PROVINCIA REGIONALE DI CALTANISSETTA

REGOLAMENTO
PER IL CORRETTO UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE

***Assessore**: Vincenzo Insalaco*

***Dirigente**: Angela Maria Vizzini*

Dicembre 2008

INDICE

Capo I

Art. 1 – Finalità

Il presente regolamento ha lo scopo di disciplinare l'utilizzo delle risorse informatiche e telematiche della Provincia Regionale di Caltanissetta al fine di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati e all'immagine dell'Amministrazione stessa.

Art. 2 - Definizioni

Definizione di Servizio Sistema Informatico Provinciale

Il *Servizio Sistema Informatico Provinciale* – da qui in avanti indicato con l'acronimo *S.S.I.P.* -, istituito con atto di C.P. n. 91 del 05/08/2002, si basa su un insieme di *reti locali*, una per ogni plesso in cui sono dislocati gli uffici della Provincia, comprese le sedi periferiche (*Gela, Mazzarino, Mussomeli, etc.*), collegate in *rete geografica* al fine di realizzare un'unica *rete privata virtuale* (*VPN*).

Tutti i personal computer utilizzati dal personale dipendente, sono quindi, collegati sulla rete locale (*LAN*) di appartenenza e tramite questa all'intera rete della Provincia.

Il collegamento ad *internet* ed i servizi di *posta elettronica* sono realizzati tramite un unico punto di raccordo che collega, con un canale a *larga banda*, tutta la VPN della provincia all'*internet service provider (ISP)* che fornisce la connettività con la rete nazionale ed internazionale.

Definizione di alcune figure interne al Servizio Sistema Informatico Provinciale

1. Viene definito Responsabile del S.S.I.P. il Direttore del Settore Informatica, Statistica e Programmazione.
2. Viene definito Amministratore di Sistema colui che:
   - Si occupa della gestione, manutenzione e controllo dei sistemi;
   - Verifica la corretta esecuzione dei lavori secondo gli standard fissati.
3. Viene definito Responsabile della Rete e della Sicurezza colui che:

- Ha la gestione della rete locale e remota.
- Ha la gestione degli strumenti dedicati alla sicurezza della rete.

Definizione di incaricato

Viene definito incaricato l'utente incaricato, ai sensi dell'art. 30 del d.lgs.vo n.196/2003, del trattamento dei dati personali e/o sensibili.

Definizione di Utente

Viene definito utente "Chiunque utilizzi un elaboratore, un'applicazione locale o web, una risorsa o un servizio erogato dal S.S.I.P., sia che il collegamento avvenga dall'interno della rete locale (Lan), sia che esso avvenga in remoto, come nel caso di cittadini, imprese o Enti esterni che consultano il sito internet della Provincia Regionale di Caltanissetta."

Capo II

Art. 3 – Utilizzo del Personal Computer

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.
2. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per l'accesso ad ogni tipo di applicazione, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios) senza la preventiva autorizzazione da parte del Responsabile del S.S.I.P. o del Responsabile della rete e della sicurezza.
3. Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione dell'Amministratore di Sistema e/o del Responsabile della rete e della sicurezza, in quanto sussiste il grave pericolo di introdurre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

4. Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal Responsabile del S.S.I.P.. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Amministrazione a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
5. Non è consentito all'utente modificare le caratteristiche impostate sul proprio P.C., senza la preventiva autorizzazione dell' Amministratore di Sistema.
6. Il Personal Computer deve essere spento ogni giorno 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. Dovrà, comunque, attivarsi lo screen saver e la relativa password.
7. Non è consentita l'installazione sul proprio P.C. di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, switch, ecc.), se non con l'autorizzazione espressa del Responsabile della rete e della sicurezza.
8. Agli utenti incaricati del trattamento dei dati sensibili è fatto divieto l'accesso contemporaneo con lo stesso account da più Personal Computer.
9. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile della rete e della sicurezza nel caso in cui vengano rilevati virus, adottando quanto previsto all'art. 12 del presente regolamento relativo alle procedure di protezione antivirus.
10. 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.
11. Non è consentito, senza la preventiva autorizzazione del Responsabile della rete e della sicurezza, collegare alla rete della Provincia P.C. portatili, se non quelli assegnati in dotazione dall'Ente stesso.

Art. 4 – Utilizzo della Rete

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, vengono svolte regolari attività di controllo, amministrazione e backup da parte sia del Responsabile della rete e della sicurezza che dell'Amministratore di Sistema.
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 altri nomi utente.
3. Il Responsabile della rete e della sicurezza può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui P.C. degli incaricati sia sulle unità di rete.
4. Costituisce buona regola la pulizia degli archivi, da effettuarsi almeno ogni sei mesi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
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 (molto lunghi o non supportati, come ad esempio file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

Art. 5 – Gestione delle Password e delle User-id

1. Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono attribuite dal Responsabile della rete e della sicurezza e/o dall'Amministratore di Sistema.
2. L'incaricato deve provvedere a modificare la password al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, d.lgs.vo n.196/2003) con contestuale comunicazione al proprio Dirigente.

3. La password deve essere composta da almeno otto caratteri e formata da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema.
4. La password deve essere segreta e quindi non conoscibile da terzi. Ogni incaricato dovrà adottare le necessarie cautele per assicurare la sua segretezza.
5. La password non deve contenere riferimenti agevolmente riconducibili all'interessato (nomi, cognomi, soprannomi, date di nascita, ecc.).
6. Nessuno, neppure il Titolare del trattamento (art. 28 del d.lgs.vo n.196/2003), può accedere allo strumento elettronico, utilizzando la credenziale di autenticazione dell'incaricato.

   Eccezione a tale regola si ha solo se si verificano congiuntamente le seguenti condizioni:

   - Prolungata assenza o impedimento dell'incaricato;
   - L'intervento è indispensabile e indifferibile;
   - Vi sono concrete necessità di operatività e di sicurezza del sistema.

   A tal fine gli incaricati dovranno:

   - Predisporre una copia della parola chiave, provvedendo a trascriverla su un foglio ed inserendola in una busta chiusa;
   - Consegnare tale copia al proprio Dirigente.

   Solo al verificarsi delle condizioni sopraesposte, il Titolare o un responsabile potranno richiedere la busta contenente la password al Dirigente.

   Rientrano tra i compiti del Dirigente:

   - Conservare in luogo sicuro e chiuso a chiave le buste contenenti le password;
   - Provvedere ad informare, tempestivamente e per iscritto, l'incaricato cui appartiene la parola chiave, dell'accesso effettuato;
   - Verificare la regolare consegna nei tempi previsti (sei o tre mesi) delle buste con le nuove password da parte degli incaricati.
7. La password deve essere immediatamente sostituita, dandone comunicazione al Dirigente, nel caso si sospetti che la stessa abbia perso la segretezza.
8. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all'Amministratore di Sistema e/o al Responsabile della rete e della sicurezza.

9. Il codice di identificazione (user-id), che l'Amministratore di Sistema e/o il Responsabile della rete e della sicurezza provvede a fornire all'incaricato, deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi.
10. Le credenziali di autenticazione (password e user-id) devono essere disattivate nei seguenti casi:
    - Immediatamente, nel caso in cui l'incaricato perda la qualità che gli consentiva di accedere allo strumento: ciò non accade solo se la persona cessa di lavorare, ma può ad esempio avvenire anche se l'incaricato viene trasferito da un ufficio all'altro, con conseguente cambio delle mansioni e degli ambiti di trattamento dei dati personali, che rendessero necessaria l'attribuzione di una nuova chiave.
    - In ogni caso, entro sei mesi di mancato utilizzo. Fa eccezione il caso delle chiavi che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo assume generalmente caratteristiche di sporadicità (ad esempio, potrebbero essere utilizzate solo una volta l'anno, nel quadro della verifica globale, sulla funzionalità complessiva del sistema).

Art. 6 – Utilizzo dei supporti magnetici

1. Tutti i supporti magnetici riutilizzabili (dischetti, cassette, CD, DVD, cartucce) 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.
2. I supporti magnetici riutilizzabili (dischetti, cassette, CD, DVD, cartucce) contenenti dati sensibili devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.
3. Al cessare delle ragioni della conservazione dei dati, dovranno essere adottati gli opportuni accorgimenti per rendere non intelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti magnetici, al fine di impedire che essi vengano carpiti da persone non autorizzate al trattamento. Si devono quindi cancellare i dati, se possibile, o distruggere i supporti, se necessario.
4. I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

5. Non è consentito scaricare files contenuti in supporti magneto/ottici non aventi alcuna attinenza con la propria attività lavorativa.
6. Tutti i files di provenienza incerta od esterna, ancorchè attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo.
7. Ogni incaricato deve prestare la massima attenzione ai supporti di origine esterna, avvertendo il responsabile della rete e della sicurezza nel caso in cui siano rilevati virus ed adottando quanto previsto dal presente Regolamento relativamente alle procedure di protezione antivirus.
8. Nel caso di P.C. portatili accessibili per mezzo di smart card o tessere magnetiche in possesso a proprio uso, ogni incaricato dovrà conservare (es. non abbandonandole sulla scrivania) e proteggere (es. non avvicinandole a fonti di calore) tali dispositivi con la massima cura.

Art. 7 – Utilizzo di Personal Computer portatili

1. L'utente è responsabile del P.C. portatile assegnatogli dal Responsabile del S.S.I.P. e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai P.C. portatili si applicano le regole di utilizzo previste per i P.C. connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
3. I P.C. portatili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Art. 8 – Salvataggio e ripristino dei dati

1. I dati personali devono essere salvati con cadenza almeno mensile.
2. I dati residenti su Server devono essere salvati con cadenza giornaliera.
3. Per i dati sensibili l'incaricato deve essere in grado di provvedere al ripristino degli stessi entro sette giorni.

Capo III

Art. 9 – Uso della Posta Elettronica

1. La casella di posta, assegnata dall'Amministrazione all'incaricato, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
2. È fatto divieto di utilizzare le caselle di posta elettronica istituzionali "iniziale nome.cognome***@provincia.caltanissetta.it***" per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
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.
4. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Amministrazione deve essere visionata od autorizzata. In ogni modo, è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
5. Per la trasmissione di file all'interno dell'Amministrazione è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
6. È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
7. È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, non si devono in alcun caso attivare gli allegati di tali messaggi.

Art. 10 – Uso della Rete Internet e dei relativi servizi

1. Il P.C. abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

2. È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile della rete e della sicurezza.
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 dall'Amministrazione e con il rispetto delle normali procedure di acquisto.
4. È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
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).

Capo IV

Art. 11 – Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nel Documento programmatico sulla Sicurezza redatto annualmente ai sensi del disciplinare tecnico allegato al d.lgs.vo n. 196/2003.

Art. 12 –Protezione antivirus

1. Il Responsabile della rete e della sicurezza gestisce la sicurezza del sistema informatico attraverso strumenti software sempre aggiornati e le cui licenze d'uso sono rinnovate annualmente dal S.S.I.P.
2. Ogni incaricato deve tenere comportamenti tali da proteggere i dati personali contro il rischio di intrusione e dall'azione di programmi (virus) aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento (art.615-quinquies del codice penale).

3. Nel caso che il software antivirus rilevi la presenza di un virus, l'incaricato dovrà immediatamente:
    - Sospendere ogni elaborazione in corso senza spegnere il computer;
    - Segnalare l'accaduto al Responsabile della rete e della Sicurezza.
4. Non è consentito l'utilizzo di floppy disk, cd rom, cd riscrivibili, dvd, dvd riscrivibili, nastri magnetici di provenienza ignota.
5. Ogni dispositivo magnetico di provenienza esterna, prima del suo utilizzo, dovrà essere verificato mediante il programma antivirus; nel caso venga rilevato un virus, dovrà essere consegnato al Responsabile della rete e della Sicurezza.

Art.13 - Competenze e responsabilità

Le competenze e le responsabilità del personale dell'Amministrazione Provinciale per ciò che concerne l'utilizzo dei servizi di rete e telematici, sono definite nei commi seguenti.

1. Il Responsabile del S.S.I.P. è tenuto a:
    - Informare il personale sulle disposizioni in merito all'uso consentito delle risorse del sistema informatico dell'Ente;
    - Assicurare che il personale a lui assegnato, i fornitori e/o eventuale personale incaricato esterno uniformino le proprie attività alle regole ed alle procedure descritte nel presente Regolamento.
2. I Dirigenti dei vari settori sono tenuti a:
    - Informare il proprio personale sulle disposizioni in merito all'uso consentito delle risorse del S.S.I.P. ed verificare che questo si uniformi alle regole ed alle procedure descritte nel presente Regolamento;
    - Adempiere a tutti gli obblighi inerenti la responsabilità loro affidata in materia di trattamento di dati personali, in applicazione del d.lgs.vo n.196/2003 e del *Documento Programmatico sulla Sicurezza* (*D.P.S.*).
3. L'amministratore di Sistema è incaricato di:
    - Monitorare i sistemi al fine di individuare un eventuale uso non corretto degli stessi, nel rispetto della privacy degli utenti;
    - Segnalare immediatamente al Responsabile del S.S.I.P. ogni eventuale attività non autorizzata sui sistemi;

- Effettuare il salvataggio di tutti gli oggetti dei sistemi centralizzati, quotidianamente nelle ore notturne, in maniera tale da garantirne il ripristino in qualsiasi momento.

4. Il Responsabile della rete e della sicurezza informatica è tenuto a svolgere le seguenti attività:
   - Elaborazione delle regole relative all'utilizzo del S.S.I.P;
   - Segnalazione immediata al Responsabile del S.S.I.P. di ogni eventuale attività non autorizzata sulla rete;
   - Implementazione delle policy di sicurezza (linee di condotta precise e chiare alle quali tutti gli utenti devono attenersi) del S.S.I.P..
5. L'utente è responsabile per ciò che concerne:
   - Il rispetto delle regole del presente regolamento;
   - La pronta segnalazione di ogni eventuale attività non autorizzata di cui sia venuto a conoscenza per motivi di ufficio;
   - L'uso delle credenziali assegnategli;
   - I backup periodici del proprio lavoro su supporti magnetici e/o su dispositivi indicati dal S.S.I.P.. Non è consentito effettuare backup aggiuntivi su dispositivi e/o punti di memorizzazione diversi da quelli di cui sopra.

Art. 14 –Non osservanza della normativa interna

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.

Art. 15 – Aggiornamento e revisione

Tutti i Dirigenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento.

La revisione del presente Regolamento sarà curata dal Dirigente del Settore Informatica Statistica e Programmazione.