

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI E DEGLI STRUMENTI DI
COMUNICAZIONE DEL C.I.S.A.

Approvato con deliberazione dell'Assemblea Consortile n. 8 del 20.04.2010

PREMESSE

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone il C.I.S.A. e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso, quindi, che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il C.I.S.A. ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del D. Lgs. 30 giugno 2003 n. 196 e del Documento tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Considerato, inoltre, che il C.I.S.A., nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

1. Premesse

Le premesse fanno parte integrante e sostanziale del presente atto e ne esprimono le finalità

2. Entrata in vigore del regolamento e pubblicità

Il nuovo regolamento entrerà in vigore il _____.

Copia del regolamento, oltre ad essere affisso nella bacheca aziendale, verrà consegnato a ciascun dipendente.

3. Campo di applicazione del regolamento

Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

4. Utilizzo del Personal Computer

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente

all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

Il personal computer dato in affidamento all'utente permette l'accesso alla rete del C.I.S.A. solo attraverso specifiche **credenziali di autenticazione**.

Il C.I.S.A. rende noto che il personale incaricato che opera presso il servizio Information and Communication Tecnology (nel seguito per brevità "Servizio ICT") dello stesso C.I.S.A. è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Consorzio, si applica anche in caso di assenza prolungata od impedimento dell'utente.

Il personale incaricato del servizio ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio ICT per conto del C.I.S.A. né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, salvo quelli preventivamente autorizzati dall'amministrazione. L'inosservanza della presente disposizione espone il C.I.S.A. a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software vengono sanzionate anche penalmente.

Non è consentito installare sul proprio PC, dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ...).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il responsabile nel caso in cui siano rilevati virus ed adottando le procedure di protezione antivirus.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. 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.

5. Gestione ed assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del Servizio ICT, previa formale richiesta del Responsabile Amministrativo.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio ICT, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.

La password deve rispettare opportuni criteri quali:

- ◆ Lunghezza minima: 8 caratteri
- ◆ Deve contenere almeno una cifra e/o un simbolo speciale
- ◆ Non deve essere una parola di senso compiuto
- ◆ Non deve riferirsi a dati ricollegabili al titolare.

L'utente è responsabile per le attività che vengono svolte utilizzando il suo nome utente e la sua password.

L'utente che si allontana dal posto di lavoro deve preventivamente provvedere a spegnere l'apparecchiatura o, comunque, ad attivare un sistema di "screen saver" dotato di password di sblocco, qualora il sistema non preveda tale funzionalità di blocco in automatico.

6. Utilizzo della rete del C.I.S.A.

Per l'accesso alla rete del C.I.S.A. ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Le cartelle utenti presenti nei server del C.I.S.A. 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. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del personale del Servizio ICT.

Il personale del Servizio ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

7. Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio ICT e seguire le istruzioni da questo impartite.

In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

E' vietato l'utilizzo di supporti rimovibili personali.

L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

8. Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli dal Servizio ICT 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 dal presente regolamento. I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

9. Uso della posta elettronica

La casella di posta elettronica assegnata 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 xxxx@cisa-tortona.it per motivi diversi da quelli strettamente legati all'attività lavorativa.

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 il C.I.S.A. ovvero contenga documenti da considerarsi riservati in quanto attinenti al servizio, deve essere visionata od autorizzata dal Responsabile d'ufficio.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, ...), devono essere autorizzate e firmate dalla Direzione e/o dai Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse.

È obbligatorio porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.

Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato della sicurezza potrà accedere al contenuto del messaggio inviato alla stessa casella.

10. Utilizzo privato del servizio ITC

È ammessa tolleranza per l'uso privato della rete internet e della posta elettronica, purchè del tutto occasionale, non prolungato e non interferente nell'attività lavorativa, conformemente a quanto previsto dalla Direttiva n. 2 del 26.05.2009 del Dipartimento della Funzione Pubblica.

11. Navigazione in Internet

Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo le eccezioni ammesse dall'art. 10 del presente Regolamento.

In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio ICT);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione (o eventualmente dal Responsabile d'ufficio e/o del Servizio ICT);
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- 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) se non espressamente autorizzati dal Responsabile d'ufficio;

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il C.I.S.A. rende, peraltro, nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevenano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.

Gli eventuali controlli, compiuti dal personale incaricato del Servizio ICT potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre due mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza del Consorzio.

12. Protezione antivirus

Il sistema informatico del C.I.S.A. è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio ICT.

Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio ICT.

13. Utilizzo dei telefoni, fax e fotocopiatrici aziendali

Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.

La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.

Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o

comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale del Servizio ICT.

È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

14. Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione ad incaricato del trattamento dei dati ai sensi del Documento Programmatico per la Sicurezza allegato al D.Lgs. n. 196/2003.

15. Coordinamento normativo

Il presente Regolamento integra e non sostituisce le regole di comportamento previste dal Documento programmatico sulla Sicurezza dell'Ente e da tutte le altre normative nazionali in materia.

16. Accesso ai dati trattati dall'utente

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione, tramite il personale del Servizio ICT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

17. Sistemi di controlli graduali

In caso di anomalie, il personale incaricato del servizio ICT effettuerà controlli anonimi che si concluderanno con un avviso generalizzato diretto ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

18. Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL Enti Locali, nonché con tutte le azioni civili e penali consentite.