Regolamento per l'utilizzo dei sistemi informativi

(Approvato con deliberazione G.C. n. 15 del 22.03.2010)

INDICE

1. INTRODUZIONE

La postazione di lavoro fornita agli utenti a supporto dello svolgimento dell'attività lavorativa è dotata di strumenti, come il personal computer (fisso, portatile o palmare aziendali) ed altri apparati (stampanti, scanner, modem, ecc…), che sono utilizzati per attività erogate dall'Ente Ca.Do.S. L'utilizzo di queste tecnologie informatiche, pur apportando benefici e vantaggi notevoli, la espone parallelamente a rischi di un coinvolgimento sia dal punto di vista patrimoniale che penale, creando potenziali problemi di immagine e sicurezza.

Per far fronte a tali problematiche, garantendo al contempo adeguata protezione di strumenti, sistemi e servizi informatici utilizzati e delle informazioni in essi contenute, il Ca.Do.S. ha adottato il presente regolamento.

2. SCOPO

Con il presente documento il Ca.Do.S. si propone di far conoscere ai prestatori di lavoro impiegati presso l'ente assegnatari di una postazione di lavoro informatica, le regole interne di comportamento comune adottate con la finalità di garantire la sicurezza del Sistema Informativo e contribuire alla diffusione della cultura della sicurezza, evitando, così, comportamenti inconsapevoli e/o scorretti suscettibili di dare origine a minacce o problemi, con particolare riferimento alla sicurezza nel trattamento dei dati personali nel rispetto della normativa vigente. A tal riguardo si rammenta che l'utilizzo delle risorse informatiche e telematiche messe a disposizione dal Ca.Do.S. deve sempre ispirarsi ai principi di diligenza e correttezza, comportamenti questi che si pongono a fondamento nell'ambito di ogni rapporto di lavoro.

3. AMBITO DI APPLICAZIONE E DESTINATARI

Il presente regolamento si rivolge a tutti i dipendenti, collaboratori e consiglieri che prestano la propria attività lavorativa presso il Ca.Do.S. e che fanno uso dei sistemi informativi in qualità di utenti.

4. UTILIZZO DELLA POSTAZIONE DI LAVORO

4.1 Personal computer

Il Personal Computer è uno strumento di lavoro di proprietà del Ca.Do.S., affidato in via temporanea all'utente, da utilizzare esclusivamente per lo svolgimento dei compiti e delle mansioni assegnate, coerentemente con lo svolgimento dell'attività lavorativa.

L'utente deve utilizzare il PC in modo appropriato, evitandone danneggiamento e/o manomissione. Non è perciò consentito, se non a seguito di espressa e formale autorizzazione rilasciata dal Responsabile del Sistema Informativo:

a) rimuovere software/hardware/periferiche incluse nella dotazione informatica assegnata;

b) copiare il software installato sul PC e/o modificare le impostazioni di sistema predefinite;

c) copiare e esportare o creare autonomamente banche dati differenti e/o ulteriori rispetto alle esistenti;

d) impostare connessioni di qualsiasi genere verso internet o altre reti private o pubbliche;

e) utilizzare il PC (compresa la navigazione Internet e la posta elettronica) per scopi personali, quando non previsti nell'ambito di attività consentite e regolamentate, e per finalità illecite o non consentite, quali ad esempio memorizzazione di documenti personali non attinenti l'attività lavorativa, esecuzione di

programmi di intrattenimento, giochi o multimedialità non pertinenti alla mansione assegnata. Il Sistema Informativo si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema, o comunque acquisiti o installati in violazione del presente regolamento.

Non è consentita l'effettuazione, per scopi personali non legati all'attività lavorativa, di operazioni quali transazioni finanziarie, ivi comprese le operazioni di remote banking, acquisiti on-line e simili con pagamento o fatturazione a carico dell'utente, è consentita, nel pieno rispetto delle normali procedure di acquisto.

In caso di allontanamento temporaneo dalla propria postazione di lavoro, se l'utente è certo di rientrarvi entro la fine della giornata lavorativa, è tenuto a chiudere tutti i documenti aperti e ad attivare le funzioni di log out.

Al termine dell'attività lavorativa giornaliera l'utente deve spegnere il proprio PC, provvedendo, altresì, alla chiusura dell'attività lavorativa sulla postazione. In particolare è tenuto a:

- salvare i documenti informatici nel rispetto delle procedure relative all'utilizzo degli spazi su disco di rete e delle modalità comunicate dall'Ente Ca.Do.S.;
- spegnere completamente la postazione di lavoro attenendosi alle procedure di chiusura del sistema in uso.

Si rende noto che nei casi in cui è indispensabile o indifferibile accedere ai dati trattati dall'utente, ed agli strumenti informatici in dotazione allo stesso, sia per le esigenze organizzative e di servizio, sia per la sicurezza ed operatività dello stesso sistema informatico, l'Ente Ca.Do.S. potrà accedere ai dati e agli strumenti elettronici mediante l'intervento del personale appositamente incaricato ad operare presso i servizi informativi. La stessa facoltà, sempre ai fini di garantire la salvaguardia e la sicurezza del sistema informatico e per ulteriori motivi tecnici e manutentivi, si applica anche in caso di assenza prolungata o impedimento dell'utente.

4.2 PC Portatile

Il PC portatile ha la caratteristica di essere trasportabile con facilità e presenta, quindi, peculiarità in termini di utilizzo e di sicurezza. Per le modalità generali di utilizzo l'utente deve osservare, in quanto applicabili, le regole stabilite al punto 4.1 del presente regolamento.

Il PC portatile non deve essere mai lasciato incustodito, in particolare, durante le ore notturne o in periodo di assenza non deve mai essere lasciato sulla scrivania ma deve essere custodito in modo opportuno (es. riposto in armadi chiusi a chiave o portato a seguito). Durante l'utilizzo in ufficio l'utente deve assicurare il PC portatile avvalendosi degli appositi cavi di sicurezza forniti dall'Ente Ca.Do.S.

Durante gli spostamenti all'esterno è cura dell'utente proteggere il PC portatile da possibili furti o danneggiamenti; il dispositivo assegnato non deve mai, nemmeno per breve tempo, rimanere incustodito, soprattutto in luoghi pubblici quali, ad esempio, aeroporti, stazioni ferroviarie, stazioni di servizio, ristoranti, bar, fiere, manifestazioni, etc. Durante i viaggi deve essere sempre trasportato come bagaglio a mano, e non va mai lasciato in vista nelle stanze di hotel, residence, alloggi, etc., bensì deve essere opportunamente richiuso in valigia o in un armadio, o in cassaforte in caso di assenza prolungata.

Ogni utente è responsabile dell'integrità dei dati che conserva in locale sul proprio PC portatile, e deve tenere in considerazione il fatto che i dati potrebbero essere persi o compromessi. A tale riguardo l'utente è tenuto a:

- memorizzare in forma protetta (es. accesso al file con password), in modo adeguato al loro livello di criticità o riservatezza, eventuali informazioni riservate/segrete residenti sul PC;
- effettuare, con cadenza quotidiana, durante i periodi di permanenza in ufficio, la connessione alla rete al fine di procedere alle operazioni di allineamento dei dati inerenti l'attività lavorativa salvati in locale, alle cartelle appositamente predisposte sui dischi di rete (si rammenta all'utente che gli spazi su disco di rete

sono gli unici per i quali è garantito l'espletamento delle attività di backup). Nei casi di periodi lavorativi al di fuori dell'ufficio l'utente è tenuto alla sincronizzazione dei dati coi dischi di rete al primo rientro.

In caso di furto, danneggiamento o smarrimento del PC portatile l'utente è tenuto ad effettuare immediata denuncia all'autorità giudiziaria competente dandone contestuale segnalazione all'Ente Ca.Do.S.

4.3 Supporti di memorizzazione removibili

In caso di comprovate necessità attinenti allo svolgimento dell'attività lavorativa, in via eccezionale e temporanea, può essere assegnato all'utente un supporto rimovibile di memorizzazione, previo autorizzazione scritta rilasciata dal Responsabile di funzione. L'utente assegnatario è responsabile del supporto, dell'utilizzo dello stesso e dei dati in esso contenuti. In particolare, i supporti assegnati possono contenere esclusivamente dati attinenti all'attività lavorativa (nel rispetto di quanto stabilito al punto 4.1 lettera e) del presente regolamento), devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, alterato, distrutto o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità dei supporti removibili assegnati contenti dati sensibili o informazioni critiche , ciascun utente è tenuto a contattare il personale del Sistema Informativo, ed a seguire le istruzioni da questi impartite.

5. UTILIZZO DELLE RISORSE DI RETE

5.1 Rete comunale

Le risorse di rete sono strumenti di proprietà dell'Ente Ca.Do.S., messe a disposizione degli utenti esclusivamente per fini lavorativi e da utilizzare entro i limiti previsti dal profilo di autorizzazione personale.

L'accesso alla rete, per il quale deve essere utilizzato il proprio profilo personale, è protetto da password ed è consentito soltanto alle stazioni di lavoro assegnate e/o autorizzate. È vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Responsabile di Funzione. Non sono ammesse connessioni di stazioni di lavoro esterne (collaboratori, consulenti, etc.) salvo specifiche deroghe dietro formale autorizzazione da parte del Responsabile di Funzione.

È vietato utilizzare la rete comunale per fini non inerenti l'attività lavorativa o comunque non espressamente autorizzati. Pertanto, qualunque file che non abbia una connotazione a carattere lavorativo, non può essere dislocato, nemmeno per brevi periodi, in queste unità.

Gli utenti sono tenuti a rispettare le procedure relative all'uso degli spazi su disco di rete, in particolare per quanto riguarda la cancellazione di file, dati e informazioni obsoleti e il rispetto delle modalità di archiviazione comunicate dal Sistema Informativo. Il Sistema Informativo si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente regolamento.

Nel corso dell'ordinario svolgimento dei compiti e delle mansioni assegnate, l'utente è tenuto, ai fini dell'archiviazione del lavoro svolto, a fare uso degli spazi su disco di rete, in quanto questi sono gli unici per i quali è garantito l'espletamento delle attività di salvataggio.

5.2 Posta elettronica (ai sensi della delibera n. 13 del 1 marzo 2007 Garante Privacy)

La casella di posta elettronica assegnata deve essere utilizzata solo per motivi di lavoro osservando le regole e limiti di utilizzo definiti dal presente regolamento.

Gli utenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. E' fatto divieto di utilizzare le caselle di posta elettronica assegnate per la partecipazione a dibattiti, forum o mailing list, salvo diversa ed esplicita autorizzazione da parte del Responsabile di funzione.

Per non appesantire la rete comunale, sono vietate le attività di flooding (letteralmente "inondazione di messaggi", ovvero invio massivo a più destinatari di messaggi di posta elettronica), salvo che non siano preventivamente autorizzate.

Analogamente, è proibita qualunque attività di spamming (messaggio di posta elettronica non richiesto, inviato a molti destinatari contemporaneamente).

E' sempre vietato spedire e-mail che:

- possano danneggiare la reputazione e l'immagine dell'Ente Ca.Do.S. o compromettere le relazioni i terzi;
- siano diffamatorie, oscene, pornografiche, offensive, tali da recare danno, o che possano essere considerate da altri fonte di molestia o discriminazione religiosa, sessuale, razziale, politica o sindacale;
- possano infrangere la legislazione vigente;
- possano diffondere virus in rete;
- costituiscano e-mail "spazzatura" o siano c.d. "catene di Sant'Antonio informatiche".

La posta elettronica è lo strumento più utilizzato per diffondere virus informatici e compromettere l'integrità dei dati ed il funzionamento dei sistemi informatici. Nonostante la presenza di sistemi automatici di protezione (antivirus, antispam, etc.), l'utilizzatore deve diffidare di tutte le mail che siano sospette, di provenienza o dai contenuti sconosciuti. Qualora si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Responsabile del Sistema Informativo. Non si devono in alcun caso attivare gli allegati di tali messaggi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. I messaggi non più necessari ai fini lavorativi devono essere cancellati regolarmente dagli utenti. E' in ogni caso opportuno che gli allegati vengano rimossi o salvati come files per non esaurire la capienza della casella assegnata.

La policy di utilizzo della posta elettronica adottata dell'Ente Ca.Do.S prevede inoltre:

- l'adozione di apposite funzionalità di sistema (risponditore automatico), che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto incaricato o altre utili modalità di contatto della funzione di appartenenza.;
- la possibilità, in caso di assenza improvvisa, non programmata o prolungata, di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e ad inoltrare al responsabile od al personale di competenza quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa; in tal caso dovrà essere redatto a cura del fiduciario un apposito verbale e dovrà essere informato il lavoratore interessato alla prima occasione utile.

5.3 Rete Internet (ai sensi della delibera n. 13 del 1 marzo 2007 Garante Privacy)

L'accesso a Internet è limitato alle sole necessità lavorative e non è mai consentito un uso di tale strumento per fini personali.

L'uso incauto può essere una fonte di rischi per la sicurezza dei sistemi informativi. L'inserimento di dati su Internet (ad esempio, la compilazione di moduli on-line, ancorché pertinente al proprio lavoro) deve essere

sempre valutata con molta attenzione. Qualora l'utente debba indicare una password per un qualsiasi servizio su Internet, tale password dovrà rispettare i requisiti esplicitati nel presente documento.

Inoltre, senza la preventiva ed espressa autorizzazione del proprio Responsabile di funzione in accordo con il Responsabile del Sistema Informativo, è vietata ogni forma di:

- accesso o registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- iscrizione a siti, mailing-list, newsgroup e comunità virtuali di cui non è effettivamente riconosciuta e dimostrata l'utilità ai fini lavorativi e per i quali non si è ottenuta formale autorizzazione;
- partecipazione a Forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (nicknames);
- visualizzazione, scaricamento e memorizzazione di immagini, video, audio e documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- utilizzo di sistemi di webmail personali per inviare/ricevere comunicazioni e/o file contenenti dati e informazioni attinenti l'attività lavorativa o inerenti l'Ente Ca.Do.S;
- modifica della configurazione del proprio browser.

6. IDENTIFICAZIONE E AUTENTICAZIONE AL SISTEMA INFORMATIVO

6.1 User ID e Password

Al fine di prevenire accessi non autorizzati al Sistema Informativo dell'Ente Ca.Do.S, ogni attività sulle risorse informatiche necessita di una preventiva autenticazione basata sulla combinazione di un identificativo utente (UserID) e una parola chiave (password). Per consentire l'accesso a reti, sistemi, dati o applicazioni è assegnato in modo univoco, ad ogni utente chiaramente identificato, uno User-ID al quale è associata una password. La responsabilità della segretezza della password è dell'assegnatario, il quale deve custodirla con cura senza rivelarla a nessuno, e deve astenersi dal trascriverla in qualsiasi forma. Qualora sussista il dubbio di violazione della segretezza, l'utente dovrà provvedere al cambiamento della password.

Al primo accesso al sistema l'utente è obbligato a cambiare la password assegnata di default ed a porre in essere una gestione sicura della stessa nel rispetto dei seguenti requisiti:

- la password deve essere diversa dallo User-ID;
- non deve essere breve (minimo 8 caratteri);
- deve essere modificata dall'utente almeno ogni 90 giorni;
- le 4 password precedentemente usate non possono essere riutilizzate;
- è fatto divieto all'utente di utilizzare password banali, ovvie o facilmente memorizzabili; la password non deve essere costituita da predefinite sequenze alfanumeriche, né contenere riferimenti scontati o facilmente deducibili (nome del mese corrente, sequenze con numeri progressivi, etc.) o riferimenti a carattere personale (date, numeri di telefono, nomi di persona, etc.).

Si rammenta, altresì, all'utente che:

- in caso di allontanamento temporaneo dalla propria postazione di lavoro, e comunque in caso di non utilizzo del PC per oltre dieci minuti, si attiva la funzione automatica di logout con avvio del salvaschermo protetto da password;

- dopo 5 tentativi consecutivi falliti di accesso, il sistema si blocca e l'utente dovrà contattare il personale addetto ai sistemi informativi per il ripristino.

7. SISTEMI DI CONTROLLO

L'Ente Ca.Do.S, al fine di ridurre il rischio di usi impropri delle risorse informatiche, prevenire comportamenti illeciti od incauti degli utenti, garantire il rispetto dello standard di sicurezza adottato e di tutta la normativa vigente in materia, effettua controlli sull'osservanza da parte degli utenti di quanto statuito nel presente documento.

I controlli saranno svolti in conformità alla legge e nel rispetto dei diritti e delle libertà fondamentali di lavoratori e soggetti terzi, attenendosi rigorosamente ai principi di legge fissati dalla vigente normativa di riferimento, tenendo conto, altresì, della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Al fine di garantire l'efficacia e l'applicabilità del presente documento, nonché la sicurezza dei sistemi informativi prevenendo utilizzi impropri anche involontari, l'Ente Ca.Do.S. ha adottato una serie di accorgimenti tecnici ed organizzativi tesi al rispetto delle procedure di autenticazione (autenticazione con user id e password, logout automatica, scadenza password, etc.), al corretto utilizzo di delle postazioni di lavoro informatiche (impostazioni predefinite dal Sistema Informativo, istruzioni sull'utilizzo, sistemi di criptazione e cifratura dei dati, etc.), al corretto utilizzo di Posta Elettronica.

Nei casi vengano riscontrate anomalie od incidenti suscettibili di impattare sul normale svolgimento dell'attività lavorativa o sulla la sicurezza ed operatività del sistema informativo, l'Ente Ca.Do.S attraverso il personale appositamente incaricato, effettuerà controlli in maniera anonima su dati aggregati riferiti all'intera struttura lavorativa o alle determinate aree in cui si è verificata l'anomalia. Qualora dall'attività di monitoraggio risulti un utilizzo irregolare degli strumenti informatici, si provvederà a diffondere un avviso generalizzato con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. Nel caso in cui l'anomalia sia invece circoscritta a particolari aree o settori, l'avviso sarà inoltrato solo al personale appartenente a tali strutture.

In presenza di successive e reiterate anomalie, si procederà ad effettuare controlli individuali/nominativi o su singoli dispositivi e postazioni, nel rispetto della normativa vigente; l'inizio di tale attività sarà preceduta da un avviso. L'attività di controllo sarà comunque sempre:

- condotta nella maniera meno invasiva possibile;
- mirata alle sole aree di rischio
- non prolungata nel tempo e limitata a brevi periodi
- pertinente e non eccedente la finalità per cui è stata intrapresa
- svolta da personale appositamente incaricato.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione dei dati relativi all'uso degli strumenti elettronici è temporanea. I sistemi software utilizzati per le attività di monitoraggio e controllo sono programmati e configurati in modo da cancellare periodicamente ed automaticamente attraverso procedure di sovraregistrazione i file di log relativi agli accessi, ad Internet. Un eventuale prolungamento dei tempi di conservazione potrà aver luogo solo in relazione all'indispensabilità dell'informazione rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

8. INOSSERVANZA E SANZIONI

L'osservanza di quanto statuito dal presente regolamento deve considerarsi parte essenziale delle obbligazioni contrattuali a cui è soggetto il personale dell'Ente Ca.Do.S. Il mancato rispetto o la violazione delle disposizioni in esso contenute sarà perseguibile nei confronti del personale dipendente con l'applicazione dei provvedimenti disciplinari previsti dal contratto di lavoro applicato, nonché con tutte le azioni civili e penali consentite dalla legge.