DISCIPLINARE PER L'UTILIZZO DELLA RETE INFORMATICA

Approvato con deliberazione del Consiglio di Amministrazione n.2/9 del 23.12.2011

INDICE

Art. 1 - Oggetto del disciplinare

Il presente disciplinare, con preciso riferimento alle Linee guida del Garante della Privacy-Deliberazione n.13 del 01/03/2007, regolamenta l'utilizzo della posta elettronica e della rete internet in ambito lavorativo, specificando:

- modalità di utilizzo della posta elettronica e della rete internet da parte dei dipendenti dell'ASP
- corretto utilizzo degli strumenti informatici messi a disposizione (Personal Computer, computer portatili, ecc.)
- misure per la prevenzione di utilizzi indebiti
- quali informazioni sull'attività informatica sono memorizzate e per quanto tempo
- modalità di effettuazione di eventuali controlli.

Art. 2 - Campo di applicazione

Le regole indicate dal presente disciplinare devono essere rispettate da tutto il personale dell'ASP delle Terre d'Argine, a qualsiasi titolo in servizio, nonché dai consulenti esterni.

Art. 3 - Principi generali

Le risorse tecnologiche ed informatiche, messe a disposizione dall'ASP delle Terre d'Argine, si configurano quali strumenti di lavoro da utilizzarsi, in base a criteri di correttezza e professionalità e nel rispetto delle norme vigenti, per attività connesse agli incarichi di lavoro attribuiti.

L'utilizzo di tali strumenti, quando non riferito all'attività lavorativa, può comportare maggiori rischi per la sicurezza della rete informatica aziendale, disservizi e aggravi di costi di manutenzione.

Le registrazioni delle attività informatiche attuate dall'ASP sono finalizzate esclusivamente al controllo dell'efficienza e sicurezza dei sistemi informatici e i dati registrati non vengono utilizzati per il controllo a distanza dei dipendenti.

Le norme comportamentali del presente disciplinare sono state predisposte nel rispetto della seguente normativa :

- D.lgs 196/2003
- Linee guida del Garante della Privacy-Deliberazione n.13 del 01/03/2007 "Codice in materia di protezione dei dati personali"
- Legge 20/05/1970 n.300 "Statuto dei lavoratori"
- Costituzione della Repubblica Italiana, in particolare Art.15 sulla libertà e segretezza della corrispondenza.
- Art. 616 del C.P. che tutela espressamente la riservatezza della corrispondenza.

Art. 4 - Utilizzo del computer

4.1 La postazione di lavoro

L'ASP assegna al personale accreditato per l'accesso al sistema informatico, in funzione delle mansioni attribuite, una postazione di lavoro informatica per l'accesso alla rete aziendale, ad internet ed al servizio di posta elettronica. La configurazione dei servizi di accesso viene eseguita esclusivamente dal personale autorizzato.

Per qualsiasi accesso del personale agli strumenti elettronici connessi alla rete aziendale è obbligatoria l'adozione di una procedura di autenticazione che prevede il riconoscimento dell'utente attraverso la digitazione di un codice di autentificazione (login) associato ad una parola chiave (password), univoci e corrispondenti ad un profilo personale per ogni singolo utente. Ulteriori credenziali sono previste quando, una volta avvenuto l'accesso al sistema, si dovrà accedere ad un ulteriore gruppo di dati presenti sul sistema o a particolari banche dati**.**
Nel caso si tratti di gruppi di utenti che accedono allo stesso strumento informatico l'accesso dovrà comunque avvenire sul profilo dell'utente con relativa digitazione di login e password.

4.2 Regole di utilizzo

Per la corretta gestione della propria postazione di lavoro, dotata di personal computer e/o portatile, il dipendente/utente della rete aziendale deve attenersi alle seguenti norme:

- Deve essere mantenuta la corretta configurazione del proprio computer, non modificando software ed hardware predisposti, né installando altri software se non preventivamente autorizzati dall'Amministratore di Sistema;
- Non è consentita l'installazione di programmi software non predisposti da ASP, ne la loro riproduzione o duplicazione. L'utilizzo di software non di proprietà dell'Asp, oltre ad essere vietata nel rispetto della normativa vigente sul diritto di proprietà intellettuale, si configura quale reato in relazione al grave rischio di trasmettere virus informatici e di compromettere la sicurezza del PC e della rete aziendale;
- Non utilizzare supporti magnetici asportabili (dischetti, CD-Rom,ecc.) di incerta provenienza
- Non utilizzare in azienda risorse informatiche private (PC, periferiche, USB, ecc.) salvo specifica autorizzazione;
- Non salvare file audio, video e file non istituzionali nelle connessioni di rete su cui viene eseguito giornalmente il back-up;
- Non è consentita l'installazione non autorizzata di dispositivi di connessione propri come Access Point, Router ecc. per accedere alla rete aziendale;
- La postazione di lavoro e le relative periferiche, quali stampanti locali e di rete, scanner, ecc. devono essere spente al termine della giornata lavorativa e in caso di assenza prolungata nell'arco della giornata;
- Durante le pause di lavoro non deve essere mai lasciato incustodito il PC connesso alla rete, per evidenti ragioni di sicurezza e protezione dei dati, occorre pertanto accertarsi dell'attivazione dello screen saver con password;

Per la protezione del **computer portatile**, oltre alle precedenti norme, occorre prestare ulteriore attenzione alla custodia sia durante lo svolgimento dell'attività lavorativa che al termine del lavoro provvedendo a conservarlo in luogo sicuro.

Occorre, inoltre, prima della riconsegna del portatile rimuovere file eventualmente elaborati sullo stesso

L'utente è responsabile delle attrezzature assegnate e deve mantenerle efficienti, avendo cura di segnalare con tempestività ogni disfunzione riscontrata, secondo il protocollo aziendale di attivazione dell'assistenza tecnica e software.

4.3 Gestione della Password

L'utente è consapevole che la conoscenza della propria password da parte di terzi consente a questi l'accesso non autorizzato alla rete aziendale, l'utilizzo dei servizi connessi e l'accesso alle banche dati abilitate; ne consegue un grave rischio di accesso a informazioni riservate, distruzione o modifica di dati, lettura della propria posta. Tali accessi non autorizzati sono registrati nei log di registrazione degli accessi informatici a nome dell'utente titolare.

Per una corretta gestione della propria password, oltre a quanto già previsto nel Documento aziendale per la protezione dei dati ed espressamente indicato nella lettera di incarico al trattamento dei dati, l'utente si impegna ad osservare le seguenti regole:

- la password non deve essere comunicata a terzi
- non deve essere permesso ad altri di operare utilizzando il proprio identificativo di utente
- non deve essere trascritta su supporti accessibili a tutti (promemoria, post-it)
- una volta attivata la procedura di autenticazione non cedere la propria postazione di lavoro a persona non autorizzata
- non utilizzare credenziali di altri utenti, nemmeno se fornite volontariamente o di cui si è venuti casualmente a conoscenza

Si evidenzia, inoltre, la Procedura per la custodia delle copie di credenziali e accesso straordinario adottata da ASP al fine di assicurare la segretezza della parola chiave e nel contempo la disponibilità dei dati e degli strumenti elettronici: l'Amministratore di Sistema, per manutenzioni o altre attività autorizzate, attiva l'accesso al sistema informatico modificando la password impostata dall'utente; ed imposta il comando di richiesta di cambio password che si attiva automaticamente al successivo primo accesso da parte dell'incaricato autorizzato.

Art. 5 - Utilizzo della posta elettronica

5.1 Il servizio di posta elettronica (e-mail)

ASP ha predisposto un servizio di posta elettronica aziendale, disponibile per ogni dipendente accreditato, in forma centralizzata e protetta; al dipendente/utente viene assegnata una casella di posta; l'indirizzo di posta è composto da:

Inizialenome.cognome@aspterredargine.it

Il servizio di posta elettronica è uno strumento di lavoro da utilizzarsi, di norma, per attività strettamente riferite al proprio incarico, oltre che alla corrispondenza inerente l'attività sindacale dei lavoratori.

Per quanto riguarda la ricezione di e-mail è stato predisposto un apposito programma di filtraggio delle e-mail che limita o riduce il cosiddetto spamming e che permette all'amministrazione di sistema di decidere quali siano i messaggi graditi oppure la corrispondenza da eliminare.

Per l'invio di e-mail si ricorrerà sempre ad indirizzi noti per i quali si è ricevuto il relativo consenso all'invio di e-mail.

Nel testo dell'e-mail in partenza verrà aggiunto il seguente testo:

> "L'art. 616 del C.P. tutela espressamente la riservatezza della corrispondenza, considerando reato l'uso, la copia, la distribuzione o la divulgazione della stessa da parte di chi non ne sia il destinatario. Pertanto, l'e-mail, eventualmente a voi arrivata per errore, non va letta, ma restituita allo scrivente e distrutta, previo cortese preavviso al numero +39-059641407"

5.2 Regole di utilizzo

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. La posta elettronica è uno strumento che rende la comunicazione tempestiva, efficace ed economica. Alcune semplici norme possono aiutare a migliorarne l'utilizzo:

- La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
- È possibile utilizzare la ricevuta di ritorno per avere conferma dell'avvenuta lettura del messaggio da parte del destinatario
- In caso di ricezione accidentale sulla propria casella di messaggi di valenza ufficiale per l'Azienda , quali comunicazione con contenuti rilevanti, impegni contrattuali o precontrattuali con l'Azienda gli stessi devono essere inoltrati tempestivamente alla Direzione o al proprio Responsabile d'area.
- Per la trasmissione di file all'interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati (ad esempio per dimensioni superiori a 2 Mbyte è preferibile utilizzare le cartelle di rete condivise).
- In caso di spedizione all'esterno di file allegati provvedere a ridurne la dimensione con il sistema di zippatura nei casi di dimensione superiore a 5 Mbyte.
- È facoltà del lavoratore avere un proprio indirizzo personale presso sistemi esterni WEB; l'utilizzo di tale posta elettronica privata è consentito entro tollerabili limiti temporali.

In particolare nell'uso della Posta Elettronica non sono consentite le seguenti attività:

a) La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (D.lgs. 196 del 30/6/2003);

b) L'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;

È obbligatorio controllare i file Attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, http o FTP non conosciuti) e accertarsi dell'identità del mittente.

c) Inoltrare "catene" di posta elettronica (tipo catene di S.Antonio e simili), anche se afferenti a presunti problemi di sicurezza (se si ricevono messaggi di tale tipo segnalarlo all'Amministratore di sistema e in ogni caso non attivare gli eventuali allegati)

d) Inviare o memorizzare messaggi offensivi o discriminanti;

e) inviare messaggi personali o partecipare a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.

Art. 6 - Utilizzo di internet

6.1 Finalità

Le postazioni di lavoro abilitate all'accesso ai servizi internet costituiscono uno strumento necessario allo svolgimento della propria attività lavorativa.

Per garantire l'integrità dei sistemi informatici la navigazione internet tramite PC connessi alla rete aziendale è protetta da appositi dispositivi di sicurezza informatica

Tale accesso di norma deve essere motivato da finalità strettamente legate al proprio incarico di lavoro e in ogni caso nel rispetto di precise modalità di utilizzo e di norme comportamentali.

6.2 Regole di utilizzo

La disponibilità di accesso ai servizi internet è vincolata al rispetto delle seguenti regole:

a) presentarsi sempre con il proprio nome, mai sotto il nome altrui
b) non registrarsi a siti i cui contenuti non siano legati all'attività lavorativa
c) non scaricare materiale da internet senza preventiva autorizzazione, anche al fine di non ledere il diritto di proprietà intellettuale
d) non trasferire sul proprio computer file da siti sconosciuti
e) non partecipare a forum, chat line ecc., se non per motivi professionali
f) non scaricare e non usare software gratuito o shareware prelevato da siti internet salvo i casi in cui è richiesto per lo svolgimento delle proprie mansioni
g) qualora fosse richiesta una tassa di registrazione per scaricare file necessari al proprio lavoro e comunque indispensabile chiedere preventiva autorizzazione scritta al proprio responsabile
h) non utilizzare la modalità peer to peer (P2P)

Art. 7 - L'amministrazione delle risorse informatiche

Le attività connesse all'amministrazione delle risorse informatiche sono affidate ad esperti (Amministratori di sistema) interni ed esterni all'azienda, ai quali è riconosciuta la capacità di operare per la sicurezza delle banche dati e di sovrintendere alla corretta gestione delle reti telematiche.

Le funzioni attribuite agli amministratori di sistema, quali manutentori /gestori della rete informatica e amministratori di base di dati, sono svolte in un contesto che rende ad essi tecnicamente possibile l'accesso, anche non voluto, a dati personali (servizio gestione del personale, servizio di posta elettronica, ecc.) evidenziando pertanto aspetti di particolare criticità.

A fronte di tali considerazioni l'ASP attua misure di verifica e controllo dell'attività degli amministratori di sistema anche in relazione al rispetto della privacy e sul segreto nella comunicazione; inoltre, in applicazione del Provvedimento del Garante per la Privacy del 27/11/2008, provvede a registrare gli accessi (raccolta dei Log di accesso) alla rete informatica e agli archivi elettronici.

Al fine della tutela dei diritti dell'interessato l'identità delle persone fisiche alle quali sono attribuite funzioni di amministratori di sistema è resa nota ai lavoratori.

Art. 8 - Monitoraggio del sistema e Controlli

8.1 Programmi che consentono controlli "indiretti"

L'ASP, al fine della manutenzione o per rilevare anomalie della rete e degli strumenti informatici, può avvalersi legittimamente, nel rispetto dell'art.4 - c.2 dello Statuto dei lavoratori, di sistemi che consentano indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori, nel rispetto di quanto previsto dal paragrafo 5 del Provvedimento del Garante n.13 del 01/03/2007.

8.2 Prevenzione dell'utilizzo improprio

Per prevenire possibili controlli e contemperare le esigenze di regolare svolgimento dell'attività lavorativa con l'esigenza di tutela della sfera personale dei dipendenti, nell'ambito delle Linee Guida del Garante per la privacy, qui richiamate e convenendo che il luogo di lavoro e anche luogo di relazioni personali e sociali si prevedono i seguenti accorgimenti:

per l'uso di internet:

- tolleranza per l'uso privato, purché del tutto occasionale, non prolungato e non interferente con l'attività lavorativa (durante la pausa o, in caso di situazioni particolari, previa autorizzazione del proprio responsabile)
- tale utilizzo in deroga alle Regole lettera b) - Regole di utilizzo - Art.6, comporta in ogni caso il rispetto di tutte le altre regole lett. a) c) d) e) f) g) h) i).

per l'uso della posta elettronica:

- tolleranza per l'uso privato, purché del tutto occasionale, non prolungato e non interferente con l'attività lavorativa (durante la pausa o, in caso di situazioni particolari, previa autorizzazione del proprio responsabile)
- disponibilità di funzionalità di sistema che, in caso di assenza programmate del dipendente, consentano l'invio automatico di messaggi di risposta che avvisano dell'assenza del destinatario ed eventualmente, in accordo con il Responsabile di area, contengano le coordinate per l'inoltro della mail ad altro soggetto o altre modalità di contatto presso l'azienda
- previsione della possibilità di delegare un collega (tutor) che, in caso di assenza improvvisa ed esclusivamente per necessità lavorative, possa accedere alla casella di posta elettronica del dipendente assente o quantomeno la persona che può ricevere la posta del lavoratore assente.
- In caso di assenza prolungata non programmata, il Responsabile di area può contattare il Responsabile del sistema informativo/Amministratore di sistema per far modificare l'autorizzazione di accesso alla casella di posta dell'utente assente e gestire la posta in arrivo al fine di assicurare il buon funzionamento dell'attività lavorativa.
- Dopo tre mesi di assenza, l'account verrà disattivato e con esso la posta sarà trasferita ad un nuovo utente.

8.3 Modalità e graduazione dei controlli

L'attività di controllo esercitata nel caso in cui si rilevino anomalie di funzionamento o si rendano necessarie attività di manutenzione o, comunque, in tutte le ipotesi in cui sia a rischio la sicurezza del sistema informatico è pertanto lecita e dettata dal principio di necessità.

L'ASP, in ogni caso procederà secondo i successivi criteri e principi.

a. Le comunicazioni effettuate attraverso il servizio di posta elettronica aziendale sono riservate. Il contenuto di tali comunicazioni non può essere in nessun caso oggetto di alcuna forma di verifica, controllo o censura da parte dell'azienda di da parte di altri soggetti

b. Le attività sull'uso del servizio di accesso ad internet e alla rete aziendale vengono automaticamente registrate in forma elettronica attraverso i LOG di sistema. La raccolta dei LOG avviene giornalmente memorizzati in forma criptata

c. L'ASP non effettua trattamenti di dati personali mediante sistemi che mirano al controllo a distanza dei lavoratori grazie ai quali sia possibile ricostruire la loro attività e che vengano svolti attraverso i seguenti mezzi:
   - lettura e registrazione sistematica dei messaggi di posta elettronica dei dipendenti ovvero dei relativi dati esteriori. al di fuori di quanto tecnicamente necessario per fornire e gestire il sevizio di posta elettronica
   - riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal dipendente
   - lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi
   - analisi occulta di computer portatili affidati in uso

d. Il trattamento dei dati conservati nei LOG può avvenire esclusivamente in forma anonima in modo da precludere l'identificazione degli utenti e delle loro attività. I dati anonimi aggregati, riferibili all'intera struttura o a sue aree, sono a disposizione del Direttore generale

e. I dati personali contenuti nei LOG potranno essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:
   - Per corrispondere ad eventuali richieste della polizia postale o dell'autorità giudiziaria
   - Su richiesta del Direttore generale quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento
   - Su richiesta del Direttore generale unicamente in caso di ripetuto utilizzo improprio ed anomalo degli strumenti aziendali da parte degli utenti di una specifica struttura/area (rilevato esclusivamente dai dati aggregati) e già precedentemente avvertiti, con esplicito invito, ad attenersi ai compiti assegnati ed alle istruzioni impartite

f. I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di attività organizzative e di sicurezza, comunque non superiori a 200 gg. e sono periodicamente cancellati automaticamente dal sistema (180 gg richiesti dalla normativa per controllo accessi dell'Amministratore di sistema più margine del 10% di sicurezza).

g. Un eventuale prolungamento del periodo di conservazione può verificarsi esclusivamente
   - Quando tali dati sono indispensabili al fine dell'esercizio o alla difesa di un diritto in sede giudiziaria
   - Per obbligo di custodire o consegnare i dati su specifica richiesta dell'autorità giudiziaria

Art. 9 - Non osservanza del regolamento

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.

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigenti.

Art. 10 - Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Consulente dell'Ente. Il presente Regolamento è soggetto a revisione con frequenza annuale.