ISTRUZIONE OPERATIVA DELLA PG20

REVISIONE N. 2 DEL 2 SETTEMBRE 2013

EMESSO DA:
Il RQA
Giuliana Mazzoleni

APPROVATO DA:
Il Responsabile SIA
Mario Tribbia

IL DIRIGENTE
SISTEMA INFORMATIVO STRATEGICO
DOTT. MARIO TRIBBIA

INDICE

SCOPO

La presente istruzione operativa definisce le norme d'uso della rete aziendale.
In particolare regola l'utilizzo appropriato di:

- PC Postazione di Lavoro (PdL),
- strumenti di posta elettronica, Lotus Notes e Posta Elettronica Certificata (PEC) istituzionale (per alcune specifiche funzioni di Lotus Notes si rinvia a IOIT08),
- servizio di navigazione Internet dalla rete aziendale.

CAMPO DI APPLICAZIONE

L'istruzione operativa si applica a tutti i dipendenti dell'ASL e ai medici convenzionati di Continuità Assistenziale (CA), in quanto titolari di una PdL SISS fornita da ASL.

RESPONSABILITÀ

La responsabilità generale é del Responsabile del SIA; la responsabilità operativa è del personale del SIA e di tutto il personale ASL, per quanto di competenza.

RIFERIMENTI E DOCUMENTI

Legge n° 300/70, aggiornata e modificata dalla legge n° 92/2012 "Statuto dei Lavoratori"
D.Lgs. n° 196 del 30.06.2003 "Codice in materia di protezione dei dati personali" (Legge sulla Privacy)

MODALITÀ OPERATIVE

Per garantire l'efficienza del sistema di comunicazione aziendale e di navigazione Internet e per tutelare l'immagine dell'ASL anche sotto il profilo legale (civile e penale) sono definite le modalità di:

1. Accesso ai servizi di rete;
2. Utilizzo della postazione di lavoro (PdL);
3. Utilizzo di specifici servizi di rete;
4. Indicazioni relative ai virus informatici;
5. Attività di controllo.

1. ACCESSO AI SERVIZI DI RETE

La richiesta di un identificativo aziendale e della relativa password va inoltrata al SIA dal Responsabile del servizio richiedente tramite l'applicativo Help Desk, cliccando il tasto "Inserisci richiesta credenziali di accesso" e la voce "RETE AZIENDALE – Account per Accesso".
L'accesso ai servizi di rete è subordinato al possesso di un identificativo aziendale (*account*) che si associa ad una parola chiave personale (*password*).
L'utilizzo combinato di *account* e *password* è condizione necessaria per accedere alla rete ed ai suoi servizi aziendali e per l'attivazione della "Sessione di lavoro".
L'attivazione dei servizi di rete è concessa su base personale ed esclusivamente per ragioni e finalità connesse ai compiti istituzionali del dipendente, titolare dell'*account:* pertanto non è consentito cedere a terzi, neppure temporaneamente la "Sessione di lavoro" o le informazioni necessarie ad attivarne una.
È fatto perciò divieto di detenere o diffondere abusivamente password e di accedere ai servizi di rete in modo abusivo.
L'IOIT06 "Gestione password di accesso a Client Windows" definisce la modalità di gestione della *password*.

2. UTILIZZO DELLA POSTAZIONE DI LAVORO (PdL)

Le postazioni di lavoro, da tavolo o portatili, sono dotate di dispositivo (hardware) e di programmi (software) tali da conformarsi agli standard aziendali e alle necessarie licenze d'uso. L'installazione e l'aggiornamento di dispositivo e programmi è di esclusiva competenza del personale SIA o delle Ditte esterne espressamente incaricate.
Si fa, conseguentemente

Divieto

1. di compromettere il funzionamento dei servizi di rete e degli apparecchi che li costituiscono con virus o programmi diretti a danneggiare od interrompere il sistema,
2. di distruggere, deteriorare o rendere inservibili programmi, informazioni o dati altrui,
3. di installare software,
4. di modificare il software o le sue configurazioni,
5. di asportare o copiare in parte o tutto il software,
6. di utilizzare le risorse aziendali (unità di disco, floppy, cdrom o dvd-rom ma anche i dispositivi mobili di archiviazione dati, rinvio a IOUQ15) delle PdL come desposito anche temporaneo di dati e/o programmi che nulla hanno a che fare con l'attività lavorativa (es.: foto, film, musica, contenuti digitali coperti da copyright ma non forniti dall'ASL). Lo stesso discorso si applica, a maggior ragione, alle risorse remote ("cartella personale" e eventuale "cartella condivisa" (rinvio a IOIT16 "File server ASL"),
7. di modificare, aggiungere o rimuovere dispositivi hardware,
8. di utilizzare dispositivi di comunicazione diversi da quelli di cui è dotata la PdL,
9. di disattivare il sistema antivirus,
10. di aprire sessioni di lavoro tramite modem da stazioni di lavoro connesse alla rete aziendale.

Il software "shareware" o "freeware" scaricabile da Internet è generalmente esente da licenza solo per uso amatoriale (privato). Il suo utilizzo su PdL appartenenti ad un ente è subordinato alla acquisizione della licenza d'uso (ricadono in questa categoria software molto comuni quali: screensaver, compressori, programmi di crittografia, ecc...).
Nel caso in cui risultasse necessario superare uno dei precedenti divieti è indispensabile segnalare tale esigenza, per scritto, al SIA.

Il SIA garantisce l'adozione degli apparati di difesa dalle intrusioni (Firewall) alle apparecchiature aziendali: i sistemi, che riguardano tanto l'hardware che il software, sono sempre attivi e si aggiornano automaticamente. Stesso discorso è valido per il sistema Antivirus.
Il SIA garantisce il ripristino del PC dell'utente (PdL) ed è tenuto al ripristino dei soli dati aziendali e non di quelli privati.

3. UTILIZZO DI SPECIFICI SERVIZI DI RETE

a. Internet

L'ASL si riserva la facoltà di bloccare l'accesso a siti ritenuti non consoni allo svolgimento dell'attività lavorativa o comunque non affidabili. A tal fine, il SIA ha istituito una "black list" sulla base della quale viene impedito a priori l'accesso a particolari indirizzi contenenti parole specifiche. La lista è parte integrante della configurazione del firewall aziendale Fortinet; viene costantemente aggiornata dal SIA.
Il dipendente non può accedere a Internet per perseguire scopi privati e/o vietati dalla legge ma solo per ragioni di lavoro al fine di raggiungere obiettivi di studio, ricerca e documentazione. Egli è considerato **direttamente responsabile** per:

1. un eventuale accesso illecito,
2. l'appropriazione indebita del materiale cartaceo utilizzato per stampare i risultati della navigazione,
3. il danneggiamento della rete aziendale a causa dei virus informatici introdotti (salvo il diritto dell'ASL di chiedere l'ulteriore risarcimento del danno).

Inoltre, poiché il *download* di documenti di grandi dimensioni può compromettere le prestazioni della rete, si raccomanda di effettuare tali attività in orari opportuni, preferibilmente all'inizio o alla fine dell'orario di lavoro.

b. Posta elettronica – Lotus Notes

La posta elettronica aziendale utilizza il sistema Lotus Dominio, che risiede su server di proprietà, posizionati all'interno della sala macchine ASL.
L'accesso alla posta elettronica può avvenire secondo due modalità:

- tramite Client Lotus Notes installato sul PC aziendale. Necessita di un file ID (tipicamente nel formato mbianchi.id) installato sul computer e di una *password*, fornita dal SIA ma modificabile dall'operatore stesso;
- tramite browser (es.: Internet Explorer), accedendo all'URL (indirizzo internet) fornito dal SIA, utilizzando nome utente e da un'ulteriore *password*.

Il dipendente titolare di una casella di posta elettronica aziendale (email) è responsabile della manutenzione della stessa. Il SIA, periodicamente, sensibilizza gli utenti sulla necessità di verificare la propria casella facilitandone le correzioni tramite comandi semplificati. Il personale SIA effettua il controllo sulla capacità del disco ASL inviando un messaggio ad ogni utente che si è scostato sensibilmente dai limiti di occupazione previsti.

Il dipendente deve avere cura di:

1. **garantire il presidio della mail,** controllando regolarmente la posta in arrivo e rimanendo nei limiti di occupazione previsti (1000MB) mediante la cancellazione dei messaggi non più utili.
   Per il controllo della casella di posta ci si deve posizionare sull'area "Area di lavoro – Lotus Notes", aprire la propria casella di posta e cliccare sulla voce "Allegati XL" del menù di sinistra. Vengono visualizzati tutti i messaggi maggiori di 5MB in ordine di dimensione. Questi messaggi vanno eliminati oppure, se l'allegato deve essere conservato, si deve archiviare nel proprio PC o sul disco Z;

2. **segnalare al SIA l'eventuale cambio o non utilizzo della mail** tramite l'applicativo Help Desk,

3. **conoscere le seguenti norme di utilizzo:**
   1. l'utilizzo della casella di posta aziendale per la ricezione o l'invio di messaggi personali è consentito ma tali messaggi devono essere raccolti in cartelle separate (cartella "Posta Personale");
   2. il sistema di posta elettronica dell'ASL non deve essere utilizzato per la creazione e la distribuzione di messaggi dal contenuto dannoso, pornografico od offensivo (commenti riguardanti la razza, il genere, le disponibilità l'età, gli orientamenti sessuali, i credo religiosi, le opinioni politiche, l'origine nazionale). Tali messaggi, quando ricevuti da altre mail ASL, vanno segnalati ai propri responsabili;
   3. se, per esigenze lavorative, viene utilizzata la posta elettronica per spedire o ricevere documenti contenenti dati sensibili (es.: dati sulla salute di assistiti citati nominalmente) va usata la massima cautela, evitato l'invio delle mail a destinatari esterni ASL o interni ASL ma non coinvolti nel processo di "Trattamento Dati sensibili" relativo (rinvio a IOAGLO6 "Regolamento per la gestione dei dati personali") e mantenuto il *file* nella propria mail, anche se inviato erroneamente;
   4. i dipendenti devono utilizzare la massima cautela nell'inviare messaggi dal sistema di posta elettronica dell'ASL verso reti esterne, accertandosi della titolarietà del destinatario e non comunicando mai dati sensibili o riservati (es.: password di accesso, strategie aziendali, informazioni sullo stato di salute, ecc...);
   5. i dipendenti ASL non possono, per fini lavorativi o personali, utilizzare da postazioni aziendali altri sistemi di posta elettronica, anche se ciò non comporta oneri diretti per l'ASL.

4. **osservare i seguenti divieti:**
   1. Vietato innescare o aderire a catene di Sant'Antonio o di avvenimenti legati a minacce relative a virus. Le comunicazioni relative all'avviso di virus, spam, spyware, ecc... sono di esclusiva competenza del SIA.
      I Referenti del Servizio di CA autorizzati provvederanno a eliminare di messaggi relativi a catene di S. Antonio, messaggi pubblicitari e spam giunti alle postazioni di CA;
   2. Vietato inviare a terzi esterni all'ASL materiale di proprietà dell'ASL di Bergamo senza preventiva autorizzazione da parte del responsabile del servizio.
   3. Vietato inviare messaggi non pertinenti alle attività aziendali o comunque comunicazioni non richieste (spamming);
   4. Vietato intercettare, impedire od interrompere comunicazione di altri utilizzatori sulla rete ed installare apparecchiature finalizzate a tale scopo;
   5. Vietato utilizzare la posta elettronica aziendale per l'invio di informazioni aziendali riservate all'esterno dell'ASL.

Si ricorda che la documentazione ricevuta o inviata resta di proprietà aziendale e che l'ASL si riserva di verificare, nei modi ed ai fini consentiti dalla legge, il rispetto delle modalità di utilizzo del servizio di posta elettronica.

c. **Posta elettronica – PEC Istituzionale (Posta Elettronica Certificata)**

Il servizio di PEC è fornito da Lombardia Informatica per conto della Regione Lombardia.
L'ente fornisce le credenziali ai richiedenti.
Sono stati identificati da AGL gli uffici che hanno diritto alla casella PEC.

Tale casella viene attivata su richiesta del Responsabile, che ne rimane titolare all'accesso, pur essendo il nome della casella definito per ufficio.
Per l'attivazione viene compilato il Modulo 5 bis Lisit PEC "Assegnazione casella".
È attualmente in uso la sola modalità "PEC Istituzionale". Al momento della creazione della casella e della consegna delle credenziali di accesso vengono forniti anche il manuale e le istruzioni operative.

4. INDICAZIONI RELATIVE AI VIRUS INFORMATICI

I dipendenti ASL devono astenersi da:

1. aprire o eseguire *file* o macro allegate a messaggi di posta elettronica di provenienza sconosciuta o sospetta (specialmente in lingua inglese). Vanno perciò eliminati tali messaggi;
2. scaricare *file* provenienti da fonti non sicure;
3. condividere dischi di memoria (a meno che non sussista imprescindibile esigenza di servizio);

I dipendenti sono invece tenuti ad eseguire regolarmente salvataggi dei dati importanti su CD-ROM e/o su DVD-ROM e/o sulla propria cartella nel server (disco Z).
Si rinvia alla IOIT09 per altre indicazioni relative alla protezione dai virus informatici.

5. ATTIVITÀ DI CONTROLLO

L'ASL si riserva la facoltà di verificare a livello informatico, per finalità di sicurezza e tutela del proprio patrimonio, l'esistenza di un comportamento illecito del dipendente nell'uso della PdL, nell'uso delle risorse di rete, nell'uso della posta elettronica e nell'accesso a Internet.
Le verifiche si svolgono nel rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dalla normativa vigente. Tali verifiche vengono svolte solo su richiesta della Direzione Aziendale ASL.

Sono verificati gli accessi a Internet e i tempi di connessione senza indagare sui siti oggetto di accesso, in ottemperanza a quanto previsto dal Garante della Privacy.
A seguito delle verifiche informatiche potrebbero essere raccolti dati personali che saranno trattati in modo lecito a secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza della finalità di tutela della sicurezza e del patrimonio.
Eventuali informazioni di natura sensibile potranno essere trattate dall'Azienda, se necessario, per far valere o difendere un diritto.

DOCUMENTAZIONE RICHIAMATA

IOIT06 "Gestione password di accesso a Client Windows"
IOIT08 "Lotus Notes – Funzioni di interesse aziendale"
IOIT09 "Utilizzo e aggiornamento del sistema antivirus"
IOIT15 "Computer portatili e dispositivi mobili di archiviazione dati"
IOIT16 "File server ASL"

IOAGLO6 "Regolamento per la gestione dei dati personali"

Modulo 5 bis Lisit PEC "Assegnazione casella"