Azienda Ospedaliera Universitaria Federico II

Manuale per la Sicurezza

AD USO DEGLI INCARICATI DEL TRATTAMENTO DEI DATI

EDIZIONE 2012

A CURA DEL SERVIZIO INFORMATICA AMMINISTRATIVA

Introduzione

Il Codice in materia di protezione dei dati personali, entrato in vigore con il decreto legislativo 196/2003, raccoglie in forma di testo unico tutte le disposizioni in materia di tutela delle persone rispetto al trattamento dei dati personali ed alle attività connesse. Il Codice sancisce il diritto alla protezione dei dati personali e garantisce che il trattamento di queste informazioni "si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".
Esso si ispira ai principi di semplificazione, efficacia ed armonizzazione delle modalità di esercizio dei diritti e delle libertà fondamentali dell'interessato e degli adempimenti degli obblighi da parte dei titolari dei trattamenti (art. 2, comma 2).
Ai sensi dell'art.33 e dell'art.34 del Codice, il trattamento dei dati personali è consentito solo se vengono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B del Codice determinate misure di sicurezza, distinte a seconda che il trattamento sia effettuato con o senza l'ausilio di strumenti elettronici.

Questo documento, che sostituisce le eventuali versioni precedenti, fornisce agli incaricati del trattamento una panoramica sulle loro responsabilità rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione. Inoltre, invita gli stessi incaricati al rispetto dei criteri minimi ambientali nell'utilizzo delle apparecchiature a loro affidate.

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti fondamentali, e precisamente:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;

Integrità: Le informazioni non devono essere alterate da incidenti o abusi;

Disponibilità: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.

Le precauzioni di tipo tecnico, in particolare, possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

Con questo documento, inoltre, si ricorda agli incaricati che è vietata l'installazione e l'utilizzo di qualsiasi software non acquisito in conformità alla vigenti disposizioni legislative e che, un comportamento diverso costituisce illecito perseguibile penalmente e civilmente e comporta un automatico procedimento disciplinare.

Si rappresenta, infine, che i trattamenti dei dati effettuati senza specifiche direttive da parte del titolare o del responsabile del trattamento dei dati sui personal computer utilizzati per produttività individuale sono eseguiti sotto la diretta responsabilità del consegnatario/utilizzatore dell'apparecchiatura informatica.

Nell'effettuare trattamenti con l'ausilio di strumenti elettronici le misure minime di sicurezza da rispettare sono:
a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico (**almeno annuale**) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.
Nell'effettuare trattamenti senza l'ausilio di strumenti elettronici le misure minime di sicurezza da rispettare sono:
a) aggiornamento periodico (**almeno annuale**) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.
In ogni caso, qualunque sia la tipologia di trattamento effettuato, l'omissione da parte di chiunque (responsabile o incaricato) dell'applicazione delle misure minime di sicurezza è sanzionabile penalmente, in base a quanto sancito dall'art. 169 del Codice. Inoltre, l'adozione di misure di sicurezza inadeguate (cioè non coerenti con quanto disciplinato dal Codice o dalla legge) rende il trattamento illecito, per cui il titolare non può più utilizzare i dati raccolti e l'interessato può ottenerne la cancellazione.

Linee guida per la sicurezza

Le **"misure minime"** di sicurezza sono un insieme di misure tecniche, informatiche, organizzative, logistiche e procedurali che l'Azienda Ospedaliera Universitaria Federico II è tenuta ad adottare per evitare i casi di distruzione o di perdita, anche accidentale, dei dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
Il presente Manuale, coerentemente con le misure minime definite nel Codice, contiene le istruzioni, le regole e le prassi a cui devono attenersi i Responsabili e gli incaricati per la tutela dei dati personali trattati dall'Azienda Ospedaliera Universitaria Federico II.

Adempimenti di carattere generale previsti per tutte le tipologie di PC

Il sistema di autenticazione

L'autenticazione consente ad un utente autorizzato di accedere ai servizi ed alle informazioni cui ha legittimamente diritto e, contemporaneamente, impedisce qualunque tipo di accesso a chi, invece, non ha le autorizzazioni necessarie. Il sistema di autenticazione, quindi, deve essere in grado di memorizzare in modo sicuro le credenziali di ogni utente, di riconoscerlo all'atto della richiesta di un determinato servizio e di garantire che non avvengano manipolazioni delle richieste di accesso.
Tutti i PC devono essere accessibili attraverso l'utilizzo di un sistema di autenticazione, mediante l'utilizzo di password da inserire all'atto dell'accensione della macchina. I meccanismi da implementare dipendono dalla tipologia di PC (se collegato in rete locale, oppure no), dalle caratteristiche tecniche del PC e dalla disponibilità di idonee infrastrutture di servizio (ad esempio, la presenza di server di dominio).

Sicurezza del software e dell'hardware

Se nell'utilizzo del PC viene rilevato un problema che può compromettere la sicurezza dei dati, l'incaricato ne dà immediata comunicazione al responsabile del trattamento che, a sua volta, provvede ad attivare la struttura aziendale preposta alla manutenzione dei PC che analizzerà il problema segnalato ed adotterà tutte le misure tecniche necessarie a risolverlo.
All'utente è vietato installare programmi non attinenti le normali attività d'ufficio, né nuovi programmi necessari, né modificare le configurazioni hardware e software delle apparecchiature, senza la preventiva autorizzazione del proprio responsabile. Gli utenti, con cadenza almeno mensile, verificano la disponibilità (ad esempio, per gli utilizzatori di sistemi Windows/Vista, sul sito ufficiale della Microsoft), di correzioni software per problemi di sicurezza, applicabili alla propria versione di sistema operativo. Se nel corso di tale verifica si rileva la presenza di correzioni software per problemi di sicurezza (aggiornamenti critici), l'incaricato è tenuto a scaricare ed installare tali aggiornamenti sulla propria postazione di lavoro, seguendo le istruzioni impartite dal fornitore.
Tale adempimento è applicabile a tutti gli utenti le cui postazioni di lavoro sono collegate alla rete internet.
Tutti gli incaricati evitano qualsiasi azione tesa a superare le protezioni applicate ai sistemi e alle applicazioni. A conclusione dell'intervento di manutenzione, il Responsabile del trattamento è tenuto a verificare che il PC sia riportato nella situazione originaria per quanto riguarda le misure minime (password di accensione del PC, presenza del programma antivirus). E' espressamente vietata qualsiasi azione volta a superare il blocco con password all'accensione del PC.
È necessario, inoltre, seguire le seguenti indicazioni:

1. **UTILIZZATE LE CHIAVI**

   Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete.

2. **CONSERVATE I DISCHETTI O I COMPACT DISC IN UN LUOGO SICURO**

   Per questi supporti si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. Non appena avete finito di usarli, riponeteli sotto chiave.

3. **UTILIZZATE LE PASSWORD**

   Vi sono svariate categorie di password, ognuna con un proprio ruolo preciso:

   a. La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
   b. La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
   c. La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
   d. La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.

4. **CUSTODIA DELLE PASSWORD**

   Al fine di consentire l'uso del personal computer anche in caso di impedimento dell'incaricato che lo utilizza normalmente, questi dovrà consegnare al responsabile della Struttura di afferenza una busta chiusa contenente la propria password e provvedere a sostituirla in occasione dell'adozione di una nuova password.

   Il responsabile della Struttura, in caso di impedimento temporaneo di un dipendente, qualora sia indispensabile utilizzare il personal computer a questi assegnato, aprirà la busta contenente la relativa password e la fornirà ad un altro dipendente per consentirgli l'utilizzo del suddetto personal computer. La busta, con l'indicazione della data e dell'ora di apertura, dovrà essere conservata a cura del responsabile fino alla consegna della busta contenente la nuova password da parte del dipendente che è stato temporaneamente impedito.

5. **ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI**

   Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

6. **NON BUTTATE I DOCUMENTI NEI CESTINI**

   Se si trattano dati sensibili, considerate la necessità di dotarvi di macchine distruggi documenti per l'eliminazione di stampe o documenti non più necessari oppure riducete gli stessi documenti in modo da renderli inutilizzabili. In particolare, in caso di trattamenti con dati sensibili, si incorre nella necessità di stampare più bozze prima di avere la copia definitiva di un documento, per cui distruggete le bozze personalmente. In ogni caso, non gettate mai documenti cartacei senza averli prima fatti a pezzi.

7. NON LASCIATE TRACCIA DEI DATI RISERVATI

Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio che usiate un nuovo supporto.

8. CONDIVISIONI DI FILE

Al fine di limitare la diffusione di virus, furti e danneggiamenti di documenti, problemi di funzionamento delle stazioni di lavoro, è fatto espressamente divieto di condividere il disco fisso del proprio computer o anche solo parte di esso.

Nel caso vi siano delle esigenze di condividere documenti e/o dati, dovete farlo presente al Responsabile per il trattamento dei dati che, con l'Amministratore di sistema, provvederà ad analizzare il problema e, qualora possibile e consentito dalle normative vigenti, verrà creata una apposita area di scambio sui server di rete con le opportune autorizzazioni e protezioni.

9. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, è obbligatorio installare un buon programma di cifratura del disco rigido e utilizzare una procedura di backup periodico.

10. NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

11. CUSTODITE LE PASSWORD IN UN LUOGO SICURO

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

12. NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÁ

Personale esterno può avere bisogno di installare, per manutenzione e/o riparazioni hardware, del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

13. NON UTILIZZATE APPARECCHIATURE NON AUTORIZZATE

L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete dell'Azienda, ed è quindi vietata. Allo stesso modo è vietata l'installazione di apparecchiature wireless e qualsiasi modifica all'impianto di trasmissione dati utilizzato. Per l'utilizzo di altre apparecchiature, richiedete l'intervento del Servizio Informatico Aziendale.

14. NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi istituzionali o acquistati dall'Azienda con regolare licenza sono autorizzati. I soggetti che utilizzano qualsiasi altro software sono direttamente responsabili secondo le vigenti disposizioni di legge (L. 248/2000 e successive modifiche ed integrazioni). Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il responsabile del trattamento dati.

15. APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati. L'utilizzatore dell'apparecchiatura informatica in dotazione è tenuto alla verifica del corretto aggiornamento del software antivirus e del sistema operativo installato. La mancanza di tali verifiche determinerà precise responsabilità in ordine al normale funzionamento dell'apparecchiatura in dotazione e del Sistema Informativo Aziendale.

16. CONTROLLATE LA POLITICA LOCALE RELATIVA AI BACKUP

I vostri dati potrebbero essere gestiti da un *file server*, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Verificate con il personale del Servizio Informatico dell'Azienda la situazione. E' fondamentale che ogni utente salvi i propri documenti critici anche se non ha accesso ai server adibiti al backup dati. L'utente è tenuto ad informare il Responsabile per il trattamento dei dati qualora non si possa ricorrere al salvataggio su risorse di rete, ed effettuare le copie dei propri dati su supporti esterni. Tali copie dovranno essere tenute chiuse a chiave in armadi blindati e ignifughi collocati in luogo differente rispetto a quello dove risiede l'elaboratore; quest'ultima accortezza è utile soprattutto in caso di incendio: più le copie di sicurezza sono distanti dall'elaboratore e meno è probabile che vengano distrutte con esso.

17. PRESCRIZIONI PER L'ACCESSO AD INTERNET

I servizi internet usufruibili sono quelli indispensabili alle specifiche attività lavorative dell'utente e comunque rispettando le disposizioni contenute nella Direttiva n. 2/2009 del Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri.

Non è consentito il collegamento ad internet, tramite modem, a provider diversi dal C.S.I. dell'Ateneo "Federico II".

18. SICUREZZA DEI TRATTAMENTI

Nell'utilizzo del personal computer per l'esecuzione dei trattamenti dei dati occorre che l'addetto osservi con scrupolosità quanto già definito e comunicato ai singoli incaricati.

Per i trattamenti dei dati effettuati, invece, senza specifiche direttive e incarico da parte del titolare o del responsabile del trattamento dei dati sui personal computer utilizzati per produttività individuale questi sono eseguiti sotto la diretta responsabilità del consegnatario/utilizzatore dell'apparecchiatura informatica.

19. AGGIORNAMENTO SISTEMA OPERATIVO E SOFTWARE DI PRODUTTIVITÀ INDIVIDUALE

Per garantire la sicurezza del personal computer è necessario che l'utilizzatore effettui con regolarità l'aggiornamento del sistema operativo utilizzato accedendo al sito del fornitore del software. Tali eventuali aggiornamenti consentono l'eliminazione di malfunzioni e/o anomalie che possono essere utilizzate dai virus.

20. AGGIORNAMENTO DEL SOFTWARE ANTIVIRUS

Per tutelare in modo efficace e continuativo occorre procedere con regolarità all'aggiornamento, ove è utilizzato un software antivirus non di rete, del software citato connettendosi al sito del produttore.

Per coloro che utilizzano il software antivirus di rete Aziendale (in genere sono tutte le stazioni collegate al Server centrale e utilizzanti le procedure applicative Aziendali) occorre obbligatoriamente verificare che all'accensione del personal computer risulti operativo il software antivirus. In caso contrario non utilizzate il personal computer e contattate il servizio informatico aziendale.

21. DISINSTALLAZIONE E/O MODIFICA DI HARDWARE E SOFTWARE APPLICATIVO

Eventuali modifiche dell'hardware (aggiunta di nuove periferiche, aggiunta di scheda wireless, l'utilizzo di USB-driver, etc…) e/o disinstallazione di software (patch di sicurezza del sistema operativo, software antivirus, etc….) o modifiche dei parametri del software (disabilitazione antivirus, cancellazione di password, modifiche configurazioni per l'accesso in rete, condivisioni di risorse locali senza le relative password, etc…..), compromettono la sicurezza dei dati e dei sistemi; Non è consentito, pertanto, procedere alle suddette operazioni senza l'ausilio del Servizio Informatico Aziendale.

22. PERSONALIZZAZIONE PER ACCESSO ALLA RETE TELEMATICA AZIENDALE

Per garantire la sicurezza degli accessi alla rete telematica dell'Azienda, è vietato modificare i parametri necessari al collegamento (indirizzo IP, etc…..). Inoltre, l'utilizzo di diverso IP rispetto a quello assegnato costituisce appropriazione indebita di altro assegnatario; tale azione rappresenta azione penalmente perseguibile e contraria ai doveri d'ufficio. Il Servizio Informatico Aziendale è tenuto al monitoraggio e al conseguente rilevamento di eventuali azioni per i successivi provvedimenti.

23. SALVATAGGIO PERIODICO DEI DATI

Per garantire la disponibilità dei dati personali trattati con PC il Responsabile è tenuto a verificare che, con cadenza almeno settimanale, tali dati siano archiviati su supporti di memorizzazione rimovibili (floppy disk,CDROM, DVD) e che tali supporti siano conservati in armadi o cassetti muniti di serratura.

24. MECCANISMO DI AUTENTICAZIONE PER I PC NON COLLEGATI IN RETE

Per i PC non collegati in rete, il meccanismo per l'autenticazione deve essere necessariamente implementato in locale, sul PC.

Se sul PC è installato un sistema della famiglia Windows 9x (Windows 95, Windows 98, Windows 98 SE, Windows ME) che non prevede un sistema di autenticazione "nativo", la password di accensione deve essere in tal caso necessariamente di BIOS. La lunghezza minima della password è di 6 caratteri, o comunque del massimo consentito dal BIOS del PC; la password BIOS deve essere modificabile dall'incaricato e variata almeno ogni sei mesi. Nel caso in cui sul PC risiedano dati sensibili o giudiziari, tale password deve essere modificata dall'incaricato almeno ogni tre mesi.

I PC più recenti, (MAC OS, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista) sono invece dotati di sistemi di autenticazione ed autorizzazione completi che permettono non solo l'utilizzo di user-id e password, ma anche di credenziali di autenticazione "forte" quali token o device di riconoscimento biometrico. L'utilizzo dell'autenticazione "locale" non esclude l'adozione anche della password BIOS.

Per quanto attiene alle restanti misure minime di sicurezza, gli incaricati provvedono ad eseguire:

- con cadenza almeno mensile, da disco rimovibile, l'aggiornamento del sistema operativo presente sul proprio PC e del programma antivirus;
- con cadenza almeno settimanale, al salvataggio dei propri dati personali su supporti di memorizzazione rimovibili (floppy disk, CDROM, DVD) che devono essere conservati in armadi o cassetti muniti di serratura;
- ad impostare la protezione mediante screen-saver con password.

25. MECCANISMO DI AUTENTICAZIONE PER I PC COLLEGTAI IN RETE MA NON ALLE APPLICAZIONI CENTRALIZZATE

Se il PC è collegato alla rete locale, l'autenticazione deve essere preferibilmente gestita da un sistema centralizzato di autenticazione. In tal caso, la password deve essere di

lunghezza non inferiore a 8 caratteri o, comunque, al massimo numero di caratteri consentiti dal sistema di autenticazione utilizzato.

L'utilizzo di un sistema centralizzato di autenticazione, in generale, permette:

- la protezione e la gestione delle password (lunghezza minima, scadenza della password, rinnovo della password, cessazione dell'utenza, regole di composizione della password, ecc.) grazie ad un'unica procedura di accesso alle risorse di rete;
- la profilatura utente grazie all'impostazione di privilegi per il controllo dell'accesso agli oggetti della directory e ai singoli elementi dati che li costituiscono;
- la gestione della sicurezza anche dei sistemi client collegati;
- la sicurezza nell'accesso ad Internet attraverso il supporto per i protocolli sicuri standard di Internet ed i meccanismi di autenticazione degli utenti;
- la pre-impostazione centralizzata della protezione mediante screen-saver;
- gestione della lista degli incaricati al trattamento dei dati in relazione al profilo di autorizzazione ed al conseguente ambito di trattamento consentito.

26. MECCANISMO DI AUTENTICAZIONE PER I PC COLLEGATI IN RETE ED ALLE APPLICAZIONI CENTRALIZZATE

Ad ogni utente delle applicazioni informatiche centralizzate, per ciascuna applicazione, sono associati un codice identificativo personale, una password ed eventualmente un profilo di abilitazione.

Il responsabile del trattamento dei dati dovrà individuare tassativamente per iscritto, gli incaricati dei trattamenti informatizzati mediante procedure centralizzate. Tale incarico conferisce, implicitamente, anche l'autorizzazione all'utilizzo della corrispondente procedura informatica.

Ad ogni utente delle applicazioni informatiche centralizzate è associato un codice identificativo personale (user-id), una password ed un profilo di abilitazione.

Utilizzo della rete internet

Un utilizzo improprio della connessione alla rete internet può danneggiare il sistema informativo dell'A.O.U Federico II ed i dati in esso contenuti; inoltre, attraverso tale rete, possono penetrare nel sistema virus informatici ed utenti non autorizzati. Allo scopo di evitare questi pericoli, gli Incaricati che dispongono di PC collegati in rete, curano l'applicazione delle seguenti regole:

1) utilizzano la connessione ad internet esclusivamente per lo svolgimento dei compiti istituzionali dell'Ufficio;

2) si astengono da un uso di internet illegale o non etico;

3) rispettano l'obbligo di non collegarsi a siti con materiale illegale e/o inappropriato;

4) si astengono dall'inviare, ricevere o mostrare testi o immagini che possono essere offensivi per le persone presenti;

5) rispettano i diritti di proprietà intellettuale facendo solo copie autorizzate di programmi o dati coperti da copyright;

6) non danneggiano né alterano il Setup o la configurazione software della propria postazione di lavoro, evitando inoltre di installare prodotti software non licenziati e/o non certificati a corredo della postazione per la specifica destinazione d'uso;

7) rispettano la privacy delle altre persone non facendosi passare per un altro utente della rete, non tentando di modificare o accedere a file, password o dati che appartengono ad altri, non cercando di disattivare il controllo di autorizzazione all'accesso a qualunque sistema o rete di computer;

8) non diffondono messaggi di posta elettronica di provenienza dubbia, non partecipano a sequenze di invii di messaggi (catene di S. Antonio) e non inoltrano o diffondono messaggi che annunciano nuovi virus;

9) sono responsabili dell'uso della casella di posta elettronica istituzionale loro assegnata, non utilizzano le caselle di posta elettronica istituzionali per fini privati o personali, limitano allo stretto indispensabile l'invio di messaggi di posta elettronica con allegati, scegliendo, ove necessario, il formato degli allegati che occupa meno spazio;
10) non utilizzano servizi di comunicazione e condivisione files che esulino dalle ordinarie funzioni di browsing internet (http), posta elettronica e trasferimento files;
11) sono a conoscenza degli articoli del Codice Penale 615 ter – "*Accesso abusivo ad un sistema informatico o telematico*", 615 quater – "*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*", 615 quinquies – "*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*", nonché del Decreto legge 22 marzo 2004 n.72 convertito in legge con modificazioni dalla Legge 21 maggio 2004 n.128, (Legge Urbani) che sanziona la condivisione e/o la fruizione di file relativi ad un'opera cinematografica o assimilata protetta dal diritto d'autore.

Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi provenienti da fonti non ufficiali;
2. Attraverso le macro dei programmi di automazione d'ufficio.

COME *NON* SI TRASMETTE UN VIRUS:

1. Attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi;
2. Quando si copiano dati da dischetti;
3. Quando si scaricano dati o programmi da Internet.

QUALI EFFETTI HA UN VIRUS?

1. Effetti sonori e messaggi sconosciuti appaiono sul video;
2. Nei menù appaiono funzioni extra finora non disponibili;
3. Lo spazio disco residuo si riduce inspiegabilmente;

COME PREVENIRE I VIRUS:

1. **USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE**
   Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. **ASSICURATEVI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER DA DISCHETTO, DA COMPACT DISC O DA DISPOSITIVI USB ESTERNI**
   Infatti se i supporti fossero infettati, il virus si trasferirebbe nella memoria RAM e potrebbe espandersi ad altri file.

3. **PROTEGGETE I VOSTRI DISCHETTI DA SCRITTURA QUANDO POSSIBILE**
   In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

4. **ASSICURATEVI CHE IL VOSTRO SOFTWARE ANTIVIRUS SIA AGGIORNATO**
   La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre, è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte digitali" dei nuovi virus. Questi file di identificativi sono rilasciati, di solito, con maggiore frequenza rispetto alle nuove versioni dei motori di ricerca dei virus. Informatevi con il responsabile del trattamento dati per maggiori dettagli.

5. **SPYWARE**
   Non di frequente capita che in seguito a collegamenti anche sporadici a siti internet vi si installino all'insaputa dell'operatore, nel personal computer utilizzato, programmi che per loro natura effettuano trasferimenti di dati verso l'esterno senza controllo e autorizzazione.
   Pertanto, costituisce un reale pericolo e, quindi, l'installazione e l'aggiornamento di prodotti anti-spyware (versione anche freeware) è assolutamente indispensabile prima di effettuare collegamenti internet.

6. **NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA**
   Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: le mail di questo tipo sono dette con terminologia anglosassone *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro capo, da vostra sorella o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli *hoax* più diffusi).

7. **NON PARTECIPATE A "CATENE DI S. ANTONIO" E SIMILI**
   Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti *hoax* aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

8. NON EFFETTUARE COPIE O TRASMISSIONE DI DATI

Nel caso che vi siano fondati sospetti che il personal computer sia interessato da virus si invita a non effettuare copie di dati su supporti informatici e/o trasmissione di dati via internet. In caso contrario appare reale il pericolo di diffusione di virus.

9. NON EFFETTUARE L'INSTALLAZIONE DI PIÙ ANTIVIRUS

L'installazione di più antivirus può generare, in alcuni casi, conflitti e malfunzionamenti senza, peraltro, aumentare la sicurezza del personal computer. Appare, invece, necessario disporre di un antivirus perfettamente aggiornato e funzionante.

Scelta delle password

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.
Nella gestione delle password è necessario attenersi alle indicazioni di seguito riportate.

COSA NON FARE

1. NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome.
2. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer.
3. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.
4. NON scegliete password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
5. NON crediate che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
6. NON usate il Vostro nome utente. È la password più semplice da indovinare.
7. NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE

1. Cambiate la password a intervalli regolari. Chiedete al vostro responsabile del trattamento quali sono le sue raccomandazioni sulla frequenza del cambio; a seconda del tipo di sistema l'intervallo raccomandato per il cambio può andare da tre mesi fino a sei mesi.
2. Usate password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione.
3. Utilizzate password distinte per sistemi con diverso grado di sensibilità. In alcuni casi la password viaggia in chiaro sulla rete e può essere, quindi, intercettata; per cui, oltre a cambiarla spesso, è importante che sia diversa per quella usata da sistemi "sicuri". Il tipo di password in assoluto più sicuro è quello associato a un supporto di identificazione come un dischetto o una carta a microprocessore; la password utilizzata su un sistema di questo tipo non deve essere usata in nessun altro sistema. In caso di dubbio, consultate il vostro responsabile del trattamento.

Scelta delle password per le procedure centralizzate

Le procedure centralizzate, come già di vostra conoscenza, sono conformi a quanto previsto dal decreto legislativo 196/2003 - Codice in materia di protezione dei dati personali-.
Per la scelta e l'utilizzo delle password è utile riferirsi a quanto riportato nel paragrafo precedente. In particolare, inoltre, seguite con attenzione quanto richiesto dalla specifica funzione operativa proposta dalla singola procedura applicativa (esempio : lunghezza chiave, periodo validità, etc.).

Linee guida per il rispetto criteri minimi ambientali nell'utilizzo delle attrezzature elettroniche

Il DM Ambiente del 22 febbraio 2011 detta i criteri minimi ambientali da rispettare nell'utilizzo delle attrezzature elettriche ed elettroniche da ufficio.

In particolare:

- limitate il numero di copie, incrementando l'utilizzo della posta elettronica per la diffusione e la condivisione dei documenti ed evitare la copia di documenti che possono essere consultati a video;
- adottate la modalità di fronte/retro e preferire la stampa/copia di più pagine per foglio;
- utilizzate, quando possibile, la modalità di copia/stampa in "bozza" e adottare il carattere c.d. "Eco-font";
- utilizzate formati ridotti;
- limitate l'uso del colore ove non strettamente necessario;
- assicuratevi che l'apparecchio non rimanga collegato alla rete elettrica (per esempio spegnendo l'interruttore a muro o la multipresa a cui è collegato o, in assenza di questi, scollegando il cavo dell'alimentazione) al termine dell'orario di lavoro;
- impostate la funzione di risparmio energetico;
- attivate le opzioni di risparmio energetico previste dal sistema operativo;
- spegnete e staccate dalla presa di corrente le apparecchiature alla fine della giornata di lavoro, se non saranno utilizzate per lungo periodo.

L'impiego razionale delle attrezzature elettriche ed elettroniche da ufficio consente notevoli vantaggi ambientali ed economici legati al risparmio energetico e alla conseguente riduzione di emissioni di CO2, alla riduzione del consumo di carta e di toner e alla maggiore durata della vita utile del prodotto.

Inoltre, per una corretta raccolta differenziata, vogliate utilizzare, ove presenti:

- cestini per la raccolta separata della carta nelle vicinanze degli apparecchi;
- contenitori per la raccolta differenziata dei toner esausti.