

IL DIRETTORE GENERALE ALL'ORGANIZZAZIONE, PERSONALE, SISTEMI  
INFORMATIVI E TELEMATICA

Visto il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali";

Viste le deliberazioni della Giunta regionale:

- n. 960 del 27/06/2005 con cui è stata adottata la Direttiva in materia di trattamento di dati personali;
- n. 1264 del 01/08/2005 con cui sono state adottate le Linee guida della Giunta della Regione Emilia-Romagna in materia di protezione dei dati personali;

Vista inoltre la propria determinazione n. 1035/2006 "Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna" che definiva il carattere sperimentale delle prescrizioni in esso contenute.

Considerato che la sperimentazione, condotta per la durata di un anno, non ha evidenziato criticità tali da prevedere una modifica delle prescrizioni già individuate bensì solo revisioni di mera forma per migliorarne la chiarezza espositiva;

Sentito il parere del Comitato di Direzione nella seduta del 26/02/2007;

Dato atto di aver rispettato le vigenti disposizioni in materia di relazioni sindacali;

Dato atto del parere di regolarità amministrativa espresso dal Responsabile della Sicurezza della Giunta, ai sensi della deliberazione della Giunta Regionale n. 960 del 27/06/2005;

DETERMINA

1. di approvare l'allegato "Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna";
2. di applicare all'interno delle proprie strutture l'allegato "Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna";
3. di procedere alla diffusione del contenuto dell'allegato "Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna" a partire dalla data di approvazione del presente atto a tutti gli utenti dei sistemi informativi dell'Ente.

IL DIRETTORE GENERALE  
(Gaudenzio Garavini)

Allegato

## **Disciplinare tecnico per utenti sull'utilizzo dei sistemi informativi nella Giunta della Regione Emilia-Romagna**

## INDICE

<b>1. Premessa</b> .....	<b>3</b>
<b>2. Applicabilità</b> .....	<b>3</b>
<b>3. Sicurezza fisica</b> .....	<b>4</b>
3.1 Sicurezza dei locali .....	4
3.2 Postazioni di lavoro.....	4
3.3 Dispositivi mobili .....	5
<b>4. Controllo degli accessi</b> .....	<b>6</b>
4.1 Accesso ai dati .....	6
4.2 Autenticazione .....	6
4.3 Gestione delle credenziali .....	7
4.4 Password.....	7
4.5 Verifiche di sicurezza.....	8
<b>5. Protezione dei dati trattati senza l'utilizzo di strumenti elettronici</b> .....	<b>9</b>
<b>6. Confidenzialità e disponibilità dei dati</b> .....	<b>10</b>
6.1 Confidenzialità dei dati .....	10
6.2 Disponibilità dei dati.....	10
6.3 Dati su dispositivi mobili .....	11
<b>7. Protezione delle reti e delle comunicazioni</b> .....	<b>12</b>
7.1 Sicurezza della rete interna.....	12
7.2 Navigazione in Internet .....	12
7.3 Utilizzo della posta elettronica .....	12
7.4 Spamming.....	13
7.5 Phishing .....	14
7.6 Virus.....	14
7.7 Software autorizzato .....	15
7.8 Telelavoro e accesso remoto .....	15
<b>8. Prevenzione e gestione degli incidenti informatici</b> .....	<b>16</b>
<b>Appendice A: Glossario</b> .....	<b>17</b>

## **1. Premessa**

Il presente disciplinare tecnico descrive le regole tecniche ed organizzative da applicare per garantire la sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche nella Giunta della Regione Emilia-Romagna (di seguito denominata "Ente").

Si precisa che quanto riportato nel presente disciplinare tecnico non esaurisce tutte le prescrizioni contenute nelle vigenti normative relative ad illeciti disciplinari, civili e penali, con particolare riferimento alle violazioni di sicurezza e ai reati informatici.

Ai fini del presente disciplinare tecnico, si intende per sistema informativo il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni.

I destinatari del presente disciplinare devono considerare le minacce di sicurezza e le contromisure disponibili (comportamenti da evitare o da tenere) relativamente a dati e informazioni, secondo le indicazioni fornite nei paragrafi seguenti.

Tali paragrafi disciplinano i seguenti aspetti della sicurezza globale del sistema informativo:

- sicurezza fisica;
- controllo degli accessi;
- protezione dei dati trattati senza l'ausilio di strumenti elettronici;
- protezione e disponibilità dei dati;
- protezione delle reti e delle comunicazioni;
- prevenzione e gestione degli incidenti informatici.

## **2. Applicabilità**

La protezione dei dati e delle informazioni nel loro complesso è condizione necessaria per garantire il rispetto dei requisiti di sicurezza che la **normativa vigente** impone a tutti i soggetti che, a vario titolo, effettuano il trattamento di **dati personali**. A causa dell'interconnettività e dell'interdipendenza fra le componenti di un sistema informativo, infatti, i problemi di sicurezza su una sola di esse propagano i loro effetti, incidendo gravemente sulla sicurezza del sistema (per es. una postazione di lavoro non adeguatamente protetta può rendere vulnerabile la intranet dell'Ente anche in presenza di firewall o altri sistemi di sicurezza perimetrale).

Per quanto sopra, l'ambito di applicabilità del disciplinare tecnico si estende non solo ai c.d. **responsabili** e **incaricati** del trattamento di dati personali individuati dal **titolare**, ma a tutti i dipendenti appartenenti all'organico dell'Ente che utilizzano le risorse dei sistemi informativi, nonché a tutti coloro che a vario titolo le utilizzano in nome e/o per conto dell'Ente, ovvero che sono autorizzati, in base ad uno specifico titolo (per es. convenzioni, contratti, ecc.) ad utilizzarlo. Nel seguito del disciplinare, i soggetti di cui sopra sono denominati "utenti".

### **3. Sicurezza fisica**

#### **3.1 Sicurezza dei locali**

##### **Minacce**

Accesso non autorizzato ai locali, accesso non autorizzato alle risorse, accesso non autorizzato ai dati.

##### **Contromisure**

- A. Rispettare le regole indicate nel "*Disciplinare tecnico relativo al controllo degli accessi ai locali della Giunta della Regione Emilia-Romagna*" per l'accesso ai locali dell'Ente.
- B. Custodire con massima cura le credenziali di autorizzazione per l'accesso ai locali ove previste (per es. badge, chiavi, tessere identificative, ecc.).
- C. Dare immediata comunicazione al proprio responsabile funzionale dell'eventuale smarrimento delle suddette credenziali.

#### **3.2 Postazioni di lavoro**

##### **Minacce**

Utilizzo delle postazioni di lavoro da parte di personale non autorizzato, trattamento non consentito di dati personali.

##### **Contromisure**

- A. Utilizzare la postazione di lavoro, fornita dall'Ente quale supporto all'attività lavorativa, in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi.
- B. Proteggere i computer e le altre strumentazioni informatiche, in caso di assenza, anche temporanea, dalla postazione di lavoro, tramite la sospensione o il blocco della sessione di lavoro. In particolare:
  - a. L'utente che si allontana dalla propria postazione di lavoro, ma sia certo di ritornarvi entro la fine della giornata lavorativa, è tenuto a:
    - accertarsi di aver chiuso tutti i documenti aperti, per permettere ad altri utenti di utilizzare gli stessi se condivisi su server di rete;
    - bloccare il sistema (per es. sui sistemi Windows 2000/XP con la combinazione di tasti CTRL+ALT+CANC e quindi "Blocca computer") o attivare la funzione di logout (per es. sui sistemi Windows 2000/XP con la combinazione di tasti CTRL+ALT+CANC e quindi "Disconnetti");
    - impostare l'attivazione dello screen saver entro pochi minuti di inattività per impedire la lettura dei dati presenti a video; è necessario che l'accesso al sistema dopo l'intervento dello screen saver sia vincolato all'**autenticazione** dell'utente, abilitando l'opzione "Al ripristino proteggi con **password**".
  - b. L'utente che si allontana dalla propria postazione di lavoro per non ritornarvi entro la fine della giornata lavorativa, è tenuto a terminare la sessione di lavoro (per es.

arrestando il sistema o attivando la funzione “Disconnetti”).

### 3.3 Dispositivi mobili

#### **Minacce**

Furto dei dispositivi, danneggiamento involontario, accesso non consentito ai dati contenuti nei dispositivi.

#### **Contromisure**

A. Prevedere, in aggiunta alle regole indicate ai paragrafi 3.1 e 3.2, ulteriori misure di sicurezza per i dispositivi mobili (computer portatili, palmari, telefoni cellulari, pendrive, macchine fotografiche digitali, videocamere, ecc.) che tengano conto dei seguenti fattori:

- *natura dei dispositivi*: i dispositivi mobili sono facilmente trasportabili ed occultabili;
- *natura dei dati presenti sui dispositivi*: sui dispositivi mobili possono essere presenti copie parziali e/o temporanee di dati personali o comunque di importanza strategica per la sicurezza dei sistemi;
- *modalità di utilizzo dei dispositivi*: i dispositivi mobili possono essere utilizzati in contesti diversi anche al di fuori di sedi dell'Ente ed in aree non sicure. Ciò rappresenta una minaccia per la sicurezza dei sistemi nel momento in cui, per esempio, un portatile si riconnette alla rete interna.

B. Non lasciare incustoditi, in nessun caso, i dispositivi mobili. In particolare, sia all'interno delle sedi dell'Ente sia all'esterno, l'utente è tenuto a:

- custodire adeguatamente i dispositivi durante le ore notturne o in periodi di assenza (per es. non lasciare i dispositivi sulla scrivania ma custodirli invece in armadi o cassetti chiusi a chiave, dotare i portatili di dispositivi di fissaggio, ecc.);
- trasportare i dispositivi come bagaglio a mano durante i viaggi in aereo;
- non lasciare i dispositivi incustoditi, neanche temporaneamente, durante i viaggi effettuati in treno o con altri mezzi di trasporto;
- non lasciare i dispositivi in auto, se non in casi eccezionali, e comunque chiuderli nel bagagliaio non a vista in modo da non evidenziarne la presenza dall'esterno;
- non lasciare i dispositivi in vista nelle stanze degli hotel, ma chiuderli in un armadio o in una valigia o depositarli in cassaforte se si prevede un'assenza prolungata.

C. Osservare le istruzioni del fabbricante per la protezione dei dispositivi durante il trasporto nei confronti di urti, campi elettromagnetici, sbalzi di temperatura.

D. Non utilizzare i dispositivi mobili, all'interno dei locali dell'Ente, per l'effettuazione di registrazioni audio e/o video, se non per scopi espressamente collegati a specifiche attività istituzionali.

E. Osservare, in caso di utilizzo di dispositivi mobili per telelavoro, le disposizioni illustrate al paragrafo 7.8.

F. I dispositivi mobili ad uso individuale devono essere utilizzati esclusivamente dall'utente

a cui gli stessi sono stati assegnati.

- G. L'utilizzo dei dispositivi mobili assegnati alle strutture deve essere regolamentato dalle stesse in funzione delle proprie peculiarità ed in modo tale da garantire il controllo sul loro utilizzo. In ogni caso, deve essere individuato un referente che deve provvedere al collegamento dei dispositivi alla LAN dell'Ente almeno una volta ogni 30 giorni per effettuare gli aggiornamenti automatici del software antivirus e delle [patch](#) di sicurezza.
- H. Non portare al di fuori dei locali dell'Ente dispositivi mobili contenenti dati personali, se non espressamente autorizzati.

#### **4. Controllo degli accessi**

##### **4.1 Accesso ai dati**

###### ***Minacce***

Accesso ai dati da parte di personale non autorizzato.

###### ***Contromisure***

- A. L'accesso ai dati, ed alle strumentazioni informatiche utilizzate per trattarli, è consentito esclusivamente al personale espressamente autorizzato.
- B. Nel caso di dati personali, l'accesso è consentito ai soli responsabili o incaricati del trattamento, individuati secondo le modalità previste al paragrafo 7 della Delibera di Giunta numero 960 del 27/06/05.

##### **4.2 Autenticazione**

###### ***Minacce***

Accesso ai sistemi da parte di personale non autorizzato.

###### ***Contromisure***

- A. L'accesso ai dati trattati con strumentazioni informatiche deve avvenire esclusivamente previa autenticazione, ossia tramite una procedura che verifica anche indirettamente l'identità di chi vi accede.
- B. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'utente, eventualmente associata a un codice identificativo o a una parola chiave. Per esempio:
- credenziali di autenticazione basate su parola chiave segreta: le credenziali (userid+password) utilizzate per l'accesso alle risorse di dominio (postazioni di lavoro, posta elettronica, server intranet, ecc.) o per l'accesso alle applicazioni SAP o Mainframe;
  - credenziali di autenticazione basate su dispositivo in possesso e uso esclusivo dell'utente: le credenziali (carta+pin) utilizzate per l'accesso ad aree riservate

tramite smartcard;

- credenziali di autenticazione basate su caratteristica biometrica dell'utente: le credenziali (impronta+pin) utilizzate per gli accessi ai palmari tramite riconoscimento dell'impronta digitale.

### 4.3 Gestione delle credenziali

#### **Minacce**

Accesso ai sistemi da parte di personale non autorizzato, impersonificazione di utenti legittimamente autorizzati, furto di credenziali di accesso ai sistemi.

#### **Contromisure**

- A. Ogni credenziale di autenticazione si riferisce ad un singolo utente. Non è consentito l'utilizzo della stessa credenziale da parte di più utenti.
- B. Custodire le proprie credenziali di accesso ai sistemi adottando le necessarie cautele per assicurare la segretezza della componente riservata (per es. il PIN o la password) e la diligente custodia dei dispositivi in proprio possesso ed uso esclusivo.
- C. Richiedere l'attivazione di credenziali di accesso ai sistemi informativi tramite il proprio responsabile funzionale o referente regionale di progetto. In materia di trattamento dei dati personali, le credenziali di autenticazione sono concesse esclusivamente al personale individuato quale responsabile o incaricato del trattamento.
- D. Attivarsi immediatamente in caso di furto delle credenziali seguendo le opportune procedure specifiche di ogni singolo caso (per es. nel caso di furto della propria smartcard: richiedere la sospensione immediata del certificato digitale al Certificatore; sporgere denuncia alle Autorità competenti; trasmettere al Resp. del Servizio Amministrazione e Gestione del Personale la richiesta di revoca del certificato digitale su apposito modulo e la copia della denuncia di furto o smarrimento).

### 4.4 Password

#### **Minacce**

Accesso ai sistemi da parte di personale non autorizzato, impersonificazione di utenti legittimamente autorizzati, furto di credenziali di accesso ai sistemi.

#### **Contromisure**

- A. Ogni utente è responsabile della sicurezza delle proprie password e deve adottare le necessarie cautele per mantenerle segrete. Le password sono infatti strettamente personali e non devono in nessun caso essere comunicate ad altri (per es. non scrivere la password su *post-it* affissi al monitor o sotto la tastiera, non dare la password a colleghi prima di assenze o periodi di ferie, ecc.).
- B. Qualora fosse necessario durante periodi di assenze o di ferie mettere a disposizione di altri utenti dati o informazioni presenti sulla postazione di lavoro individuale, la password non deve essere comunicata ad altri bensì sono da individuare soluzioni di condivisione dei dati (ad es. tramite cartelle di rete condivise su sistemi centrali o cartelle condivise su Outlook o funzione di delega di lettura della casella di posta elettronica).

- C. Modificare la password quando si effettua l'accesso ad un sistema per la prima volta. La password deve essere lunga almeno 8 caratteri. Ove la tecnologia non lo consenta, la lunghezza della password deve essere comunque uguale a quella massima consentita dal sistema.
- D. Modificare la password, nel caso di trattamento di dati personali, almeno ogni 180 giorni.
- E. Modificare la password, nel caso di trattamento di dati **sensibili** e/o **giudiziari**, almeno ogni 90 giorni.
- F. Modificare la password nel caso in cui si sospetti che altri ne siano venuti a conoscenza. Contattare in tal caso l'indirizzo di posta dedicato alle problematiche di sicurezza (i riferimenti sono disponibili sul sito di supporto Computer Amico) per darne immediatamente comunicazione.
- G. Scegliere la password in modo che non sia collegata alla propria vita privata (per es. il nome o il cognome di famigliari, la targa dell'auto, la data di nascita, la città di residenza, ecc). Eventuali tentativi di indovinare la password partiranno infatti da queste possibilità.
- H. Non scegliere come password parole comuni riportate in un vocabolario: molti programmi fraudolenti utilizzati per la forzatura di password si basano infatti su ricerche sistematiche effettuate su parole comuni contenute in file di vocabolario.
- I. Scegliere il grado di complessità della password in funzione del valore dei dati e delle risorse da proteggere. Password di account con privilegi amministrativi, per esempio, richiedono complessità superiori rispetto a quelle di account non privilegiati. In ogni caso, è preferibile scegliere password che contengano combinazioni di lettere maiuscole e minuscole, numeri, caratteri speciali (per es. !, \*, /, ?, #).
- J. Non utilizzare la medesima password su sistemi differenti (per es. scegliere una password di dominio differente da quella per l'accesso alle Informazioni al Dipendente o impiegata per siti web esterni all'Ente).

## 4.5 Verifiche di sicurezza

### **Minacce**

Utilizzo non consentito delle risorse, perdita di efficienza e disponibilità delle risorse.

### **Contromisure**

- A. Le attività dell'utenza sono soggette a *logging*: ciò significa che alcune operazioni eseguite dagli utenti di sistemi informativi possono essere memorizzate in formato elettronico e conservate per un certo periodo di tempo. Il *logging* è necessario per ragioni di sicurezza, anche ai fini di adempimenti di legge: il livello del *logging* dei diversi servizi, ossia il livello di dettaglio dei dati memorizzati, è funzionale unicamente al controllo della sicurezza con la quale i servizi sono erogati e per nessun motivo è funzionale al controllo dell'attività lavorativa.
- B. Per necessità di manutenzione e per ridurre i tempi di intervento, il personale della struttura di help desk o gli amministratori di sistema, possono utilizzare strumenti di

controllo remoto.

- C. I sistemi informativi dell'Ente sono verificati sia periodicamente sia su segnalazione di incidenti di sicurezza, allo scopo di garantirne l'efficienza, la disponibilità ed il rispetto di leggi e regolamenti, ed in particolare dei requisiti minimi di sicurezza previsti dalla normativa vigente in materia di protezione dei dati personali.
- D. Le verifiche, che potrebbero in alcuni casi rilevare il contenuto di comunicazioni elettroniche, sono effettuate esclusivamente da personale preventivamente autorizzato e per le sole finalità indicate alla lettera C, in quanto eventuali ulteriori verifiche finalizzate ad accertare la correttezza e la legalità dell'utilizzo delle strumentazioni fornite dall'Ente per lo svolgimento dell'attività lavorativa sono definite in altro specifico Disciplinare tecnico.
- Nel caso in cui le verifiche rivelino la password di accesso ai sistemi di un utente, il personale addetto al controllo ne dà tempestiva notifica all'utente stesso che deve provvedere alla immediata sostituzione con una nuova password.

## **5. Protezione dei dati trattati senza l'utilizzo di strumenti elettronici**

### **Minacce**

Accesso ai dati da parte di persone non autorizzate, perdita di confidenzialità dei dati, mancata disponibilità dei dati.

### **Contromisure**

- A. L'accesso ai dati trattati senza l'utilizzo di strumenti elettronici è consentito esclusivamente al personale espressamente autorizzato.
- B. Nel caso di dati personali, l'accesso è consentito ai soli responsabili o incaricati del trattamento, individuati secondo le modalità previste dalla Delibera di Giunta n. 960 del 27/06/05.
- C. Prevedere, per determinati atti o documenti di rilevante importanza, procedure per la conservazione in archivi ad accesso selezionato, disciplinando le modalità di accesso a tali archivi in modo da consentire l'identificazione degli utenti che vi accedono.
- D. Controllare e custodire, fino alla restituzione, gli atti e i documenti contenenti dati personali sensibili e/o giudiziari prelevati da archivi ad accesso controllato, impedendo che ad essi possano accedere persone non autorizzate. In particolare, non lasciare incustoditi, neppure per brevi periodi, tali atti e documenti, provvedendo, qualora ciò fosse necessario, a riporli in armadi o cassette chiuse a chiave. In ogni caso, restituire tali atti e documenti al termine delle operazioni di trattamento affidate, ricollocandoli negli archivi ad accesso riservato da cui sono stati prelevati.
- E. Raccogliere prontamente, nel caso di utilizzo di stampanti di rete o fax ubicati in locali comuni (per es. corridoi), i documenti stampati o ricevuti via fax, soprattutto se contenenti dati personali, in modo da preservarne la riservatezza dei contenuti.
- F. Assicurarsi, al termine della giornata lavorativa, che i documenti contenenti dati personali o rilevanti ai fini della sicurezza del sistema informativo dell'Ente, non siano lasciati a vista sulla scrivania ma conservati in cassette o armadi.

G. Conservare con le dovute cautele le chiavi utilizzate per i cassetti e gli armadi contenenti dati personali e sensibili/giudiziari. In particolare, prevedere opportuni meccanismi per garantire la disponibilità delle stesse anche durante periodi di assenza (per es. copia delle chiavi depositate in segreteria, registro di presa in carico delle chiavi, ecc.).

## **6. Confidenzialità e disponibilità dei dati**

### **6.1 Confidenzialità dei dati**

#### ***Minacce***

Accesso ai dati da parte di persone non autorizzate.

#### ***Contromisure***

A. Adottare, nello svolgimento della propria attività lavorativa, le necessarie cautele per assicurare la confidenzialità di:

- dati personali;
- dati che possono fornire indicazioni utili ad un eventuale attaccante dei sistemi informativi dell'Ente (per es. dati relativi ad incidenti di sicurezza pregressi, alla topologia di rete, alla configurazione dei software, all'ubicazione dell'hardware, al personale preposto alla gestione ed alla sicurezza dei sistemi).

B. In particolare si evidenzia che:

- i dati salvati in locale nella cartella "Documenti" nei sistemi Windows 2000/XP (*C:\Documents and Settings\cognome\_n*) sono accessibili al solo utente proprietario o agli appartenenti al gruppo locale della macchina "Administrators" e non ad altri utenti che eventualmente accedono alla macchina. Utilizzare quindi questa cartella, o sue sottocartelle, nel caso in cui sia necessario salvare temporaneamente in locale dati ritenuti riservati o comunque importanti ai fini della sicurezza del sistema;
- l'utilizzo di cartelle locali condivise è consentito solo se esistono controlli degli accessi tali da garantire permessi di lettura e/o scrittura esclusivamente al personale autorizzato, e comunque per periodi di tempo limitati. È in ogni caso preferibile utilizzare cartelle di rete condivise sui sistemi server centrali, da richiedere come indicato al paragrafo [6.2 lettera C](#). In caso di dubbi contattare il proprio referente informatico o, in sua assenza, la struttura preposta alla creazione delle cartelle di rete condivise (i riferimenti sono disponibili sul sito di supporto Computer Amico).
- nel caso di utilizzo della posta elettronica, osservare quanto disposto al paragrafo [7.3](#).

### **6.2 Disponibilità dei dati**

#### ***Minacce***

Mancata disponibilità dei dati, indisponibilità di un servizio.

### **Contromisure**

- A. Utilizzare, in caso di trattamento di dati personali, le cartelle di rete o altri supporti di memorizzazione messi a disposizione dall'Ente al fine di garantire la disponibilità dei dati anche a seguito di errori o eventi accidentali. Le policy di backup centralizzato dell'Ente prevedono infatti l'esecuzione periodica di copie di sicurezza dei dati salvati su tali unità di rete sui sistemi di backup centrale. Le cartelle di rete, per cui si dispone delle necessarie autorizzazioni, sono accessibili tramite l'icona "Risorse del Computer" posta sul desktop.
- B. Utilizzare per le copie di sicurezza dei dati di uso quotidiano trattati in locale (per es. disco C:) la cartella di rete personale identificata come unità di rete *U:* (visibile nelle "Risorse del computer" come cartella denominata *cognome\_n\$*). Anche per tale cartella valgono infatti le regole di backup centralizzato dell'Ente.
- C. Non salvare copie multiple e ridondanti di file o documenti.
- D. Richiedere tramite il proprio referente informatico, in caso di necessità ed in ogni caso motivandolo, l'ampliamento della propria cartella di rete personale o ulteriori cartelle di rete condivise per memorizzare i dati trattati da più di un incaricato. In caso di dubbi contattare il proprio referente informatico o, in sua assenza, la struttura preposta alla creazione delle cartelle di rete condivise (i riferimenti sono disponibili sul sito di supporto Computer Amico).
- E. Prevedere, in caso di trattamento di dati sensibili e/o giudiziari, idonee misure per garantire il ripristino dei dati in tempi inferiori ai sette giorni, impiegando strumenti preventivamente concordati con il proprio referente informatico o con le strutture informatiche centrali.
- F. Prevedere opportune misure che consentano, in caso di assenza dal luogo di lavoro, ad altri utenti autorizzati l'accesso a dati potenzialmente necessari (per es. salvare i dati presenti sul proprio disco rigido in cartelle condivise su file server, utilizzare cartelle di Outlook condivise, utilizzare la funzione di delega di Outlook, ecc.).

## **6.3 Dati su dispositivi mobili**

### **Minacce**

Mancata disponibilità dei dati, indisponibilità di un servizio, accesso ai dati da parte di persone non autorizzate.

### **Contromisure**

- A. Memorizzare in forma protetta i file contenenti dati sensibili/giudiziari o che comunque possono compromettere la sicurezza dei sistemi informativi dell'Ente (per es. proteggere l'accesso a cartelle o file tramite password, utilizzare appositi tool di cifratura concordandoli con il proprio referente informatico o con le strutture informatiche centrali, ecc.).
- B. Distruggere i supporti rimovibili contenenti dati sensibili e/o giudiziari, o rendere inintelligibili i dati in essi contenuti, se non più utilizzati, impiegando strumenti preventivamente concordati con il proprio referente informatico o con le strutture informatiche centrali.

- C. Provvedere, al momento della riconnessione alla intranet, al salvataggio su unità di rete di eventuali file copiati o creati in locale, rimuovendoli dal dispositivo mobile.
- D. Non salvare in locale credenziali che consentano l'accesso alla rete o ad applicazioni dell'Ente.

## **7. Protezione delle reti e delle comunicazioni**

### **7.1 Sicurezza della rete interna**

#### **Minacce**

Accesso ai sistemi da parte di persone non autorizzate.

#### **Contromisure**

- A. Non connettere ad Internet, tramite modem o altri apparati di accesso remoto non espressamente autorizzati, macchine collegate alla rete interna dell'Ente.
- B. Non connettere alla rete interna dell'Ente strumenti elettronici personali o comunque non espressamente autorizzati.
- C. Non utilizzare strumenti **peer-to-peer** (per es. Skype, Emule, Limewire, Kazaa, Ares, BitTorrent, BitTornado, eDonkey, WinMX, Napster, Morpheus, Filetopia, SoulSeek, Shareaza, Azureus, ecc.).
- D. Non utilizzare strumenti di **sniffing**, **cracking** o **scanning**.
- E. Non introdurre o diffondere volontariamente programmi nocivi (per es. **virus**, **worm**, **spyware**, ecc.) nella rete o nei sistemi.

### **7.2 Navigazione in Internet**

#### **Minacce**

Perdita di confidenzialità dei dati, utilizzo non appropriato di beni dell'Ente.

#### **Contromisure**

- A. Utilizzare l'accesso ad Internet, fornito dall'Ente in quanto supporto all'attività lavorativa, in modo pertinente alle specifiche finalità della propria attività, nel rispetto delle esigenze di funzionalità e di sicurezza della rete e dei sistemi.
- B. Non modificare le configurazioni standard del **browser web** fornito dall'Ente.
- C. Non scaricare o eseguire alcun software o altro contenuto attivo, anche se gratuito, da siti Internet se non per finalità istituzionali e solo se strettamente necessario. In tal caso, verificare la provenienza e l'autenticità del software (per es. tramite meccanismi di firma digitale) e attenersi a quanto prescritto al paragrafo 7.7.

### **7.3 Utilizzo della posta elettronica**

La posta elettronica è uno strumento fornito dall'Ente esclusivamente quale supporto all'attività lavorativa e ciascun utente viene dotato di una casella di posta elettronica individuale al momento dell'assunzione e/o attivazione del contratto. L'attivazione di una

ulteriore casella di posta elettronica, per esempio di gruppo o di struttura, deve essere richiesta tramite il referente informatico o il responsabile funzionale.

### **Minacce**

Perdita di confidenzialità di dati riservati, utilizzo non appropriato di beni dell'Ente.

### **Contromisure**

- A. Utilizzare la posta elettronica esclusivamente per le specifiche finalità della propria attività lavorativa, nel rispetto delle esigenze di funzionalità e sicurezza dei sistemi informativi.
- B. Accertarsi, in caso di invio di e-mail contenenti dati personali, dell'identità del ricevente e della sua legittimità a ricevere tali dati. I dati personali devono infatti essere trasmessi soltanto all'interessato oppure a soggetti specificatamente autorizzati a trattarli in quanto designati quali responsabili o incaricati. Nel caso di trasmissione di dati all'interessato, l'identità del ricevente è accertata quando lo stesso ha presentato via e-mail una richiesta per l'invio dei dati firmata digitalmente ovvero ha inviato, oltre alla richiesta di dati presentata via e-mail o telefonicamente, anche una copia semplice di un documento di identità in corso di validità (anche tramite e-mail o fax). Nel caso di ragionevole certezza sull'identità del richiedente (ad esempio perché l'interessato è conosciuto personalmente oppure nel caso in cui trattasi di incaricati o responsabili del trattamento) ovvero in casi di improrogabile urgenza, l'accertamento sull'identità del ricevente può essere effettuata tramite telefonata di verifica. Quest'ultima modalità non deve essere utilizzata per l'invio di dati all'interessato qualora i dati da trasmettere siano dati sensibili e/o giudiziari.
- C. Trattare via e-mail dati sensibili e/o giudiziari solo con l'utilizzo di opportune tecniche di cifratura utilizzando strumenti preventivamente concordati con il proprio referente informatico o con le strutture informatiche centrali, ovvero impiegando soluzioni alternative che rendano i dati temporaneamente inintelligibili e permettano di identificare gli interessati solo in caso di necessità (per es. mandare in e-mail separate i dati sensibili/giudiziari dagli altri dati personali, utilizzare codici identificativi al posto di nome e cognome, ecc.).
- D. Non aprire allegati di posta in e-mail dal mittente e/o dall'oggetto sospetti per prevenire le minacce rappresentate software nocivi (per es. virus, worm, spyware, ecc.). Cancellare immediatamente tali messaggi e, in caso di dubbio, contattare l'indirizzo di posta dedicato alle problematiche di sicurezza (i riferimenti sono disponibili sul sito di supporto Computer Amico).
- E. Utilizzare il campo Bcc: (copia nascosta) nel caso di invio di e-mail a uno o più destinatari che non si vogliono rendere noti.
- F. Non falsificare i dati di intestazione dei messaggi di posta elettronica.

## **7.4 Spamming**

### **Minacce**

Utilizzo non appropriato di beni dell'Ente, indisponibilità di un servizio.

### **Contromisure**

- A. Non rispondere mai a messaggi di presunto **spamming**, neppure se al momento della cancellazione della mail viene richiesta conferma di lettura dal mittente, poiché ciò consente al mittente di verificare l'effettiva esistenza dell'indirizzo di posta dell'utente.
- B. Limitare al minimo indispensabile la diffusione del proprio indirizzo di e-mail su siti web pubblici (per es. forum, mailing list, ecc.).
- C. Non rispondere o inoltrare e-mail di c.d. "Catene di S. Antonio", ovvero messaggi dal contenuto ambiguo che esortano ad inoltrare urgentemente delle copie ad altre persone.

## **7.5 Phishing**

### **Minacce**

Perdita di confidenzialità di dati riservati.

### **Contromisure**

- A. Il **phishing** è una tecnica di attacco che sfrutta e-mail e siti web "fantasma", del tutto simili nell'aspetto agli originali, per ingannare l'utente e carpire informazioni confidenziali o personali. Prestare massima attenzione, quindi, alle e-mail che richiedono di fornire dati riservati quali password o numeri di carta di credito, attraverso la compilazione di moduli web (per es. da parte di una banca, di un operatore telefonico, di studi legali o di fornitori di servizi quali Yahoo!, Postecom, ecc.). Banche, studi legali o altre organizzazioni non inviano mai, infatti, richieste di informazioni riservate per posta elettronica, poiché facilmente contraffabili.
- B. In caso di dubbio, contattare l'indirizzo di posta dedicato alle problematiche di sicurezza (i riferimenti sono disponibili sul sito di supporto Computer Amico).

## **7.6 Virus**

### **Minacce**

Utilizzo non appropriato di beni dell'Ente, indisponibilità di un servizio.

### **Contromisure**

- A. Adottare le necessarie cautele, nell'utilizzo delle risorse informatiche dell'Ente, per ridurre il rischio di infezione virale della propria o altrui postazione di lavoro. In particolare:
  - non rimuovere il programma antivirus installato sulla postazione di lavoro;
  - non alterare la configurazione del programma antivirus installato sulla postazione di lavoro;
  - verificare la presenza di eventuali virus prima di utilizzare supporti rimovibili;
  - segnalare alla struttura di Help Desk problemi eventualmente riscontrati sulla corretta installazione e funzionamento del programma antivirus installato sulla postazione di lavoro.

B. Seguire le sottoindicate regole, nel caso in cui il software antivirus rilevi la presenza di un virus:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare l'evento alla struttura di Help Desk;
- non inviare messaggi di posta elettronica contenenti segnalazioni del virus ad altri utenti.

## **7.7 Software autorizzato**

### ***Minacce***

Utilizzo non appropriato di beni dell'Ente, indisponibilità di un servizio, perdita di confidenzialità dei dati, mancato rispetto delle norme sul diritto d'autore.

### ***Contromisure***

- A. Utilizzare sulle postazioni di lavoro esclusivamente il software autorizzato e fornito dall'Ente.
- B. Richiedere eventuale software aggiuntivo, rispetto all'installazione standard, al proprio referente informatico o al proprio responsabile funzionale o all'assistenza utenti del Servizio competente in materia di informatica individuale.
- C. Segnalare sempre, in ogni caso e preventivamente al proprio referente informatico o all'assistenza utenti del Servizio competente in materia di informatica individuale, la necessità di installare eventuale software aggiuntivo rispetto all'installazione standard, anche se gratuito e necessario per lo svolgimento dell'attività lavorativa.

## **7.8 Telelavoro e accesso remoto**

### ***Minacce***

Perdita di confidenzialità dei dati, utilizzo non appropriato di beni dell'Ente.

### ***Contromisure***

- A. La postazione di telelavoro o accesso remoto è installata, configurata e mantenuta a carico dell'Ente.
- B. L'utente è tenuto ad utilizzare la postazione di lavoro fornitagli esclusivamente per motivi inerenti l'attività lavorativa, a rispettare le norme di sicurezza indicate nel presente disciplinare, a non manomettere in alcun modo gli apparati e l'impianto generale, a non variare la configurazione della postazione di telelavoro, a non sostituirla con altre apparecchiature o dispositivi tecnologici.
- C. La postazione di telelavoro o accesso remoto non può essere impiegata con collegamenti alternativi o complementari a quello installato dall'Ente ed il suo utilizzo non può essere consentito ad altri soggetti all'infuori del telelavoratore incaricato.
- D. Gli utenti dotati di dispositivi mobili devono provvedere al collegamento degli stessi alla LAN dell'Ente almeno una volta ogni 30 giorni per gli aggiornamenti automatici del software antivirus e delle patch di sicurezza.

## **8. Prevenzione e gestione degli incidenti informatici**

### **Minacce**

Mancata rilevazione di incidenti di sicurezza, indisponibilità di un servizio.

### **Contromisure**

- A. Operare tempestivamente e in uno spirito di collaborazione per prevenire, rilevare e rispondere efficacemente agli incidenti di sicurezza nel minor tempo possibile.
- B. Reagire agli incidenti di sicurezza con prontezza e con spirito di cooperazione segnalando all'indirizzo di posta dedicato alle problematiche di sicurezza (i riferimenti sono disponibili sul sito di supporto Computer Amico) le violazioni di sicurezza interna o gli eventi che possono portare a credere che vi sia stata un'elusione delle misure di sicurezza previste.
- C. Attenersi scrupolosamente alle indicazioni ricevute dal personale addetto alla sicurezza ed alla gestione della rete e dei sistemi. Tali indicazioni sono fornite agli utenti attraverso gli strumenti di comunicazione interna dell'Ente quali il sito Internos, il sito del supporto tecnico e la posta elettronica interna.

## **Appendice A: Glossario**

**Autenticazione:** l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità dell'utente che accede ai sistemi informativi.

**Browser web:** programma che consente all'utente di guardare, interagire e, in generale, scorrere o sfogliare file in Internet (per es. Internet Explorer, Mozilla Firefox, Opera, ecc. ).

**Cracking (strumenti di):** software che consentono l'aggiramento illecito delle misure di sicurezza di un sistema informatico.

**Dati giudiziari:** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

**Dati personali:** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

**Dati sensibili:** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

**Incaricato:** la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

**Normativa vigente:** il "Codice in materia di protezione dei dati personali", Decreto Legislativo numero 196 del 30 Giugno 2003, entrato in vigore il 1° Gennaio del 2004 (il c.d. "Codice della Privacy").

**Password:** sequenza di caratteri alfanumerici che costituisce la chiave d'accesso ad un sistema protetto. In assenza di altri dispositivi, la password costituisce il meccanismo di sicurezza base per la protezione dell'accesso a risorse informatiche.

**Patch:** aggiornamento di un software per la correzione di un problema di sicurezza o di funzionalità.

**Peer-to-peer (strumenti):** software che permettono l'utilizzo di una postazione di lavoro in modalità server per consentire lo scambio di file con altri utenti, anche esterni alla rete dell'Ente.

**Phishing:** tecnica finalizzata all'acquisizione, per scopi illegali, di dati riservati (codici di accesso, password, numeri carte di credito e altre informazioni personali) tramite l'invio di e-mail dal contenuto e dal mittente opportunamente falsificati (per es. simulando la provenienza del messaggio da parte di una banca o di uno studio legale).

**Responsabile:** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

**Scanning:** attività di raccolta di informazioni su un sistema propedeutica alla fase di attacco informatico vero e proprio.

*Sniffing (strumenti di):* software che consentono di intercettare ed analizzare il traffico in transito su una rete informatica.

*Spamming:* l'invio di grandi quantità di messaggi elettronici non richiesti (generalmente commerciali). Può essere messo in atto attraverso qualunque media, ma il più usato è Internet, attraverso l'e-mail.

*Spyware:* software che raccoglie informazioni riguardanti un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata.

*Titolare:* la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

*Worm:* programma in grado di autodiffondersi sulla rete e verso altri sistemi.

*Virus:* programma in grado di autoreplicarsi in un sistema, per esempio copiando una parte di se stesso all'interno del codice di un altro programma.