ISTITUZIONI DI RICOVERO E DI EDUCAZIONE VENEZIA IRE

Regolamento per l'uso degli strumenti informatici e la sicurezza dei dati personali

Approvato con Deliberazione del Consiglio di Amministrazione n. 26 del 29 aprile 2010

Sommario

1. Premessa

1.1 La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Ente ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.
Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza, l'I.R.E. ha adottato il presente documento anche per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Internet è una rete mondiale di computer che contiene milioni di pagine di informazioni; parte di queste possono avere contenuti offensivi o illegali, con cui si può entrare accidentalmente in contatto, ad esempio attraverso interrogazioni a motori di ricerca effettuate per scopi "innocui". Inoltre la diffusione del proprio indirizzo di posta elettronica mediante Internet, ad esempio inserendolo in mailing list non adeguatamente gestite, può facilmente portare a essere fatti oggetto di invii di messaggi indesiderati di posta. Per queste ragioni l'Amministrazione non si ritiene responsabile per il materiale acceduto o scaricato da Internet da parte degli utenti ma cerca di minimizzare i rischi connessi all'uso di Internet mediante l'applicazione di quanto contenuto nel presente documento, cui gli utenti sono tenuti ad attenersi. A tale scopo l'amministrazione si riserva altresì il diritto di bloccare l'accesso a siti Internet aventi contenuto offensivo o illegale mediante uso di appositi strumenti software.

La natura stessa della posta elettronica la rende meno sicura di quanto si possa immaginare. Ad esempio, i messaggi di posta elettronica spediti ad una persona possono essere facilmente inoltrati ad altri destinatari. L'Amministrazione non può proteggere gli utenti da fatti come quelli descritti che esulano dalle proprie possibilità e compiti. Gli utenti pertanto devono esercitare la massima cautela nell'uso della posta elettronica per comunicare informazioni riservate o dati sensibili.
I messaggi di posta elettronica, creati e conservati sia su apparati elettronici forniti dall'Amministrazione che su altri sistemi, possono costituire registrazioni di attività svolte dall'utente nell'espletamento delle sue attività lavorative. E' possibile quindi che venga richiesto di accedere ai contenuti dei messaggi per un eventuale utilizzo nell'ambito di contenziosi che coinvolgano l'Amministrazione. L'Amministrazione non darà corso automaticamente a tutte le richieste di accesso, ma le valuterà in relazione a precisi obblighi di legge derivanti dal quadro normativo di riferimento applicabile, con particolare riguardo alle vigenti disposizioni in materia di Privacy e trattamento di dati personali. Gli utenti devono però tener presente che, per quanto detto, in nessun caso l'Amministrazione può garantire che non saranno accedute informazioni personali degli utenti presenti in messaggi di posta elettronica residenti sui sistemi dell'Amministrazione stessa.
L'Amministrazione, in generale, non può e non intende porsi come valutatore dei contenuti dei messaggi di mail scambiati, né può proteggere gli utenti dalla ricezione di messaggi che possano essere considerati offensivi. Gli utenti sono comunque fortemente incoraggiati a usare nella posta elettronica le stesse regole di buona condotta che adopererebbero in altre forme di comunicazione.
Fatta eccezione per le ipotesi di utilizzo dei sistemi di posta certificata, l'Amministrazione non può fornire, come effettivamente non fornisce, garanzia, che i messaggi ricevuti provengano effettivamente dal mittente previsto. L'Amministrazione rappresenta, inoltre, che i messaggi di posta che arrivano come "inoltro" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto suggerisce come buona prassi di riferimento che, in caso di dubbi, l'utente che riceve un messaggio di posta elettronica provveda sempre a verificare con il mittente l'autenticità delle informazioni ricevute.

2. Scopo

2.1 Il presente regolamento ha lo scopo di definire i criteri per la gestione del posto di lavoro informatizzato nell'I.R.E. di Venezia in base a quanto previsto dal Decreto Legislativo 196 del 30/06/2003 – "Codice in materia di protezione dei dati personali" (d'ora in poi denominato Codice), dal Decreto Legislativo 82 del 07/03/2005 – "Codice dell'amministrazione digitale" e dalle "Linee guida del Garante per la posta elettronica e internet" del 1/3/2007, disciplinando le modalità di accesso e di uso della Rete Informatica e telematica e dei servizi che, tramite la stessa Rete, è possibile ricevere o offrire all'interno e all'esterno dell'Amministrazione

2.2 Ulteriore scopo del presente documento è assicurare che gli utenti del sistema informativo dell'I.R.E:

- acquisiscano piena consapevolezza e comprensione delle norme, regole, e procedure operative emanate dall'Amministrazione in merito all'accesso ed utilizzo dei sistemi e dei servizi informatici messi a loro disposizione;

- rispettino le disposizioni di legge vigenti, la giurisprudenza le disposizione emanate dalle varie Authorities competenti, in relazione all'uso corretto di Internet e della posta elettronica sul luogo di lavoro;

- rispettino i principi generali della vigente normativa in materia di privacy e trattamento dei dati personali, nonché le disposizioni specifiche applicabili all'utilizzo dei sistemi e dei servizi informatici.

2.3 Il presente regolamento vale anche come informativa sulle finalità e modalità del trattamento dei dati personali, ricavabili dalle attività di controllo tecnico svolte sul sistema, ai sensi dell'art. 13 del citato D. Lgs 196/2003.

3. Ampiezza

3.1 La Rete dell'I.R.E. è costituita dall'insieme delle Risorse informatiche, cioè dalle Risorse infrastrutturali e dal Patrimonio informativo digitale. Le Risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla Rete Informatica aziendale. Il Patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.
L'I.R.E. individua nel Servizio Sistemi Informativi il servizio interno cui affidarne la gestione, la manutenzione e lo sviluppo.

3.2 Le presenti regole si applicano a tutti gli utenti Interni ed Esterni che sono autorizzati ad accedere alla Rete aziendale. Per utenti Interni si intendono tutti gli amministratori, i dirigenti, i dipendenti a tempo indeterminato e a tempo determinato e i collaboratori occasionali. Per utenti esterni si intendono: le ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse, consulenti, stagisti, collaboratori esterni ed ogni altra categoria di persone a cui venga fornito un account di accesso per lo svolgimento delle proprie attività.

4. Accesso alle aree di trattamento di dati personali

4.1 L'accesso alle aree dove vengono trattati i dati personali è consentito esclusivamente al personale dipendente o al personale collaboratore al quale è stato attribuito specifico incarico.

4.2 L'accesso da parte di estranei è ammesso sotto il controllo e la responsabilità dei dipendenti e collaboratori incaricati.

5. Gestione e utilizzo del posto di lavoro e dei luoghi di archiviazione

5.1 Gli addetti devono gestire la documentazione di lavoro nel rispetto di norme di sicurezza al fine di minimizzare i rischi inerenti la perdita e/o la visione da parte di estranei.

5.2 Sulle scrivanie devono essere posizionate esclusivamente le pratiche contenenti dati personali in uso corrente. Conclusa la pratica, essa deve essere riposta negli appositi contenitori. Particolare attenzione va posta durante l'abbandono, anche momentaneo, del posto di lavoro. In tal caso la documentazione va celata in modo tale da non consentirne la visione da parte di chi non sia non autorizzato.

5.3 A fine di giornata qualsiasi documento contenente dati personali deve essere riposto ordinatamente negli appositi contenitori o in luoghi non accessibili agli estranei.
In deroga a quanto sopra, e solo per motivi di forza maggiore e/o di urgenza, è possibile astenersi dal riporre la documentazione, a condizione che i locali vengano chiusi a chiave e che l'ufficio interessato sia frequentato solo da altro personale addetto a mansioni analoghe.

5.4 Il personale è tenuto alla riservatezza sul contenuto delle pratiche curate di persona e da parte dei colleghi, ed è tenuto inoltre ad accertare il motivo della presenza di personale non appartenente al proprio ufficio e di estranei.

5.5 In caso di ingresso di estranei l'addetto ha l'obbligo di celare ogni informazione personale presente su materiale cartaceo o sullo schermo del proprio elaboratore.

5.6 Le stampe vanno immediatamente recuperate dalla stampante. Dove possibile, ed in caso di stampanti condivise, ogni stampa deve essere preceduta da apposito separatore indicante il soggetto o l'elaboratore richiedente. Stampanti, apparecchi fax ed apparecchiature corrispondenti devono essere collocate in luoghi in cui ne sia agevole la sorveglianza. Eventuali stampe e fotocopie non più necessarie contenenti dati personali vanno eliminate mediante l'uso di apposite apparecchiature distruggi documenti.

5.7 Particolare attenzione va posta durante la digitazione dei codici di accesso (username e password). L'addetto, prima di digitare sulla tastiera i codici sopra citati, deve assicurarsi che nessuno possa prendere visione e conoscenza di quanto immesso.

6. Particolarità gestionali per i dati personali e sensibili

6.1 Gli uffici, gli archivi, gli armadi, le cassettiere e gli arredi in genere contenenti dati personali sono dotati di serratura con chiusura a chiave o altra idonea apparecchiatura.

È vietato il trattamento e la visione di dati sensibili al personale non appositamente autorizzato da parte del Titolare o dal responsabile dei trattamenti.
Ferme restando le disposizioni del precedente paragrafo, il personale deve gestire le pratiche contenenti dati sensibili con particolare diligenza: sulla propria scrivania devono essere posizionate esclusivamente le pratiche in uso corrente e deve essere prestata la massima attenzione affinché nessuno possa venire a conoscenza delle informazioni ivi contenute. Conclusa la pratica, essa deve essere immediatamente riposta negli appositi scaffali, armadi e cassetti chiusi a chiave.
Corre inoltre obbligo al Personale di informare il titolare o il responsabile del trattamento di ogni evenienza direttamente o indirettamente idonea a compromettere la riservatezza dei dati personali.
Al termine della giornata lavorativa il personale incaricato del trattamento di dati sensibili si accerta che tutti gli armadi, cassettiere e contenitori analoghi siano chiusi a chiave.
Particolare attenzione va posta durante l'abbandono momentaneo del posto di lavoro. In tal caso la documentazione va celata in modo tale da non consentire la visione o l'asportazione della stessa da parte di personale non autorizzato.

6.2 L'accesso agli archivi e uffici contenenti dati sensibili è controllato. Le persone ammesse a qualunque titolo dopo l'orario di chiusura vengono identificate e registrate. L'autorizzazione viene data dal titolare o responsabile del trattamento.

6.3 Il trasporto delle pratiche contenenti dati sensibili è concesso su specifica autorizzazione e/o per particolari esigenze che non possano essere soddisfatte altrimenti. In tal caso il materiale cartaceo è inserito all'interno di raccoglitori, cassetti, armadi ecc.. non trasparenti e opportunamente chiusi, in modo da rendere impossibile la perdita del materiale. Se ritenuto opportuno potrà essere redatto verbale nel quale vengono individuati, mediante codici, quantitativi, descrizioni sommarie, i contenitori oggetto del trasporto.

6.4 Il Titolare, attraverso i responsabili dei trattamenti, individua per iscritto i soggetti incaricati del trattamento dei dati, specificandone gli ambiti di trattamento. Tale elenco viene aggiornato trimestralmente anche ai fini dell'aggiornamento del Documento Programmatico della Sicurezza.

7. Gestione dei sistemi di elaborazione delle informazioni

7.1 L'Amministrazione considera il sistema informativo e i servizi informatici resi disponibili nell'ambito del sistema stesso, uno "strumento" fondamentale dell'attività lavorativa, tramite il quale è possibile accedere ad un vasto patrimonio di risorse informative.

7.2 Gli utenti del sistema informativo sono tenuti ad utilizzare i sistemi ed i servizi informatici in modo responsabile, cioè, rispettando le leggi, le regole e procedure secondo standard di correttezza, buona fede e diligenza professionale. L'accesso ai sistemi ed ai servizi informatici, può essere totalmente o parzialmente limitato dall'Amministrazione, anche senza preavviso e senza necessità di assenso da parte dell'utente, quando richiesto dalla legge e in conformità ad essa, o in caso di comprovati motivi che facciano ritenere la violazione del presente regolamento o delle disposizioni di legge vigenti o quando richiesto per esigenze operative critiche e improcrastinabili.

7.3 Ciascun utente è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione.
Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio elaboratore, se non previa autorizzazione esplicita da parte dell'Amministrazione.

L'utente è tenuto ad archiviare i propri files esclusivamente nelle unità di rete assegnate alla propria unità organizzativa. L'Amministrazione può mettere a disposizione di ciascun utente un'unità di rete ad accesso riservato ed uso esclusivo, di capacità limitata a GB 1, su cui archiviare i propri dati.
Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E', infatti, assolutamente da evitare un'archiviazione ridondante.
L'utilizzatore è tenuto a non installare software non esplicitamente autorizzato e certificato dall'amministrazione. Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della normativa sulla tutela del Diritto d'Autore.

7.4 Gli operatori del Servizio Sistemi Informativi possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete, nonché procedere alla ri-formattazione e re-installazione del Sistema Operativo, anche in modo centralizzato, se necessario anche senza la presenza dell'utilizzatore.

7.5 Gli elaboratori devono essere costantemente sorvegliati dall'utilizzatore. In caso di allontanamento dal proprio posto di lavoro l'utilizzatore deve provvedere ad attivare tutte le cautele necessarie ad impedire l'accesso di estranei alle informazioni, secondo le istruzioni di seguito specificate:

- Nel caso di allontanamento dal posto di lavoro e dal sistema di elaborazione in uso per un periodo presumibilmente superiore ai sessanta minuti il computer deve venire spento;
- Per periodi inferiori l'utilizzatore deve bloccare l'accesso al computer mediante le apposite funzioni del sistema operativo, della rete o degli applicativi (per esempio facendo il log-out dal sistema o dall'applicativo utilizzato).
- In mancanza di specifica autorizzazione da parte del Titolare o suo delegato non possono essere spostati e/o portati all'esterno dell'Ente dispositivi contenenti dati personali.

8. Gestione dell'autenticazione informatica

8.1 L'accesso ai sistemi informatici è consentito previa autorizzazione (lettera d'incarico) rilasciata dal responsabile del trattamento. Quest'ultimo, contestualmente all'autorizzazione, consegna al richiedente, che ne rilascia ricevuta, copia del presente documento.
Le credenziali di autenticazione sono composte dal nome utente (username) e da una password.
L'username è attribuito e gestito dall'amministratore del sistema;
La password viene inizialmente assegnata dall'amministratore del sistema, e deve essere immediatamente cambiata dall'utente dopo il primo accesso.

8.2 La password:

- Deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui ciò non sia possibile, da un numero di caratteri pari al massimo consentito.
- Non deve contenere riferimenti agevolmente riconducibili all'incaricato o ad ambiti noti;
- Deve essere obbligatoriamente cambiata dopo il primo utilizzo e successivamente almeno ogni 3 mesi nel caso di trattamento di dati sensibili e giudiziari, ed almeno ogni sei mesi negli altri casi.
- Deve essere diversa da quelle precedentemente utilizzate;
- E' nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata ad altri utenti;
- Non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere), tratta da informazioni personali;
- Non deve presentare una sequenza di caratteri identici o in gruppi di caratteri ripetuti;
- Deve essere composta da caratteri maiuscoli e minuscoli e da numeri (per esempio E21s3tHi).

- Non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet.
- Può essere annullata e sostituita con una nuova prima della scadenza per motivate necessità e previa informazione all'utente, da parte degli amministratori di sistema o loro delegati. In questo caso essa dovrà essere nuovamente modificata al primo accesso da parte dell'utente.

9. Credenziali di autenticazione per l'accesso alternativo

9.1 Ai sensi del punto 10 dell'allegato B del Codice ciascun responsabile dei trattamenti, in accordo con gli amministratori di sistema, stabilisce idonee procedure per l'accesso ai dati personali in caso di prolungata assenza o impedimento dell'incaricato. Tale accesso deve avvenire esclusivamente per urgenti ed indifferibili necessità, anche connesse con la manutenzione tecnica e non deve comunque comportare l'utilizzo delle credenziali di autenticazione dell'incaricato. Dell'accesso alternativo ai dati e delle eventuali operazioni effettuate deve essere data tempestiva comunicazione all'incaricato al suo rientro.

10. Custodia e salvataggio dei dati personali

10.1 Ai sensi del punto 18 dell'Allegato B del Codice è fatto obbligo agli addetti del Sistema Informativo aziendale di effettuare una copia di riserva dei dati (c.d. backup), al minimo, ogni sette giorni. E' fatto inoltre obbligo di porre i supporti di memorizzazione contenenti il backup di dati personali in luogo chiuso ed accessibile al solo personale autorizzato, possibilmente in locale diverso da quello in cui si trova l'elaboratore.

11. Protezione dei sistemi da virus ed altri agenti dannosi

11.1 E' fatto obbligo agli amministratori di sistema di provvedere all'aggiornamento quotidiano dei programmi antivirus, del sistema operativo e dei programmi in dotazione (ad esempio word processor, browser). E' inoltre consigliabile provvedere all'attivazione, ove disponibili, delle procedure di aggiornamento automatico on-line sia dell'antivirus che del sistema operativo e dei programmi di cui è dotato l'elaboratore.
I programmi di protezione e supporto alla sicurezza (quali ad esempio gli antivirus, antispyware, firewall ecc..) non devono per nessun motivo essere anche temporaneamente disattivati o disinstallati.
E' inoltre consigliabile provvedere periodicamente, al minimo ogni quindici giorni, preferibilmente in periodi di inattività della macchina, all'operazione di scansione antivirus. Anche in questo caso è consigliabile utilizzare la funzione di periodica attivazione automatica.
E' fatto inoltre obbligo di segnalare ai servizi a ciò dedicati (Servizio Sistemi Informativi) ogni anomalia che possa essere riconducibile all'aggressione di un agente dannoso (reindirizzamento di pagine web, messaggi indesiderati, blocco di programmi, rallentamenti, ecc..).

12. Protezione degli apparati fisici di rete

12.1 Gli apparati fisici utilizzati per la rete dell'Ente ed il cablaggio di rete devono garantire il trasporto delle informazioni, la continuità dei servizi di connettività, la fruibilità delle informazioni dalle postazioni di lavoro nel rispetto dei sistemi di autenticazione ed autorizzazione.
I collegamenti fisici alla rete vengono assicurati da cavi fissati al muro o al pavimento e protetti da apposite canaline protette o con cavi murati.

Gli apparati di rete quali hub, switch, bridge, router, gateway ed eventuali firewall sono posti inopportuni spazi custoditi o chiusi.

13. Utilizzo dei telefoni, fax e fotocopiatrici aziendali

13.1 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.

13.2 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 Sistemi Informativi.

13.3 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.

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

14. Utilizzo di PC portatili

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

14.2 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.

14.3 I PC portatili utilizzati all'esterno (attività di lavoro fuori sede, convegni, visite in azienda, ecc), in caso di allontanamento, devono essere custoditi in un luogo protetto.

14.4 II portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.

14.5 L'utente provvederà a collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.

15. Accesso e utilizzo di internet

15.1 L'utilizzo di Internet, la navigazione in rete e/o l'utilizzo della posta elettronica è consentita ai titolari di account espressamente autorizzati.

15.2 E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

15.3 Gli utenti del servizio internet sono tenuti ad usarlo in modo responsabile, nel pieno rispetto della normativa di riferimento vigente, nonché, avuto espresso riguardo alla presente ed alle altre regole e procedure e secondo normali standard di correttezza, buona fede e diligenza professionale.
L'accesso ai servizi di connettività internet può essere totalmente o parzialmente limitato dall'Amministrazione, anche senza preavviso e senza necessità di assenso da parte dell'utente, quando richiesto dalla legge e in conformità ad essa, o in caso di comprovati motivi che facciano ritenere la violazione di quanto contenuto nel presente documento o delle disposizioni di legge vigenti, o in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

15.4 E' fatto espresso divieto a tutti gli utenti di utilizzare il collegamento internet per inviare o inserire nell'ambito di blog, forum di discussione o servizi similari, messaggi di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio o testo che possa arrecare danno alla reputazione dell'Amministrazione. E' vietato scaricare o trasmettere materiale osceno, diffamatorio, intimidatorio, discriminatorio o comunque contrario alla legge sotto qualunque forma, (immagini, testi, filmati, registrazioni vocali ecc.). E' vietato trasmettere o scaricare ed installare materiale protetto da copyright. E' inoltre vietato l'uso della connessione internet a scopi commerciali o di profitto personale e per attività illegali. E' proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi che facciano richiesta di questo tipo di informazioni. E' infine proibito accedere ad Internet dalle postazioni di lavoro dell'Amministrazione aggirando i sistemi di sicurezza predisposti allo scopo, utilizzando modem o altri mezzi di accesso diretto.

15.5 Le risorse di rete e di memoria dei computer sono limitate. Tutti gli utenti hanno pertanto la responsabilità di farne un uso oculato evitando di sprecare deliberatamente dette risorse o di monopolizzarne l'uso a discapito degli altri utenti. Gli utenti devono pertanto astenersi da:

- inviare messaggi di posta elettronica ad un gran numero di destinatari o partecipare a "Catene di S. Antonio",
- spendere un'eccessiva parte del proprio tempo navigando su Internet,
- caricare o scaricare file di grandi dimensioni,
- in generale, generare immotivatamente carico eccessivo sulle strutture elaborative per scopi privati o personali.

15.6 Per motivi di sicurezza e di prestazioni tutte le connessioni ad internet richiedono, da parte degli utenti abilitati, l'autenticazione ad un proxy server che registra, in appositi file di log le seguenti informazioni:

- IP, nome utente, agente client;
- Data, ora registro;
- Nome host, IP, porta di destinazione;
- Tempo di elaborazione, byte ricevuti, byte inviati,
- Protocollo, metodo HTTP, URL;
- Rete di origine. Rete di destinazione

I file di log sono conservati per un periodo di tre mesi.
L'Amministrazione non ispeziona sistematicamente queste registrazioni. D'altro canto, l'Amministrazione potrà permettere l'ispezione e l'analisi dei file di log nei seguenti casi:

- su richiesta scritta dell'autorità giudiziaria nei casi previsti dalla legge;
- per gravi e comprovati motivi che facciano ragionevolmente ritenere sussistente un pregiudizio e/o una violazione di legge o delle regole in materia di sicurezza (definiti in Allegato A - DEFINIZIONI);

- per atti dovuti (definiti in Allegato A - DEFINIZIONI);
- in situazioni critiche e di emergenza (definiti in Allegato A - DEFINIZIONI).

15.7 Oltre a quanto indicato al precedente punto 15.6, gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la necessità di analizzare i dati risultanti dai file di log delle connessioni internet. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora si verificassero i casi citati.

16. Utilizzo della posta elettronica

16.1 L'Amministrazione incoraggia l'uso della posta elettronica per scambiare informazioni, migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro a supporto della missione istituzionale della P.A.

16.2 Il servizio di posta elettronica dell'I.R.E., erogato per il tramite dei Fornitori dei servizi in outsourcing, è proprietà dell'Amministrazione, pertanto ogni casella di posta elettronica associata alla stessa (con il dominio *irevenezia.it*) ovvero assegnata a suoi uffici o assegnata a individui o funzioni di questa, sono di proprietà esclusiva dell'Amministrazione stessa.

16.3 L'Amministrazione non può essere ritenuta responsabile per qualsiasi danno, diretto o indiretto, arrecato all'Utente ovvero a terzi e derivante:

- dall'eventuale interruzione del Servizio,
- dall'eventuale smarrimento di messaggi diffusi per mezzo del Servizio,
- da messaggi inviati/ricevuti o da transazioni eseguite tramite il Servizio,
- da accesso non autorizzato ovvero da alterazione di trasmissioni o dati dell'Utente.

16.4 Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, le presenti e altre regole e procedure dell'Amministrazione e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi di posta elettronica dell'Amministrazione può essere totalmente o parzialmente limitato dall'Amministrazione stessa, senza necessità di assenso da parte dell'utente e anche senza preavviso:

- quando richiesto dalla legge e in conformità ad essa,
- in caso di comprovati motivi che facciano ritenere la violazione del presente regolamento o delle disposizioni di legge vigenti,
- al venir meno delle condizioni in base alle quali si ha facoltà di utilizzare il servizio (ad es. cessazione per qualsiasi motivo del rapporto di lavoro con l'Amministrazione),
- in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili

16.5 L'Amministrazione è tenuta in generale ad ottenere l'assenso del titolare della casella di posta elettronica prima di ogni ispezione dei messaggi o accesso alle registrazioni o ai messaggi di posta elettronica, fatta eccezione per quanto disposto al precedente paragrafo. D'altro canto, ci si attende che il personale dell'Amministrazione soddisfi le richieste della stessa riguardanti la fornitura di copie delle registrazioni di posta elettronica in suo possesso e che riguardino le attività lavorative svolte per l'Amministrazione o richieste per soddisfare obblighi di legge, indipendentemente dal fatto che tali registrazioni risiedano o meno su computer di proprietà dell'Amministrazione. Il mancato rispetto di tali richieste può portare all'applicazione delle condizioni di cui al paragrafo precedente.

16.6 L'Amministrazione non ispeziona e non accede ai messaggi di posta elettronica dell'utente senza la sua autorizzazione. D'altro canto, l'Amministrazione potrà permettere l'ispezione, il monitoraggio o l'accesso alla posta elettronica degli utenti, anche senza l'assenso del titolare, solamente nei seguenti casi:

- su richiesta scritta dell'autorità giudiziaria nei casi previsti dalla normativa vigente;
- previo preavviso all'utente, per gravi e comprovati motivi (come definiti in Allegato A - DEFINIZIONI)
- che facciano credere che siano state violate le disposizioni di legge vigenti o le regole dell'Amministrazione in materia di sicurezza;
- per atti dovuti (definiti in Allegato A - DEFINIZIONI);
- in situazioni critiche e di emergenza (definiti in Allegato A - DEFINIZIONI).

16.7 L'Amministrazione registra e conserva, in forma anonima, i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime:

- Data, ora, oggetto, mittente e destinatario;

I file di registro sono conservati per un periodo di tre mesi.

16.8 E' fatto espresso divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente quali, a titolo esemplificativo e non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione dell'Amministrazione.

16.9 E' inoltre vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali e la fornitura (gratuita o a pagamento) a persone fisiche o giuridiche di qualsiasi lista o elenco degli Utenti del Servizio. E' proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi e-mail che facciano richiesta di questo tipo di informazioni. Chiunque riceva comunicazioni della natura sopra indicata dovrà segnalarlo al Servizio Sistemi Informativi tramite messaggio di posta elettronica inviato all'indirizzo *ict@irevenezia.it* ovvero utilizzando gli eventuali servizi di assistenza online accessibili attraverso il sito dell'Amministrazione.

a) E' consentito l'utilizzo dell'account fornito con il dominio "*irevenezia.it*" a fini privati e personali, purché, in aggiunta a quanto indicato nei punti precedenti, tale utilizzo non sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica dell'Amministrazione.
b) Oltre a quanto indicato al precedente punto 15.6, gli utenti devono tener presente che, nell'assolvimento dei propri compiti, il personale che gestisce i sistemi di elaborazione e le reti di telecomunicazione può avere, saltuariamente, la necessità di analizzare i dati transazionali dei messaggi di posta per garantire il corretto funzionamento del servizio e in queste occasioni è possibile che avvengano inavvertitamente accessi al contenuto stesso dei messaggi. Tale personale è tenuto comunque al rispetto di stretti vincoli di riservatezza qualora si verificassero i casi citati.
c) L'Amministrazione si pone come obiettivo fondamentale la fornitura di servizi di posta elettronica sicuri ed affidabili avvalendosi di fornitori altamente qualificati. Va comunque ricordato, come già detto in precedenza, che la sicurezza e riservatezza della posta elettronica non possono essere garantite in ogni circostanza, in particolare per quanto concerne i messaggi di posta scaricati sui Personal Computer. In questo caso è indispensabile che l'utente stesso provveda ad attuare le azioni adeguate a proteggere le informazioni usando tutti i mezzi disponibili, quali ad esempio password di accesso alle applicazioni e alla propria postazione di lavoro.

16.10 L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.

16.11 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

17. Controlli

17.1 Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Amministrazione verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

17.2 In caso di anomalie, gli amministratori di sistema effettueranno controlli anonimi che si concluderanno con avvisi generalizzati diretti 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 e per i casi di particolare gravità solo su autorizzazione della Direzione Generale.

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

18. Violazioni

18.1 Il personale che contravviene alle norme indicate nel presente regolamento, stanti le responsabilità individuali di tipo civile e penale verso terze parti, potrà essere oggetto di sanzioni di tipo disciplinare e/o, ove previste, di tipo amministrativo la cui entità e modalità di erogazione corrispondono a quanto previsto dalla vigente normativa e dalla contrattazione collettiva.

19. Aggiornamento e revisione

19.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente regolamento tramite comunicazione al Servizio Sistemi Informativi.
Il presente Regolamento è soggetto a revisione con frequenza almeno annuale.

ALLEGATO A - DEFINIZIONI

Grave e comprovato motivo: evidenza oggettiva, non basata quindi su semplici sospetti o illazioni, che dimostra l'avvenuta violazione di disposizioni di leggi vigenti o delle regole di sicurezza dell'Amministrazione.

Atti dovuti: circostanze in base alle quali la mancanza di adeguate azioni può comportare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte.

Situazioni critiche o di emergenza: circostanze in cui la tempestività d'azione è di fondamentale importanza al fine di evitare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte o l'interruzione dei servizi informatici e la continuità operativa dei processi dell'Amministrazione.