Sistema Socio Sanitario

Carlo Poma

Regione Lombardia

ASST Mantova

Termini e modalità di utilizzo dei servizi e dei canali telematici, di internet e della posta elettronica

Versione 1.1 | Aggiornamento al 10/08/2016

Indice

1 RIFERIMENTI NORMATIVI

[1] Piano di Organizzazione e Funzionamento Aziendale 2008-2010, A.O "Carlo Poma" Mantova.

[2] DPR 318/1999 Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali;

[3] "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni" Direttiva 16 gennaio 2002;

[4] "Codice in materia di protezione dei dati personali", Decreto Legislativo 30 giugno 2003, n. 196;

[5] "Codice dell'Amministrazione Digitale" Decreto Legislativo 7 marzo 2005, n.82;

[6] "Linee Guida per la Pubblica Amministrazione Digitale", Direttiva 18 novembre 2005;

[7] "Linee guida del Garante per posta elettronica e internet", Gazzetta Ufficiale n. 58 del 10 marzo 2007;

[8] "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro", Direttiva 02/09, Dipartimento della Funzione Pubblica

2 ACRONIMI E ABBREVIAZIONI

- **AO:** Azienda Ospedaliera
- **AdS:** Amministratore di Sistema
- **CED**: centro elaborazione dati
- **SIA**: servizio informativo Aziendale
- **SEP**: Symantec Endpoint Protection
- **PDL**: Postazioni di Lavoro
- **PIN**: Personal Identification Number
- **SISS**: Servizio Informativo Socio Sanitario
- **HD** Help Desk
- **IT** Information Technology

3 DEFINIZIONI

Trattamento: (ex art. 4 D.Lgs. 196/03) "*qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati*".

4 PREMESSA

La corretta osservanza del presente disciplinare consente non solo di adempiere gli obblighi di legge, ma anche di migliorare l'organizzazione aziendale ottimizzando i processi di lavoro attraverso l'uso di strumenti informatici.

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare ulteriori regole interne di comportamento comune, dirette ad evitare comportamenti inconsapevoli e/o scorretti.

Il disciplinare di cui in oggetto contiene un insieme di linee guida (comportamenti) da seguire al fine di ridurre a livelli accettabili i rischi derivanti da uso improprio o poco consapevole delle risorse informatiche Aziendali.

I problemi di sicurezza possono provocare la perdita di profitti, spese aggiuntive, risvolti penali, la perdita della fiducia degli utenti e l'incapacità di gestire continuativamente le risorse e i processi IT.

Gli strumenti per il monitoraggio delle reti utilizzati per identificare i punti tecnici più vulnerabili sono utili solo per risolvere i problemi tecnica, tuttavia occorre ricordare che i controlli di tipo tecnico possono essere accidentalmente o volontariamente messi fuori uso da utenti e processi, con una conseguente esposizione delle informazioni e delle reti ai rischi di natura diversa. Un approccio completo per la gestione dei rischi e la salvaguardia delle informazioni deve necessariamente prevedere l'identificazione delle vulnerabilità e delle minacce più probabili, una quantificazione del possibile impatto sulle risorse aziendali e lo sviluppo di strategie correttive capaci di ridurre il rischio a un livello accettabile.

La continua evoluzione di requisiti e sistemi impone ai professionisti della sicurezza la necessità di individuare un livello di rischio accettabile che non comprometta la disponibilità, la riservatezza e l'integrità dei dati.

Nella tabella sottostante raffiguriamo alcuni esempi di minacce, metodi, obiettivi e criteri di sicurezza, ai quali il presente documento analizza e tiene conto al fine di garantire non solo l'applicazione della normativa vigente in materia di protezione di dati, ma anche di tutela del patrimonio aziendale.

Minacce	Ragioni/Obiettivi	Metodi	Criteri di sicurezza
Dipendenti • Malintenzionati • Inesperti Non dipendenti • Aggressori esterni • Calamità naturali	• Negare i servizi • Sottrarre informazioni • Alterare le informazioni • Danneggiare le informazioni • Eliminare le informazioni • Fare uno scherzo • Mettersi in mostra	• Social engineering • Virus, trojan-horse, worm • Modifica dei pacchetti • Saturazione con posta • Strumenti di *hacking* • Identificazione password	• Vulnerabilità • Risorse • Informazioni e dati • Produttività • Hardware • Personale

4.1 ANALISI DEL RISCHIO

L'analisi del rischio costituisce una fase fondamentale di ogni percorso di sicurezza.
Questo documento in larga misura tratta dell'adozione di misure minime di sicurezza, obbligatorie per legge [2], e quindi non graduabili. La valutazione del rischio sarà comunque utilizzata per tutte quelle situazioni in cui l'adozione di misure minime sia non sufficiente e pertanto si debba valutare una gradazione delle misure adottabili.
In tali contesti, cioè qualora sia necessaria una graduazione delle misure adottabili, si dovrà adottare una valutazione del rischio basata sui seguenti criteri:

1. si considerano gravi le minacce che possono limitare e/o rendere difficoltosa l'erogazione della attività assistenziale e/o rese al pubblico;
2. si considerano gravi le minacce che portano alla divulgazione/modifica/produzione illegittima di dati sensibili o che comportino un danno patrimoniale per l'azienda;
3. si considerano gravi le minacce che portano alla perdita o sottrazione illecita dei dati

In particolare:

1. si considerano gravi le minacce che possono limitare la disponibilità di servizi informatici a supporto delle attività assistenziali o delle attività rese al pubblico;
2. si considerano gravi le minacce che portano alla modifica illecita di messaggi – e quindi di informazioni gestite dall'azienda - qualora tali messaggi abbiano un valore medico-legale o la loro modifica comporti un danno patrimoniale per l'azienda;
3. si considerano gravi le minacce di fraudolenta impersonificazione (masquerade) qualora ciò porti alla produzione di falsi atti con valore medico-legale o che comportino un danno patrimoniale per l'azienda;
4. si considerano gravi le minacce di fraudolenta impersonificazione (masquerade) qualora ciò porti alla modifica fraudolenta di atti con valore medico-legale originariamente legittimi, o qualora ciò porti ad un danno patrimoniale per l'azienda;
5. si considerano gravi le minacce di intercettazione qualora i dati intercettabili riguardino dati personali di natura sensibile ai sensi della legge sulla tutela dei dati personali.

Si considerano in genere trascurabili le minacce di analisi del traffico e di ripetizione, a patto che esse non portino a conseguenze elencate nei punti sopra elencati.

A tal fine, con l'obiettivo di garantire la continuità operativa nel rispetto della riservatezza dei dati sensibili e personali trattati dall'Azienda Ospedaliera si sono definite nel presente documento una serie di comportamenti per l'utilizzo delle risorse informatiche, della posta elettronica e dell'accesso ad internet.

4.2 RIFERIMENTI SERVIZIO INFORMATICO AZIENDALE

Sede Operativa: V.le Albertoni,1 Palazzina 2 (ex. Pronto Soccorso)

Orari: lun.-ven.: 07.30÷18.00 sab. 8.30÷12.30

Contatto telefonico: 0376 464 420 (interno 3420)

Contatto fax: 0376 464 683

Contatto email SIA: sia@asst-mantova.it

4.3 AMBITI DI APPLICAZIONE

Questo regolamento si applica:

- a tutti gli utenti che utilizzano le risorse informatiche dell'AO, siano essi dipendenti a tempo pieno o parziale, collaboratori, consulenti, studenti, dipendenti di aziende esterne legate da contratti di fornitura di servizi o altri a cui ne è concesso l'uso;
- a tutte le risorse informatiche di proprietà dell'AO e a quelle messe a disposizione nell'ambito del progetto regionale CRS-SISS;
- a tutte le operazioni di accesso a dati registrati ed archiviati elettronicamente tramite risorse informatiche aziendali;
- a tutte le forme di comunicazione interna ed esterna operate attraverso Internet e la posta elettronica;
- all'utilizzo di tutti i tipi di supporti di memorizzazione dei dati, audio e video, analogici e digitali, dedicati e non dedicati, anche se prodotti di uso non professionale, destinati all'archiviazione di dati, documenti digitali o registrazioni.

4.4 VERIFICHE

Salvo l'obbligo per ciascun utente dei Sistemi Informatici Aziendali di seguire il presente Regolamento e di segnalarne eventuali violazioni al Responsabile del Sistemi Informatici Aziendali, le funzioni di verifica del suo rispetto sono assegnate alla Struttura Complessa Servizi Informativi Aziendali che potrà compiere anche verifiche sul corretto utilizzo dei supporti di memorizzazione e delle istallazioni di software e Hardware locali. Tutti gli utenti sono tenuti a segnalare prontamente qualsiasi violazione al presente Regolamento.

Non sono ammesse segnalazioni di violazioni in forma anonima; viene comunque tutelato dall'Azienda il diritto alla Privacy degli utenti che comunicassero dette violazioni, nei limiti previsti dalla normativa italiana in vigore.

4.5 SANZIONI

Poiché, in caso di violazioni contrattuali e giuridiche, sia l'Azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni anche di natura penale, l'azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità dei propri Sistemi Informativi/Informatici (vedi 7.2.2).

In caso di violazione accertata del presente regolamento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali. Qualsiasi violazione alla normativa italiana vigente da parte degli utenti sarà segnalata alle Autorità competenti.

4.6 AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento tramite comunicazione al SIA.

La versione aggiornata del presente Regolamento, che avviene con cadenza almeno annuale da parte del SIA, è scaricabile dalla intranet aziendale (http://intra.poma.net) nella sezione "REGOLAMENTI" (http://intra.poma.net/lay_cat.php?IDCategoria=789) ed è raggiungibile seguendo il percorso:

Home -> Chi siamo → Direzione Strategica → Direzione Amministrativa → Sistemi Informativi Aziendali → REGOLAMENTI

4.7 MATERIALE INFORMATIVO

Oltre al presente documento l'Azienda potrà metterà a disposizione degli utenti ulteriori materiali informativi utili per favorire la corretta applicazione del regolamento, attraverso la pagina Intranet Aziendale o mediante circolari di richiamo.

5 POSTAZIONI DI LAVORO

5.1 UTILIZZO DELLE POSTAZIONI DI LAVORO

Le PDL, sia da tavolo che portatili, sono predisposte con la necessaria dotazione di dispositivi (hardware) e programmi (software) tali da consentirne il loro corretto funzionamento in conformità a standard aziendali e nel rispetto delle necessarie licenze d'uso.
L'installazione e l'aggiornamento dei dispositivi e dei programmi è di esclusiva competenza del personale espressamente incaricato del SIA.

È quindi vietato:

- Installare software non autorizzato;
- Modificare in parte o del tutto il software o le sue configurazioni di funzionamento;
- Asportare o copiare in parte o del tutto il software;
- Modificare, aggiungere o rimuovere dispositivi hardware;
- Utilizzare strumenti software e/o hardware atti a interpretare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- Utilizzare dispositivi di comunicazione diversi da quelli di cui è dotata la PDL (es.: modem, switch, hub, router, telefoni cellulari e palmari, apparati di rete non autorizzati);
- Disattivare o disinstallare, anche temporaneamente, il Sistema antivirus aziendale (SEP);
- Aprire sessioni di lavoro remote tramite PDL connesse alla Rete Aziendale;
- Compromettere il funzionamento dei Servizi di Rete e degli apparecchi che li costituiscono con virus o programmi diretti a danneggiare od interrompere la continuità operativa;
- Connettere alla rete aziendale computer e/o apparati anche elettromedicali non preventivamente comunicati al SIA;
- Distruggere, deteriorare o rendere in tutto od in parte inutilizzabili programmi, informazioni o dati altrui;
- Lasciare incustodita la stazione di lavoro se non in una condizione di spegnimento o blocco all'accesso.

Si sottolinea che il cosiddetto software "shareware" o "freeware" scaricabile da Internet è generalmente esente da licenza SOLO per uso amatoriale. L'utilizzo su stazioni di lavoro di una società deve essere subordinato alla formalizzazione della relativa licenza d'uso (ricadono in questa categoria software molto comuni quali: screensaver, compressori, "criptatori", ecc.), a tal proposito si richiama quanto già indicato nei punti precedenti.

Ogni PDL alla quale il dipendente può accedere deve essere considerata come **strumento di produttività**, e come tale deve essere utilizzato, inoltre nei casi in cui la stazione di lavoro venga sottoposta a qualsiasi intervento di manutenzione, sia straordinario che dietro richiesta dall'utente (ad esempio in Assistenza Remota 5.2), e vengano individuati software applicativi non riconducibili a tipiche installazioni aziendali gli operatori del SIA saranno autorizzati alla rimozione di tali software dalla PDL ripristinandone le configurazioni iniziali.

5.2 ASSISTENZA REMOTA

Il personale incaricato del servizio ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché garantire la massima sicurezza contro *virus*, *spyware*, *malware* o qualsiasi criticità dei sistemi operativi secondo le ultime segnalazioni in fatto di vulnerabilità.

L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico (esempio problemi di sicurezza). In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione in forma orale della necessità dell'intervento stesso, l'operatore contattato dovrà fornire adeguato supporto al personale del SIA al fine di garantire tempestivamente l'intervento.

L'attivazione dell'assistenza remota da parte dell'utente o l'accesso da parte del personale del SIA dietro evidenza di oggettiva necessità (come sopra descritto) comporta la liberatoria al personale incaricato delle operazioni alla visibilità del contenuto completo della propria PDL.

6 MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI

6.1 GESTIONE DEI DATI TRATTATI MEDIANTE STRUMENTI ELETTRONICI

L'AO Carlo Poma di Mantova adotta nell'ambito delle regole generali, un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza volte ad assicurare un livello minimo di protezione di dati personali e sensibili.

L'accesso dei dati trattati con l'ausilio di strumenti elettronici è disciplinato dalle seguenti misure e relative modalità di trattamento:

- Autenticazione informatica;
- Adozione di procedure di gestione delle credenziali di autenticazione;
- Aggiornamento periodico dell'individuazione dell'ambito di trattamento conseguito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, accessi non consentiti e a determinati programmi informatici;
- Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- Tenuta di un aggiornato documento programmatico sulla sicurezza;
- Adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute e la vita sessuale effettuati da organismi sanitari;
- Il trattamento di dati personali e/o sensibili con strumenti elettronici è consentito agli i**ncaricati dotati di credenziali** di autenticazione che consentano il superamento di una procedura (di autenticazione) relativa a uno specifico trattamento o a un insieme di trattamenti;
- Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (username) associato a una parola chiave (password) riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato (es. smart-card), eventualmente associato a un codice identificativo (pin) o a una parola chiave;
- Ad ogni incaricato sono assegnate o associate **individualmente** una o più credenziali per l'autenticazione: le credenziali di autenticazioni sono **strettamente personali** e per questo non devono essere in alcun modo comunicate ad altri operatori;
- Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato;

- La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili la parola chiave è modificata almeno ogni tre mesi;
- Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi;
- Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica;
- Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali;
- Sono state impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento;
- Alla fine della sessione di lavoro eseguire le procedure di uscita (logout) dall'applicativo accertandosi della chiusura di tutte le finestre nelle quali sono evidenti dati personali e/o sensibili;
- Nel caso l'autenticazione sia stata eseguita con smart-card, l'operatore si ricordi di rimuoverla dall'apposito lettore e trattenerla con se al fine di evitarne smarrimenti ed utilizzi non consentiti;
- Abilitare sulle postazioni screen-saver automatici che intervengono dopo alcuni minuti di inattività: tali screen-savers devono richiedere all'utente la ri-immissione dello username e della password;
- quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema;
- Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione;
- gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale;
- Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno giornaliera/settimanale;
- accesso limitato per i locali relativi ai Servizi I.T., nello specifico Sala Server e Laboratorio Hardware/Software.

6.2 GESTIONE DEI DATI SULLE STAZIONI DI LAVORO (GESTIONE LOCALE)

Costituisce buona regola la pulizia periodica (almeno una volta l'anno) degli archivi, con cancellazione dei file obsoleti o ritenuti inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante al fine di salvaguardare spazio e permettere alla risorsa un'operatività costante ed efficiente nonché ridurre gli intervalli di manutenzione.
Le gestioni locali dei dati dovranno essere ridotte al minimo per essere sostituite da gestioni centralizzate su server come indicato dalla normativa vigente [4].
In linea generale le banche dati presenti sulle PDL non gestite centralmente devono essere prive d'anagrafica dei pazienti e riportare unicamente un numero identificativo in loro sostituzione (es. numero della cartella clinica).
Qualunque creazione di banche dati contenente dati personali deve essere comunicata all'AS ed autorizzata singolarmente, il SIA non risponde di banche dati e archivi creati e trattati in difformità da quando stabilito in questo documento.
Nell'effettuare il trattamento dei dati personali devono essere soddisfatti i principali contenuti nella percepita normativa in materia di privacy [3] e di sicurezza dei dati trattati. I dati personali devono esser esatti e, se necessario aggiornati nonché pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati. Il trattamento deve avvenire in modo lecito, e secondo correttezza; la raccolta e registrazione dei dati stessi deve avvenire per finalità non incompatibili con tali scopi. La conservazione deve avvenire per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
In particolare si deve osservare che le informazioni archiviate elettronicamente devono essere ridotte al minimo e riguardare esclusivamente quelle previste dalla legge, necessarie all'attività lavorativa secondo finalità determinate, esplicite e legittime, osservando il principio della pertinenza e non eccedenza.

Operativamente si possono manifestare le seguenti condizioni:

- la PDL **è condivisa tra più utenti**:
  - **è assolutamente vietata** la presenza di archivi di qualsiasi formato contenenti dati sensibili e/o personali;
- la PDL **è di uso personale** (unico utente):
  - è ammissibile la presenza di archivi dati (di qualsiasi formato – es. access, excel, word, ecc..--) contenenti dati sensibili e/o personali purché protetti da meccanismi d'accesso quali : password in fase di apertura del file, crittografia dati, separazione tra le anagrafiche e i dati, ecc..

In questo caso l'onere della gestione dei dati personali e/o sensibili (comprese le operazioni di back-up e ripristino) è di completa attribuzione **dell'utente della postazione**, il SIA non risponde in alcun modo della loro presenza, gestione, trattamento, manutenzione e ripristino.

Per i consigli riguardanti la definizione della password si rimanda a quanto espresso nel cap. 7.1.2.

Gli operatori incaricati dall'azienda per la manutenzione ordinaria e straordinaria del sistema informatico possono procedere alla rimozione di ogni file o applicazione sia sulle PDL che sulle unità di rete che riterranno essere pericolosi per la Sicurezza o non conformi a quanto esplicitato nei punti precedenti, previo avvertimento dell'utente.

6.3 CARTELLE CONDIVISE

L'utilizzo di risorse (cartelle) condivise deve essere ridotto al minimo al fine di diminuire i rischi per la sicurezza informatica e la salvaguardia degli aspetti concernenti la Privacy.
In linea generale valgono le seguenti regole sull'utilizzo delle risorse (cartelle) in rete:

- Le cartelle condivise gestite a livello centrale sono preventivamente concordate, configurate (definizione degli spazi e delle credenziali d'accesso) e mantenute dal SIA, solo di queste si garantisce il back-up dei dati;
- L'accesso alle cartelle condivise deve sempre essere protetto da username e password (come espresso al cap. 7.1);
- Poiché lo spazio assegnato è contingentato sarà cura dell'operatore la manutenzione del contenuto con rimozione dei files ritenuti obsoleti e non utilizzati;
- Le cartelle di rete non vanno usate per operazioni di archiviazione e scambio di files il cui contenuto non sia riferibile all'attività lavorativa; pertanto se nel caso di manutenzione delle cartelle condivise da parte del personale del SIA si dovessero manifestare usi non corretti della risorsa il personale è autorizzato in prima istanza alla rimozione di tali files e qualora dovesse proseguire l'abuso si provvederà alla chiusura della risorsa fornita.

Il SIA non risponde di interventi di manutenzione di cartelle condivise non preventivamente concordate e configurate sugli apparati centrali dei Servizi Informativi.

6.4 UTILIZZO DI SUPPORTI MAGNETICI E DI MEMORIZZAZIONE (FLOPPY-DISK, USB-PEN, CD/DVD, DISCHI FISSI ESTERNI)

Relativamente all'utilizzo dei supporti rimovibili valgono le seguenti linee guide:

a) Prima dell'accesso alle risorse contenute sui supporti rimovibili l'operatore avrà cura di eseguire una scansione con il sistema antivirus aziendale sull'**intero contenuto del supporto** al fine di rilevare e rimuovere la presenza di virus (vedi par. 6.6);
b) Non è consentito scaricare sulla propria PDL file contenuti in supporti magnetici/ottici/usb non aventi alcuna attinenza con la propria prestazione lavorativa;
c) I supporti rimovibili contenenti dati sensibili e/o personali devono essere custoditi con cura in modo da evitarne l'utilizzo da parte di soggetti non autorizzati; la responsabilità dei dati contenuti su questi supporti è completamente attribuibile all'utente che li ha creati e gestiti;
d) I supporti rimovibili, contenenti dati sensibili, se non più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (dopo aver formattato il dispositivo o cancellato il contenuto dal dispositivo stesso).

6.5 BACK-UP (SALVATAGGIO DEI DATI)

Gli utenti sono tenuti ad effettuare, con regolarità, copie di sicurezza (backup) dei dati memorizzati sulle proprie PDL necessari per il ripristino e continuità delle funzionalità operative in caso di guasto o di perdita accidentale degli stessi; dei dati, della loro disponibilità e del loro stoccaggio essi ne sono completamente responsabili.

Il SIA **non garantisce** il ripristino dei dati dell'utente **gestiti al di fuori dei sistemi Informativi Aziendali**.

Per le UU.OO. che gestiscono in proprio i sottosistemi informatici, il backup deve essere eseguito quotidianamente su specifici supporti (nastri/cd-dvd) e gli stessi custoditi con cura, in ambienti protetti e preferibilmente diversi da quelli ospitanti i server contenenti le banche dati.

6.6 MISURE DI PROTEZIONE DAI VIRUS INFORMATICI, TROJAN-HORSE, SPYWARE, MALWARE

Al fine di prevenire le infezioni virali che potrebbero mettere a rischio la continuità operativa aziendale si adottano le seguenti misure:

1) Le PDL sono dotate di un adeguato software antivirale (Symantec Endpoint Protection –SEP) che automaticamente aggiorna le firme di definizione dei virus secondo le ultime disponibili su server aziendale;
2) I file server all'interno del confine aziendale sono dotati di software antivirale per la scansione dei documenti gestiti;
3) Ogni stazione di lavoro personale dotata di memorie di massa removibili – lettore di floppy disk e similari – che abbia strumenti di produttività personale e che mantenga documenti in locale è dotata di software antivirale.
4) Per quanto organizzativamente possibile ed appropriato, sono disabilitate sui server le funzionalità di *editor* e di *file transfer* a utenti non in possesso di credenziali di amministratore di sistema.
5) Qualora la PDL fosse sprovvista del software antivirale o fosse dubbio il suo funzionamento, si invitano gli utenti a contattare l'HELP-DESK del SIA (vedi 4.2) per le verifiche tecniche del caso, lo stesso dicasi nel caso in cui il software antivirale rilevi la presenza di virus che non è riuscito a ripulire.

Si invitano inoltre gli utenti, come specificato all'interno delle lettere di incarico, a seguire i seguenti comportamenti:

- massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione - dischetto removibile, nastro magnetico, disco magneto-ottico e ogni altro supporto di memorizzazione removibile (es. USB) - sia stato utilizzato su un computer diverso dal proprio - supponendo che il proprio PC sia immune da infezioni - occorrerà verificare l'assenza di virus mediante un programma antivirale aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato non sarà possibile utilizzare il supporto di memorizzazione - in quanto potenzialmente infetto -;
- in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte;
- è bene sempre evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure; nel caso pervenga un messaggio di tale natura procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri.

6.6.1 Le Principali Regole per limitare l'introduzione di virus sul PC

Ecco alcune utili regole di comportamento necessarie per ridurre il rischio d'introduzione dei *virus-worm-malware* all'interno della propria PDL e nella rete aziendale:

- Verificare la presenza del software antivirus aziendale accertandosi del suo corretto funzionamento;
- Effettuare le scansioni complete dei supporti rimovibili (es: pen USB, floppy, ecc..) tutte le volte che questi vengono connessi al sistema;
- Evitare l'installazione di programmi che non servono per la produttività e la cui provenienza non è ben nota;
- Prestare estrema attenzione agli allegati alle e-mail evitandone l'apertura qualora non siano preventivamente noti o comunque concordati i contenuti con il mittente del messaggio;
- Disabilitare le macro nei documenti o almeno trattarle con lo stesso sospetto dei programmi esterni;
- Prestare attenzione all'uso dei *files* crittografati o la cui estensione non è definita o conosciuta;
- Trattare con sospetto anche i file con estensioni mai viste o classificate come potenzialmente pericolose;
- Segnalare qualunque anomalia o comportamento sospetto all'indirizzo fornito al pag.8 cap.4.2.

7 POLICY AZIENDALE PER L'USO DEI SERVIZI/APPARATI IN RETE

7.1 USER ID E PASSWORD

L'accesso ai Servizi in Rete è subordinato al possesso di un identificativo (USER ID) da utilizzare associato ad una parola chiave personale (PASSWORD).
L'utilizzo combinato di USER ID e PASSWORD è quindi condizione necessaria per l'accesso ai servizi e per l'attivazione di una "sessione di lavoro".
L'attivazione dei Servizi in Rete è concessa su base personale ed esclusivamente per ragioni e finalità connesse ai compiti del dipendente titolare della USER ID: pertanto non e consentito cedere a terzi, neppure temporaneamente la "sessione di lavoro" o le informazioni necessarie ad attivarne una (USER ID+PASSWORD).
L'uso di USER ID e PASSWORD è strettamente personale per cui ogni attività non regolare verrà imputata nei limiti di legge al titolare delle stesse.
Gli utenti sono pertanto tenuti a non rivelare le proprie credenziali d'accesso avendo altresì cura che esse non vengano utilizzate in modo improprio. Gli utenti dovranno prontamente avvisare il SIA nell'ipotesi di smarrimento o anche solo di probabile diffusione presso terzi dei dati d'accesso.

E' vietato inoltre:

- Accedere abusivamente ai Servizi in Rete;
- Diffondere o detenere abusivamente password;
- Violare la sicurezza di archivi e computers;
- Connettere in rete apparati, pc fissi, pc portatili senza preventiva notifica al SIA che provvederà a verificare i requisiti e a stabilire le policy d'accesso ai servizi.

7.1.1 Password di prima attivazione e password personale

La PASSWORD di prima attivazione è comunicata dall'Azienda esclusivamente all'interessato, il quale é tenuto a cambiarla con una PASSWORD personale al primo collegamento. La PASSWORD personale è nota esclusivamente al titolare della USER ID collegata, deve essere custodita con diligenza ed attenzione e non deve essere comunicata a terzi, neppure temporaneamente.

7.1.2 Scelta della password personale

La PASSWORD personale è definita liberamente dal titolare nel rispetto dei seguenti requisiti:

- deve essere composta da almeno otto caratteri (lettere, numeri e caratteri speciali) diversi tra loro, nel caso in cui lo strumento non lo consenta la password deve essere comunque costituita dal numero massimo di caratteri consentito;
- non deve essere uguale alla USER ID, al nome o al cognome del titolare o sia comunque a lui facilmente riconducibile;
- non deve corrispondere a parole diventate di uso comune (es.:PIPPO,CICCIO,CIAO, CIELO,…);

Si rimanda al servizio di HELPDESK (vedi 4.2) per un eventuale supporto operativo per la gestione nel cambio della password personale.

Si ricorda che in ottemperanza a quanto stabilito in [4], il cambio password è obbligatorio ogni tre mesi (90gg.) per tutti gli accessi agli applicativi che trattano dati sensibili, tale intervallo si allunga a sei mesi nel caso si trattino dati personali.

7.1.3 Riattivazione della password

Nel caso il Sistema non riconosca la PASSWORD personale, è necessario contattare l' HELPDESK (così come in caso di dimenticanza della Password), che provvederà al ripristino della PASSWORD di prima attivazione, la modifica della password secondo necessità dell'utente deve essere eseguita in piena autonomia.

7.1.4 Casi particolari: dismissioni degli accessi

Come stabilito dal d.lgs 196/2003 "*Codice in materia di protezione dei dati personali*", all'interno dell'allegato B, art dal 33 al 36, relativamente alla gestione delle credenziali d'autenticazione :

> *7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.*
>
> *8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.*

Il vincolo normativo comporta che le credenziali personali per l'accesso agli applicativi aziendali e di posta elettronica vengono disabilitati quando sia i dipendenti che gli specialisti convenzionati, i collaboratori, i borsisti, gli incaricati a tempo determinato e tutto il personale che per qualsiasi motivo utilizza le piattaforme aziendali con credenziali personali cessa il rapporto di collaborazione con l'azienda per differenti motivi: collocamento a riposo, dimissioni, mobilità, termine incarico, ecc..

7.2 UTILIZZO DEI SERVIZI DI RETE

7.2.1 Internet

L'accesso ad Internet, attraverso la Rete Aziendale, è consentito per ragioni e finalità connesse ai compiti istituzionali del dipendente utilizzatore.

Quindi:

- è vietato l'utilizzo della rete internet per fini personali estranei all'attività lavorativa;
- È fatto divieto assoluto di scaricare programmi, o contenuti multimediali senza la previa autorizzazione del Responsabile I.T.;
- Non è consentita ogni genere di transazione finanziaria (acquisti/vendite on-line) e simili salvo casi direttamente autorizzati dalla Direzione Generale e con il rispetto delle normali procedure di acquisto;
- Gli utenti sono invitati a limitare al massimo il rilascio d'informazioni personali durante la navigazione via Web. L'utente è tenuto, nel corso della navigazione, a leggere con attenzione qualsiasi finestra, *pop-up* o avvertenza prima di proseguire nella navigazione stessa e in particolare prima di accettare qualsivoglia condizione contrattuale o di aderire ad iniziative online;
- Non è permesso l'uso della rete internet per attività ludiche;
- Non è permessa la partecipazione, per motivi non professionali, a forum, l'utilizzo di chat-line, di bacheche elettroniche e le registrazioni in *guest book* anche utilizzando pseudonimi (o *nickname*);
- Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza politica;
- Il SIA, su autorizzazione della Direzione Generale, ha facoltà di porre limiti alla navigazione internet escludendo dalla navigazione siti non attinenti agli scopi aziendali.
- E' tuttavia consentito (vedi [8]) l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro, ad esempio per effettuare adempimenti on-line nei confronti dei pubbliche amministrazioni e di concessionari di servizi pubblici ovvero per tenere rapporti con istituti bancari (*home-banking, remote-banking*) ed assicurativi, purché contenuto nei tempi strettamente necessati allo svolgimento delle transazioni.

Nel caso si verificasse la necessità di scaricare programmi o loro aggiornamenti dalla Rete (download), è necessario rivolgersi al SIA ed in ogni caso:

- Verificare il possesso dei necessari diritti d'uso;
- verificare la presenza sulla PDL dell' adeguato software antivirus aziendale (SEP);
- non violare regole di copyright od assimilabili.

Non potrà essere comunque fornito alcun supporto o consulenza sulle installazioni effettuate in violazione dei principi sopra enunciati.
Il "download" di documenti di dimensione considerevole può degradare significativamente le prestazione della Rete: si raccomanda di effettuare tali attività ad orari opportuni (all'inizio od al termine dell'orario di lavoro).
Esiste la possibilità tecnica di verificare l'utilizzo di Internet e, per assicurarne la funzionalità, l'Azienda si riserva il diritto di verificare, nei modi e nei fini consentiti dalla legge, le modalità di utilizzo di tale servizio.

7.2.2 Controlli

Premesso che l'Azienda potrebbe effettuare controlli generici sull'effettivo adempimento dell'attività lavorativa e il corretto utilizzo degli strumenti di lavoro si precisa quanto segue:

L'Azienda Ospedaliera "Carlo Poma" di Mantova per esigenze organizzative, di sicurezza, e di disponibilità dei servizi, può avvalersi legittimamente e nel rispetto dello statuto dei lavoratori (art. 4), di sistemi che consentono in maniera indiretta un controllo sulle attività di rete che potrebbero determinare un trattamento di dati nei confronti dei lavoratori.

Fermo restando che l'Azienda già adotta misure organizzativa e tecniche al fine di prevenire eventuali utilizzi impropri e distorti degli strumenti informatici (es. black-list, sistemi antivirus e anti spyware, sistemi intrusion prevention ecc.) gli accessi ad internet vengono comunque e per una questione di sicurezza dei sistemi centrali, registrati all'interno del sistema "firewall". L'accesso ai dati è consentito unicamente in prima battuta in forma aggregata, ovvero non è possibile individuare direttamente l'utente interessato. Nel caso in cui vengano ravvisate anomalie nel traffico dati o rischi alla sicurezza, l'Amministratore di sistema preposto invierà al Responsabile dell'area coinvolta un avviso generalizzato richiamando gli utenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite all'interno del presente documento. Solo in fasi successive e nei casi di reiterata violazione delle procedure, l'Azienda restringerà il campo di intervento ed effettuerà controlli prolungati e costanti fino ad arrivare all'analisi dei singoli file di log.
Gli stessi dati vengono conservati per un periodo di circa sei mesi e successivamente cancellati salvo esigenze tecniche o di sicurezza, se tali informazioni dovessero essere conservate, verranno giustificate tramite apposito verbale le finalità e comunque i limiti di tempo di conservazione.
Si precisa che l'adeguamento dei contenuti di black-list per l'accesso ad Internet avviene sulla base della codificazione dei gruppi e categorie individuate dalla soluzione *Fortigate* della società *Fortinet*, visibili al link:

http://www.fortiguard.com/webfiltering/webfiltering_info.html#dbcategories

I casi in cui si possono conservare i dati sono:

-Esigenze tecniche o di sicurezza particolari;

-indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria

-Obblighi su specifiche richieste dell'autorità giudiziaria

7.2.3 Posta Elettronica

La casella di posta elettronica, assegnata dall'Azienda all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
La comunicazione in forma elettronica, per scopi istituzionali, deve avvenire esclusivamente con l'utilizzo del sistema di posta elettronica dell'AO Carlo Poma di Mantova ovvero non sono consentiti l'utilizzo di comunicazioni effettuate da account differenti da quello aziendale riferito all'utente e o al servizio (esempio @libero.it, @virgilio.it,…).
Nel caso in cui un utente fosse sprovvisto di casella personale, esso è tenuto a contattare l'HELP-DESk al fine di colmare questa carenza.
L'indirizzo di posta elettronica personale dell'utente è così strutturato:

nome.cognome@asst-mantova.it

Ciascuna casella *email* viene fornita di una password di sola attivazione che l'utente avrà l'**obbligo** di modificare già dal suo primo accesso, per i dettagli tecnici dell'operazione di modifica contattare eventualmente l'HD del SIA o seguire le istruzioni riportate sul sito intranet aziendale al seguente link http://intra.poma.net/lay_not.php?IDNotizia=82418&IDCategoria=880 raggiungibile da sito intranet (http://intra.poma.net) Home → Chi Siamo → Direzione Strategica → Sistemi Informativi → POSTA ELETTRONICA: informazioni e configurazioni → NUOVA POSTA ELETTRONICA
Il SIA non risponderà nel caso vi siano stati accessi illegittimi a caselle di posta elettronica la cui password di attivazione non siano state opportunamente sostituita dall'intestatario della stessa come suggerito ai parr. 7.1.1 e 7.1.2.
La casella di posta elettronica aziendale è consultabile laddove vi è una connessione Internet unicamente in modalità web raggiungendo l'indirizzo https://webmail.asst-mantova.it (Outlook Web Access – OWA), a riguardo il SIA non fornisce alcun supporto tecnico nel caso si effettuassero accessi con Client di posta installati in autonomia.
Esistono tuttavia account condivisi associati a reparti, servizi, funzioni che vengono strutturati previo accordo con gli addetti del SIA.
Il servizio di posta elettronica è messo a disposizione degli utenti esclusivamente per attività connesse a fini istituzionali, esso è personale ed è vietato l'utilizzo della posta elettronica per scopi personali durante l'orario di lavoro; al di fuori dell'orario di lavoro e nelle pause ne è tollerato un utilizzo moderato. Tale utilizzo va effettuato utilizzando caselle nominative e non caselle di posta elettronica di tipo aziendale; è completa responsabilità dell'utente la conservazione della password d'accesso, della sua gestione e della sua modifica ad intervalli periodici.

Sono altresì previste apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza.

È vietato:

- Utilizzare altri sistemi di posta, anche se offerti gratuitamente (esempio IncrediMail) diversi rispetto agli strumenti standard aziendali (Webmail);
- Utilizzare le risorse informatiche per la comunicazione elettronica in modo anonimo o modificando la reale identità del mittente;
- Inviare a terzi, esterni all'Azienda, materiale di proprietà dell'Azienda Ospedaliera Carlo Poma di Mantova senza preventiva autorizzazione;
- Inviare messaggi o documenti con contenuti illeciti;
- Aderire o innescare "catene di Sant'Antonio";
- Rispondere allo spam o a email il cui mittente sia di dubbia natura;
- installare e/o configurare autonomamente account di posta elettronica alternativi e non direttamente riferibili all'azienda "Carlo Poma": nel caso ciò accadesse gli operatori del SIA non presteranno alcuna attività di supporto nella gestione di tali account e saranno abilitati alla loro rimozione previo avvertimento dell'utente;
- Inviare messaggi non pertinenti alle attività aziendali o comunicazioni non richieste (spamming);
- è vietato l'invio per posta elettronica di password o codici di accesso, credenziali e/o client VPN;
- Utilizzare il sistema di posta e l'indirizzo di posta elettronica, forniti dalla Società, a fini personali;
- Intercettare, impedire od interrompere comunicazioni di altri utilizzatori sulla Rete ed installare apparecchiature idonee a tale scopo.
- Nel caso in cui l'utente perdesse il diritto all'utilizzo della casella di posta elettronica aziendale ad esempio in seguito a cessazione della collaborazione, pensionamento, trasferimento, ecc.. la stessa verrà definitivamente disabilitata entro 60gg previa comunicazione (email) da parte del SIA e tutto il contenuto verrà automaticamente rimosso senza alcuna possibilità di recupero;
- Su richiesta scritta e motivata sarà concesso un *forward* verso altro account (non gestito dall'azienda ospedaliera) per un periodo di mesi tre, al termine dei quali l'account verrà definitivamente rimosso;
- Non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione e/o iscrizione a dibattiti, mailing-list, forum, bacheche elettroniche non attinenti l'attività istituzionale fatto salvo la preventiva autorizzazione da parte della Direzione.

Poiché la posta elettronica diretta all'esterno della rete aziendale è suscettibile di intercettazione da parte di estranei e talvolta malintenzionati non deve essere utilizzata per inviare documenti di lavoro riservati contenenti dati personali e/o sensibili, se tale necessità si manifesta si consiglia di attivare meccanismi di crittografia dei dati o di spedizione multiple al fine di ridurre i rischi derivanti dall'attività.

L'utilizzatore è responsabile della manutenzione della propria casella di posta elettronica ed avrà cura di:

- Controllate la posta regolarmente;
- Cancellare i messaggi non più utili;
- Non inviare messaggi contenenti dati personali e/o sensibili

Si ricorda inoltre:

- la documentazione ricevuta o inviata resta di proprietà aziendale;
- la Società si riserva di verificare, nei modi ed ai fini consentiti dalla legge, il rispetto delle modalità di utilizzo del servizio di posta, specificate in queste norme.

Va altresì ricordato che come espresso all'interno del documento [6]:

- Il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale.

Alla luce di quanto sopra esposto, qualora l'utente abbia le necessità di abilitare autorisponditori (ad esempio in caso di assenze prolungate per ferie o in seguito ad attività di lavoro fuori sede) esiste la possibilità di abilitare tali strumenti, per le operazioni del caso ci si riferisca all'HD del SIA al fine di essere guidati alla loro corretta e completa configurazione.

Ulteriori suggerimenti:

1. Si raccomanda inoltre di prevedere, ove ritenuto opportuno, mediante la funzione di inserimento automatico della firma in calce all'e-mail, la seguente avvertenza sulla Privacy e sulla confidenzialità dei messaggi inviati:

   " Questo messaggio è di carattere riservato ed è indirizzato esclusivamente al destinatario specificato. L'accesso, la divulgazione, la copia o la diffusione sono vietate a chiunque altro ai sensi delle normative vigenti, e possono costituire una violazione penale. In caso di errore nella ricezione, il ricevente è tenuto a cancellare immediatamente il messaggio, dandone conferma al mittente a mezzo e-mail. "
2. Si raccomanda agli utenti di prestare la massima attenzione nella stampa di messaggi di posta elettronica confidenziali, soprattutto nel caso si utilizzino delle stampanti di gruppo o accessibili a più persone.
3. Gli utenti sono tenuti sempre ad accertarsi che gli eventuali allegati dei propri messaggi siano "leggeri" ovvero non eccedano la dimensione massima di 10 Mb. Qualora si riscontrasse la necessità di allegare un file di dimensioni superiori è buona norma che il mittente si assicuri precedentemente con il destinatario sulla possibilità per lui di ricevere un messaggio di dimensioni maggiori.

7.2.4 Controlli

Anche nel caso dell'utilizzo della posta elettronica aziendale si veda quando espresso all'interno del cap. 7.2.2 Controlli.

7.2.5 Applicazioni

L'accesso alle applicazioni specifiche, attraverso la Rete Aziendale, é subordinato a diritti di accesso (ulteriori user ID/password) rilasciati dall'area informatica in base alle richieste di abilitazione dei diversi Responsabili di Ufficio/ Servizio. L'accesso alle applicazioni è concesso su base personale ed esclusivamente per ragioni e finalità connesse ai compiti del dipendente titolare: pertanto non e consentito cedere a terzi, neppure temporaneamente la "sessione di lavoro" e/o le credenziali d'accesso.

E' vietato:

- *Accedere abusivamente alle Applicazioni;*
- *Diffondere o detenere abusivamente password;*
- *Violare la sicurezza delle Applicazioni;*
- *Esportare dati dalle Applicazioni senza permesso;*

Le nuove abilitazioni, revoche e modifiche dei permessi di accesso alle Applicazioni, sono subordinate alle richieste dei singoli responsabili di Ufficio, Servizio, Dipartimento e U.O.. Le richieste devono necessariamente pervenire attraverso la compilazione dell'apposito modulo completo in tutti i campi previsti, ed opportunamente firmato.

8 PROGETTAZIONE E SVILUPPO DI NUOVE SOLUZIONI INFORMATIZZATE

8.1.1 Consulenza

Al fine di implementare sistemi aziendali interdipartimentali la cui conformità ai requisiti logici e fisici stabiliti ed individuati dal SIA siano salvaguardati e nell'ottica di garantire una continuità operativa necessaria per gli applicativi sanitari è vincolante ottenere la liberatoria all'implementazione delle soluzioni da parte del SIA già a partire dalle fasi progettuali; la progettazione e lo sviluppo di soluzioni che necessitino l'introduzione in azienda di apparati HW e soluzioni SW comporta la negoziazione delle specifiche in fase preliminare con gli esperti individuati dal responsabile dei Sistemi Informativi Aziendali.

Le specifiche da negoziare devono comunque riguardare i seguenti ambiti operativi:

1. Definizione delle competenze ed individuazione degli amministratori di sistema con nomina formale dei responsabili;
2. Individuazione delle responsabilità relativamente alla gestione della manutenzione;
3. Definizione delle caratteristiche connettività fisica e logica: protocollo, indirizzamento, definizione degli utenti;
4. Definizione degli standard (sistemi operativi, ecc.);
5. Definizione ed integrazione con gli eventuali sistemi aziendali;
6. Sicurezza informatica: *patching* ed antivirus aziendali

Relativamente al 3 si deve comunque sottolineare che qualunque PDL inserita sulla rete aziendale deve essere provvista di almeno un account con profilazione d'Amministratore per gli operatori del Servizio Informatico, in caso contrario, tali operatori saranno comunque autorizzati al distacco della stessa dalla rete aziendale al fine di tutelare il corretto funzionamento e la sicurezza dell'infrastruttura informatica.

9 FORNITURE DI HARDWARE E SOFTWARE

9.1.1 Acquisti

Qualunque acquisto di apparecchiatura hardware e software deve essere preventivamente concordata con il SIA al fine di poter dare parere tecnico sulla conformità rispetto alle attuali configurazioni ed integrazioni tra i sistemi.
Per ogni acquisto è comunque valida la normativa attualmente in vigore per le pubbliche Amministrazioni e le procedure in essere alla base del sistema gestionale amministrativo.
Ogni apparecchiatura hardware deve essere acquistata con una copertura di garanzia di almeno tre anni, on-site, next-day.
Per qualsiasi informazione siete pregati di inviare una comunicazione preventiva agli indirizzi forniti al par. 4.2 a pag. 8.

9.1.2 - Richieste di fornitura hardware

Saranno accettate unicamente richieste di fornitura di materiale hardware, non previste dalla gestione globale dei sistemi informativi aziendali, solo se accompagnate da motivazione e/o progetto nell'ambito del quale si rende necessario acquisire quanto indicato una volta che la copertura economica per l'acquisto sia garantita.
Le apparecchiature hardware, di qualunque genere nell'ambito informatico, non devono essere in contrasto con il regolamento SIA e della Sicurezza dei Sistemi Informativi.

10 RESPONSABILITÀ

I responsabili delle Unità Operative e/o Servizi Aziendali dovranno adottare misure idonee per un corretto utilizzo delle risorse informatiche messe a disposizione della loro struttura, esercitando una funzione di istruzione, indirizzo e controllo sugli utenti incaricati ed individuando con precisione le responsabilità per la gestione dei dati, dei salvataggi e delle risorse stesse.

In caso di cessazione del rapporto di lavoro, trasferimento ad altro servizio, o comunque di non necessità di utilizzo da parte di utenti già autorizzati, sarà data tempestiva comunicazione scritta, per gli applicativi da esso gestiti, al SIA che provvederà alla disattivazione delle credenziali di autenticazione ovvero alla loro modifica per ogni diversa esigenza.

Gli utenti che utilizzano le risorse informatiche si impegnano a rispettare il presente regolamento, ed in particolare:

a) Mantenere una adeguata riservatezza dei dati;
b) Mantenere una adeguata riservatezza sulle misure di sicurezza adottate e sulle modalità di accesso;
c) Utilizzare esclusivamente le risorse alla cui utilizzo essi sono abilitati;
d) Segnalare tempestivamente al SIA ogni malfunzionamento ed ogni accertata violazione delle norme che regolano l'utilizzo delle risorse informatiche;

Il SIA è responsabile della sicurezza, della funzionalità, della continuità operativa e del corretto impiego delle risorse informatiche centralizzate e della rete aziendale.

Non rientrano nelle proprie competenze la gestione e l'assistenza tecnica delle apparecchiature elettromedicali e dei sistemi informatici di quelle unità operative (Laboratorio Analisi, Radiologia, Centro Trasfusionale, Anatomia Patologica, etc.) che ospitano nelle loro sedi i server dedicati, rimane comunque mandatoria l'installazione su queste PDL e server del software antivirus aziendale SEP la cui installazione può essere effettuata contattando l'HELP-DESK del SIA.

La gestione e responsabilità di questi ultimi è demandata ai singoli direttori che provvedono ad assegnare agli utenti, da loro incaricati, le credenziali di autenticazione ed autorizzazione, verificano la corretta applicazione delle misure minime di sicurezza e che hanno rapporti diretti con le società fornitrici, con le quali l'Azienda ha provveduto a stipulare contratti di manutenzione ed assistenza tecnica anche con collegamenti da remoto. Per le postazioni personal computer "stand alone", ossia non collegate in rete, la responsabilità nell'applicazione delle misure minime di sicurezza è demandata all'utente finale ed al direttore dell'Unità Operativa/Sevizio che le ha in dotazione.

Va inoltre ricordato che poiché l'accesso agli applicativi aziendali è fornito tramite **account personale nominativo** protetto da **password personale** le eventuali controversie anche di natura legale che si potranno manifestare come conseguenza ad un utilizzo non congruo dello strumento saranno imputate direttamente all'utente possessore delle credenziali con le quali sono state compiute operazioni illecite.