REGOLAMENTO SULL'UTILIZZO DELLE RISORSE INFORMATICHE

Sommario

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, SO.RI SpA intende adottare un **Regolamento Informatico,** allegato al MOG 231, diretto ad evitare che comportamenti, anche inconsapevoli, possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

1. UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
Si dispone pertanto che tutto il personale usi la massima cura nella gestione delle apparecchiature informatiche di cui è responsabile e si attenga rigorosamente alle seguenti disposizioni:
1. Le apparecchiature informatiche devono essere utilizzate solo per scopi aziendali e non privati;
2. Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Responsabile IT, in quanto sussiste il grave pericolo di importare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore; in particolare, installando programmi cosiddetti "di rete" senza le necessarie verifiche di compatibilità, è possibile compromettere il funzionamento del server, dei database ivi contenuti e/o della rete stessa.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile IT di SO.RI SpA.
L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore; in merito si precisa che anche il software freeware spesso è tale solo per uso personale e non aziendale e pertanto soggetto a licenza d'acquisto.

3. I Personal Computers e i loro componenti (stampanti, casse, CD software etc.) devono essere custoditi con cura unitamente alla documentazione con cui originariamente sono stati consegnati;
4. La postazione di lavoro e le relative periferiche, quali stampanti locali e di rete, scanner, ecc.., devono essere spente al termine dell'attività lavorativa o in caso di assenze prolungate dall'ufficio. Eventuali eccezioni dovranno essere formalmente autorizzate dal Responsabile IT. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso; pertanto l'utente, ogni qualvolta si allontani dalla propria postazione, deve procedere al blocco della macchina mediante la pressione contemporanea dei tasti CTRL+ALT+CANC seguita da INVIO. Il ripristino della stessa avverrà soltanto attraverso l'immissione della password di accesso a client;
5. Gli utenti autorizzati ad accedere alla rete pubblica INTERNET possono farlo solo per scopi legati alla produttività aziendale;
6. E' assolutamente vietato scaricare da Internet dati, immagini, video e/o programmi non strettamente correlati all'attività lavorativa.
7. E' cura degli utilizzatori provvedere alla archiviazione periodica dei dati (non dei programmi): si sottolinea che i dati sono di proprietà aziendale e non personale e che la perdita degli stessi può causare grave danno alla Azienda la cui responsabilità ricade sull'utilizzatore.
8. Non è consentito all'utente modificare le caratteristiche di sistema (nome computer, indirizzi IP, DNS, Firewall, aggiornamenti automatici SW, etc.) preimpostate sul proprio PC, salvo previa autorizzazione esplicita del Responsabile IT;
9. Non è consentito connettere alla rete aziendale Personal Computer aziendali o di terzi in maniera autonoma non autorizzata dall'Ufficio Informatico; l'inosservanza di tale norma può essere causa di gravi rischi alla sicurezza e alla funzionalità aziendale;
10. Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, cellulari, lettori mp3, ecc. …), se non con l'autorizzazione espressa dell' Ufficio Informatico;
11. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile IT nel caso in cui vengano rilevati virus.

2. GESTIONE DELLE PASSWORD

Si dispone che l'accesso ai computers e ai programmi (applicativi) avvenga solo attraverso l'utilizzo di parole chiavi riservate: PASSWORD.
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema;

devono essere composte da almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato In particolare, si raccomanda di usare, preferibilmente, nella composizione della password almeno un carattere numerico, uno maiuscolo e uno speciale e non basarla su informazioni facilmente deducibili, quali il proprio nome, il nome dei famigliari, la data di nascita, il codice fiscale e simili.

- ➔ non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;
- ➔ non trascrivere la password su supporti (es. fogli, post-it) facilmente accessibili a terzi;
- ➔ non utilizzare le cosiddette "password di gruppo", ovvero generalizzate per area o mansioni di appartenenza, neanche qualora siano Responsabili d'area/servizio o Direttori/Dirigenti a richiederlo. Il lavoro dell'area deve prescindere dai dati contenuti nelle singole macchine; per lo scambio dei dati non contenuti in database sono infatti disponibili apposite cartelle di scambio sul server, accessibili dalla rete e personalizzate per gruppo di appartenenza.

La segretezza delle password utilizzate deve essere custodita dall'incaricato con la massima diligenza e non divulgata.
La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Parole chiave, identificato nel Responsabile IT, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o persona dalla stessa incaricata (Responsabile, responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali).
È necessario procedere alla modifica della password a cura dell'utente del sistema al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, d.lgs.vo n. 196/2003) con contestuale comunicazione al Custode delle Parole chiave (Responsabile IT).
Al fine di evitare la dimenticanza delle stesse o la impossibilità di accesso ai sistemi per mancanza temporanea dell'utilizzatore, le password di accesso al sistema e a ogni applicativo autorizzato devono essere consegnate, in busta chiusa controfirmata su lembi dall'utilizzatore del P.C, al "**Custode delle parole chiave"** presso l'ufficio del Responsabile IT; sulla busta deve essere indicato il nome del P.C. cui fa riferimento, il nome dell'utilizzatore e la data di consegna; all'interno della busta deve essere contenuto l'elenco degli identificativi (UserId) e delle parole chiave (password) utilizzate per ogni programma (applicativo) utilizzato.

Ad ogni modifica delle password le buste devono essere aggiornate e depositate presso l'Ufficio del Responsabile IT.
Non è consentita l'attivazione della password firmware di accensione (bios-setup), senza preventiva autorizzazione da parte dell' Ufficio del Responsabile IT.
Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.
Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere a SO.RI SpA, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento.
L'incaricato al suo rientro troverà aperta la busta a suo tempo consegnata al Custode delle parole chiave e dovrà modificare le password utilizzate.

3. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, DVD, penne USB, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

4. UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, attività di lavoro fuori sede), in caso di allontanamento,devono essere custoditi in un luogo protetto.

5. USO DELLA POSTA ELETTRONICA

La casella di posta, 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.

È fatto divieto di utilizzare le caselle di posta elettronica aziendale nome.cognome@sori.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per SO.RI SpA deve essere visionata od autorizzata dal Presidente del CdA, in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali oppure della posta elettronica certificata (PEC).
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche (o di Sant' Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Responsabile IT per poi procedere all'eliminazione degli stessi. Non si devono in alcun caso attivare gli allegati di tali messaggi.

5.1. Disponibilità dei messaggi di posta elettronica.

Il personale di SO.RI SpA, in caso di assenza programmata (ad es. per ferie o attività di lavoro fuori sede), deve adottare le misure organizzative più idonee ad assicurare la corretta gestione dei messaggi necessari al normale svolgimento dell'attività lavorativa ed alla conseguente continuità della stessa.
SO.RI SpA mette a disposizione di tutti i lavoratori apposite funzionalità di sistema che consentono di impostare un messaggio di risposta automatica (Out of Office Replay). In caso di assenza programmata, l'utente quindi è tenuto ad attivare i messaggi di risposta automatica che comunicano l'assenza dell'utente e devono contenere i riferimenti (sia elettronici che telefonici) di Uffici e/o utenti cui rivolgersi in caso di necessità.

Nel caso, invece, di eventuale assenza improvvisa e/o prolungata (ad es. per malattia) ed il lavoratore non possa attivare la procedura sopra descritta, SO.RI SpA si riserva la possibilità di attivare analogo accorgimento, avvertendo gli interessati.
Nel caso in cui si preveda la 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 o di altri dati aziendali che siano nella esclusiva disponibilità del dipendente (es. file.PST.), il Responsabile di Area

a cui fa capo l'utente, in qualità di fiduciario, può richiedere al Responsabile IT che venga effettuato il reset della password dell'utente stesso. Di tale attività deve essere redatto, a cura del suddetto Responsabile, apposito verbale e deve essere informato l'utente interessato alla prima occasione utile in modo tale da metterlo in condizione di cambiare la password.
L'utente, qualora lo ritenga opportuno, può disporre che il fiduciario sia una persona diversa dal Responsabile di Area/servizio, dandone comunicazione formale all'Ufficio del Responsabile IT, Responsabile in materia di Privacy.

5.2. Attività di Verifica.

A cura del Responsabile del trattamento dei dati (Presidente CdA) e dell'amministratore del sistema (Responsabile IT) sono periodicamente attivati controlli, anche a campione, al fine di verificare la funzionalità e sicurezza del sistema e garantire l'applicazione del regolamento.

6. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile IT.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione (Presidente CdA) e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

6.1. Attività di Verifica.

A cura del Responsabile del trattamento dei dati (Presidente CdA) e dell'amministratore del sistema (Responsabile IT) sono periodicamente attivati controlli, anche a campione, al fine di verificare la funzionalità e sicurezza del sistema e garantire l'applicazione del regolamento.

7. CESSAZIONE DEL RAPPORTO DI LAVORO.

In caso di cessazione del rapporto di lavoro, l'utente deve mettere a disposizione di SO.RI qualsiasi risorsa assegnata, sia le attrezzature informatiche sia le informazioni di interesse aziendale:

- la casella di posta elettronica individuale sarà mantenuta attiva per il tempo strettamente necessario a gestire il passaggio di consegne e concludere eventuali contatti aperti.
- l'utente non può cancellare le informazioni di interesse aziendale presenti sulle postazioni di lavoro e/o sulla rete, senza esplicita autorizzazione del Responsabile di Area/Servizio.
- qualora l'utente abbia inavvertitamente lasciato sulle postazioni di lavoro e/o sulla rete informazioni di interesse non aziendale, le stesse verranno cancellate senza alcuna responsabilità per SO.RI SpA.

8. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nel DPS aziendale.

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

9. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione (Presidente CdA) di concerto con l'Organismo di Vigilanza.

Il presente Regolamento è soggetto a revisione periodica con frequenza annuale o estemporanea allorquando se ne presenti la necessità.

Il Presidente del CdA