GESENU S.p.A.

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

Adottato dal Consiglio di Amministrazione con delibera del 25 Maggio 2009

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

1. MODALITA' PER UN CORRETTO UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

La progressiva diffusione di nuove tecnologie informatiche espone GESENU S.p.A. e le società del Gruppo GESENU (di seguito congiuntamente definite come l'"**Azienda**") a rischi di un diretto coinvolgimento vuoi di natura patrimoniale che penale, creando al contempo concrete problematiche di immagine e sicurezza.

Ed è proprio a quest'ultimo fine che l'Azienda ha inteso provvedere con riferimento, in particolare: (i) alle misure di sicurezza imposte per il trattamento di dati personali dal d.lgs. 30 giugno 2003, n. 196, e (ii) a quelle introdotte dall'art. 7 della Legge 18 marzo 2008, n. 48, recante disposizioni di "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*", mediante l'art 24-bis del decreto legislativo 8 giugno 2001, n. 231 che estendono la responsabilità amministrativa degli enti ai seguenti reati informatici, (oltre quello già previsto di frode informatica in danno dello Stato o di altro ente pubblico ex art. 640-ter c.p.):

- falsità in un documento informatico (art. 491-bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.);

a dare idonee indicazioni ed istruzioni a tutto il personale interessato dalle predette misure mediante la predisposizione del presente Regolamento per l'utilizzo dei sistemi informatici aziendali (il "**Regolamento**").

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.

2. UTILIZZO DEI SISTEMI INFORMATICI AZIENDALI

Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto:

- tali strumenti devono essere custoditi in modo appropriato adottando le precauzioni necessarie ad evitare il furto del materiale ICT messo disposizione dal datore di lavoro. Quest'ultimo è responsabile delle metodologie per la tutela del materiale informatico.
- tali strumenti possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali, tantomeno per scopi illeciti;
- debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti;
- qualunque anomalia riscontrata nel funzionamento del sistema informatico deve essere tempestivamente segnalata al proprio responsabile e/o all'Ufficio IT ove esistente.

Ai fini sopra esposti sono, quindi, da evitare atti o comportamenti contrastanti con le predette indicazioni e con quelle di seguito rappresentate.

3. UTILIZZO DEL PERSONAL COMPUTER

Onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dall'Amministratore Delegato. Inoltre:

- non è consentito l'uso di programmi non distribuiti ufficialmente dall'Azienda (si veda in proposito, gli obblighi imposti dal d.lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del *software* e dalla l. 18 agosto 2000, n. 248, contenente norme di tutela del diritto d'autore);
- non è consentito utilizzare strumenti *software* e/o *hardware* atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito modificare le configurazioni impostate sul proprio PC;
- non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio i modem);
- sui Pc dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi, *file* audio o musicali, se non a fini prettamente lavorativi.
- non è consentita la visualizzazione e il salvataggio di testi, immagini o registrazioni a carattere razzista, erotico, pornografico, sessuale, osceno o di natura simile indipendentemente da quale ne sia la fonte (es. port USB, CD, DVD).

4. UTILIZZO DI SUPPORTI MAGNETICI

Non è consentito scaricare *file* contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

Tutti i *file* di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dei rispettivi responsabili gerarchici.

5. UTILIZZO DELLA RETE AZIENDALE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque *file* che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

L'Azienda si riserva la facoltà di procedere alla rimozione di ogni *file* o applicazione che riterrà essere pericoloso per la sicurezza del sistema ovvero acquisito o installato in violazione del presente Regolamento.

6. UTILIZZO DELLA RETE INTERNET E DELLA POSTA ELETTRONICA

Navigazione in Internet:

- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente
- non è consentita 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 e con il rispetto delle normali procedure di acquisto;
- non è consentito lo scarico di software gratuiti (*freeware*) e *shareware* prelevato da siti Internet, se non espressamente autorizzato;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- 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 *nicknames*);
- non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

Posta elettronica:

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa (contenenti testi, immagini o registrazioni a carattere erotico, pornografico, sessuale, osceno, ecc.) e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- i messaggi e-mail inviati in seno all'azienda sono confidenziali e non possono essere inoltrati al di fuori della stessa o ad altri utenti a meno che non debbano essere comunicati per motivi professionali e che il destinatario possa essere qualificato come persona competente;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e dunque, non deve essere usata per inviare documenti di lavoro "strettamente riservati". Lo stesso vale per i documenti in arrivo, per i quali è preferibile richiedere l'invio tramite corriere, con ricevuta o voucher, potendo garantirne la ricezione tramite firma;
- per ogni comunicazione - interna ed esterna - che abbia contenuti rilevanti o contenga impegni per l'Azienda si deve fare riferimento alle procedure in essere per la corrispondenza ordinaria;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione;
- l'aggiunta di una garanzia "*disclaimer*" alla fine dei messaggi e-mail inviati fuori dall'Azienda è obbligatoria; questa deve essere allegata automaticamente a tutte le e-mail in uscita;
- non è consentito l'invio automatico di e.mail dall'indirizzo privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare il messaggio "*Out of Office*" facendo menzione di chi, all'interno dell'azienda, assumerà le mansioni durante l'assenza;
- è consentita la consultazione dei dati dell'Azienda da casa, utilizzando i servizi di "remote access" (accesso a distanza) eventualmente fornito dall'Azienda;
- i messaggi elettronici in entrata vengono sistematicamente analizzati nella ricerca di virus. Un messaggio contenente un virus viene automaticamente eliminato; il mittente ed il destinatario ne sono avvisati attraverso un messaggio specifico;
- non è attribuita ai destinatari alcuna responsabilità per i messaggi ricevuti quando gli stessi non sono stati sollecitati. Per contro, nell'ipotesi in cui i messaggi, contravvenendo al presente Regolamento, fossero inviati a più riprese da un utente, il destinatario deve prendere le misure appropriate affinché l'invio di tali messaggi venga interrotto;
- sono vietati i tentativi di accesso a messaggi elettronici di utenti o terzi;
- è vietato inviare posta elettronica a nome di un altro utente, salvo sua espressa autorizzazione;
- non è consentito l'invio di messaggi a gruppi numerosi di persone (> 100 persone) senza la preventiva autorizzazione scritta del proprio responsabile gerarchico;
- per non mettere in pericolo la disponibilità della rete, l'invio e la ricezione di messaggi voluminosi sono automaticamente limitati. Tutti gli allegati a un messaggio elettronico in entrata o in uscita da Internet che superi i 25MB, così come tutti gli allegati auto-eseguibili, ovvero con estensione "Executive" (.exe)

saranno eliminati. Nel caso in cui l'utente avesse necessità di inviare o di ricevere regolarmente messaggi più pesanti del limite previsto, dovrà contattare l'IT.

7. SICUREZZA E DISPONIBILITA' DEI DATI E DEI SISTEMI

Password e Log-in

L'Azienda assegna ad ogni utente una Password ed un *User-ID*. L'Azienda farà tutto il possibile per mettere a disposizione dei nuovi assunti una password ed un *User-ID* nel minor tempo possibile.

Lo *User-ID* permette di identificare l'utente all'interno del sistema informatico in modo specifico.

La Password è personale e non può essere comunicata ad altre persone.
E' severamente vietato usare la password e lo *User-ID* di un altro utente.

Sicurezza dei dati e dei sistemi

Qualunque utente che acceda al sistema informatico della Società, indipendentemente dalla modalità, è responsabile dell'uso che fa di tale sistema, in conformità con il presente Regolamento.

Le postazioni di lavoro informatiche non possono essere abbandonate per lunghi periodi senza che siano protetti gli accessi alle applicazioni (*Control-Alt-Canc/Lock Computer*).

E' severamente vietata la diffusione di informazioni confidenziali relative all'impresa ad uno o più utenti, clienti o terzi, a meno che tale diffusione sia debitamente giustificata da motivazioni di carattere professionale.

Disponibilità dei dati durante i periodi di assenza

Per poter garantire la continuità del servizio, ove si consideri necessario ed entro i limiti possibili, l'utente deve, durante le sue assenze previste, assicurarsi di:
- dare accesso al suo/suoi sostituto/i ai file necessari
- aver attivato la funzione "*Out of Office*" di Outlook, per avvisare della propria assenza e/o inoltrare i messaggi al suo/suoi sostituto/i.

8. CONTROLLI

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 del proprio sistema informatico.

L’obiettivo principale della procedura di controllo ivi descritta è di garantire il rispetto della vita privata degli utenti e di prevedere anticipatamente le regole che l’Azienda dovrebbe rispettare se intendessero effettuare un controllo sulle comunicazioni elettroniche (*internet* ed *e-mail*).

Ogni controllo verrà effettuato nel rispetto dei seguenti principi:

- **Proporzionalità:** il controllo e l’estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- **Trasparenza:** l’adozione del presente Regolamento ha l’obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.

L’individuazione del controllo delle comunicazioni elettroniche in rete è effettuata sotto la responsabilità del Presidente del Collegio Sindacale.

9. DISPOSIZIONI VARIE

Il presente Regolamento troverà applicazione ai comportamenti assunti dai soggetti interessati successivamente alla sua adozione da parte del Consiglio di Amministrazione dell’Azienda.

A tal fine, successivamente alla sua adozione, il presente Regolamento sarà portato a conoscenza dei dipendenti e dei collaboratori dell’Azienda. Copia del Regolamento sarà affissa in luogo accessibile a tutti i dipendenti. Una versione informatica dello stesso sarà altresì messa a disposizione nel sito web aziendale, www.gesenu.it

L’osservanza delle norme del presente Regolamento deve considerarsi parte essenziale delle obbligazioni contrattuali dei dipendenti dell’Azienda ai sensi e per gli effetti dell’art. 2104 del codice civile.

La violazione delle norme del Regolamento potrà costituire inadempimento alle obbligazioni primarie del rapporto di lavoro o illecito disciplinare, con ogni conseguenza di legge, anche in ordine alla conservazione del rapporto di lavoro e potrà comportare il risarcimento dei danni dalla stessa derivanti.