato.

In caso di sostituzione di PC i dati di posta conservati sul medesimo per effetto dell'utilizzo di programmi inadeguati dopo la data di entrata in vigore di questo documento non saranno trasferiti sul PC di nuova fornitura.

11.2 Utilizzo della posta elettronica aziendale

La casella di posta aziendale è uno strumento di lavoro che ha lo scopo di inviare/ricevere comunicazioni direttamente attinenti alla propria attività lavorativa e/o informazioni riguardanti l'Azienda.

Per tale motivo non è ammesso l'utilizzo di caselle di posta private (es: @virgilio.it, @libero.it, fastwebnet.it ecc.) per svolgere l'attività lavorativa.

L'accesso alle caselle mail non aziendali è ammesso esclusivamente in modalità webmail, con utilizzo del browser[4] aziendale. Non è consentito configurare un client di posta elettronica con una casella mail non aziendale.

Analogamente, non è consentito l'utilizzo della posta elettronica aziendale per svolgere attività che non rientrino tra i compiti istituzionali.

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.

Ciascun titolare di casella e-mail è direttamente responsabile del corretto utilizzo della stessa.

11.3 Attribuzione della casella PEC

La casella PEC può essere integrata nell'applicativo di gestione documentale assegnata per l'utilizzo nel sistema di protocollo aziendale o utilizzata per la corrispondenza che richieda particolari garanzie in merito all'invio e alla consegna[5] .

La PEC viene attribuita esclusivamente alla struttura di afferenza.

Non vengono assegnate caselle PEC nominative ai professionisti.

La richiesta di attivazione di una nuova casella PEC va presentata con motivazione al Servizio Affari Generali (in capo al quale è affidata la responsabilità della Gestione Documentale all'interno dell'Azienda) e che ne valuta la opportunità.

[4] Programma di navigazione: Internet Explorer, Chrome, Firefox, Edge
[5] Codice dell'Amministrazione Digitale, Art. 48

11.4 Tutela della riservatezza

Come per tutte le informazioni attinenti all'attività lavorativa è assolutamente vietata la diffusione, anche a mezzo posta elettronica, di informazioni e dati ricavati/elaborati da procedure/banche dati aziendali.

Inoltre, la comunicazione non autorizzata e la diffusione di dati personali costituiscono una grave violazione della normativa in materia di protezione dei dati personali, pertanto l'invio di messaggi di posta contenenti dati di natura particolare, come i dati di salute, è vietato. In caso di reale, estrema necessità devono essere adottate le misure di sicurezza e gli accorgimenti di seguito indicati.

11.4.1 Invio di documentazione sanitaria con posta elettronica PEC e ordinaria

Entrambe le modalità prevedono il rilascio di apposita informativa sulla sicurezza dei sistemi utilizzati e l'acquisizione del consenso dell'interessato, eventualmente utilizzando l'apposita modulistica.

- PEC: nel caso in cui l'interessato richieda l'invio di propria documentazione sanitaria mediante trasmissione alla propria casella PEC, tale documentazione potrà essere inviata dalla PEC aziendale alla PEC indicata dall'interessato, purché la documentazione costituisca un allegato alla mail e non un testo compreso nel corpo del messaggio.
- Posta elettronica ordinaria: nel caso in cui l'interessato richieda l'invio di propria documentazione sanitaria mediante trasmissione alla propria casella di posta elettronica, si potrà procedere purché la documentazione da trasmettere costituisca un allegato alla mail e non un testo compreso nel corpo del messaggio e sia protetta con una password attraverso crittografia del file (es. referto specialistico in formato pdf protetto). La password deve essere comunicata all'interessato con diverso mezzo (ad es. telefonicamente o verbalmente all'atto della richiesta).
- L'invio di referti ad altre Aziende e Strutture Sanitarie è da effettuarsi mediante PEC di struttura e con invio da PEC a PEC. In caso di necessità di utilizzare una mail tradizionale occorre applicare gli accorgimenti di cifratura descritti al punto precedente.

Nel caso in cui il paziente risieda in regione Emilia Romagna, questi va invitato ad attivare il Fascicolo Sanitario Elettronico per mezzo del quale potrà ricevere tutta la documentazione sanitaria che lo riguarda.

11.5 Regole di buon comportamento per l'utilizzo delle caselle e-mail

L'utilizzo della posta elettronica è un dovere oltre che un diritto dell'utilizzatore. Di seguito alcune indicazioni e regole cui l'utilizzatore deve attenersi nell'utilizzo dei sistemi di comunicazione.

- Controllare la posta ogni giorno, eventualmente scaricandola sul proprio pc o cancellandola dalla propria casella se non è necessario conservarla, prestando particolare attenzione alla rimozione degli allegati "pesanti". In ogni caso la conservazione dei soli messaggi di interesse semplifica la consultazione e rende più efficienti le ricerche dei messaggi. È, in ogni caso, consigliata l'articolazione delle cartelle di posta elettronica in sottocartelle, in modo da ottimizzarne il funzionamento.
- Controllare periodicamente la correttezza degli indirizzi a cui si scrive, soprattutto se in modo aggregato e automatico;
- Valutare con la massima attenzione e con razionalità il contenuto dei messaggi evitando di cadere in truffe o altri abusi: nonostante i sistemi di controllo centrali permettano di bloccare la maggior parte dei messaggi potenzialmente pericolosi, alcuni messaggi oggetto di spam[6] o phishing[7] o contenenti virus possono eludere tali sistemi, pertanto l'attenzione di chi li riceve è sempre indispensabile al fine

[6] Termine di origine goliardica che definisce un insieme messaggio inviato senza il loro permesso a una molteplicità di destinatari, comportamento considerato inaccettabile e ai limiti del fraudolento, anche perché l'elenco dei destinatari è spesso ricavato con metodi ai limiti della legalità. Lo scopo è in genere pubblicitario, ma spesso il messaggio spam può essere veicolo di informazioni denigratorie o offensive, a carattere politico, sessista o razziale. Inoltre il proliferare dello spam ha un effetto deleterio soprattutto a causa dei costi, diretti o indiretti, del traffico generato dall'invio indiscriminato.

[7] Attività illegale che consiste in un tipo di truffa mediante la quale il criminale cerca di ingannare la vittima, per es. imitando un'entità, un aspetto e un contenuto affidabili o abituali per la vittima, convincendola così a fornire informazioni personali, dati finanziari o codici di accesso segreti di cui poi farà un utilizzo illegale

di evitare spiacevoli o pericolose conseguenze quali diffusione di informazioni personali o sensibili o persino blocchi del sistema e perdita di dati

- Il personale del SICT e gli operatori del servizio di Help Desk non chiederanno mai a un utente di inserire la propria password in un modulo raggiungibile da un collegamento via mail, pertanto quando viene rivolta questa richiesta si tratta sempre di tentativi di truffa criminosi perpetrati al fine di carpire le credenziali dell'utente. Si ricorda che è piena responsabilità del titolare della casella qualunque conseguenza derivi dalla comunicazione a terzi, anche se accidentale e involontaria, dei propri dati.
- Evitare di includere nei messaggi allegati di dimensioni spropositate che hanno l'effetto di rallentare l'intero sistema e che spesso rischiano di essere rifiutati dal ricevente che a sua volta può essere vincolato a regole sulla dimensione massima ricevibile (il limite in Azienda è di 30MB – come da standard più diffuso anche tra i sistemi di posta elettronica privati/esterni). Solo se strettamente necessario allegare file di dimensione complessiva maggiore di 2MB (nel caso di più files allegati si controlli la somma delle dimensioni dei singoli files), ricorrere a compressione dei files oppure preferire i files di tipo PDF o JPEG (file più compressi per la loro tipologia).
- Scrivere messaggi sintetici che esplicitino subito il problema e che siano identificati da un oggetto chiaro;
- Firmare sempre in modo esteso i propri messaggi con l'indicazione dei dati necessari per l'identificazione e la reperibilità. Questo processo può essere automatizzato impostando opportune opzioni nel programma di posta.
- Inviare messaggi a una pluralità di destinatari solo se strettamente necessario. Tali invii, infatti, appesantiscono molto il server di posta, pertanto essi sono limitati a un invio massimo di 50 indirizzi mail, ridotto a 30 se si utilizza la webmail aziendale (si possono "superare" questi limiti tramite mailing-list o newsletter create per eventi e necessità specifiche). Sono da evitare in particolare i messaggi frivoli o inutili, specialmente se inviati a molti destinatari.
- Sono da evitare, anche se considerati socialmente simpatici e graditi, i messaggi augurali in occasione di festività o eventi particolari. L'invio multiplo di tali messaggi, infatti, soprattutto se associato a un utilizzo spropositato della funzione "rispondi a tutti" dà luogo a catene di invii che rapidamente possono paralizzare l'intero sistema di posta.
- Oltre che per la ragione esposta al punto precedente, per problemi di riservatezza, si deve sempre utilizzare con molta cautela l'opzione "rispondi a tutti". Non sempre, infatti, è opportuno che tutti i destinatari del messaggio cui si risponde abbiano visibilità della risposta. Spesso si commettono grossi errori inviando dati e informazioni riservate a destinatari inaspettati e inappropriati, solo perché questi sono presenti in un lungo elenco di destinatari precedenti al quale non si fa caso. Inoltre spesso gran parte dei destinatari di una "risposta a tutti" non è realmente interessato e coinvolto nel contenuto della risposta che al contrario si rivela spesso inutile e fastidiosa.
- Utilizzare con altrettanta cautela l'opzione di "inoltro", controllando attentamente tutta l'eventuale catena di mail che si va ad inoltrare;
- L'inoltro automatico delle mail a una diversa casella non è consentito salvo specifica autorizzazione per necessità particolari, in seguito a richiesta formale motivata. Sono comunque e sempre vietati gli inoltri automatici delle mail a caselle di posta elettronica privati e non aziendali.
- In caso di assenza prolungata impostare il sistema in modo che sia restituito al mittente un messaggio appropriato nel quale lo si avvisi dell'impossibilità di una risposta immediata (v.§ 11.8).

11.6 Considerazioni sull'attendibilità dell'identità del mittente di posta elettronica

Si deve sempre tener presente che, date le caratteristiche intrinseche dei sistemi di posta elettronica, è tecnicamente impossibile garantire l'identità e la veridicità del mittente. Esso, infatti, può essere falsificato agevolmente grazie a accorgimenti tecnici di modesta complessità che non richiedono particolari conoscenze informatiche. Lo stesso vale per loghi e altri elementi distintivi presenti all'interno dei messaggi che possono essere copiati e falsificati senza difficoltà.

11.7 Responsabilità in merito all'utilizzo della posta elettronica

Si ribadisce che ciascun titolare di casella e-mail è direttamente e totalmente responsabile del corretto utilizzo della stessa, in particolare delle conseguenze che possano derivare alla Azienda dalla comunicazione a terzi, delle proprie credenziali, tra cui l'accesso da parte di terzi ai dati contenuti nella posta, oltre che effetti dannosi sull'intero sistema di posta aziendale, fino al blocco dello stesso. Sulla base della gravità del danno provocato, l'Azienda valuterà pertanto le possibili misure disciplinari a carico dei dipendenti interessati.

11.8 Sistemi di sicurezza

Come tutti i sistemi di gestione della posta elettronica il sistema dell'Azienda USL di Modena è aperto alla ricezione di messaggi provenienti dall'esterno e quindi è anche esposto agli abusi che ne possono derivare. I più frequenti si possono classificare a grandi linee in:

- Virus informatici e programmi dannosi in generale, che si propagano tramite posta elettronica e danneggiano o compromettono per varie vie i sistemi informatici.
- Posta pubblicitaria o indesiderata (spam).
- Tentativi di truffa e raggiri di varia natura: finte proposte di transazioni economiche, messaggi contraffatti apparentemente provenienti da banche o altre istituzioni con indirizzi di siti contraffatti, proposte di lavoro ingannevoli, finte proteste e diffide, pubblicità di siti ingannevoli (tipicamente orientate al furto dei numeri di carta di credito, conto corrente, carte prepagate) ecc.

Questi abusi provocano in genere perdita di tempo e spreco di risorse, ma nei casi più gravi possono provocare danni anche rilevanti. Il fenomeno si verifica anche con i fax e la posta tradizionale, ma i bassissimi costi associati all'invio di messaggi di posta amplificano le dimensioni del problema.

A salvaguardia dell'integrità del sistema e a tutela degli utilizzatori sono attivi i seguenti sistemi di sicurezza:

- Filtri antivirus per la protezione della posta elettronica.
  Blocco alla ricezione/trasmissione e-mail di tutti gli allegati di tipo eseguibile o di altri tipi potenzialmente dannosi.
- Sistemi di content inspection che bloccano i messaggi analizzandone il contenuto.
- Sistemi di blocco da black list che bloccano i messaggi in quanto provenienti da mittenti noti come non attendibili o pericolosi.
- Blocco di auto-esecuzione da supporti di memoria esterni.
- Blocchi della navigazione verso siti malevoli o con contenuti potenzialmente pericolosi.
- Filtri anti-spam e di navigazione dinamici ed aggiornati costantemente.

Come già ribadito, non essendo tali sistemi in grado di bloccare ogni tipo di attacco, è richiesta la massima attenzione da parte degli utilizzatori dei sistemi aziendali: in caso di dubbi circa la presenza di virus in allegati a messaggi di posta elettronica, o in link presenti nel messaggio, il destinatario è invitato a non aprirli, o a non cliccare sui link. Se necessario, contattare sempre il SICT.

11.9 Gestione della casella di posta elettronica in caso di assenza dell'utilizzatore

In caso di assenza programmata (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella), si raccomanda all'utilizzatore di attivare l'opzione di invio automatico di un messaggio di risposta contenente l'indicazione di un altro indirizzo di posta elettronica aziendale a cui fare riferimento indicando eventualmente altre utili modalità di contatto della struttura.

In caso di assenza non programmata (ad esempio, per malattia), la procedura di risposta automatica - qualora non sia attivata dall'utilizzatore, anche avvalendosi del servizio webmail - potrà essere attivata dal SICT su richiesta dell'utilizzatore stesso (per es. via mail).

In caso di assenza improvvisa o prolungata, di impedimento dell'utilizzatore di attivare la funzionalità di cui sopra ovvero in caso di improrogabili necessità legate all'attività lavorativa, l'utilizzatore ha facoltà di delegare un altro utente (fiduciario) ai fini dell'inoltro e della verifica del contenuto dei messaggi e della trasmissione al Responsabile della struttura di appartenenza dell'utilizzatore assente, di quei messaggi ritenuti rilevanti per lo svolgimento dell'attività, fermi restando la riservatezza e l'utilizzo strettamente

personale delle credenziali di ciascuno. La delega di cui al periodo che precede dovrà essere esercitata per iscritto, senza particolari formalità, anche via e-mail. Il Responsabile di riferimento del delegante deve essere immediatamente avvisato dell'esistenza della delega.

In ogni caso, al fine di evitare il proliferare di inutile traffico di mail (soprattutto nei periodi contraddistinti da maggiori assenze per ferie), l'utilizzo del servizio di risposta automatica deve avvenire nel rispetto di alcune semplici regole (da impostare nella webmail):

- Apporre il flag nella casella "Rispondi una volta sola" in modo che chi invia una mail all'utente assente non riceva inutilmente la risposta automatica ad ogni mail inviata a tale destinatario;
- Inserire nella casella "Non rispondere automaticamente ai seguenti indirizzi" gli indirizzi di mailing list di cui l'utilizzatore faccia parte, gli indirizzi mail invianti informazioni (newsletter, alert tecnici, etc…) e, in generale, tutti gli indirizzi di posta ai quali non si vuole venga inviata la risposta automatica;
- Disabilitare la risposta automatica appena si rientri al lavoro.

11.10 Gestione della casella di posta elettronica al momento della cessazione del rapporto di lavoro

L'Azienda, contestualmente alla cessazione del rapporto di lavoro o delle condizioni che hanno comportato l'assegnazione di una casella di posta elettronica, è tenuta, nel rispetto di quanto definito dalla normativa vigente in materia di trattamento dei dati personali, a disattivare immediatamente la casella di posta dell'utilizzatore interessato. I relativi messaggi di posta elettronica presenti su mail server vengono temporaneamente conservati (per 90 giorni) e successivamente eliminati definitivamente.

Si specifica che l'account del dipendente cessato non viene cancellato, ma vengono inibiti in via definitiva sia la ricezione di messaggi in entrata, sia l'invio di messaggi in uscita da tale account; ciò al fine di evitare il rischio di associarlo ad un nuovo dipendente omonimo di quello cessato.

La definizione di un diverso termine di conservazione dei messaggi presenti nella casella di posta del dipendente cessato deve risultare indispensabile ed essere supportata da valide motivazioni. In tal caso la richiesta deve essere autorizzata dal Direttore di Servizio e rivolta al SICT che definirà le relative configurazioni da applicare. Deve essere comunque rispettato il principio di non eccedenza nella definizione del termine di differimento.

Laddove ritenuto utile potranno essere preventivamente adottati, su richiesta dell'utente, sistemi automatici volti a informare i terzi e a fornire a questi ultimi indirizzi alternativi riferiti esclusivamente all'attività lavorativa (es. risposta automatica che indichi a chi rivolgersi dal giorno GG/MM/AA ecc.).
È vietato il reindirizzamento automatico delle e-mail del dipendente cessato.
Non è ammesso prelevare massivamente il contenuto della casella, né conservarlo dopo la cessazione del rapporto di lavoro o delle condizioni che hanno portato al rilascio della casella di posta. I dati contenuti, infatti, sono inerenti all'attività lavorativa o di collaborazione e sono considerati riservati e di proprietà dell'Azienda USL di Modena e non dell'intestatario della casella.

11.11 Accesso alla casella di posta elettronica per ragioni di sicurezza o manutenzione

Quando motivi di sicurezza o di manutenzione lo richiedono, l'amministratore di sistema specificamente autorizzato dall'Azienda, previo avviso agli utenti interessati e anche in assenza di questi se impossibilitati, può accedere alla configurazione delle caselle di posta elettronica per le sole finalità di sicurezza e manutenzione e per esclusive finalità tecniche.

L'accesso alla configurazione di posta non comporta la visualizzazione dei messaggi della casella, salvo il caso eccezionale in cui il problema di sicurezza o di manutenzione non possa essere diversamente risolto. In quest'ultimo caso, l'avviso all'utilizzatore interessato viene rinnovato prima dell'accesso ai messaggi contenuti nella casella, fermo restando che l'accesso dell'amministratore di sistema avverrà esclusivamente per motivi di sicurezza o manutenzione come sopra precisato.

L'attività effettivamente eseguita sulle configurazioni (o sui messaggi di posta, nel caso eccezionale di cui al periodo che precede), viene sempre comunicata all'utente interessato al termine dell'intervento.

12 Utilizzo della rete Internet

12.1 Definizioni e strumenti

12.1.1 Accesso a un sito Internet

A ogni punto della rete Internet visibile pubblicamente è associato un numero identificativo (denominato indirizzo IP pubblico) che può anche essere utilizzato direttamente per l'accesso: per es. il sito Internet della Azienda ha l'indirizzo IP pubblico 34.252.77.35. Tuttavia, per semplificare molto la gestione, l'indirizzo IP è trasformato dal sistema Internet in un testo comprensibile che identifica in modo esplicativo il punto della rete richiesto - indirizzo del sito internet: per es. il sito Internet della Azienda ha l'indirizzo www.ausl.mo.it. - Digitando questo testo nel programma di accesso si raggiunge direttamente il sito desiderato.

L'intero indirizzo comprensivo delle indicazioni relative al protocollo e alla pagina desiderata è denominato URL (Universal Resource Locator: per esempio la pagina di presentazione della Azienda ha URL: http://www.ausl.mo.it/home). Infine anche l'URL, che può essere costituito da un testo molto lungo o complicato, può essere a sua volta mascherato da un elemento grafico o testuale di una pagina (denominato link) cliccando il quale si attiva la connessione corretta.

In genere il punto cui si accede costituisce un "sito Internet" quando è organizzato in un insieme di contenuti (pagine), collegati tra loro secondo una precisa gerarchia (ipertesto), mediante l'utilizzo di appositi strumenti informatici. Tali contenuti si possono consultare agevolmente utilizzando esclusivamente il mouse. Il termine "navigazione" (in Internet) nasce appunto da questa modalità di consultazione che consente di spostarsi da un argomento all'altro e da un punto all'altro della rete con grande semplicità e velocità.

12.1.2 Connessione a Intranet

L'Intranet è il sito interno aziendale che è costituito dal complesso sistema di informazioni e di servizi di utilità generale accessibili solo dalla rete interna. Tale sito può essere reso disponibile anche all'esterno della rete aziendale, in questo caso si parla di Extranet.

Tutti i dipendenti e collaboratori aziendali hanno accesso alla rete intranet e sono invitati a prendere sempre visione dei suoi contenuti informativi.

12.2 Abilitazione alla connessione internet

La navigazione in Internet viene abilitata per tutte le postazioni e gli utenti che facciano parte del dominio aziendale SIADOM.

Salvo diversa indicazione da parte del Responsabile, ogni dipendente, mediante le proprie credenziali istituzionali, può navigare in Internet da qualsiasi stazione di lavoro purché abilitata.

Per motivi di sicurezza, stazioni di lavoro particolarmente critiche per il tipo di attività effettuato o per il tipo di dati gestiti non vengono abilitate alla navigazione in Internet: tale scelta può essere fatta dal Responsabile della unità operativa di appartenenza o dal servizio gestore dell'attrezzatura (SICT o SUIC).

12.3 Utilizzo delle connessioni a internet

L'Azienda consente di connettersi a Internet per fini istituzionali, con lo scopo di approfondire le proprie conoscenze, documentarsi, accrescere la propria professionalità. Le postazioni abilitate alla navigazione in Internet costituiscono uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

L'utilizzo di Internet per svolgere attività per esigenze personali, che dunque non rientrino tra i compiti istituzionali può essere consentito, nei limiti del carattere di eccezionalità e saltuarietà.

Sono invece sempre vietati:

- La connessione a siti a carattere ludico e di intrattenimento
  La definizione va intesa in senso lato e include tutti i siti inerenti anche in senso generico all'intrattenimento o all'organizzazione del tempo libero (giochi on-line, case discografiche, agenzie

di viaggi, proposte di vacanze, strutture di accoglienza alberghiera, agenzie e compagnie aeree, sistemi di trasporto, ristoranti ecc.). Rientrano in questa esclusione anche i siti commerciali cui si acceda per uso personale (per es. concessionari o case automobilistiche, centri commerciali, fabbricanti e distributori di prodotti di consumo o servizi ecc.). Vi rientrano, infine, anche le testate giornalistiche on-line, nonché i siti di associazioni e i siti a carattere religioso o politico.

- La connessione a siti a carattere erotico e pornografico
  La definizione va intesa in senso lato e include tutti i siti inerenti anche in senso generico alla trattazione o raffigurazione di soggetti erotici o di carattere osceno. Si ricorda che l'accesso a taluni siti (per es. a contenuto pedo-pornografico) costituisce un reato penale.
- La connessione a siti che consentano transazioni commerciali e pagamenti on-line per l'acquisto di prodotti e servizi ed accesso/utilizzo di siti/software web di home-banking.
- La connessione a siti interattivi
  In questa categoria rientrano vari tipi di servizi quali le conversazioni scritte (es. chat e messenger) e telefoniche (es. Skype, VoIP) online, a meno che non siano utilizzate per uso istituzionale (es. partecipazione a meeting on-line, attività di assistenza, corsi di formazione ecc.); la compilazione di modulistica (form) on-line; la partecipazione a luoghi di incontro su temi specifici (forum) o la partecipazione a mailing-list non inerenti all'attività aziendale.
- L'utilizzo di siti di storage online che permettono di salvare, scaricare e condividere file e documenti su siti Internet.
- Lo scarico (download) di file e programmi
  Non è consentito il download di file musicali, video, immagini, programmi, aggiornamenti sia in forma gratuita sia in seguito a transazione commerciale. Fanno eccezione esclusivamente i file utilizzati per la propria funzione aziendale con la sola limitazione a copie di documenti (in genere in formato testo, word o pdf) o di immagini da inserire nei propri documenti. Resta il divieto di download di programmi informatici e dei loro aggiornamenti salvo, nel caso sia ritenuto necessario per l'attività lavorativa, diversa autorizzazione scritta del SICT su richiesta motivata. È inoltre vietato il caricamento (upload) dei medesimi file su Internet eccetto i casi previsti dall'attività istituzionale.

12.4 Regole di buon comportamento per l'utilizzo di internet

Di seguito alcune indicazioni e regole cui l'utente deve attenersi nell'utilizzo dei sistemi di comunicazione:

- Limitare la connessione al solo tempo necessario alle operazioni richieste. Anche la connessione inattiva, infatti, consuma le risorse del sistema rendendolo meno disponibile agli altri utilizzatori.
- Controllare accuratamente la correttezza degli indirizzi a cui ci si connette e la qualità delle informazioni in essi contenute. Va sempre ricordato infatti che Internet è un mondo assolutamente libero nel quale chiunque può inserire informazioni anche se non è autorizzato o qualificato per farlo. Inoltre chiunque, con estrema facilità, può costruire ad arte un sito millantando conoscenze, titoli o qualifiche false o inesistenti.
- Valutare con razionalità il contenuto delle pagine visitate evitando di cadere in truffe o altri abusi. In particolare evitare l'inserimento dei propri dati anagrafici o di altre informazioni personali in moduli di acquisizione on-line. A maggior ragione evitare l'inserimento di dati altrui (in questo caso il comportamento da incauto si trasforma in vero e proprio illecito).
- Nel caso si utilizzi Internet per comunicare/ricevere dati personali e in particolare dati di natura particolare (es. per compilazione di moduli online, upload o download di documenti personali ecc.), l'utente è tenuto a verificare che vengano utilizzati canali di comunicazione sicuri, ovvero che adottino idonee tecniche di cifratura (HTTPS/SSL/VPN, crittografia) o altri sistemi di sicurezza (es. credenziali dedicate, One Time Password ecc.). Nel caso non sia in grado di verificare la sicurezza del canale di trasmissione, l'utilizzatore deve astenersi e fare riferimento al SICT.
- Ricordare che la disponibilità su Internet di documenti, immagini e file di qualsiasi genere non garantisce che questi siano liberamente prelevabili o utilizzabili. Non vale la buona fede, ma vale sempre, al contrario, la restrittiva normativa sul diritto d'autore che configura la copia o l'utilizzo illegale come un reato penale, anche se eventuali informazioni sul copyright non siano immediatamente evidenti. In modo particolare occorre accertarsi della sussistenza di eventuali diritti

di copyright prima di inserire in propri documenti (per es. in word o in presentazioni powerpoint) immagini, dati, informazioni o altro prelevati in qualsiasi modo da Internet.
- In merito al tema del diritto d'autore, inoltre, va precisato che le normative dei diversi Stati (soprattutto extraeuropei) sono differenti tra loro, pertanto ciò che è reso disponibile in quanto lecito in un determinato stato potrebbe non esserlo nel nostro Paese: basti pensare alla facilità con cui è possibile reperire in rete brani musicali che sono con tutta evidenza soggetti a vincoli di copyright. Si rammenta in proposito che il solo possesso di tali file può dar luogo alla contestazione di un reato penale, è sufficiente dimostrare il fine di lucro (ma attenzione, anche il mancato pagamento dei diritti potrebbe essere considerato tale).

12.5 Responsabilità in merito all'utilizzo di internet

L'utente è direttamente e totalmente responsabile dell'uso del servizio di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta e consulta, delle informazioni che recupera o vi immette e delle modalità con cui opera. È responsabile inoltre delle conseguenze di qualsiasi natura che derivino dal loro utilizzo.

12.6 Responsabilità in merito all'accesso a internet

L'utente è responsabile della corretta conservazione della propria credenziale di autenticazione (account e password), che deve essere nota a lui soltanto. Ogni accesso avvenuto con tale credenziale, infatti, sarà sempre imputato a lui come assegnatario. È sconsigliato, pertanto, utilizzare il salvataggio automatico sul proprio browser di credenziali di accesso a siti internet e programmi web e lasciare incustodita senza opportuno blocca schermo la postazione di lavoro assegnata. Infatti, una persona diversa dal titolare, che abbia accesso anche temporaneo al PC, potrebbe accedere a siti Internet e programmi web con le credenziali salvate nel browser senza che questi ne abbia visibilità.

12.7 Revoca delle credenziali o dei diritti di accesso a internet

L'accesso a Internet può essere revocato o non concesso nei seguenti casi:

- Se vengono meno le condizioni per il rilascio dell'autorizzazione (per es. per cessazione della condizione di dipendente o collaboratore autorizzato).
- In caso di accertamento di un uso non corretto del servizio anche in violazione del presente regolamento.
- In caso di diffusione o comunicazione imputabili direttamente all'utente di informazioni riservate (inclusa la propria credenziale di accesso) anche in violazione della normativa sulla protezione dei dati.
- In caso di richiesta formale e motivata da parte del Responsabile del Servizio di appartenenza.

12.8 Sistemi di sicurezza e categorie di siti bloccate da sistemi automatici

Per garantire la sicurezza della postazione e dell'utilizzatore, oltre al blocco selettivo dei siti ritenuti non di interesse istituzionale, l'Azienda si è dotata dei seguenti sistemi di sicurezza:

- Filtri della navigazione web (a protezione da siti malevoli).
- Blocco allo scaricamento, volontario o involontario, di file compressi e file eseguibili o di altra natura ritenuta pericolosa, dannosa o non pertinente, durante la navigazione Internet.
- Filtri alla navigazione sulla base di sistemi di classificazione dei contenuti dei siti.

Fermi restando i divieti precedentemente elencati anche se i siti non sono bloccati dal sistema di controllo, questo inibisce in modo preventivo l'accesso a molti siti inserendoli nella così detta "black list", anche se non è in grado di mappare tutti i siti indesiderati.

La lista precisa delle categorie non accessibili e vietate (per i motivi sopra) può essere richiesta al SICT da chiunque.

In caso di motivate ragioni, potrà essere autorizzata la navigazione su un sito originariamente bloccato, mediante rimozione dalle categorie vietate: è sufficiente cliccare sul link presente nella pagina di blocco alla

navigazione al sito stesso, verrà predisposta una mail pronta ad essere inviata al SICT con i dettagli tecnici del sito, in questa mail è importante indicare le motivazioni di tale richiesta di eccezione.

Le categorie vietate vengono periodicamente aggiornate da sistemi esterni all'Azienda (in base ad analisi sui siti stessi, operate da ditte specializzate).

12.9 Pubblicazione di contenuti e realizzazione di siti personali

L'utente non è autorizzato in alcun caso a produrre e a pubblicare siti web personali utilizzando risorse aziendali né a pubblicare autonomamente siti riferiti alla struttura di appartenenza.

Ogni eventuale necessità di realizzare siti web personali o di struttura utilizzando risorse aziendali dovrà essere espressamente richiesto al SICT (che potrà avvalersi della consulenza del Servizio Relazioni Esterne e Comunicazione per le valutazioni del caso).

Per il corretto utilizzo del logo aziendale in siti e documenti si invita a leggere le norme indicate nella sezione corrispondente della Intranet Aziendale.

È fatto assoluto divieto di realizzare funzioni di Hosting utilizzando risorse aziendali.

12.10 Connessione a provider diversi da quello aziendale

È vietato l'utilizzo di accessi internet mediante Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti Provider, anche con abbonamenti privati.

Infatti tali connessioni rappresentano un potenziale rischio per la sicurezza dell'intero sistema informatico aziendale di cui l'utilizzatore è pertanto responsabile.

12.11 Utilizzo dell'ambiente cloud aziendale per la condivisione temporanea di documenti

Nel caso risulti necessario, per esigenze aziendali, condividere documenti, anche di grosse dimensioni, con persone, sia interne che esterne alla Azienda, è possibile utilizzare il sistema di cloud aziendale chiamato "NextCloud". L'utilizzo di questo strumento è dettagliatamente spiegato nella rispettiva sezione sulla Intranet Aziendale.

Tale sistema è da ritenersi un deposito temporaneo in cui i documenti devono permanere per il tempo necessario per il loro recupero da parte della persona destinataria. Tale periodo non deve superare il limite di 7 giorni (verranno automaticamente eliminati i dati troppo vecchi).

L'accesso a NextCloud è consentito mediante credenziali aziendali (username e password del dominio SIADOM), ed è utilizzabile, per esigenze esclusivamente aziendali, da tutti gli utenti dotati di tali credenziali.

Il sistema NextCloud permette altresì all'utilizzatore aziendale di depositare documenti per potervi poi accedere dall'esterno della rete aziendale mediante l'uso delle proprie credenziali. In questo caso, si raccomanda che vengano caricati su NextCloud esclusivamente i documenti per i quali vi sia necessità di accesso dall'esterno e che al termine dell'utilizzo vengano quanto prima rimossi da NextCloud.

Si precisa che il sistema NextCloud non è da considerarsi un'alternativa all'utilizzo dei File Server Aziendali (sistemi da usare per salvataggio dei file lavorativi ed importanti), bensì uno strumento utile per condivisione di dati con utenti esterni, come sopra precisato.

Il sistema NextCloud non deve essere utilizzato per condividere con l'esterno documenti contenenti dati di natura sensibile, mentre può essere usato per condividere o accedere a tali dati con utenti che dispongano di credenziali aziendali. NextCloud consente la condivisione di file contenenti dati di natura particolare, anche dati sensibili o sanitari, con l'esterno, ma tali file devono essere protetti da password (ad es. una cartella compressa protetta da password).

12.12 Utilizzo di server esterni per backup/gestione/condivisione documenti aziendali

Salvo casi particolari che devono essere espressamente autorizzati, è vietato caricare documenti aziendali riservati e contenenti dati di natura sensibile su sistemi di memorizzazione esterni (ad esempio cloud quali Dropbox, Google Drive, SkyDrive, icloud ecc.).

Per ogni necessità occorre utilizzare il servizio cloud aziendale NextCloud.

Ciò in quanto tali sistemi possono essere soggetti ad attacchi informatici e i dati possono essere sottratti o manipolati illegalmente. Inoltre tali sistemi potrebbero essere ospitati in paesi non soggetti a regolamentazioni sulla privacy analoghe a quella europea.

Non saranno pertanto effettuate abilitazioni specifiche che permettano la connessione a tali sistemi, salvo casi particolarissimi da valutare e autorizzare singolarmente (per es. accessi temporanei per prelevare dati da gruppi di lavoro già esistenti).

Gli utenti aziendali dotati di Office nella versione online possono accedere a OneDrive[8] mediante credenziali aziendali; infatti in tal caso si ha la garanzia che i dati siano conservati nell'Unione Europea, secondo la relativa normativa di protezione dei dati, tuttavia permane il divieto di collocare su tale cloud dati riservati o di natura sensibile.

12.13 Assistenza da remoto (VPN e altre tipologie)

Sono ammessi collegamenti remoti dall'esterno per l'accesso alle risorse aziendali, sia per lo svolgimento di specifiche attività da una sede esterna, sia per manutenzione di attrezzature da parte di ditte esterne. Tali collegamenti sono previamente autorizzati dal SICT. In particolare, qualora l'Azienda si avvalga di attrezzature la cui gestione in sicurezza ricada sotto la responsabilità di personale non dipendente o a questi assimilabile (ad es. ditte fornitrici di applicativi aziendali), dovrà essere formalmente definito un "Responsabile del trattamento" 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.

13 Utilizzo dello smartphone aziendale

Al fine di assicurare il servizio di pronta reperibilità e lo svolgimento della attività istituzionale, in taluni casi l'Azienda fornisce smartphone aziendali ai propri dipendenti, previa valutazione da parte del relativo Direttore di Dipartimento o del Delegato al trattamento, il quale sottoscrive la richiesta, utilizzando l'apposito modulo reperibile sulla Intranet Aziendale.

Di norma l'abilitazione del cellulare aziendale è limitata alle sole chiamate, tuttavia è possibile abilitare anche la trasmissione dati, sempre previa richiesta del Direttore della macrostruttura di afferenza, il quale assume l'onere di vigilanza sul corretto utilizzo del dispositivo.

Tra gli utilizzi impropri del cellulare aziendale rientra la comunicazione di dati di natura sensibile (in particolare referti e informazioni relative alle attività cliniche) o informazioni soggette a segreto d'ufficio/segreto professionale attraverso app/programmi di messaggistica istantanea come WhatsApp, altri sistemi di chat, social media ed altro (compresa la messaggistica di testo come gli SMS).

Tali comunicazioni sono dunque vietate.

Per motivi di sicurezza e protezione la posta elettronica aziendale potrà essere installata solo su smartphone aziendali, salvo richieste specifiche, motivate ed esplicitamente autorizzate dal SICT.

14 Utilizzo dello smartphone personale

Analogamente è vietata la trasmissione di dati di natura sensibile (in particolare referti e informazioni relative alle attività cliniche) o di informazioni soggette a segreto d'ufficio/segreto professionale, attraverso app/programmi di messaggistica istantanea come WhatsApp, altri sistemi di chat, social media ed altro (compresa la messaggistica di testo come gli SMS) mediante il proprio cellulare personale. Indipendentemente dallo strumento utilizzato, infatti, i dipendenti sono tenuti a mantenere un comportamento rispettoso della riservatezza e della tutela dei dati di cui siano in possesso per motivi professionali.

[8] Si tratta del servizio fornito da Microsoft con il pacchetto Office online

15 Modalità di prestazione dei servizi

Il SICT si impegna a fornire continuità ai servizi erogati, riservandosi la possibilità di interromperli esclusivamente per le manutenzioni ordinarie e cercando di arrecare il minor disagio possibile agli utilizzatori. Salvo impedimenti, le interruzioni per interventi di manutenzione saranno comunicate agli utenti.

Per poter fornire assistenza e supporto tempestivi nel caso di guasti e malfunzionamenti, su ciascun computer fisso o portatile è installata un'applicazione che consente ai tecnici del SICT di collegarsi da remoto, senza bisogno di intervenire sul luogo.

Pertanto la manutenzione alle stazioni di lavoro viene generalmente effettuata, in prima battuta, mediante tali sistemi software di manutenzione remota. Solo nel caso di mancata soluzione del problema in modalità remota, viene effettuato un intervento in loco.

I suddetti sistemi di controllo remoto sono configurati affinché gli operatori che intervengono per la manutenzione possano farlo esclusivamente previo consenso dell'utilizzatore della postazione (consenso che viene richiesto in tempo reale sullo schermo del pc); non sarà richiesta l'autorizzazione solo nei casi in cui si renda necessario effettuare installazioni o aggiornamenti software da remoto, che non prevedono la possibilità di accesso ai dati presenti nel computer.

Inoltre l'utente può verificare l'attività effettuata in remoto dal tecnico rimanendo presso la postazione.

Gli interventi sono eseguiti da personale identificato e autorizzato che afferisce al SICT direttamente o tramite contratti di fornitura di servizi.

16 Installazione di Microsoft Office sulle postazioni di lavoro

L'Azienda ha avviato un percorso di progressiva introduzione di sistemi open source di automazione d'ufficio (es. LibreOffice), pertanto sui PC di nuova fornitura saranno installate esclusivamente queste versioni.

Sono previste eccezioni per esigenze specifiche, che devono essere adeguatamente motivate e autorizzate, quali:

- Procedure Aziendali che richiedano necessariamente l'utilizzo di MS Office.
- Necessità di compatibilità con vecchie procedure Access.
- Gestione di documenti che presentano evidenti incompatibilità con i sistemi e i formati open.

Si precisa che le licenze di MS Office installabili sui PC aziendali sono solo quelle acquistate dall'Azienda (non sono ammesse né licenze personali né licenze universitarie).

17 Rilevazione a fini diagnostici delle attività informatiche e telefoniche

Premesso che nel rispetto della normativa vigente, l'Azienda non effettua verifiche che possano configurare il controllo a distanza dell'attività dei lavoratori, quali:

- Lettura e registrazione sistematica dei messaggi di posta elettronica o dei relativi dati esteriori, fatto salvo quanto tecnicamente necessario per svolgere il servizio e-mail;
- Riproduzione o eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- Lettura o registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- Analisi occulta di eventuali computer o dispositivi portatili affidati in uso;

l'Azienda si riserva tuttavia il diritto di effettuare controlli tesi a garantire il corretto utilizzo delle attrezzature informatiche aziendali e il corretto funzionamento del sistema informatico e di telefonia, in particolare nel caso in cui sospetti manomissioni alle configurazioni del sistema informatico, telematico, telefonico aziendale e/o accessi indebiti allo stesso, ovvero riscontri diffusioni indebite di informazioni atte a pregiudicare la sicurezza del sistema stesso o il suo buon funzionamento e/o a garantire ad altri accessi o privilegi non dovuti, o ancora abbia concrete ragioni che portino a pensare che la sicurezza del sistema tecnologico aziendale possa essere minacciata.

In tali casi l'Azienda, nel rispetto dei principi di liceità, correttezza e trasparenza di cui all'art. 5 del GDPR e del disposto dell'art. 4 della L. 300/1970 (c.d. Statuto dei Lavoratori) procede ai controlli, con esclusione della possibilità del controllo informatico all'insaputa dei lavoratori e in ottemperanza ad un criterio di graduazione, secondo il quale:

- In via preliminare saranno eseguiti controlli su dati aggregati e anonimi, riferiti all'intera struttura lavorativa. In assenza di anomalie non si effettueranno controlli ulteriori.
- Nel caso siano rilevate anomalie, sarà diramato un avviso generalizzato. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
- Qualora si rilevasse il perdurare delle anomalie, si procederà a controlli su base individuale.
- Nel caso di abusi singoli o reiterati si procederà all'invio di avvisi individuali e, in seguito, saranno eseguiti controlli nominativi.

Il riscontrato o reiterato uso non conforme delle risorse informatiche e di telefonia, evidenziatosi secondo la procedura sopra indicata, qualificandosi come violazione degli obblighi del dipendente, comporta l'adozione da parte della Azienda delle opportune misure disciplinari, anche con accesso ai dati di dettaglio necessari per il completamento dell'istruttoria.

In caso di problemi inerenti alla sicurezza della infrastruttura tecnologica l'Azienda si riserva il diritto di adottare tutte le misure tecniche che garantiscano la gestione della contingenza, ad esempio isolando dalla rete stazioni che siano state infettate da virus che ne pregiudichino il buon funzionamento, aggiornando configurazioni software e/o hardware ecc. Tutte le azioni messe in atto sono valutate in una logica di costo/beneficio e sono improntate a un criterio di minimizzazione del disservizio.

L'Azienda si riserva la possibilità di interrompere i servizi informatici per le manutenzioni ordinarie e straordinarie e per la gestione dei guasti, impegnandosi, nel limite del possibile, ad avvertire preventivamente gli utilizzatori di dette interruzioni.

È esclusa in ogni caso l'ammissibilità di controlli prolungati, costanti o indiscriminati.

17.1 Gli accessi a Internet

Tutti gli accessi ad Internet vengono memorizzati per finalità di sicurezza del sistema in appositi file di log. 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. Questi log non sono oggetto di operazioni di backup e tengono traccia dei seguenti dati per ogni accesso:

- Data e ora dell'accesso
- Riferimento al sito visitato (URL)
- Esito della consultazione
- Tipologia di operazione richiesta e informazioni sugli eventuali file scaricati
- Numero di byte trasferiti dall'elaboratore remoto e viceversa

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; entrambe le attività si svolgono su dati anonimi.

Nel rispetto del principio secondo cui la conservazione nel tempo dei dati deve essere strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza, i log sono trattati e conservati per un massimo di sette giorni esclusivamente per ragioni tecniche (es. per individuare un problema di blocco di navigazione), dopodiché sono distrutti a cura del Servizio ICT.

L'Azienda procederà ad emettere un avviso generalizzato che informa della sospensione - per un periodo limitato e indicato nell'avviso stesso - dei controlli anonimi e del fatto che i log di sistema verranno utilizzati per l'individuazione di problemi qualora si rilevino 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;

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 del Servizio ICT.

L'Azienda potrà utilizzare 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 stessa.

I log potranno essere oggetto di provvedimenti da parte dell'Autorità Giudiziaria 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.

17.2 Utilizzo della posta elettronica

Il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i file allegati, riguarda forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali.

Pertanto non viene conservato alcun log relativo al contenuto delle e-mail inviate e ricevute dagli utenti con il servizio di posta elettronica aziendale. 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 per le stesse finalità indicate relativamente agli accessi ad Internet.

Il sistema di posta elettronica tiene traccia di tutte le e-mail inviate e ricevute, conservando nei log:

- Identificativo della stazione di lavoro che ha inviato il messaggio
- Data e ora
- Indirizzo di posta del mittente
- Indirizzo del destinatario

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.

17.3 Telefonia

L'Azienda, mediante configurazioni sugli apparati tecnologici, impedisce l'effettuazione di chiamate dalla rete aziendale verso determinate categorie di numeri, quali i numeri a pagamento per servizi particolari. L'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, attraverso i servizi del provider telefonico, delle telefonate effettuate, se queste costituiscono un onere economico per l'Azienda; mentre non sono tracciate le telefonate in ingresso. In particolare viene registrato:

- Il numero del chiamante
- Il numero chiamato
- Data e ora di inizio e data e ora di fine della telefonata

Tutti i log sopra citati vengono conservati dall'Azienda per 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 al trentuno dicembre di ciascun 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.

17.4 Cessazione della disponibilità dei servizi informatici aziendali

Ai sensi del presente Regolamento, la disponibilità a un utente dei servizi informatici aziendali cesserà totalmente nel caso non sussista più la condizione di dipendente o di collaboratore esterno; inoltre può cessare o essere limitata nei privilegi assegnati in caso di:

- Revoca dell'autorizzazione all'uso fornita dal Responsabile (per es. per cambio di mansione, ruolo, Servizio ecc.).
- Accertato uso non corretto o comunque estraneo alla sua attività lavorativa dei servizi informatici aziendali.
- Accertate manomissioni e/o interventi illeciti sull' hardware e/o sul software.
- Accertate diffusione o comunicazione imputabili direttamente o indirettamente all'utilizzatore, di password, procedure di connessione, indirizzo IP e altre informazioni tecniche riservate.
- Accesso illecito e intenzionale dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili, in particolare se l'attività dell'utente comporti danno, anche solo potenziale al sito contattato.
- Violazione delle regole essenziali stabilite dal presente regolamento.

Si precisa che in caso di cessazione della condizione di dipendente o collaboratore a una certa data la casella di posta dell'utente sarà immediatamente disattivata.

Si ricorda inoltre che, una volta cessata la condizione di dipendente o collaboratore è vietato asportare dati aziendali prodotti nell'attività istituzionale. Non sarà dato seguito, pertanto, alla richiesta di scarico massivo (per es. su supporto esterno) delle mail dell'utente, né di altri file contenuti nei file server o nei personal computer.

17.5 Responsabilità dell'utilizzatore delle risorse informatiche

L'utilizzatore è direttamente e totalmente responsabile dell'uso che egli fa del servizio di posta elettronica e di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

All'utilizzatore è consentito utilizzare il servizio solo per ragioni professionali connesse alla propria attività, in modo individuale, salvo eccezioni.

L'utilizzatore non può servirsi o dar modo ad altri di servirsi della rete aziendale e dei servizi da essa messi a disposizione per utilizzi illeciti che violino o trasgrediscano diritti d'autore, marchi, brevetti, comunicazioni private o altri diritti tutelati dalla normativa corrente, per utilizzi contro la morale e l'ordine pubblico, per recare molestia alla quiete pubblica o privata, per recare offesa o danno diretto o indiretto all'Azienda o a terzi.

18 Ulteriori istruzioni per la tutela delle informazioni gestite dagli operatori

18.1 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 solamente 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).

18.2 Comunicazioni telefoniche e via fax

Nel caso in cui sia necessario effettuare comunicazioni telefoniche agli interessati:

- Accertarsi che chi risponde al telefono sia l'interessato stesso
- Prestare attenzione a discutere, comunicare o comunque trattare dati personali o di salute 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 deve essere sempre collocato in luogo non accessibile a terzi non autorizzati.

18.3 Rapporti di front office

Agli operatori addetti ad attività di front office è richiesto il rispetto delle seguenti regole:

- 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) 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 occorre fare attenzione alla digitazione ed all'inserimento corretto dei dati identificativi dell'interessato chiedendo l'esibizione di un documento di identità valido.
- È 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.

18.4 Corretta comunicazione dei dati

La richiesta di comunicazione o documentazione di dati personali e di natura particolare può essere evasa nei confronti dell'interessato o di un terzo a ciò delegato (per iscritto) o legittimato per legge. In tal senso assoluta attenzione deve essere 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.

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.

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.

19 Disposizioni finali

Il presente Regolamento entra in vigore alla data della adozione della relativa Delibera di approvazione e sarà diffuso tra tutti i lavoratori ai quali, per effetto del rapporto di lavoro o di collaborazione l'Azienda abbia assegnato una casella di posta elettronica e la possibilità di accesso alla rete internet.