ISTRUZIONI PER LA SICUREZZA DEI DATI

Azienda USL 1 Sardegna

Misure di sicurezza da applicare nei trattamenti di dati con strumenti elettronici

Documento	DPS-IST01/1
Edizione	21/11/2005

Introduzione

L'**Autorità Garante della Privacy**, istituita nel 1996, si propone di tutelare il diritto alla privacy di tutti, sia che si tratti di persone fisiche ovvero di persone giuridiche, enti o associazioni. Vengono quindi focalizzati tutti i processi aziendali che interessano dati personali, entrando nel merito delle finalità e della liceità dei "trattamenti" che vengono effettuati.

In questo contesto l'Azienda USL 1 Sardegna, in qualità di titolare dei trattamenti dei dati necessari per l'espletamento della propria missione, dopo aver provveduto agli adempimenti previsti dalla Legge, intende sensibilizzare tutto il personale alle misure di sicurezza per la tutela dei dati e della Privacy .

> ***Privacy e Sicurezza pur essendo distinte, sono intimamente legate tra loro.***
>
> ***Le misure di sicurezza sono il presupposto operativo e strumentale, certamente necessarie, ma non sufficienti per garantire quanto si prefigge il Garante.***
>
> ***Gli adempimenti richiesti dal Garante, le sanzioni e le pene, previste in caso di inadempienza, sono gli strumenti che la Legge usa per regolamentare ed intervenire.***
>
> ***Tuttavia, la vera tutela della Privacy non può che essere il risultato di un codice deontologico aziendale, fondato su valori etici e regole di comportamento che tutti devono conoscere, adottare e far rispettare.***

Queste linee istruzioni sono destinate a tutto il personale Incaricato di effettuare trattamenti di dati con strumenti elettronici.

Indice del Contenuto

1 Introduzione

Il "Testo Unico sulla Privacy" (Dlgs.196/03) entrato in vigore il primo gennaio 2004, riprende ed integra la normativa introdotta dalla Legge 675/96 e dal DPR.318/99, prevedendo l'obbligo di garantire la sicurezza, l'integrità e la disponibilità dei dati personali. Esso sancisce che:

"Chiunque ha diritto alla protezione dei dati personali che lo riguardano."

"I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità."

Si tratta di una regola di ordine generale in specie per i sistemi e i programmi che verranno d'ora in poi predisposti.

1.1 Definizioni

Riportiamo le definizioni del Codice:

a**) "trattamento"**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) **"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;

c) **"dati identificativi",** i dati personali che permettono l'identificazione diretta dell'interessato;

d) **"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;

e) **"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;

f) **"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;

g) **"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;

h**) "Incaricati",** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i**) "interessato",** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) **"comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) **"diffusione",** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) **"dato anonimo",** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o**) "blocco",** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) **"banca di dati",** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) **"Garante",** l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2 L'insieme delle misure di sicurezza

La sicurezza non deve essere intesa solo come protezione da eventi negativi, accidentali o intenzionali, ma anche come limitazione degli effetti causati dall'eventuale verificarsi di tali eventi di:

- **distruzione o perdita, anche accidentale, dei dati**: ossia si deve impedire che dati, informazioni e risorse siano resi irreperibili da persone, mediante processi non autorizzati, o da eventi accidentali. Nel mondo informatico si ricorre la concetto di ***disponibilità del dato,*** in tale ambito assume inoltre una particolare valenza il requisito della ***integrità del dato***, che deve essere quello originario o legittimamente modificato, in relazione alla relativa facilità di procedere fraudolentemente a modifiche senza lasciare indizi;

- **accesso non autorizzato ai dati**: nel mondo fisico è immediato pensare ad estranei, che nella notte si introducono in un'azienda per rubare dei dati o farne delle copie, piuttosto che a personale dell'azienda stessa che viola determinati archivi durante l'orario di lavoro. Nel mondo informatico si parla di ***confidenzialità*** o ***riservatezza,*** con ciò intendendosi che un determinato dato deve essere accessibile solo a chi è autorizzato: si dovrà quindi fare in modo che il personale non possa consultare files che non lo riguardano; che estranei non possano accedere abusivamente al sistema informativo; che durante la trasmissione di dati da un computer ad un altro, dei malintenzionati non intercettino i messaggi per violare le informazioni in essi contenuti. Correlato a tali aspetti vi è il requisito della ***autenticità*** dei dati, che concerne la garanzia e certificazione della loro provenienza;

- trattamento non consentito o non conforme alle finalità della raccolta.

L'insieme delle misure di sicurezza viene quindi concettualmente suddiviso in tre sottoinsiemi, distinguendo le ***misure***:

- ***organizzative***, che si sostanziano nella definizione di una serie di norme e procedure, miranti a regolamentare l'aspetto organizzativo del processo di sicurezza.

- ***fisiche,*** il cui scopo è di proteggere le aree, le apparecchiature, i dati e le persone da eventi di natura accidentale (es. incendi) e da intrusioni, di personale non autorizzato o di terzi.

- ***logiche***, il cui campo di applicazione riguarda la protezione delle informazioni, con particolare riferimento a quelle gestite con i sistemi informativi (dati, applicazioni, sistemi e reti), sia in relazione al loro corretto utilizzo, che in relazione alla loro gestione e manutenzione nel tempo

2.1 Sensibilizzazione alla sicurezza

> ***Tutto il personale deve tenere presente che le attività relative alla sicurezza non rappresentano un appesantimento del lavoro quotidiano, ma una volta che entrano nel ciclo standard delle operazioni da compiere, contribuiscono a***

> ***garantire tutti dal rischio di perdere, o comunque compromettere, parte del lavoro fatto.***

La *sensibilizzazione* alle tematiche della sicurezza, ed a costanti comportamenti coerenti con le disposizioni date in merito, deve interessare tutto il personale dell'Azienda, ad ogni livello di responsabilità ed attività: ciò al fine di diffondere una cultura generalizzata della sicurezza, che consenta tra l'altro di favorire la miglior efficacia ed efficienza delle misure prese, oltre che di sopperire ad eventuali mancanze delle stesse.

3 L'organizzazione per la sicurezza

L'Azienda Unità Sanitaria 1 di Sassari, nella consapevolezza che un sistema complesso quale la sicurezza può funzionare solo se i suoi meccanismi sono formalizzati e verificabili nonché posti in essere da personale adeguatamente formato e motivato, per l'applicazione e la gestione della normativa sulla privacy, ha provveduto ad adottare la seguente organizzazione per la sicurezza.

3.1 Titolare del trattamento

Ai sensi dell'art.4, lett. f) del Codice in materia di protezione dei dati personali, il Titolare dei trattamenti è l'Azienda USL N. 1 di Sassari nella persona del Direttore Generale.

Il Titolare verificherà periodicamente che le istruzioni e le norme di legge in tema di privacy vengano correttamente applicate dai Responsabili.

3.2 Responsabili del trattamento

il Titolare, nella persona del Direttore Generale dell'Azienda USL N. 1 di Sassari, ha nominato Responsabili dei Trattamenti tutti i Dirigenti di Struttura Semplice o Complessa.

3.3 Responsabile per la Sicurezza Informatica

il Titolare, nella persona del Direttore Generale dell'Azienda USL N. 1 di Sassari, ha nominato Responsabile della Sicurezza Informatica il dirigente responsabile del Sistema Informativo ed Informatico.

Al Responsabile per la Sicurezza Informatica sono assegnati i compiti di:

- progettare, realizzare e mantenere in efficienza le misure di sicurezza, conformemente a quanto previsto dagli articoli 31 e 33 Dlgs 196/2003;
- sovrintendere alle risorse del sistema informativo e di consentirne l'utilizzazione.

3.4 Incaricati

il Titolare, nella persona del Direttore Generale dell'Azienda USL N. 1 di Sassari, ha assegnato ai Responsabili la delega per la designazione obbligatoria degli Incaricati nelle strutture organizzative di pertinenza.

Ogni Incaricato ha, in ordine al trattamento, la responsabilità di eseguire correttamente le funzioni operative corrispondenti alle mansioni svolte nella struttura di pertinenza.

Le operazioni di trattamento di dati personali possono essere effettuate solo dagli Incaricati autorizzati dal Titolare o dai Responsabili.

> ***Si tenga presente che tutto il personale medico e amministrativo dell'Azienda USL (medici, paramedici ed impiegati amministrativi) che in qualche misura svolge attività che implicano il trattamento di dati personali, con particolare attenzione per quelli sensibili e giudiziari, dovrà essere designato quale Incaricato dei trattamenti di competenza.***

4 Direttive ed istruzioni di carattere generale

Al fine di una corretta applicazione del D. Lgs. n. 196/2003 (di seguito "il Codice"), nonché di una adeguata tutela dei diritti degli interessati, i soggetti nominati Incaricati del trattamento dei dati personali dovranno osservare le seguenti direttive ed istruzioni generali.

> ***Occorre ricordare che per trattamento di dati deve intendersi: "qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di strumenti elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati".***
>
> ***Sono dati personali tutte le informazioni che permettano l'identificazione del soggetto cui si riferiscono (es. dati anagrafici, recapiti telefonici, ecc.).***

4.1 Modalità di trattamento e raccolta dei dati personali

L'Incaricato che riceve ed utilizza informazioni personali con modalità cartacee ed informatiche, raccolte presso gli stessi interessati o di altre fonti, deve sincerarsi che i dati siano da lui:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati soli per scopi stabiliti, espliciti e legittimi;
- compatibili con quelli utilizzati in altre procedure e con gli scopi per i quali i dati sono stati raccolti;
- esatti e, se necessario, aggiornati;
- pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in modo tale che l'identificazione dell'interessato sia possibile per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

A tal fine, il soggetto Incaricato dovrà:

- trattare tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle proprie funzioni, in modo lecito e secondo correttezza;
- effettuare la raccolta, l'elaborazione, la registrazione, ecc. di dati personali esclusivamente per lo svolgimento delle proprie mansioni;
- accertarsi che gli atti e/o documenti nei quali sono contenuti i dati personali oggetto di trattamento dovranno essere custoditi presso gli archivi della propria struttura di riferimento e/o presso idonei ripiani del proprio ufficio, debitamente muniti di serratura;

- evitare che i documenti prelevati per il trattamento siano lasciati incustoditi, in modo da non consentirne l'accesso a persone non autorizzate;

- aggiornare trimestralmente/semestralmente tutte le banche dati cui ha accesso;

- mantenere assoluto riserbo sui dati personali di cui venga a conoscenza nell'esercizio delle proprie funzioni.

E' fatto assoluto divieto di comunicare, diffondere, utilizzare i dati personali provenienti dalle banche dati aziendali (dello studio, dell'associazione ecc.), in assenza dell'autorizzazione del Responsabile.

> ***L'Incaricato deve verificare la sussistenza di tali requisiti in tutte le fasi del trattamento affidatogli, riportando al proprio Responsabile ogni situazione di criticità che dovesse rilevare.***

Non è consentito all'Incaricato:

- utilizzare informazioni personali al di fuori di quelle necessarie per compiere le operazioni connesse alle sue specifiche mansioni;

- creare banche dati nuove senza espressa autorizzazione del titolare e/o del responsabile;

- conservare dati personali in archivi e banche dati al di fuori di quelle espressamente indicate nel Documento Programmatico sulla Sicurezza (DPS) o autorizzate dal Responsabile, considerato che eventuali nuovi trattamenti o trattamenti non censiti nel DPS dovranno immediatamente essere comunicati al Responsabile prima dell'avvio ;

- asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione del Responsabile;

- comunicare o diffondere dati personali di cui gli Incaricati vengano a conoscenza nello svolgimento del proprio lavoro.

4.2 Particolari cautele per i dati personali "sensibili"

Gli Incaricati possono trovarsi, nell'esercizio delle propri funzioni, a trattare dati personali "sensibili".

> ***Sono dati sensibili quei "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".***

Costituendo tali dati il nucleo più intimo e personale della vita di ciascuno, il Codice prevede una disciplina particolarmente restrittiva e severa per il loro trattamento, prescrivendo anche ulteriori misure di sicurezza e modalità specifiche per la loro custodia.

Ne consegue che, in questi casi, l'Incaricato del trattamento di tale tipologia di dati, dovrà mantenere un comportamento adeguato alla cura ed al rispetto degli individui cui i dati si riferiscono, *adottando ogni precauzione che impedisca il rischio di perdita dei dati stessi o di cognizione (accesso) da parte di soggetti non autorizzati* ad esserne informati.

4.2.1 Dati sensibili in documenti cartacei

Nello specifico, a titolo esemplificativo e non esaustivo, le precauzioni che l'Incaricato sarà tenuto ad adottare nel caso in cui si trovasse a trattare dei dati sensibili, riprodotti su formato cartaceo, nello svolgimento delle proprie mansioni, sono le seguenti:

- gli atti ed i documenti che riproducono i dati sensibili dovranno essere conservati negli archivi del proprio ufficio o reparto, muniti di serratura;
- l'Incaricato potrà accedervi solo per motivi professionali ed esclusivamente durante l'orario di lavoro, nei limiti in cui ciò sia strettamente necessario per prelevare e riporre i documenti per lo svolgimento dei propri compiti;
- qualora dovesse assentarsi durante le sessioni di lavoro dalla propria postazione di lavoro, i documenti e gli atti dovranno essere custoditi negli armadi, scrivanie o cassetti, muniti di serratura, in modo da non consentire l'accesso a persone non autorizzate;
- in ogni caso, al termine delle operazioni di trattamento, gli atti ed i documenti dovranno essere riposti negli archivi, muniti di serratura, di cui al primo punto, da cui sono stati prelevati.

4.2.2 Dati sensibili in documenti informatici e/o elettronici

Per le cautele da adottare nel caso di trattamento di dati personali anche sensibili, effettuato mediante strumenti elettronici e/o informatici, si rinvia alle istruzioni dei capitoli seguenti relativi all'uso corretto degli strumenti informatici.

5 Modalità per un corretto utilizzo delle risorse informatiche aziendali

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi ai principi di diligenza e correttezza che sono alla base di ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, in coerenza con le previsioni di legge - artt. 2104 e 2105 c.c. - e contrattuali, si ritiene utile fornire ulteriori regole interne di condotta comune, dirette ad evitare comportamenti inconsapevoli e/o scorretti.

Nei casi in cui l'Azienda lo ritenga opportuno, tali regole potranno essere soggette a modifiche o integrazioni, tenuto conto anche dell'evoluzione normativa in materia e del progresso tecnologico, nonché degli sviluppi delle infrastrutture informatiche e produttive dell'Azienda, di cui tutti gli Incaricati verranno portati a conoscenza.

Le indicazioni che seguono si riferiscono a tutte le risorse informatiche di proprietà dell'Azienda USL N. 1 di Sassari(nel seguito "l'Azienda") e si applicano a tutti i soggetti che le utilizzano (nel seguito "Utenti"), ivi incluso il personale esterno che accede alle risorse informative ed ai sistemi informatici dell'Azienda.

Per risorse informatiche si intendono i dati, le applicazioni e i sistemi (hardware e software di base).

L'Azienda emanerà periodicamente comunicazioni e direttive alle quali tutti gli Utenti sono tenuti a conformarsi.

5.1 Accesso alle risorse informatiche

Gli utenti hanno diritto ad accedere alle risorse informatiche aziendali per le quali sono stati espressamente autorizzati e ad utilizzarle esclusivamente per gli scopi inerenti le mansioni svolte.

Tali autorizzazioni sono strettamente personali e non cedibili.

Gli strumenti adottati dall'Azienda per l'accesso alle risorse informatiche (es. codici di accesso, user-id, ecc.) sono anch'essi di uso strettamente personale e, pertanto, l'Utente è tenuto a custodirli in modo appropriato.

Gli accessi alle banche dati informatizzate e/o ai dati personali oggetto di trattamento dovrà avvenire tramite l'elaboratore/gli elaboratori assegnati, anche temporaneamente, di cui l'Utente è personalmente responsabile durante il periodo in cui svolge la prestazione lavorativa, anche al di fuori del normale orario di lavoro; in particolare per quanto riguarda la corretta applicazione delle procedure e misure di sicurezza di seguito indicate.

Ai dati presenti nelle banche dati l'Utente è autorizzato a procedere per consultazioni, elaborazioni, aggiornamenti e cancellazioni secondo le sole esigenze richieste dalle sue mansioni professionali.

5.2 Utilizzo delle credenziali di autenticazione

Gli accessi tramite il computer agli archivi informatici sono protetti da una o più credenziali di autenticazione consistenti in uno o più user-id (identificativo utente) e da una o più password univoche, ovvero associate esclusivamente a ciascun Utente.

A ciascun Utente sono attribuiti, pertanto, una user-id nominativa ed una password di accesso ai sistemi informatici dell'Azienda. Saranno inoltre assegnate ulteriori user-id e password per l'accesso ai sistemi o a parte di essi a cui ciascun Utente è autorizzato ad accedere secondo i profili di autorizzazione riconosciuti.

Le password e lo/gli user-id verranno forniti per la prima volta dal *Responsabile della Sicurezza Informatica (*o da un suo incaricato espressamente autorizzato)*.*

Successivamente al primo utilizzo della password inizialmente comunicata l'Utente è tenuto a modificare la password fornita dal Responsabile della Sicurezza Informatica *(*o da un suo incaricato espressamente autorizzato) e cambiarla con la frequenza e secondo le regole qui riportate e che verranno di volta in volta indicate.

Qualora per motivi di necessità ed urgenza sia indispensabile eseguire delle operazioni di trattamento di dati disponibili esclusivamente attraverso l'utilizzo delle credenziali di autenticazione e degli strumenti elettronici appartenenti ad altri Utenti (ad es Posta elettronica), ed in caso di loro prolungata assenza od impedimento, sarà comunicato all'Utente interessato una password provvisoria di accesso, previa autorizzazione del proprio "Responsabile.

Al termine delle operazioni effettuate l'Utente interessato dovrà comunicare al proprio "*Responsabile*" di aver terminato l'intervento indicando le operazioni da esso compiute.

Si fa presente che le password di accesso ai sistemi informatici sono di uso strettamente personale e devono essere mantenute riservate.

Non è permesso comunicarle ad alcuno.

Le password scelte dovranno avere una lunghezza non inferiore agli otto caratteri salvo che il sistema, l'applicazione o lo strumento elettronico non lo consentano e comunque, in questi ultimi casi, il numero dei caratteri dovrà essere uguale a quello massimo consentito.

Al fine di evitare accessi non autorizzati o non consentiti, rischi di intrusione nei sistemi informativi aziendali, di distruzione o perdita dei dati l'Utente è tenuto a non:

- comunicare la password per telefono o altro mezzo a soggetti che si presentano come colleghi, tecnici, supervisori ecc;
- digitare la password davanti ad altri (ad es. colleghi o estranei);
- scrivere la password su foglietti apposti al personal computer, lasciati sulla scrivania o dentro ad un cassetto;
- mantenere copia della/e password utilizzate, salvo che la copia sia conservata in un luogo accessibile al solo Utente.

Le tecniche più frequentemente impiegate per scoprire le password consistono in programmi che attingono ad esempio a dizionari o ad elenchi telefonici.

Nella misura in cui il sistema non lo imponga in maniera automatica è, quindi, raccomandabile non utilizzare una password facilmente deducibile da parte di terzi e quindi:

- non usare una password che:
  - sia un nome proprio di persona o derivante dallo userid (identico, inverso, con le lettere raddoppiate, ecc.);
  - sia composta di sole cifre o di una sola lettera o carattere anche ripetuto più volte, o ancora digitata attraverso l'uso della sola barra spaziatrice;
  - abbia riferimenti riconducibili a dati personali (indirizzo, telefono, codice fiscale, numero della patente,ecc.) o a dati dell'azienda (denominazione sociale, ufficio, struttura, ecc.) o alla data corrente;
  - sia uguale alle ultime tre utilizzate o uguale alla precedente tranne che per un carattere.
- effettuare la sostituzione della password almeno ogni 30 giorni.

In generale, qualora si avesse anche solo il dubbio che sia venuta a conoscenza di altri è necessario:

- provvedere immediatamente alla modifica della password;

  segnalare al Responsabile della Sicurezza Informatica la sospetta violazione.

5.3 Utilizzo del Personal Computer

All'Utente, nell'ambito del rapporto di lavoro, sono affidate in uso risorse informatiche dell'Azienda come personal computer, computer portatili, relativi programmi e/o applicazioni nonché informazioni in essi contenute. E' quindi necessario:

- custodirli in modo appropriato;
- utilizzarli per lo svolgimento delle attività lavorative, nell'ambito delle mansioni assegnate;
- non utilizzarli per scopi illeciti;
- mettere in atto tutti gli strumenti e le precauzioni necessarie al fine di evitare l'accesso alla risorsa da parte di soggetti non autorizzati, ogniqualvolta ci si allontana dal personal computer (ad es. procedere al blocco del computer oppure all'attivazione dello screen saver protetto da password).

Al fine di assicurare il corretto funzionamento delle applicazioni del personal computer (PC), nonché di evitare il grave pericolo di introdurre virus informatici all'interno della rete dell'Azienda, è opportuno che l'Utente:

- non modifichi, senza preventiva autorizzazione, le configurazioni impostate sul proprio PC;
- non rimuova o modifichi, senza preventiva autorizzazione, alcun dato o apparecchiatura aziendale;
- non installi sul proprio PC mezzi di comunicazione o altre periferiche proprie, senza preventiva autorizzazione (ad es.: modem, masterizzatori, etc..);
- non installi ed utilizzi software non autorizzati e comunque non di proprietà dell'Azienda;
- non utilizzi software ricevuto in uso al di fuori delle finalità lavorative, evitando, in particolare, di realizzare copie da cedere, a qualsiasi titolo, a terzi;
- non distribuisca (anche via e-mail) ed utilizzi software che possa danneggiare le risorse informatiche.

> ***L'utilizzo di computer portatili richiede che gli Utenti applichino la dovuta attenzione all'attuazione delle procedure poste in essere dall'Azienda a garanzia della sicurezza informatica, specifiche per tali dotazioni, come ad esempio la necessità di collegarsi periodicamente alla rete aziendale per consentire l'aggiornamento delle configurazioni (aggiornamento patch e antivirus).***

In particolare, il personale esterno non può connettersi alla rete aziendale con il proprio Personal Computer portatile se non previa esplicita autorizzazione dell'Amministratore del Sistema interessato.

In generale, è richiesta da parte dell'Utente l'adozione di cautele atte ad evitare qualunque tipo di azione il cui effetto consista nel provocare danni, anche permanenti, a sistemi informatici o telematici, nonché a dati, documenti e comunicazioni.

5.4 Utilizzo dei servizi aziendali di Rete

L'utilizzo delle risorse aziendali di rete (ad es. Posta elettronica, Internet) per motivi non attinenti allo svolgimento delle mansioni assegnate, provoca una distorsione dell'utilizzo delle risorse informatiche verso attività non produttive per l'Azienda.

> ***Alcuni atti, anche involontari, possono inoltre danneggiare seriamente l'Azienda.***

Al fine di scongiurare tale pericolo è necessario che l'Utente eviti comportamenti come quelli qui di seguito richiamati a titolo indicativo.

5.4.1 Posta elettronica

Nel precisare che la Posta Elettronica è uno strumento di lavoro, si ritiene utile segnalare che l'Utente deve evitare di:

- utilizzare l'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mailing-list non direttamente attinenti l'attività lavorative e le proprie mansioni, salvo diversa ed esplicita autorizzazione;
- effettuare ogni genere di comunicazione non afferente a ragioni di servizio, salvo diversa ed esplicita autorizzazione;

- simulare l'identità di un altro utente;
- inoltrare messaggi, comunicazioni o circolari non aventi contenuti di interesse aziendale utilizzando le liste di distribuzione;
- usare provider di posta elettronica diversi da quello aziendale, salvo esplicita autorizzazione del proprio Responsabile;
- prestare la massima attenzione nell'aprire allegati di posta elettronica "ambigui" (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati aziendali).

5.4.2 Internet

Per quel che riguarda le modalità di utilizzo della rete Internet, è opportuno segnalare che l'Utente deve evitare di:

- effettuare ogni genere di comunicazione non afferente a ragioni di servizio, salvo diversa ed esplicita autorizzazione;
- partecipare, per motivi non professionali a Forum, l'utilizzo di chat-line, di bacheche elettroniche e registrazioni in guest-book anche utilizzando pseudonimi (o nicknames);
- scaricare software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente e preventivamente autorizzato;
- scaricare file multimediali per finalità non direttamente afferenti l'attività lavorativa, comunque sempre con esplicita autorizzazione del proprio Responsabile;
- scaricare documenti informatici di natura oltraggiosa o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione o appartenenza sindacale o politica.

5.4.3 Intranet

Le unità di rete aziendali sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi, pertanto gli Utenti non devono:

- modificare gli indirizzi IP assegnati ai propri PC;
- dislocare, nemmeno per brevi periodi, in queste unità, qualunque files che non sia legato all'attività lavorativa;
- trasferire su cartelle pubbliche dati non destinati alla diffusione, nonché dati d'interesse strategico aziendale (se non preventivamente autorizzati).

5.5 Gestione dei supporti fisici rimovibili

Per quanto concerne i supporti fisici rimovibili (es. floppy disk, dischi ZIP, CD….), contenenti dati personali, devono essere attuate misure che garantiscano il salvataggio dei dati con frequenza almeno settimanale.

L'Azienda USL N. 1 di Sassari prescrive inoltre agli Incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati o distrutti, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;

- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.