Tribunale di Asti

MANUALE PER LA SICUREZZA DEI DATI PERSONALI

Introduzione

Questo documento fornisce agli Incaricati del Trattamento una panoramica sulle **responsabilità** loro spettanti, rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione.

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

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

Integrità: *Le informazioni non devono essere alterabili 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 informatici ma anche gli opportuni meccanismi organizzativi; come è necessario che l'utente finale si attenga alle norme sottoelencate.

LINEE GUIDA PER LA SICUREZZA

1. UTILIZZATE LE CHIAVI!

Chiudete i documenti a chiave nei cassetti. A fine giornata chiudete a chiave il vostro ufficio.

2. NON LASCIARE INCOSTUDITE LE STAMPE DI DOCUMENTI RISERVATI ED I SUPPORTI DI MEMORIZZAZIONE.

Conservate i supporti di memorizzazione (es: floppy disk, Pen Drive, CD, DVD ...) in luogo sicuro!
Utilizzate la stessa attenzione che avete per i documenti cartacei. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sottochiave non appena avete finito di usarli. Anche in caso di file cancellati o di dispositivi formattati i dati non vengono effettivamente cancellati e sono facilmente recuperabili.

3. UTILIZZATE LE PASSWORD!

- 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.
- La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
- La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
- La password del salvaschermo (screen saver), infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.

4. 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 iscritto, non lasciate in giro i fogli utilizzati. **Non fatevi spiare quando state digitando le password.**

5. CONTROLLATE LA POLITICA LOCALE RELATIVA AL SALVATAGGIO DEI DATI (BACKUP).

I vostri dati se salvati solo su PC possono essere facilmente persi in conseguenza di guasti hardware, infezioni di virus, cancellazioni involontarie. Una buona politica di salvataggio su server può prevenire tali spiacevoli inconvenienti. Non installate programmi non autorizzati sulle postazioni di lavoro dell'ufficio

6. DIVIETO ASSOLUTO AGLI UTENTI DI EFFETTUARE COLLEGAMENTI TELEMATICI NON AUTORIZZATI!

Non effettuare connessioni a reti esterne (es: internet) attraverso modem o internet key (chiavetta usb) o a postazioni di lavoro non appartenenti all'amministrazione della giustizia. L'utilizzo di modem o chiavetta usb su postazioni di lavoro collegate alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete giustizia, ed è quindi vietata. Per l'utilizzo di altri apparecchi consultatevi con il responsabile del trattamento.

7. NON FATE USARE IL VOSTRO PC A PERSONALE ESTERNO.

Non collegate alle postazioni di lavoro dell'ufficio dispositivi di proprietà del personale esterno o del Pubblico (es. Floppy, pen drive, hard disk esterni, internet key (chiavetta usb...).

8. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI.

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

9. SEGNALARE TEMPESTIVAMENTE MALFUNZIONAMENTI O GUASTI DEL SISTEMA INFORMATIVO.

Contattare tempestivamente il personale tecnico locale alla presenza di malfunzionamenti, guasti, rotture del proprio PC, stampante, scanner e segnalare senza indugio anomalie al funzionamento dei programmi e della rete. Gran parte delle riparazioni alle apparecchiature può avvenire in garanzia se tempestivamente segnalate e tale collaborazione è necessaria al fine di mantenere in efficienza l'intero sistema informativo.

LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e 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:

- Attraverso programmi provenienti da fonti non ufficiali (Internet, posta elettronica, copie da floppy disk, Pen Drive,...).
- Attraverso le macro dei programmi di automazione d'ufficio (file Word, Excel, Access,...).

COME NON SI TRASMETTE UN VIRUS:

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

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

Quando si installano programmi, si copiano dati da dischetti e Pen Drive e si scaricano dati o programmi da Internet.

COME PREVENIRE I VIRUS:

1. **USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE**
   Ogni programma deve essere sottoposto alla scansione prima di essere installato.
2. **ASSICURATEVI DI NON FAR PARTIRE ACCIDENTALMENTE IL VOSTRO COMPUTER CON IL FLOPPY DISK O PEN DRIVE INSERITI.**
3. **ASSICURATEVI CHE IL VOSTRO SOFTWARE ANTIVIRUS SIA AGGIORNATO.**

COME NON PREVENIRE I VIRUS:

1. **NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA**
   Se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: mail di questo tipo sono detti 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, o da un tecnico informatico.
2. **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.

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.

COSA FARE:

1. **Cambiare la password a intervalli regolari.**
   Chiedete al Vostro amministratore di sistema 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 due anni.
2. **Usare password lunghe almeno sei caratteri con un misto di lettere, numeri e segni di punteggiatura.**
   Utilizzate password distinte per sistemi con diverso grado di sensibilità.

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 dove può 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.

COME SCEGLIERE UNA PASSWORD:

Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe. La frase "C'era una volta una gatta che aveva una macchia nera sul muso" può ad esempio fornire, tra le tante possibilità, "Cr1VIt]1Gtt".
Ecco alcuni esempi:

Frase	Possibile password
57% di Finlandesi hanno detto si alla EU	57%DFNHDSAEU
Roma è la capitale d'Italia	RMCPIEST
La mia macchia costa 27 milioni	MOPL27KKL
Meglio un uovo oggi che una gallina domani	MGLO/GLND
To be or not to be	(2B)V(!2B)
Nel 1970 ho traslocato a Roma	I1701->RM
"Esc" si trova in alto a sinistra	"E"sStULK
Gnu è un acronimo ricorsivo	GstACRR
Tutto è bene quel che finisce bene	2TBCFNB

Si ordina la trasmissione a tutto il personale, la pubblicazione sul sito del Tribunale e l'affissione in bacheca.

Asti, 11 DIC. 2024

La Dirigente amministrativa

La Presidente del Tribunale