SEUS – SICILIA EMERGENZA-URGENZA SANITARIA SCpA
Sede Legale: Via Villagrazia, 46 Edificio B - 90124 Palermo
Registro delle Imprese di Palermo
Codice Fiscale e Partita Iva. 05871320825

REGOLAMENTO AZIENDALE – rev.1 del 15.10.2014

PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI

Approvato dal Consiglio di Gestione con delibera del 20.03.2014

INDICE

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai personal computer, espone l'Azienda a rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e alla sua immagine.

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi a diligenza e correttezza, principi basilari nel rapporto di lavoro, la S.E.U.S. ScpA, ha adottato il presente regolamento per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti, anche inconsapevoli, possano innescare problemi o minacce alla sicurezza.

Il Regolamento aziendale di seguito riportato viene incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e contiene informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza informatica di tutta l'Azienda.

1. Ambito di applicazione

Il presente Regolamento è applicato a tutti i dipendenti della S.E.U.S. SCpA che utilizzano gli strumenti informatici aziendali.

2. Definizioni

Per sistema informatico si intende un insieme di computer, composti da hardware e software che elaborano dati e informazioni per restituire altri dati e informazioni utili.
Nello specifico, per hardware si intende tutto ciò che è palpabile e visibile (Personal Computer; notebook; stampanti; server).
Software è invece, un termine utilizzato per definire i programmi necessari a far funzionare la macchina o lo strumento (ovvero l'hardware). Sono Software sia i sistemi operativi (es. Windows) sia le applicazioni o i programmi (es. excel).

3. Utilizzo del Personal Computer

I Personal Computer (PC) sono strumenti di lavoro; i PC fissi sono assegnati agli uffici mentre i PC portatili, i tablet e gli Ipad sono affidati al dipendente. Ogni dipendente deve avere un suo login sul sistema operativo. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato se può determinare disservizi, costi di manutenzione e minacce alla sicurezza.
Il PC deve essere spento ogni sera prima di lasciare gli uffici, o in caso di assenze prolungate dall'ufficio. Le informazioni archiviate informaticamente devono essere quelle previste dalla legge o necessarie all'attività lavorativa.
Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È, infatti, assolutamente da evitare un'archiviazione ridondante sui client (es. PC).
La tutela della gestione locale di dati su stazioni di lavoro personali (PC che gestiscono localmente documenti e/o dati) è demandata all'utente finale che dovrà eseguire, ove non previsto diversamente, con frequenza al più settimanale, copie di backup dei dati presenti nel proprio PC su supporti di rete o su supporti rimuovibili (Pen drive, CD, DVD ecc.) curando in tal caso la conservazione degli stessi in luoghi aziendali idonei. Ogni utente dovrà inoltre verificare il buon esito della copia provando a campione il ripristino di file dalla copia al PC.
È comunque vietato l'installazione di programmi diversi da quelli autorizzati e la riproduzione o la duplicazione di programmi informatici ai sensi della legge n. 128 del 21.05.2004. Non si possono memorizzare file non pertinenti l'attività produttiva. L'utilizzo di tali indispensabili risorse informatiche deve avvenire nell'ambito dei doveri di diligenza, fedeltà e correttezza che devono caratterizzare l'operato del lavoratore all'interno del rapporto di lavoro, in modo che siano adottate tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non avveduto degli strumenti in questione può provocare. L'inosservanza è passibile di sanzione penale e/o disciplinare.
Gli operatori dell'Ufficio ICT possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

4. Utilizzo del Notebook

L'utente è responsabile del Notebook assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.
Ai Notebook si applicano le regole di utilizzo previste per i PC connessi in rete.
I Notebook utilizzati all'esterno (convegni, trasferte) devono essere custoditi in luogo protetto.
Il Notebook non deve mai essere lasciato incustodito e sul disco devono essere conservati solo i file strettamente necessari.
E' necessario collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'anti virus ed eventuali sistemi di backup.

5. Utilizzo della Rete Aziendale

È vietato utilizzare la rete aziendale per fini non espressamente autorizzati.
È vietato monitorare ciò che transita in rete.
È vietato connettere in rete apparati non aziendali, ivi compresi tablet e smartphone, se non dietro esplicita e formale autorizzazione.
E' vietato usare la rete e le attrezzature aziendali per memorizzare e/o scambiare materiale non pertinente le attività lavorative, a maggior ragione se questo materiale è protetto da copyright (MP3, film in DivX o DVD, software commerciale, ecc…) ciò è vietato per legge e soggetto a sanzioni penali.

6. Utilizzo della E-mail aziendale

La casella di posta, assegnata dalla Società all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse (art. 615 comma 5 e segg. c.p.).
La "personalizzazione" dell'indirizzo anche se nominativo (es. nome.cognome@118sicilia.it) non comporta la sua "privatezza", in quanto trattasi di strumento di esclusiva proprietà aziendale, messo a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.
Il sistema di posta non è concepito per costituire un "archivio" delle mail ricevute e inviate, pertanto la casella di posta deve essere mantenuta "in ordine", cancellando documenti inutili e soprattutto allegati ingombranti. In caso di email importanti da conservare si deve fare ricorso all'archiviazione in locale della posta.
Nel caso in cui si debba inviare un documento sia all'interno sia all'esterno della Società, è preferibile utilizzare un formato protetto da scrittura e effettuare eventuali scansioni ponendo attenzione alla risoluzione, al colore..etc..In caso di invio di file pesanti si prega di utilizzare i formati compressi (ad es. zip).
E' importante limitare il numero dei destinatari allo stretto indispensabile; è sconsigliato, inoltre, l'inserimento di destinatari in "copia conoscenza riservata". Limitare anche l'utilizzo della ricevuta di ritorno e l'utilizzo della funzione "risposta con cronologia".

Nel caso in cui si debba rispondere con cronologia, eliminare gli allegati presenti nella e-mail ricevuta.
Si deve anche evitare che la diffusione incontrollata di “Catene di Sant’Antonio” (messaggi a diffusione capillare e moltiplicata) limiti l’efficienza del sistema di posta.
Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.
Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.
E’ vietato inviare messaggi offensivi o utilizzare linguaggio scurrile, tramite posta elettronica.
L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

7. Utilizzo dei telefoni aziendali (fissi e mobili)

Il telefono è uno strumento di lavoro, pertanto deve essere utilizzato solo per fini professionali. L’utilizzo per fini personali è consentito solo nel caso di necessità ed urgenza.
L’utente cui è assegnato un cellulare aziendale è responsabile del suo utilizzo e della sua custodia.
Si consiglia di limitarne l’uso alle comunicazioni urgenti e di contenuto breve, oppure nei casi in cui è utile un confronto professionale dialettico per prendere una decisione. In tutti gli altri casi si consiglia di utilizzare la posta elettronica aziendale. In particolare quando si deve fornire un’informazione, oppure formulare una domanda che non richiede una risposta urgente. L’e-mail, infatti, rappresenta spesso lo strumento più efficace nella comunicazione aziendale, poiché consente di esporre in modo diffuso, ordinato e completo gli argomenti, non determina interruzioni nelle attività del destinatario e fornisce informazioni consultabili anche successivamente.

8. Utilizzo dei Software aziendali

Tutti i Software installati sui PC aziendali rappresentano uno strumento di lavoro, pertanto è vietato ogni utilizzo non inerente all’attività lavorativa che può determinare disservizi e costi di manutenzione.
Non è consentita l’installazione o la duplicazione di software non coperti da regolare licenza.
Non è consentita l’installazione di software “open source” non soggetti a licenza d’uso, senza autorizzazione.
Non è consentita infine, l’inibizione o la sospensione, anche temporanea, del funzionamento del software antivirus installato.

9. Navigazione sul Web

Il PC abilitato alla navigazione in internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.
È assolutamente vietata la navigazione in internet per motivi diversi da quelli strettamente legati all’attività lavorativa stessa.

Non possono essere utilizzati modem privati per il collegamento alla rete.
I software gratuiti (freeware) e shareware prelevati da siti internet possono essere scaricati solo su specifica autorizzazione da parte dell'Ufficio ICT.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat-line (esclusi gli strumenti autorizzati), di bacheche elettroniche, le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
È vietato accedere ai social network, quale ad esempio, Facebook tranne se non sia legato a esigenze di lavoro.

10. Gestione delle Password

L'utente è tenuto a conservare nella massima segretezza le password di accesso e qualsiasi altra informazione legata al processo di autenticazione.
Le password, quando previste dal sistema di autenticazione, devono essere composte da almeno otto caratteri alfanumerici ed è consigliabile l'utilizzo di caratteri speciali oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
È opportuno fare in modo che le password non contengano riferimenti agevolmente riconducibili all'utente.
Le password devono essere modificate immediatamente nel caso si sospetti che le stesse abbiano perso la segretezza. In ogni caso devono essere modificate almeno ogni tre mesi.
Copia della password va consegnata in busta chiusa datata e con il riferimento all'utente e al codice macchina (es ID 54) al proprio responsabile che ne cura la custodia, al fine di consentire, in caso di assenza dall'ufficio prolungata, l'accesso all'archivio di posta ed ai dati aziendali.
Nella fattispecie per quanto riguarda la gestione delle password di accesso, essendosi dotata l'azienda di Documento Programmatico sulla Sicurezza e relativo manuale, si rimanda alla lettura dei seguenti punti:

Dal DPS:

- 4A7: misure di prevenzione e protezione; tabella: misure fisiche e logistiche: registrazione e autenticazione accessi.
- 4A10: misure di sicurezza suppletive.

Dal manuale:

- Pag 9, 04, c

Inoltre, vengono esposte precisamente le modalità di gestione nella lettera di nomina per incaricato al trattamento che ogni dipendente amministrativo ha dovuto sottoscrivere.

11. Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale di virus o di qualsiasi altro software aggressivo (es. non aprire mail o relativi allegati sospetti, non navigare su siti non professionali).

Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale.
Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito a pulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il PC e segnalare l'accaduto all'Ufficio ICT.
Fermo restando che l'utilizzo di supporti removibili personali sono vietati, ogni dispositivo di archiviazione di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso sia rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.

12. Risorse Condivise

Si definisce risorsa condivisa tutto ciò che può essere utilizzato da uno o più utenti, quali: Stampanti, Fax, Server, Stampanti, Spazio Disco.
Per l'utilizzo di ognuna di queste risorse condivise valgono le regole del buon senso: ogni utilizzo non inerente all'attività lavorativa può contribuire a innescare disservizi e costi di manutenzione.
Non è consentito ai singoli modificare le caratteristiche impostate previa autorizzazione esplicita.
E' opportuno evitare di inviare per fax documenti in chiaro contenenti dati sensibili se non si è certi della presenza del destinatario sul luogo di ricezione. In caso contrario è opportuno comunicare un codice identificativo del soggetto interessato e quindi di inviare la copia della documentazione contrassegnata dal codice, senza il nominativo dell'interessato.

13. Furti, smarrimenti e danneggiamenti dei Notebook e accessori

In caso di furto o smarrimento si dovrà fare la denuncia alle autorità competenti e avvisare l'Ufficio ICT, al quale dovrà essere inviata una copia della denuncia.
In caso di danneggiamento si dovrà informare l'Ufficio ICT ed inviargli il Notebook.
L'Ufficio ICT valuterà i danni, effettuerà, se possibile, il back up dei dati e provvederà a sostituire o riparare la macchina.

14. Non osservanza della normativa aziendale

L'ufficio preposto al controllo e alla vigilanza è l'ICT.
Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari previsti dal CCNL (richiamo verbale, scritto, multa, sospensione dal lavoro e dalla retribuzione, licenziamento) nonché con le azioni civili e penali previste dalle leggi e di seguito riportati.
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Ufficio ICT.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

NORMATIVA

Legge 22 aprile 1941, n. 633, articoli 171, 171 bis e 171 ter.
Allegato B al D. Lgs. 196/03 Disciplinare tecnico in materia di misure minime di sicurezza.
Cod. Penale:
- **Art.594:** Ingiuria
- **Art.595:** Diffamazione
- **Art.600 ter:** Pornografia minorile
- **Art.600 quarter:** Detenzione di materiale pornografia
- **Art.600 quater bis:** Pornografia virtuale
- **Art.600 sexies:** Circostanze aggravanti ed attenuanti
- **Art.600 septies:** Confisca e pene accessorie
- **Art.615 ter:** Accesso abusivo ad un sistema informatico o telematico
- **Art.615 quarter:** Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- **Art.615 quinques:** Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- **Art.617 quarter:** Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- **Art.617 quinquies:** Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche.
- **Art.617 sexies:** Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche
- **Art.618:** Rivelazione del contenuto di corrispondenza
- **Art.635 bis:** Danneggiamento di informazioni, dati e programmi informatici
- **Art. 635-quater c.p**. (Danneggiamento di sistemi informatici o telematici)
- **Art.640:** Truffa
- **Art.640 ter:** Frode informatica