

Allegato a)



CITTÀ DI
VENARIA REALE

SERVIZIO ATTIVITÀ PRODUTTIVE

CITTÀ DI VENARIA REALE

Provincia di Torino

SETTORE AMMINISTRAZIONE GENERALE

Sviluppo Informatico

REGOLAMENTO

**PER L'ACCESSO E L'UTILIZZO DEI SERVIZI AZIENDALI DI INTERNET
E DI POSTA ELETTRONICA**

Approvato con deliberazione del Commissario Straordinario n. 59 del _____

21 MAG. 2015

REGOLAMENTO

PER L'ACCESSO E L'UTILIZZO DEI SERVIZI AZIENDALI DI INTERNET E DI POSTA ELETTRONICA

INDICE

Premessa

- 1) Utilizzo del Personal Computer
- 2) Utilizzo della rete
- 3) Gestione delle Password
- 4) Utilizzo dei supporti magnetici
- 5) Utilizzo di PC portatili
- 6) Uso della posta elettronica
- 7) Uso della rete Internet e dei relativi servizi
- 8) Restrizioni nell'utilizzo delle reti
- 9) Protezione antivirus
- 10) Osservanza delle disposizioni in materia di Privacy
- 11) Controlli e responsabilità

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone il Comune di Venaria Reale ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

Le Pubbliche Amministrazioni, in quanto datori di lavoro, sono tenute ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informatici. A fronte del potere di controllo dell'Amministrazione / datore di lavoro, esiste in capo ai dipendenti l'obbligo, sancito dalle norme di legge (anche di rilevanza penale) e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli ai beni mobili ed agli strumenti ad essi affidati, tra i quali vi sono le attrezzature ICT ed i sistemi informatici messi a disposizione dall'Amministrazione. Pertanto l'utilizzo delle risorse ICT da parte dei dipendenti, oltre a non dover compromettere la sicurezza e la riservatezza del Sistema Informatico, non deve pregiudicare ed ostacolare le attività dell'Amministrazione od essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici.

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

Tali prescrizioni si aggiungono ed integrano le specifiche istruzioni che vanno fornite a tutti gli incaricati in attuazione del D.lgs 196/03 - Testo Unico in materia di protezione dei dati personali.

1. Utilizzo del Personal Computer

1.1 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.

1.2 L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Le password devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che lo preveda, per lo screen saver.

Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Responsabile del Servizio Sistemi Informativi.

1.3 Il Responsabile dell'Ufficio Sviluppo Informatico - di seguito anche solo "U.S.I." - e lo staff da lui diretto, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, anche delegando a terzi con specifico informale mandato, in relazione agli scopi di volta in volta identificati, osservando il principio di pertinenza e non eccedenza. Non sono ammessi metodi di controllo sistematico occulto e/o remoto. L'accesso agli archivi di posta e ai dati deve comunque avvenire dopo esplicito consenso del lavoratore espresso anche tramite chiamata helpdesk. Il lavoratore stesso, a sua discrezione, potrà essere presente durante l'intervento in essere.

1.4 Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del Responsabile dell' U.S.I. ed una richiesta scritta da parte del dirigente responsabile del Settore cui è assegnato il PC.

In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcuni settori ed i relativi dirigenti, deve essere comunque richiesta per iscritto l'autorizzazione preventiva da parte del Responsabile dell' U.S.I. , per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Sussiste infatti il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi.

1.5 Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dell' U.S.I. del Comune di Venaria Reale (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).

1.6 Non è consentito all'utente ed ai dirigenti modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso e le configurazioni delle reti LAN/WAN presenti nelle sedi, salvo autorizzazione esplicita del Responsabile dell' U.S.I.

1.7 È responsabilità del dirigente verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

1.8 Il Personal Computer e tutti i dispositivi ad esso collegati – comprese le stampanti - devono 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. In ogni caso deve essere attivato lo screen saver e la relativa password o comunque bloccato il Personal Computer con la consueta sequenza di tasti (CTRL-ALT-CANC).

1.9 Non è consentita l'installazione sul proprio PC o il collegamento sulla rete LAN di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pc portatili ed apparati in genere...), se non con l'autorizzazione espressa del Responsabile dell' U.S.I. , previa richiesta scritta da parte del dirigente responsabile del Settore cui è assegnato il PC o il segmento di rete LAN.

1.10 Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più PC (art. 5 del DPR 318/99) nel periodo transitorio in cui tale tipologia di accesso è ancora permesso. È fatto altresì obbligo di distruggeré eventuali copie di sicurezza o supporti di tipo removibile (floppy, CDROM, Nastri) una volta non sia possibile rendere irrecuperabili i dati in essi contenuti.

Ai sensi del Dlgs 196/03 è fatto divieto di divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati dell'ente se non disciplinate da appositi protocolli di intesa.

1.11 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile dell' U.S.I. nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo articolo 9 del presente Regolamento relativo alle procedure di protezione antivirus.

1.12 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.

1.13 È prevista l'erogazione di tutti servizi di supporto (Help Desk) per le problematiche funzionali di tipo hardware e software, attraverso procedure informatiche centralizzate. Il Servizio Informatico si riserva di non intervenire per anomalie segnalate senza l'utilizzo delle procedure concordate di volta in volta con il Responsabile dell'U.S.I.

2. Utilizzo della rete del Comune di Venaria Reale

2.1 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. Su

queste unità, potranno essere svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema.

Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è fatto divieto di replicare su dischi locali dei PC dati aziendali, banche dati e documenti sensibili senza esplicita autorizzazione del Responsabile dell' U.S.I. e senza l'adozione di adeguate politiche di sicurezza, quali la criptazione dei dati stessi e l'adozione di politiche di backup comprensive della dotazione di idonei archivi protetti.

2.2 Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con nomi utente diversi dai propri o dal proprio nel caso di accesso univoco. (Global Sign-On).

2.3 Il Responsabile dell'U.S.I. 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.

2.4 Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

2.5 È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

È buona regola evitare di stampare documenti o file non adatti (es. molto lunghi) su stampanti comuni; per tali operazioni è attivo il centro stampa. In caso di necessità la stampa in corso può essere cancellata.

2.6 Non è consentito ai Dirigenti collegare reti di pc od altri dispositivi alla rete aziendale senza la preventiva autorizzazione scritta dell'Amministratore di Sistema ed una verifica della conformità agli standard tecnici presenti.

3. Gestione delle Password

3.1 Le password di ingresso alla rete, di accesso ai programmi e al Personal Computer, sono previste ed attribuite dal Responsabile dell'U.S.I. e/o gestore del programma. È comunque obbligatoria l'autonoma sostituzione da parte dell'utente della Password di Accesso al Personal Computer/rete secondo le procedure di sicurezza e le tempistiche previste dalla legge. È facoltà dell'utente sostituire periodicamente le password di accesso ai programmi utilizzati al fine di garantire una maggiore sicurezza. In qualsiasi momento il Responsabile dell'U.S.I., il gestore del programma o un terzo incaricato ha la facoltà di resettare le password per motivi di sicurezza o manutenzione.

3.2 Le password devono essere lunghe almeno 8 caratteri, (salvo impedimenti tecnici delle applicazioni), formate da lettere (maiuscole e/o minuscole), numeri e caratteri speciali quali & % ^ # \$, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (per es. nomi/date di nascita e simili).

3.3 Le password utilizzate dagli incaricati al trattamento hanno una durata massima di 6 mesi, trascorsi i quali le password devono essere sostituite.

3.4 È dato incarico ai dirigenti di comunicare tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia all'ufficio del personale che all'Amministratore di Sistema, per iscritto, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario.

4. Utilizzo dei supporti magnetici

4.1 Tutti i supporti magnetici/ottici riutilizzabili (dischetti, cassette, cartucce, chiavi usb, cd, dvd, ecc..) contenenti dati sensibili 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.

4.2 I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

4.3 Non è consentito scaricare files contenuti in qualunque tipo di supporto non aventi alcuna attinenza con la propria prestazione lavorativa.

4.4 Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati/installati/testati.

Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo da parte del Responsabile dell' U.S.I. e/o del suo staff tecnico.

5. Utilizzo di PC portatili

5.1 L'utente è responsabile del PC portatile assegnatogli dall'Amministratore del Sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

5.2 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.

5.3 I PC portatili utilizzati all'esterno (convegni etc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.

5.4 Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente a cura del Responsabile dell' U.S.I. e del suo staff tecnico. È vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN.

6. Uso della posta elettronica

6.1 La casella di posta, assegnata all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Si rammenta che i sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse; si raccomandano pertanto gli utenti di non inoltrare dati ed informazioni classificabili "sensibili" o "riservate" con questo mezzo.

6.2 È fatto divieto di utilizzare le caselle di posta elettronica su dominio dell'ente (es.: @comune.venariareale.to.it) per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per l'ente, salvo diversa ed esplicita autorizzazione.

6.3 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. È previsto un dimensionamento massimo per ciascuna casella in relazione alla disponibilità di spazio dei sistemi di posta di volta in volta disponibili, che non potrà essere superato per evitare l'appesantimento della gestione dei server stessi.

6.4 Dai divieti di cui ai punti precedenti non sono compresi i messaggi di posta tra i rappresentanti sindacali e tra questi con le rispettive OO.SS.; puramente è consentito l'accesso ai siti contenenti messaggi di natura sindacale. Qualora tecnicamente sia possibile non si esclude l'apertura di una casella di posta riservata alle relazioni sindacali.

6.5 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune di Venaria Reale ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analogha dicitura, deve essere visionata od autorizzata dal Dirigente cui si riferisce l'attività ed indirizzata alla casella istituzionale prevista dal Manuale di Gestione del Protocollo Informatico e dei Flussi Documentali.

6.6 Per la trasmissione di file all'interno del Comune di Venaria Reale è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati; se di dimensioni consistenti si consiglia di utilizzare le directory di scambio presenti sui file server, eventualmente notificando a mezzo mail al destinatario la disponibilità del file stesso.

6.7 È obbligatorio fare attenzione nell'apertura di file allegati ai messaggi di posta elettronica, evitando l'utilizzo di file derivanti da fonti sconosciute. Nel caso di dubbi si raccomanda di chiedere consiglio allo staff tecnico dell'U.S.I. Non eseguire download di file eseguibili o documenti da mail non richieste/inattese, siti Web o Ftp non conosciuti.

6.8 È vietato inviare catene telematiche (o di Sant'Antonio). Non si deve in alcun caso attivare gli allegati di tali messaggi.

7. Uso della rete Internet e dei relativi servizi

7.1 Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È deprecata la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.

7.2 È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile dell' U.S.I. .

7.3 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 dai Dirigenti dei settori interessati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.

7.4 È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

7.5 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), se non attinenti l'attività lavorativa svolta.

7.6 L'U.S.I. si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con i Dirigenti, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.

7.7 Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

8. Restrizioni nell'utilizzo delle reti

8.1 L'Amministrazione adotta misure di filtraggio che permettono di inibire o restringere l'accesso a siti i cui contenuti siano classificati pericolosi o non attinenti agli scopi istituzionali oppure che permettono l'accesso solo a determinati siti la cui consultazione sia stata ritenuta dai singoli Dirigenti dei Settori utile in relazione agli scopi istituzionali.

8.2 Sono vietate azioni idonee ad eludere le misure di filtraggio di cui al precedente comma a meno che non siano concordate con l'U.S.I. e su indicazione del dirigente di Settore.

8.3 Il Responsabile dell'U.S.I., nel caso si prefiguri un uso improprio o che metta a repentaglio la sicurezza del sistema informatico dell'ente, ha la facoltà di inibire temporaneamente, anche senza preavviso, la navigazione in internet alle postazioni di lavoro interessate.

8.4 Ai soli fini di gestione e di salvaguardia degli interessi dell'Ente e dei propri dipendenti, il sistema di gestione della navigazione in internet provvede alla tracciatura secondo la normativa vigente, che prevede esclusivamente la registrazione delle URL senza entrare nel merito delle attività svolte (compilazione form, contenuti web-mail, etc). Il tempo di mantenimento di tali dati

viene stabilito in 6 mesi, in analogia a quanto previsto nel provvedimento del 24.7.2008 del Garante per la protezione di dati personali.

9. Protezione antivirus

9.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

9.2 Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

9.3 Nel caso in cui l'utente abbia sentore di problematiche relative a virus, dovrà immediatamente provvedere ad effettuare una segnalazione tramite lo strumento di helpdesk; la stessa metodologia dovrà essere effettuata anche nel caso in cui il software antivirus rilevi la presenza di un virus.

9.4 Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, nastri magnetici, od altri supporti magneto/ottici di provenienza ignota.

9.5 Ogni dispositivo magnetico/ottico 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 consegnato all'amministratore di sistema.

10. Osservanza delle disposizioni in materia di Privacy

10.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza. Tale norma andrà indicata nelle lettere di individuazione dell'incaricato al trattamento dei dati ai sensi del D.lgs 196/03.

11. Controlli e responsabilità

11.1 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.

11.2 L'Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti in materia di privacy e di tutela della dignità del lavoratore, del presente regolamento e dello Statuto dei lavoratori.

11.3. Per esigenze organizzative, produttive e di sicurezza l'Amministrazione effettuerà controlli automatizzati generali che avranno carattere anonimo ed avranno ad oggetto dati aggregati, riferiti a Settori, Servizi o Uffici, con l'obiettivo di individuare potenziali rischi per la sicurezza o usi impropri del sistema informatico.

11.4 Qualora i controlli di cui al precedente comma evidenzino potenziali rischi o problemi oppure nei casi di sospetta violazione delle norme di cui al presente regolamento, l'Amministrazione potrà altresì effettuare controlli e ispezioni su postazioni individuali.

11.5 Tali controlli ed ispezioni dovranno avvenire con gradualità, nel rispetto dei principi di pertinenza e non eccedenza. I suddetti procedimenti di controllo saranno opportunamente documentati (tipo di controlli, nome del sistemista che opera i controlli, log di accesso ai sistemi, riscontri dei controlli).