# *Tribunale di Pordenone*

*Presidenza*

N. 1347/18 prot. u.

Pordenone, 29 GIU. 2018

Al Consiglio Superiore della Magistratura
protocollo.csm@giustiziacert.it

Al Ministero della Giustizia
Dipartimento dell'organizzazione giudiziaria, del personale e dei servizi
prot.dog@giustiziacert.it

Al Presidente della Corte d'Appello di Trieste
prot.ca.trieste@giustiziacert.it

A tutti i magistrati

A tutto il personale amministrativo

All'Ufficio del Giudice di Pace

All'UNEP

Al Presidente dell'Ordine degli Avvocati
Sede

**Premessa**

A seguito dell'emanazione del Regolamento europeo 679/2016 sulla privacy *"direttamente applicabile dal 25 maggio 2018"* negli Stati dell'Unione, il quadro normativo italiano appare in via di evoluzione, di qui la necessità di redigere un documento che armonizzi nell'ambito del contesto del Tribunale di Pordenone la normativa di interesse vigente, tenuto comunque conto che la legge di delegazione europea n. 163 del 2017 (nonché l'art. 32 della legge italiana n. 23 del 24.12.2017 che ha posto il principio del *"riassetto e della semplificazione normativa con*

*l'indicazione esplicita delle norme abrogate*") ha affidato ai legislatori nazionali delegati "*la potestà di verificare se e quali disposizioni vigenti e, segnatamente, quelle recate attualmente dal codice in materia di protezione dei dati personali, debbano essere espressamente abrogate per incompatibilità con il regolamento; poi, la potestà di verificare se e quali disposizioni di detto codice siano da modificare ma "limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute" nello stesso regolamento, ed infine la scelta dello strumento tecnico-normativo più lineare ed efficace per realizzare detti risultati*". Nell'ambito di tale regolamento, tra le norme direttamente applicabili, di interesse particolare per le Amministrazioni pubbliche (il regolamento europeo, peraltro, non prevede disposizioni distinte per i soggetti privati e quelli pubblici, rilevanti essendo le finalità del trattamento), va ricordata quella (dettata dall'art. 37 del Reg. UE 679/2016) che prevede la nuova figura del *Responsabile della protezione dei dati* (RPD), che può anche essere esterna all'ente ed "*assolvere i suoi compiti in base ad un contratto di servizi*" (art. 37, c. 6) di nomina e competenza ministeriale, come risulta dalla nota del Ministero di Giustizia n. 21611U del 27.06.2018.

Un'altra norma immediatamente efficace e d'interesse per le pubbliche amministrazioni è quella dettata dall'art. 30 Reg. UE 679, che pone l'obbligo di istituire registri, tenuti dal titolare e dai responsabili del trattamento, ove siano annotate le attività di trattamento. Anche in questo caso, tuttavia, appare opportuno attendere direttive che meglio definiscano, per gli uffici giudiziari, i modelli da adottare.

In attesa di disposizioni attuative per la esauriente applicazione della normativa in materia, si provvede con il presente documento che descrive i criteri e le norme di sicurezza nonché le misure tecniche ed organizzative da adottare per garantire, in relazione ad un contesto espresso in termini di dati, il mantenimento della disponibilità, autenticità, integrità e riservatezza delle informazioni trattate, in applicazione delle normative in materia di trasparenza, di accesso e di privacy.

Si raccomanda di prestare particolare attenzione nell'osservanza di tutte le disposizioni del presente provvedimento e delle misure dettate, atteso anche che il Reg.UE 679/2016, accentuando la tutela dei dati personali, non reca più una distinzione netta tra meri dati personali e dati sensibili per cui tutti i dati, per cautela, andranno trattati adottando rigorosamente le regole stabilite.

Soggetti dell'ufficio interessati dal trattamento dati

Si individuano le seguenti figure:

1. titolare del trattamento: la persona fisica, la persona giuridica, la P.A. e qualsiasi altro organismo cui competono le decisioni in ordine alle finalità, alla modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi incluse le procedure di sicurezza. Egli è tenuto a vigilare sulla correttezza delle operazioni di trattamento dei dati e sull'osservanza, da parte dei responsabili ed incaricati, delle istruzioni impartite al fine che interessa, nonché sull'attuazione del presente documento (Ministero della giustizia –Tribunale Ordinario di Pordenone – Capo dell'ufficio)

2. responsabile del trattamento: Permane, nel nuovo quadro normativo, la figura del responsabile del trattamento, che viene così definita dall'art. 4, n. 8:*"«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento,* è dunque il soggetto preposto a vigilare, nell'ambito del proprio settore e sfera di intervento, a che il trattamento medesimo avvenga in maniera corretta, ed in specie che i dati stessi siano:
    - trattati in maniera lecita;
    - raccolti e registrati per scopi determinati, espliciti, legittimi ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
    - esatti ed aggiornati;
    - pertinenti, completi e non eccedenti, rispetto alle finalità per cui sono raccolti e/o successivamente trattati.

In riferimento alla struttura organizzativa si individuano i responsabili del trattamento:

- Settore amministrativo - Dirigente
- Settore civile – Direttore responsabile
- Settore penale – Direttore responsabile

3. incaricato: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile. (Magistrati, personale amministrativo).

**Sono trattati i seguenti dati personali**:
- Dati relativi al personale dipendente dell'ufficio;
-Dati relativi alle persone fisiche, persone giuridiche, ente o associazioni identificati o identificabili, anche indirettamente mediante riferimento a qualsiasi altra informazione, che vengono comunicati all'ufficio per motivi istituzionali o di servizio.
Si indicano a scopo esemplificativo:

- i dati relativi alle persone che svolgono funzioni giudiziarie onorarie
- i dati del personale in servizio presso l'ufficio
- i dati delle ditte fornitrici
- delle persone non dipendenti che, a qualsiasi titolo prestano servizi nell'ambito della struttura giudiziaria
- i dati relativi a dipendenti che hanno prestato servizio in passato presso l'ufficio e che sono stati trasferiti, transitati verso altre amministrazioni o cessati dal servizio.

**I rischi che incombono sui dati sono:**

1. Eventi naturali e comportamenti umani: i dati devono essere disponibili per gli utenti autorizzati e devono essere messe in atto le misure idonee ad evitare che eventi naturali quali incendi, allagamenti, ed umani quali attentati, sottrazione di materiale ecc ne riducano la disponibilità;

2. Comportamenti colposi o dolosi che compromettono l'integrità dei dati: i dati possono elaborati, modificati, cancellati solo dalle persone autorizzate. La registrazione, l'elaborazione, la modifica, la cancellazione e le altre operazioni sui dati possono essere svolte solo dai dipendenti autorizzati con ordine di servizio o altro provvedimento.
3. Comportamenti che compromettono l'autenticità dei dati: deve essere certificata e garantita la provenienza dei dati. I certificati e gli altri documenti sono rilasciati secondo procedure validate e dalle persone autorizzate.
4. Comportamenti che compromettono la riservatezza di dati: I dati personali ed i dati giudiziari devono essere trattati secondo i principi dettati dal D.lvo n. 196 del 2003 e successive modifiche od integrazioni. Le informazioni possono essere fruite solo dalle persone legittimate ed è vietata la diffusione e la comunicazione a persone diverse da quelle autorizzate.

**Gestione del rischio e Beni da proteggere**

Essenziale è rilevare lo scenario esistente, specificando i beni da proteggere, le vulnerabilità del sistema (le varie possibilità/modalità di essere attaccati e danneggiati), le minacce (eventi che possono arrecare danni ai beni e/o pregiudizio all'integrità, riservatezza, autenticità, e disponibilità dei dati e processi), e i criteri di protezione per la riduzione del rischio.

Rilevando che sebbene le disposizioni in materia di sicurezza informatica costituiscono tuttora il presidio normativo per l'ufficio con riguardo alle attività svolte con l'ausilio dei mezzi telematici, molto è sottratto alla diretta disponibilità degli Uffici data la interdistrettualizzazione dei Server per cui anche eventuali procedure di aggiornamento ed adeguamento alla normativa vigente dovranno provenire dalla DIGSIA.

I beni informatici da proteggere sono suddivisi in tre categorie:

1. **apparati e strumenti informatici**
   - 1.1. individuali (PC desktop)
   - 1.2. di rete (Switch, Hub, Router, Firewall, PC Server, modem)
   - 1.3. supporti di Back-up (DISCHI ESTERNI, CD)
2. **software e dati trattati con strumenti elettronici.**
   - 2.1. software commerciale;
   - 2.2. applicativi di rilevanza nazionale;
   - 2.3. "dato personale", 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;
   - 2.4. "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
   - 2.5. "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, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

2.6. "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;

3. **tutte le informazioni, sia su supporto cartaceo che su supporto informatico**, che riguardano il sistema informatico nella sua interezza (tra cui l'elenco del materiale hardware e del software, le relative configurazioni).

Si ritiene necessario che l'Ufficio Giudiziario, mediante l'ufficio competente, rediga e mantenga aggiornato, segnalando tali aggiornamenti al CISIA competente, l'inventario dei beni informatici di

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

1. **Riservatezza**: Prevenzione contro l'accesso non autorizzato alle informazioni;
2. **Integrità**: Le informazioni non devono essere alterabili da incidenti o abusi;
3. **Disponibilità**: Il sistema deve essere protetto da interruzioni impreviste.

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

Le strategie individuate sono suddivise in criteri per macro aree:

- Criteri di protezione fisica delle aree e delle procedure di controllo degli accessi (custode, vigilanza in entrata, videosorveglianza, archivi chiusi a chiave e non accessibili senza chiave dagli ascensori, inferriate alle finestre del pianterreno, segnali acustici all'apertura delle uscite di sicurezza, chiave a disposizione di persone individuate per l'accesso alla sala server, dotata di impianto antincendio e condizionamento);

Si individuano in tale contesto le seguenti aree:

*Sale Server*

Le macchine Computer Server sono ubicate in un apposito locale dotata di:

Impianto antincendio adeguato a locali contenenti apparati informatici

Impianto di condizionamento ambientale opportunamente dimensionato

Porte blindate e finestre con inferriate

Impianto elettrico a norma;

*Gruppo di continuità.*

L'accesso alla sala Server è consentito solo alle persone espressamente autorizzate dal titolare del trattamento dati, oltre che al personale dell'assistenza sistemistica ove presenti.

*Sale supporti Backup*

Le sale in cui sono custoditi i supporti di backup, diverse dalle sale server, sono dotate di apposito armadio per supporti informatici, blindato non trasportabile.

I locali degli uffici in cui sono presenti apparecchiature e dati importanti sono protetti con impianti idonei contro eventi catastrofici, quali incendio ed allagamento, e dotati di controllo di accesso.

Tutte le chiavi di accesso, card elettroniche e manuali, ai locali sono custodite dal personale delegato dal titolare del trattamento. Qualsiasi rilascio di copia delle chiavi dovrà essere autorizzato.

Gli armadi che contengono gli apparati di rete devono essere chiusi a chiave, le chiavi custodite in un armadio blindato, posto in un locale distante dalla sala Server, non trasportabile e dotato di impianto antifurto.
Su tutte le apparecchiature di rete dotate di accesso remoto per la loro gestione devono essere attivate funzioni di autenticazione obbligatorie.

- Sicurezza del software

Presso l'ufficio è consentita l'installazione esclusiva delle seguenti tre categorie di software:

a) Software commerciale, dotato di licenza d'uso;
b) Software realizzato specificamente per l'Amministrazione, a livello nazionale;
c) Software realizzato specificamente per l'Ufficio, a livello locale.

La conformità dei software di cui alle voci a), c) viene certificata dall'ufficio della Direzione Generale per i Sistemi Informativi Automatizzati (DGSIA).

Il software, di cui si ha licenza d'uso, deve essere installato solo tramite supporti fisici originali o copie rilasciate dall'Amministrazione.

Su ogni computer è installato un software antivirus da aggiornare settimanalmente.

## Riservatezza dei dati

Data la elevata sensibilità dei dati trattati dagli uffici giudiziari, si seguono le seguenti prescrizioni di sicurezza nei casi riportati di seguito:

**1. sostituzione, assegnazione ad altro utente o dismissione del Personal Computer**

In concomitanza di una di queste operazioni, è necessario provvedere alla rimozione irreversibile di tutti i dati sensibili dall'apparecchiatura oggetto dell'operazione. La rimozione va effettuata dopo l'avvenuta copia dei dati sensibili su un opportuno supporto di memorizzazione (Hard Disk di un nuovo PC, se si tratta di una sostituzione di PC oppure su CD, DVD, Pen Drive, Iomega ZIP, ecc.) da consegnare all'utente.

**2. assistenza hardware per riparazione del Personal Computer**

In questo caso, qualora la ditta ritenesse opportuno, per i necessari controlli, trasferire il Personal Computer (PC) presso i propri laboratori, nel rispetto delle politiche di sicurezza deve essere adottata una delle seguenti precauzioni:

- estrazione dal PC del supporto di memorizzazione magnetica (hard disk) contenente i dati utente prima di consegnare il PC alla ditta; custodia del supporto da parte dell'utente; successiva reinstallazione sul PC da parte della ditta nel momento in cui il PC viene riconsegnato all'utente.
- operare come se si trattasse di una sostituzione o riassegnazione nel caso in cui la ditta, a seguito di esigenza motivata, dovesse giocoforza portar via anche l'hard disk contenente dati sensibili.
- richiedere l'autorizzazione al capo dell'ufficio, nel caso in cui la ditta ritenga necessaria la sostituzione in loco dell'hard disk oppure chiedere alla ditta la consegna dell'hard disk non più funzionante.

Tale raccomandazione si estende naturalmente per motivi di integrità e riservatezza dei dati a tutti i supporti di memorizzazione contenuti nei PC cosiddetti Server dell'Ufficio ancora presenti

Si prevede uno dei metodi seguenti per la distruzione dei dati presenti nei supporti di memorizzazione non più utilizzati:

- utilizzo di un software di riscrittura per la cancellazione irreversibile dei dati
- distruzione fisica del supporto di memorizzazione

Il personale è tenuto a comportamenti che di fatto tutelino la riservatezza dei dati detenuti anche in formato cartaceo, pertanto non devono essere custoditi in luogo con accesso al pubblico atti e fascicoli, anche archiviati; il personale di cancelleria deve vigilare sulla riservatezza dei dati detenuti e pertanto non consentire l'accesso all'interno delle cancellerie ad estranei non autorizzati inclusi gli addetti agli i studi legali e gli stessi legali, usando gli appositi front-office.

**Autenticazione informatica**

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

1.1. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

1.2 Gli incaricati del trattamento dovranno adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale che non dovrà essere comunicata a terzi e la custodia dei dispositivi.

Nome utente e password sono strettamente personali. L'utente è tenuto:

- **A non comunicare a terzi le password;**
- **A non annotare le password su supporti posti in vicinanza della propria postazione di lavoro, o comunque incustoditi;**
- **Le password dovranno essere diverse tra loro;**

Ad attenersi a tutte le indicazioni contenute nel manuale per la sicurezza. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

**Ulteriori misure in caso di trattamento di dati sensibili o giudiziari**

Tutti i dati rilevanti devono essere protetti contro l'accesso abusivo di cui all'art. 615 ter del codice penale attraverso i sistemi e le procedure appresso descritte:

- quando gli atti e i documenti contenenti dati personali o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
- l'accesso agli archivi contenenti dati è controllato.
- le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

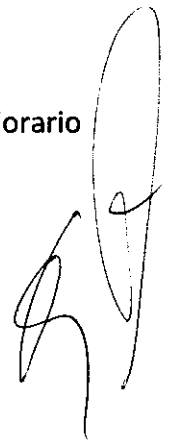
E' fatto divieto assoluto agli utenti di effettuare collegamenti telematici distinti da quelli previsti salvo autorizzazioni del Titolare del trattamento dei dati, sentito il parere dell'organo tecnico che dovrà essere informato sulla eventuale autorizzazione rilasciata.

In particolare, non sono autorizzate, salvo autorizzazioni del Titolare del trattamento dei dati:

1. connessioni dirette dalla rete dell'ufficio verso reti esterne diverse dalla rete Giustizia
2. connessioni effettuate tramite modem da postazioni collegate alla rete dell'ufficio
3. connessioni effettuate con PC portatili dirette dalla rete dell'ufficio verso reti esterne inclusa la rete Giustizia.
4. connessioni con hub o switch alle prese di rete a muro del cablaggio di rete informatica.

Agli incaricati del trattamento dei dati sono impartite le seguenti istruzioni dirette al controllo alla custodia degli atti per l'intero ciclo necessario alle operazioni di trattamento degli atti e documenti:

1. I documenti, atti, fascicoli contenenti i dati personali non possono essere consultati da persone diverse da quelle incaricate del trattamento;
2. Sono trattenuti dagli incaricati solo per il tempo strettamente necessario alle operazioni di trattamento, al termine di queste andranno riposti;
3. L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato.
4. Sarà tenuto un registro per l'identificazione delle persone ammesse all'accesso dopo l'orario di chiusura.
   In esso andranno annotati:
   - provvedimento di autorizzazione
   - nominativo della persona
   - documento di riconoscimento
   - scopo dell'accesso



Per quanto non previsto nel presente documento si applicano le disposizioni di legge vigenti .
In considerazione degli obblighi e dei termini per adempiervi previsti dagli artt. 33 e 34 del Reg. UE 679/16 a carico del titolare del trattamento, è necessario ed opportuno che eventuali rischi di violazione delle norme poste a tutela dei dati personali siano immediatamente comunicate al titolare del trattamento stesso (Presidente del Tribunale).

Si allega manuale per l'utente già allegato al **documento programmatico sulla sicurezza dei dati trattati con strumenti elettronici e redatto ai sensi del d.lvo n.196/2003 - Anno 2012**

Pordenone, 29 giugno 2018

*La dirigente*
*Dott.ssa Daniela Ciancio*

*Il Presidente*
*dott. Lanfranco Maria Tenaglia*

# Allegato 1) Manuale di sicurezza per gli utenti[1]

***Chiudere a chiave cassetti ed uffici.***

Il primo livello di protezione di qualunque sistema è quello fisico. E' certamente 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 o visibili su uno schermo. Pertanto, chiudete a chiave il vostro ufficio alla fine della giornata ed ogni volta che vi assentate. Inoltre chiudete i documenti a chiave nei cassetti quando possibile.

***Spegnere il computer se ci si assenta per un periodo di tempo lungo***

Lasciare un computer acceso non crea problemi al suo funzionamento ed al contrario velocizza il successivo accesso. Tuttavia, un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno.

***Non lasciare lavori incompiuti sullo schermo***

Chiudete sempre le applicazioni con cui state lavorando quando vi allontanate dal posto di lavoro per più di pochi minuti: potreste rimanere lontani più del previsto, e un documento presente sullo schermo è vulnerabile (quasi) quanto uno stampato o copiato su dischetto.

***Salvaschermo***

Ogni postazione di lavoro deve avere il salvaschermo attivato, con richiesta di password per poter riprendere il controllo della postazione.

***Proteggere attentamente i dati***

Bisogna prestare particolare attenzione ai dati importanti di cui si è personalmente responsabili. Poiché può risultare difficile distinguere tra dati normali e dati importanti, è buona norma trattare tutti i dati come se fossero importanti. Come minimo posizionarli in un'area protetta da password e non dare di default a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.

[1] Allegato al documento di sicurezza informatico del Tribunale di Pordenone redatto nel 2012

***Conservare supporti di memoria e stampe in luoghi sicuri***

Alla conservazione dei supporti di memoria (CD, dischetti) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli.

***Maneggiare e custodire con cura le stampe di materiale riservato***

Non lasciate accedere alle stampe persone non autorizzate. Se la stampante non si trova sulla vostra scrivania recatevi il più in fretta possibile a ritirare le stampe. Per stampe riservate cercate di usare una stampante non condivisa oppure usate la modalità di stampa ritardata impostando un tempo sufficiente a permettervi di raggiungere la stampante prima dell'inizio della stampa. Distruggete personalmente le stampe quando non servono più.

***Non gettare nel cestino le stampe di documenti che possono contenere informazioni confidenziali.***

Se trattate dati di particolare riservatezza, considerate la possibilità di dotarvi di una macchina distruggi-documenti (shredder). In ogni caso non gettate mai documenti cartacei senza averli prima fatti a pezzi.

***Non riutilizzare i dischetti per affidare a terzi i vostri dati***

Quando un file viene cancellato da un disco magnetico, i dati non vengono effettivamente eliminati dal disco ma soltanto marcati come non utilizzati e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati dai dischi. Solo l'uso di un apposito programma di cancellazione sicura garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un dischetto nuovo.

***Prestare particolare attenzione all'utilizzo dei computer portatili***

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, proteggetelo con una password sul BIOS, fate installare un programma di cifratura del disco rigido (per impedire la lettura dei dati in caso di furto) ed effettuate periodicamente il backup.

***Fare attenzione a non essere spiati mentre si digita una password o qualunque codice di accesso.***

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate una password questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura. Chiedete agli astanti di guardare da un'altra parte quando introducete una password o controllate che nessuno stia guardando.

***Proteggere il proprio computer con una password. Abilitare ove possibile l'accesso tramite password***

La maggior parte dei computer offre la possibilità di impostare una password all'accensione. Anche alcuni applicativi permettono di proteggere i propri dati tramite password. Imparate a utilizzare queste caratteristiche che offrono un buon livello di riservatezza.

***Non permettere l'uso del proprio computer o del proprio account da personale esterno***, a meno di non essere sicuri della loro identità. Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

***Non utilizzare apparecchiature non autorizzate o per cui non si è autorizzati***

L'utilizzo di modem su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al vostro computer ma a tutta la rete di cui fate parte. E' quindi vietato l'uso di modem all'interno della rete locale. Nel caso che ciò sia strettamente necessario, disconnettere fisicamente la postazione di lavoro dalla rete locale prima di effettuare il collegamento via modem. Per l'uso di altre apparecchiature, chiedere consiglio all'amministratore di sistema.

***Non installare programmi non autorizzati.***

Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale.

***Diffidare dei dati o dei programmi la cui provenienza non è certa.***

Per proteggersi di virus ed altri agenti attivi di attacco, diffidate di tutti i dati e programmi che vi vengono inviati o consegnati, anche se la fonte appare affidabile o il contenuto molto interessante. Infatti molti sistemi di attacco inviano dati che sembrano provenire da un utente noto al destinatario per vincerne la naturale diffidenza nei confronti degli estranei.

***Applicare con cura le linee guida per la prevenzione da infezioni da virus***

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore rispetto alla correzione degli effetti di un virus. Inoltre, se non avete attivato adeguate misure anti-virus potreste incorrere in una perdita irreparabile di dati o in un blocco anche molto prolungato della vostra postazione di lavoro.

***Usare, se possibile, il salvataggio automatico dei dati. Non dimenticare i salvataggi volontari.***

Molti programmi applicativi, ad esempio quelli di videoscrittura, salvano automaticamente il lavoro a intervalli fissi, in modo da minimizzare il rischio di perdita accidentale dei dati. Imparate comunque a salvare manualmente il vostro lavoro con una certa frequenza, in modo da prendere l'abitudine di gestire voi stessi i dati e non fare esclusivo affidamento sul sistema.

***Utilizzo del PC***

L'utente deve attenersi scrupolosamente all'utilizzo del PC solo ed esclusivamente per attività di Ufficio, ed è fatto divieto, salvo operazioni semplici (p.e., sostituzione di mouse, di tastiera) che non possano compromettere la funzionalità del PC, assumere iniziative personali per porre rimedio ad eventuali problemi tecnici, in particolar modo di tipo hardware; in tale caso è consigliabile rivolgersi al proprio ufficio che curerà la pratica di assistenza (Ufficio Informatica, laddove presente, o Ufficio Economato/Beni Patrimoniali e in caso di urgenza ai tecnici dell'assistenza sistemistica o, in assenza di questi, all'amministratore di sistema dell'ufficio.

***Amministrare correttamente le password***

Non scrivere 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.

***Non violare le leggi in materia di sicurezza informatica.***

Ricordatevi che anche solo un tentativo di ingresso non autorizzato in un sistema costituisce un reato. Se siete interessati a studiare la sicurezza della vostra postazione di lavoro o della rete di cui fate parte, chiedete preventivamente l'autorizzazione al Responsabile della sicurezza del singolo Ufficio. Non utilizzate senza autorizzazione software che possa creare problemi di sicurezza o danneggiare la rete, come port scanner, security scanner, network monitor, network flooder, fabbriche di virus o di worm.

***Segnalare tempestivamente qualsiasi variazione del comportamento della propria postazione di lavoro*** perché può essere il sintomo di un attacco in corso.

***Segnalare comportamenti che possano far pensare a tentativi di ridurre la sicurezza del sistema informativo***

Ad esempio segnalate al Responsabile della sicurezza dell'Ufficio se un altro utente insiste per avere accesso ai vostri dati o per conoscere la vostra password o per poter lavorare sulla vostra postazione di lavoro. Analogamente non fidatevi e segnalate telefonate o messaggi che sembrano provenire da un sistema e vi chiedono di fare operazioni strane sul vostro computer (ad esempio, cambiare subito la password con una datavi al telefono o nel corpo del messaggio).

Si fa presente che per ogni ulteriore informazione sulle modalità di comportamento da tenere sul luogo di lavoro è necessario far riferimento al responsabile o al titolare del trattamento dei dati.