Regolamento per la corretta gestione degli archivi informatici, delle apparecchiature informatiche e degli archivi cartacei

INDICE

Premessa **2**
Organizzazione del Servizio Informatico Aziendale **3**
Definizioni di natura giuridica **5**
Definizioni di natura tecnica **7**
L'utilizzo della strumentazione informatica da parte del dipendente pubblico **10**
Il Regolamento Informatico Aziendale **11**
Misure minime di sicurezza in materia di privacy **12**
Regole di utilizzo **13**
Premessa : 13
Accesso alle risorse informatiche e di rete 13
Utilizzo delle risorse informatiche e di rete 13
Responsabilità degli utenti 13
Software e licenze d'uso 14
Descrizione dei sistemi presenti **14**
Caratteristiche della Rete Trasmissione Dati 15
Caratteristiche dei sistemi informatici 15
Misure di sicurezza adottate/da adottare **16**
Prescrizioni di sicurezza 16
Misure Logiche 17
Controllo Accessi ai dati: autenticazione – autorizzazione - abilitazione 17
Protezione antivirus 18
Protezione delle rete 18
Misure Organizzative 19
Amministratori di sistema 19
Aspetti della sicurezza riguardo il trattamento dei dati e la detenzione degli archivi
Norme comportamentali degli utenti (Responsabili ed incaricati) **21**
Sicurezza fisica 21
Sicurezza logica 21
Sicurezza del software e dell'hardware 24
Protezione da virus informatici 25
Utilizzo della rete internet 26

Premessa

Il Codice unico in materia di protezione dei dati personali (D.Lgs. 30 giugno 2003 n° 196), entrato in vigore il 1° gennaio 2004 è finalizzato a regolamentare le finalità e le modalità di trattamento dei dati personali, trattati a vario titolo nell'ambito di strutture pubbliche e private
L'art. 3 del D.lgs. 196/03 sancisce il principio di necessità, fondamento della liceità nel trattamento dei dati personali. Questo principio limita il trattamento dei dati personali ai soli dati ritenuti necessari per l'adempimento dei doveri istituzionali. Coloro che trattano dati devono raccogliere le informazioni che rivestono un carattere personale rispettando la riservatezza, limitando la registrazione dei dati agli scopi previsti dalle finalità del trattamento
Il Codice si articola sulla base di direttive e regole valide per tutti i trattamenti: il trattamento deve essere lecito, corretto e pertinente ovvero non eccedente rispetto agli scopi richiesti dal trattamento . Le finalità del trattamento devono essere esplicite e legittime, rese note all'interessato mediante una informativa che deve essere fornita in maniera standardizzata, anche nel caso in cui non sussista l'obbligo di acquisire il consenso da parte dell'interessato.
Occorre, pertanto, acquisire un comportamento improntato al rispetto della riservatezza e delle indicazioni deontologiche emanate dal Garante della privacy e prestare un'attenzione particolare ai dati sensibili ovvero ai dati personali che sono, fra l'altro, idonei a rivelare lo stato di salute dei soggetti interessati. Ancor prima della responsabilità derivante dal trattamento dei dati, riconducibile alla normativa sulla protezione dei dati personali, esiste una responsabilità connessa alla adeguatezza nelle procedure di applicazione concernenti le regole tecniche che attengono alla gestione del sistema informatico aziendale . La mancata osservanza delle regole tecniche descritte nel presente regolamento potrebbe arrecare danni di natura anche patrimoniale, a causa di eventuali danneggiamenti del sistema operativo informatico aziendale
E' il caso di precisare che mancato rispetto delle norme tecniche nonché la mancanza delle citate misure di osservanza della riservatezza potrebbe comportare non solo effetti sanzionatori dettati dalla normativa in materia di privacy, ma anche la sanzione civilistica relativa alla "Responsabilità per l'esercizio di attività pericolosa", art. 2050 c.c., nel caso di inadempienze derivanti da violazione di norme concernenti sia le modalità di trattamento che il danno patrimoniale.
Scopo di questo documento è illustrare le misure di sicurezza che devono essere ottemperate durante le operazioni eseguite in funzione e nell'ambito del sistema operativo informatico aziendale e che devono rispecchiare le misure Fisiche, Logiche ed Organizzative contemplate nel Codice della privacy al fine di garantire l'integrità dei dati e delle applicazioni dell' Azienda ospedaliera "Antonio Cardarelli" , con particolare riferimento ai dati soggetti ad archiviazione. Nel caso specifico dei dati personali, identificati come tali ai fini D.Lgs. 196/2003, le misure individuate e di seguito descritte, sono tali da soddisfare i requisiti generali della vigente normativa e le misure minime di sicurezza descritte nell' allegato B del Testo Unico, "Disciplinare tecnico in materia di misure minime di sicurezza".
I termini Titolare, Responsabile, Incaricato, Amministratore di Sistema, Trattamento, Dato personale e Dato sensibile sono usati in conformità alle definizioni dettate dalla normativa.

Organizzazione del Servizio Informatico Aziendale

ATTIVITA' TECNICO - AMMINISTRATIVE	
Procedure per l'acquisizione, il collaudo, l'alienazione delle apparecchiature informatiche	• Configurazione delle apparecchiature in relazione alle esigenze • Formulazione capitolati tecnici • Collaudo ed assegnazione • Presa in carico e distribuzione apparecchiature • Alienazione apparecchiature fuori uso • Gestione contratti di assistenza e manutenzione
Assistenza hardware	• Interventi di 1° livello e diagnosi • Affidamento in manutenzione o fuori uso • Interventi di riconfigurazione o upgrade
Assistenza software	• Acquisizione telematica aggiornamenti software dei pacchetti applicativi • Interventi di 1° livello e diagnosi malfunzionamenti software • Attività sistemistiche di installazione ed upgrade sistemi operativi • Attività sistemistiche di installazione e collaudo programmi applicativi, gestionali ed antivirus informatici • Attività di ricognizione, diagnosi, rimozione virus, riconfigurazione del sistema operativo e degli applicativi
Collegamenti telematici con la P.A. (Ministeri, Regione)	• Gestione dei collegamenti telematici con le istituzioni • Coordinamento attività di raccolta e trasmissione dati
Istruzione	• Alfabetizzazione informatica di nuovi utenti • Addestramento addetti sui tools di sistema ed utility

Organizzazione del Servizio Informatico Aziendale

LAN ADMINISTRATION	
Amministrazione della rete	• Gestione della configurazione fisica della rete • Assegnazione e gestione degli indirizzi di rete • Monitoraggio della rete • Diagnosi dei guasti ed interventi di ripristino • Progettazione implementazioni di rete e verifiche di conformità agli standard fissati
Rete di Rilevazione delle presenze	• Gestione del collegamento alla rete di campus
Assistenza	• Interventi di 1° livello ed individuazione componente/apparecchiatura di rete in avaria • Ripristino funzionalità di rete
Sicurezza	• Abilitazione accessi consentiti

Organizzazione del Servizio Informatico Aziendale

DATA BASE ADMINISTRATION	
Gestione archivi magnetici	• Gestione dei dispositivi di storage • Definizione e gestione delle procedure di backup • Ripristino dei dati o ricostruzione archivi danneggiati
Rete di Rilevazione delle presenze	• Parametrizzazione della procedura • Gestione dello scambio dati dei vari ambienti applicativi • Monitoraggio della rete dei terminali lettori di badge
Programmazione	• Acquisizione, trascodifica, mi-

	grazione dati • Reporting e statistiche
Sicurezza	• Definizione e gestione dei profili utente e gestione password
Istruzione	• Formazione utenti sulle procedure di sicurezza
Assistenza	• Ricostruzione archivi danneggiati

Organizzazione del Servizio Informatico Aziendale	
ATTIVITA' OPERATIVE	
Interventi hardware	• Interventi di 1° livello e diagnosi su server e postazioni utenti
Interventi rete	• Interventi di 1° livello e e diagnosi su schede di rete, hub, switch, router
Interventi software di sistema ed applicativo	• Formattazione dischi • Installazione sistemi operativi • Installazione utilità, applicativi • Ripristino/copia dati
Gestione della sicurezza dei dati	• Backup di sistema periodici ed occasionali • Ripristino dati

Definizioni di natura giuridica

- **Accesso abusivo a sistema informatico:** condotta penalmente perseguibile; è punibile chiunque si introduce in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantiene contro la volontà di chi ha titolo per escluderlo;
- **Accesso non autorizzato ad un sito:** accesso abusivo di un soggetto ad un sito appartenente ad un terzo; integra un reato penale;
- **Attentato ad impianti di pubblica utilità:** condotta penalmente perseguibile; è punibile chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità; oggetto dell'azione criminosa possono essere un sistema informatico o telematico di pubblica utilità, dati, informazioni o programmi contenuti o pertinenti a tali sistemi;
- **Banche dati:** è punibile chiunque al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca dati, o distribuisce, vende o concede in locazione una banca dati;
- **Danneggiamento informatico:** condotta penalmente perseguibile; è punibile chiunque distrugge, deteriora o rende totalmente o parzialmente inservibili sistemi informatici o telematici altrui, programmi, informazioni o dati;

- **Dato giudiziario :** 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;
- **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;
- **Dato sensibile :** 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;
- **Detenzione e diffusione abusiva codici di accesso a sistemi informatici o telematici:** condotta penalmente perseguibile; è punibile chiunque al fine di procurare a sé o ad altri un profitto o di arrecare a terzi un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o fornisce istruzioni o indicazioni idonee al suddetto scopo;
- **Diffusione programmi diretti a danneggiare o interrompere un sistema informatico:** condotta penalmente perseguibile; è punibile chiunque diffonde, comunica, consegna un programma informatico da esso o da altri redatto, ed avente lo scopo o l'effetto di danneggiare un sistema informatico o telematico di dati o programmi in esso contenuti o pertinenti, ovvero l'interruzione totale o parziale o l'alterazione del suo funzionamento;
- **Duplicazione abusiva software:** condotta penalmente perseguibile; è punibile chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla SIAE;
- **Falsificazione, alterazione e sottrazione di comunicazioni informatiche:** condotta penalmente perseguibile; è punibile chiunque al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto anche occasionalmente intercettato, di talune delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- **Falso informatico:** condotta penalmente perseguibile; è punibile chiunque compie una falsità su un documento informatico o colloca abusivamente un documento digitale all'interno di un sistema informatico;
- **Frode informatica:** condotta penalmente perseguibile; è punibile chiunque alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno;
- **Installazione abusiva di apparecchiature per le intercettazioni informatiche:** condotta penalmente perseguibile; è punibile chiunque fuori dai casi consentiti dalle legge, installa apparecchiature atte ad intercettare impedire o interrompere comunicazioni relative ad un sistema informatico o telematico, ovvero intercorrente tra più sistemi;
- **Intercettazione di comunicazioni informatiche o telematiche:** condotta penalmente perseguibile; è punibile chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi ovvero le impedisce o

le interrompe; è parimenti punibile chiunque riveli mediante qualsiasi mezzo di informazione al pubblico in tutto o in parte, il contenuto delle suddette comunicazioni;

- **Rivelazione del contenuto di corrispondenza telematica:** condotta penalmente perseguibile; è punibile chiunque che essendo venuto abusivamente a cognizione del contenuto di una corrispondenza a lui non diretta, che doveva rimanere segreta, senza giusta causa lo rivela, in tutto o in parte;
- **Rivelazione del contenuto di documenti informatici segreti:** condotta penalmente perseguibile; è punibile chiunque essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti informatici, pubblici o privati, non costituenti corrispondenza lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto se dal fatto deriva nocumento;
- **Rimozione o elusione dispositivi di protezione software:** condotta penalmente perseguibile; è punibile chiunque per trarne profitto, ponga in essere una condotta tale da consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori;
- **Trattamento :** qualunque operazione o complesso di operazioni, effettuate 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;
- **Violazione, sottrazione e soppressione di corrispondenza informatica:** condotta penalmente perseguibile; è punibile chiunque prende cognizione del contenuto della corrispondenza telematica a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne perdere cognizione, una corrispondenza a lui non diretta, ovvero in tutto o in parte la distrugge o la sopprime;

Definizioni di natura tecnica

- **Client:** In informatica, con client (in italiano detto anche cliente) si indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware o al software. Un computer collegato ad un server tramite una rete informatica (locale o geografica) ed al quale richiede uno o più servizi, utilizzando uno o più protocolli di rete è un esempio di client hardware. Un programma di posta elettronica è un esempio di client software. Sono sempre di più i software, come il web, l'e-mail, i database, che sono divisi in una parte client (residente ed in esecuzione sul pc client) ed una parte server (residente ed in esecuzione sul server). Il termine client indica anche il software usato sul computer client per accedere alle funzionalità offerte dal server.
- **Cookies:** files in formato testo che vengono registrati per tracciare una attività on site dell'utente;
- **Firewall:** è un componente passivo di difesa perimetrale (quindi un dispositivo hardware) che può anche svolgere funzioni di collegamento tra due o più tronconi di rete. Usualmente la rete viene divisa in due sottoreti: una, detta esterna, comprende l'intera Internet mentre l'altra interna, detta LAN (Local Area Network), comprende una sezione

più o meno grande di un insieme di computer locali. In alcuni casi è possibile che si crei l'esigenza di creare una terza sottorete detta DMZ (o zona demilitarizzata) atta a contenere quei sistemi che devono essere isolati dalla rete interna ma devono comunque essere protetti dal firewall.

- **Hardware (HW):** parte fisica di una apparecchiatura informatica. Generalmente è anche riferito a qualsiasi componente fisico di una periferica o di una apparecchiatura elettronica.
- **Log:** lista documentata sugli eventi di una determinata attività;
- **Password:** è una sequenza di caratteri e numeri che viene usata per accedere in modo esclusivo ad una risorsa informatica. Non è necessario che abbia senso compiuto e può essere costituita anche da una frase (nel qual caso si parla anche di passphrase)
- **Rete geografica (WAN):** rete informatica usata per connettere insieme più reti locali (*local area network* o LAN) in modo che un utente di una rete possa comunicare con utenti di un'altra rete. Molte WAN sono costruite per una particolare organizzazione e sono private. La funzionalità delle WAN è generalmente la connessione degli host. Questa struttura forma una *communication subnet* o semplicemente subnet, che in genere appartiene ad una compagnia telefonica o a un ISP.
- **Rete locale (LAN**): Nel campo dell'informatica LAN è l'acronimo per il termine inglese local area network, in italiano rete locale. Identifica una rete costituita da computer collegati tra loro (comprese le interconnessioni e le periferiche condivise) all'interno di un ambito fisico delimitato (ad esempio in una stanza o in un edificio, o anche in più edifici vicini tra di loro) che non superi la distanza di qualche chilometro. Le LAN hanno dimensioni contenute, il che favorisce il tempo di trasmissione, che è noto. Le LAN tradizionali lavorano tra 10 Mbps e 100 Mbps, hanno bassi ritardi e pochissimi errori. Le LAN recenti operano fino a 1 Gbps (ma sono utilizzate solo in ambienti server o storage di grosse dimensioni).
- **Server:** Un server (detto in italiano anche servente o serviente) è una componente informatica che fornisce servizi ad altre componenti (tipicamente chiamate client) attraverso una rete. Si noti che il termine server, così come pure il termine client, possono essere riferiti sia alla componente software che alla componente hardware. Pertanto è comune riferirsi ad un computer di alte prestazioni ed alta affidabilità dedicato primariamente a fornire servizi chiamandolo server. È altrettanto comune usare lo stesso termine per riferirsi ad un processo (ovvero un programma software in esecuzione) che fornisca servizi ad altri processi (es. Server FTP).
- **Single Sign-On:** sistema di identificazione univoco tramite il quale qualsiasi operatore che voglia e possa accedere alle risorse informatiche aziendali si collega alle medesime digitando una **User-id** (cfr. succ.) ed una **Password** (cfr. prec.) che gli consentiranno di utilizzare tutti gli applicativi per i quali risulti abilitato.
- **Software (SW):** indica un programma o un insieme di programmi in grado di funzionare su un elaboratore.
- **Spamming:** invio non richiesto da parte di terzi di e-mail ad utenti della rete; spesso può provocare danni causati dall'eccessivo spazio occupato da queste e-mail che hanno sovente fini pubblicitari;

- **User-id:** Un numero, un nome o una sequenza alfanumerica che identifica univocamente (generalmente in associazione con una password) un utente di un computer, di una rete, o di un sito
- **Virus (informatici) e Antivirus:** è un frammento di software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all' hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento.
- **Workstation:** è un termine generico per indicare un computer da scrivania ad alte prestazioni, utilizzato da professionisti per il lavoro su disegno tecnico (CAD), ricerca scientifica, o produzioni audio/video.

L'utilizzo della strumentazione informatica da parte del dipendente pubblico

Il tema della sicurezza dei Sistemi Informativi è di fondamentale importanza, soprattutto alla luce dell'attuale progresso tecnologico che ha prodotto un rinnovamento organizzativo all'interno della Pubblica Amministrazione. Se pensiamo alla grande quantità e varietà di dati comuni e personali che l'ospedale Cardarelli gestisce attraverso le varie forme di trattamento, comprendiamo l'importanza di disciplinare l'utilizzo della strumentazione informatica; in quanto da un impiego non corretto delle apparecchiature informatiche possono derivare gravi conseguenze sia sul piano tecnico, come la perdita di dati, che sul piano della responsabilità civile, senza dire che possono delinearsi criticità che vanno a ripercuotersi negativamente sull'immagine dell'Azienda

Il processo di semplificazione dei procedimenti amministrativi, avviato già negli anni novanta con le normative sulla trasparenza e sul nuovo ordinamento degli Enti locali, sospinto dallo sviluppo tecnologico e dall'esigenza crescente di ottimizzare e velocizzare i procedimenti che consentono la comunicazione degli atti e l'archiviazione dei documenti, ha prodotto, nelle pubbliche amministrazioni, il crescente fenomeno di digitalizzazione dei procedimenti amministrativi.
Questa prassi, adottata in maniera diffusa e generalizzata ha comportato la realizzazione di un nuovo modello organizzativo ed ha richiesto l'intervento del legislatore, che ha emanato svariate norme, culminanti nel D.Lgs n. 82 del 7-03-05. o "Codice dell'Amministrazione digitale"
A queste norme di primo grado va ad aggiungersi la normativa in materia di privacy che fa il suo esordio con la Legge 675/96 per poi approdare al Testo unico sulla protezione dei dati personali (Dlgs 196/03), che prevede nell'allegato B o Disciplinare tecnico l'obbligo di predisporre misure minime di sicurezza per tutelare la riservatezza nel trattamento dei dati personali . L'adozione delle misure di sicurezza è imposta anche nelle Linee guida per la definizione di un piano di sicurezza pubblicate dall'AIPA nel 1999 (oggi CNIPA, Consiglio Nazionale per l'Informatica nella Pubblica Amministrazione).
L'Azienda Cardarelli si tutela adottando una policy improntata alla trasparenza ed alla legalità e quindi, comunicando con chiarezza al dipendente le modalità di utilizzo degli strumenti informatici assegnati per lo svolgimento delle mansioni attribuite, nonché i rischi derivanti da uno scorretto impiego sia sul piano della sicurezza del sistema informatico che sul piano della responsabilità civile e penale. Si tratta di cautele necessarie, la cui adozione limita i rischi della responsabilità legale che potrebbe implicare, in maniera sanzionatoria, l'Azienda. Si ritiene opportuno, pertanto, responsabilizzare gli incaricati del trattamento dei dati sugli aspetti connessi alla liceità nell'utilizzo del mezzo informatico.

Il Regolamento Informatico Aziendale

Il regolamento informatico è un documento interno redatto in funzione della struttura e delle esigenze aziendali, in cui sono contenute le specifiche relative all'utilizzo della strumentazione informatica utilizzata in Azienda: dalla regolamentazione dell'installazione del software, a quella relativa all'uso della casella di posta elettronica. Il regolamento può pertanto definirsi come quello strumento di prevenzione in grado, innanzitutto, di dimostrare l'attenzione e la volontà di evitare eventi estranei all'attività lavorativa da parte dell'Azienda, e dall'altra come strumento di indicazione per i dipendenti su come utilizzare le risorse informatiche aziendali senza per questo incorrere, anche in buona fede, in illeciti.

L'adozione di precise politiche viene fatta nell'intento di:

- garantire la massima efficienza delle risorse di calcolo per il perseguimento delle attività lavorative;
- garantire la riservatezza delle informazioni e dei dati;
- provvedere ad un servizio continuativo nell'interesse dell'Azienda;
- provvedere ad un'efficiente attività di monitoraggio e controllo;
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche.

E' responsabilita' del Servizio Informatico Aziendale:

- adottare tutti i dispositivi di sicurezza necessari a difendere i propri sistemi informatici;
- implementare meccanismi di controllo e monitoraggio;

E' compito dell'estensore del documento programmatico:

- responsabilizzare e informare gli utenti circa i rischi penali, civili, amministrativi connessi all'uso indebito dei mezzi informatici o alla riproduzione non autorizzata di *software*;
- evitare che i propri utenti, utilizzando gli strumenti di calcolo, si introducano abusivamente in sistemi informatici, o che si verifichino casi di abusiva duplicazione e/o commercializzazione di programmi software.

Misure minime di sicurezza in materia di privacy

Il Codice in materia di protezione dei dati personali nell'allegato B o disciplinare tecnico indica in maniera dettagliata le misure di sicurezza da adottare per garantire la tutela della privacy nelle forme di trattamento e quindi di archiviazione dei dati, che richiedono l'impiego delle apparecchiature informatiche

Vige pertanto, da parte di coloro che sono abilitati ad utilizzare il sistema informatico aziendale in qualità di Responsabili del trattamento dei dati, Amministratori di sistema o di semplici incaricati, l'obbligo di adottare le misure minime di sicurezza

Si definiscono misure minime di sicurezza informatica quel complesso di regole tecniche, organizzative, logistiche e procedurali che configurano il livello minimo di protezione dai rischi richiesto dalla normativa vigente, soprattutto in materia di privacy. In pratica, il Codice sulla privacy identifica tali misure attribuendo ad esse una connotazione applicativa e funzionale in base alle finalità ed alle modalità del trattamento dei dati. Tali misure di sicurezza prendono la denominazione di misure fisiche, logiche ed organizzative

Il primo passo per garantire l'osservanza delle norme di sicurezza applicate ai supporti ed ai dispositivi informatici consiste nel predisporre l'utilizzazione di un **sistema di autenticazione informatica**. L'accesso al trattamento dei dati personali deve essere consentito solo agli incaricati muniti di credenziali di autenticazione, cioè di un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata e conosciuta esclusivamente dall'incaricato stesso, sul quale grava l'obbligo di adozione delle cautele necessarie al fine di assicurare la segretezza della componente riservata della credenziale, nonché l'obbligo di custodire diligentemente i dispositivi in suo possesso. Peraltro, il legislatore stabilisce un minimo di otto caratteri per quanto riguarda la parola chiave (salvo il caso in cui lo strumento elettronico non lo consenta dovendo pertanto adottare una parola chiave composta secondo il numero massimo di caratteri consentiti); altra misura di sicurezza è identificata nell'obbligo di modifica della parola chiave almeno ogni sei mesi, salvo tre nei casi in cui il trattamento con strumenti elettronici abbia ad oggetto dati sensibili o giudiziari.

Altro obbligo da rispettare riguarda le credenziali di autenticazione non utilizzate da almeno sei mesi: le stesse debbono essere disattivate, derogando solo nell'ipotesi di un utilizzo meramente finalizzato alla gestione tecnica, per cui non è richiesta tale scadenza di modifica (ad. es. Amministratore di Sistema).

Gli archivi contenenti dati personali, ancor più quelli contenenti dati sensibili, vanno sottoposti a cura degli utilizzatori a procedure di back-up con frequenza almeno settimanale.

Vige l'obbligo di individuare anche le modalità che possono essere poste a favore del ripristino della disponibilità dei dati qualora si verifichino episodi di distruzione o danneggiamento (è il caso di ricordare che per il trattamento di dati sensibili o giudiziari e' garantito il ripristino entro 7 giorni).

Regole di utilizzo

PREMESSA :

- le seguenti regole devono essere seguite attentamente da tutti gli utenti;
- per quanto non specificato nei presenti documenti è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede;
- resta valida in ogni caso l'assunzione di responsabilità personale per la propria macchina;
- in caso di dubbi, necessità di informazioni, sospetto di tentativi di intrusione ecc., rivolgersi immediatamente all'Amministratore di Sistema.

ACCESSO ALLE RISORSE INFORMATICHE E DI RETE

- l'accesso alle risorse di elaborazione e reti è riservato ai dipendenti della AO A. Cardarelli;
- il personale utilizzatore della risorsa di calcolo deve avere esperienza, capacità e affidabilità che garantiscano il pieno rispetto del presente regolamento;
- in ogni caso il Servizio Informatico Aziendale, o suo delegato, si riserva il diritto ad accedere alla risorsa di calcolo per compiti di monitoraggio, controllo e/o aggiornamenti, ai fini della sicurezza del sistema e della rete, nel rispetto della presente politica di gestione e della riservatezza dei dati personali (ai sensi del D. Lgs. 196/03).

UTILIZZO DELLE RISORSE INFORMATICHE E DI RETE

- **Le risorse informatiche di rete dell'AO A. Cardarelli possono essere utilizzate esclusivamente per le attività istituzionali dell'Ente;**
- sono comunque vietate:
    - attività che esulino dal normale utilizzo destinato all'espletamento delle attività lavorative;
    - tutte le attività che possono rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software brevettato;
    - tutte le attività che compromettono in qualsiasi modo la sicurezza delle risorse di calcolo e reti;
    - le attività illegali.

RESPONSABILITÀ DEGLI UTENTI

- l'accesso alle risorse di calcolo e reti è personale e non può essere condiviso o ceduto;
- gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso;
- gli utenti devono proteggere i propri account mediante password;
- gli utenti sono obbligati a segnalare immediatamente al Servizio Informatico Aziendale ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;

- l'utente/incaricato deve provvedere a sostituire la password iniziale, assegnatagli dall'Amministratore di Sistema, con una di sua scelta nel rispetto delle norme specificate nel presente regolamento.

SOFTWARE E LICENZE D'USO

- il responsabile risponde del software installato sul computer che gli è affidato;
- è vietato distribuire software soggetto a Copyright acquistato dall'Azienda, al di fuori dei termini delle licenze;
- è vietato distribuire software che possa danneggiare le risorse di elaborazione, anche via e-mail;
- è vietato accedere a dati e/o programmi per i quali non vi è autorizzazione o esplicito consenso da parte del proprietario.

Le seguenti attività sono in generale vietate; possono essere svolte a scopo di monitoraggio e per garantire la sicurezza, solo dal Servizio Informatico Aziendale o da personale preventivamente autorizzato, nel rispetto delle norme sulla riservatezza dei dati personali:

- utilizzare strumenti che potenzialmente sono in grado di consentire l'accesso non autorizzato alle risorse di calcolo (ad esempio cracker o software di monitoraggio della rete);
- configurare servizi gia' messi a disposizione in modo centralizzato, quali DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol), mailing, Web Server, accesso remoto (dial-up);
- effettuare operazioni di routing, bridging, tunneling;
- intercettare pacchetti sulla rete, utilizzare sniffer o software analoghi.

Descrizione dei sistemi presenti

I sistemi informatici presenti nelle strutture dell'AO A. Cardarelli possono essere suddivisi in:

- Sistemi periferici
- Sistemi centralizzati

I sistemi periferici sono costituiti da apparecchiature hardware e software di tipo client distribuite sul territorio nelle diverse sedi dell'azienda di cui le più diffuse sono:

Sistemi operativi client:

- ✓ Microsoft Windows 2000 pro;
- ✓ Microsoft Windows XP home e/o professional
- ✓ Microsoft Windows 7
- ✓ Microsoft Windows 8

Per ragioni di sicurezza e protezione, considerato che la societa' Microsoft non supporta piu' ne' aggiorna la protezione dei Sistemi operativi precedenti a Windows 7, dal 1 gennaio 2013 l'unico sistema operativo client autorizzato e supportato dal Servizio Informatico e' Windows 7.

Applicativi di produttività individuale

- ✓ Microsoft office (Word, Access, Excel, Powerpoint);
- ✓ Adobe Acrobat (formato pdf);
- ✓ Software locali per il funzionamento e la gestione di apparecchiature sanitarie (per lo più dispositivi di diagnostica)

Per ciò che riguarda i sistemi Centrali, alle apparecchiature menzionate in precedenza vanno aggiunti i Server su cui sono presenti le procedure informatiche centralizzate e quelle locali ove risultino installati tutti i programmi applicativi in uso sia per l'area Amministrativo/Contabile che per l'area Sanitaria.

CARATTERISTICHE DELLA RETE TRASMISSIONE DATI

La rete di connessione dell'intero sistema informativo dell'AO. A. Cardarelli prevede le seguenti misure di Sicurezza :

Sicurezza passiva – Firewalling

- ✓ Firewall configurati con logiche estremamente conservative per non permettere nulla di non esplicitamente consentito;
- ✓ Politiche di sicurezza tali da escludere qualsiasi possibilità di accesso diretto da internet a macchine interne, se non espressamente previsto da policies interne.

Sicurezza attiva – Cifratura

- ✓ Sistemi antivirus.

CARATTERISTICHE DEI SISTEMI INFORMATICI

Le piattaforme informatiche correntemente utilizzate rispondono a diversi principi architetturali a seconda delle diverse esigenze di servizio e alle diverse caratteristiche dei software utilizzati.
L'accesso alle piattaforme informatiche avviene esclusivamente attraverso la rete locale ed è controllato mediante autorizzazioni specifiche della piattaforma.

Misure di sicurezza adottate/da adottare

PRESCRIZIONI DI SICUREZZA

Vengono, qui di seguito, specificatamente descritte le misure di sicurezza Fisiche, Logiche ed Organizzative, relative alle applicazioni che consentono il trattamento dei dati effettuati con l'impiego delle strumentazioni informatiche.
Le misure sono formulate in modo da rispettare gli obblighi previsti dalla vigente normativa in materia di Protezione dei dati personali.
Sono oggetto quindi delle prescrizioni di sicurezza i seguenti standard:

- misure di sicurezza fisiche riguardanti la sicurezza passiva ed il controllo accessi ai locali dell' AO. A. Cardarelli contenenti apparecchiature e supporti di memorizzazione;

- misure di sicurezza logiche adottate dal personale riguardanti il controllo dell'accesso alle piattaforme, agli archivi ed ai database, alle applicazioni;

- misure di sicurezza logiche adottate dal personale relative alle procedure di archiviazione informatica e finalizzate ad assicurare la riservatezza e l'integrità dei dati;

- misure di sicurezza relative alla rete, alla rete locale ed alla interconnessione con servizi esterni quale Internet;

- misure di sicurezza adottate dal personale relative alla salvaguardia delle informazioni detenute su supporto informatico e/o cartaceo.

MISURE LOGICHE

Le misure di sicurezza logiche riguardano i criteri implementati nei diversi programmi software, di sistema o applicativi, per controllare l'accesso degli utilizzatori alla rete locale (ed eventuali interconnessioni esterne), alle stazioni di lavoro individuali, agli elaboratori ed alle funzionalità applicative.
Le prescrizioni di sicurezza, per quanto attiene i trattamenti manuali e gli archivi cartacei derivanti da archiviazioni informatiche sono indicate nella sezione relativa alle misure organizzative.

CONTROLLO ACCESSI AI DATI: AUTENTICAZIONE – AUTORIZZAZIONE - ABILITAZIONE

L'accesso a tutte le risorse informatiche avviene attraverso un'unica User- Id (Single Sign On) e tramite il relativo profilo di autorizzazione collegato che definisce per ogni soggetto tutte le abilitazioni relative a:

- le applicazioni presenti sugli elaboratori per cui viene data abilitazione di accesso e le relative funzionalità applicative abilitate;
- la possibilità di interconnessioni con reti esterne e/o piattaforme;
- accesso limitato ai trattamenti autorizzati che prevedono l'utilizzo di dati sensibili.

La funzione di controllo delle abilitazioni nonché della correttezza delle modalità con cui vengono effettuati i trattamenti è eseguita dal Responsabile a cui afferisce il trattamento informatico stesso.
L'accesso diretto agli elaboratori, nonché il compito di vigilare sul corretto uso della strumentazione informatica è consentito esclusivamente all'incaricato Amministratore di Sistema nonché al Responsabile del Servizio Informatico Aziendale.

Ogni utilizzatore del sistema è identificato mediante un unico codice identificativo personale (pubblico) e relativa password (privata); solo in casi eccezionali ed a seguito di insuperabili vincoli tecnici, ad uno stesso soggetto potranno essere assegnate più di un codice identificativo di accesso.

Archivi sulle stazioni di lavoro individuale
Non è consentito sulle singole stazioni di lavoro condividere in rete archivi mediante funzionalità *server*.

IDENTIFICAZIONE DEGLI UTENTI (AUTENTICAZIONE)

Codice identificativo (User-id)
A tutti coloro cui è attribuito un incarico per il trattamento dei dati verra' rilasciato un codice identificativo personale unico per l'utilizzo delle risorse informatiche (Single Sign On). Detto codice verra' abbinato ad un profilo utente in cui saranno memorizzate tutte le abilitazioni relative all'utente; queste abilitazioni consentiranno all'utente di accedere unicamente agli applicativi per i quali sara' autorizzato. Lo stesso codice non può, neppure in tempi diversi essere assegnato a persone diverse ed una volta disattivato il codice non potra' piu' essere utilizzato ne' riutilizzato

dallo stesso utente in caso di revoca dell'incarico e/o delle autorizzazioni, è responsabilità dell'Incaricato comunicare immediatamente il codice identificativo che deve essere disattivato.
L'Assegnazione della user-id e relativa password va effettuata da persona a cui sia stato affidato l'incarico di Amministratore Sistema per il rilascio delle password.

PROTEZIONE ANTIVIRUS

Tutte le risorse informatiche per le quali è applicabile l'antivirus sono protette contro il rischio di intrusione ad opera di programmi ai sensi dell'art 615- quinquies del Codice Penale *(Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico - Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l' interruzione, totale o parziale, o l' alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni*).
La protezione avviene mediante l'utilizzo di adeguati programmi antivirus il cui aggiornamento e' cadenzato da parte del produttore del software sulla base dei rilevamento avvenuti a livello internazionale e per i quali sono state predisposte le relative misure protezionistiche.

PROTEZIONE DELLE RETE

Tutte le risorse utilizzate per la interconnessione della rete locale con le reti e/o sottoreti esterne sono protette con adeguate apparecchiature:

- Firewall (apparato che opportunamente configurato o settato filtra in maniera centralizzata tutti i pacchetti sia in entrata che in uscita controllando la loro rispondenza alle regole impostate);
- Proxy (apparato che opportunamente configurato sovrintende alla navigazione web diventando l'unico punto di accesso alla rete esterna(internet) surrogando in questo modo anche l'attivita' di firewalling; tramite il proxy viene regolato l'accesso ai siti sulla base delle regole applicate e vengono effettuati il monitoraggio e le statistiche sull'utilizzo di internet.
- DNS (Domain Name System) e' il sistema che consente l'utilizzo di Internet effettuando la conversione dal nome in chiaro normalmente digitato dagli utenti nella riga del Browser web nel relativo indirizzo IP. Una implementazione del sistema DNS consente di effettuare la protezione da abusi, il filtraggio ed il reindirizzamento delle richieste provenienti dai client.

Misure Organizzative

AMMINISTRATORI DI SISTEMA

Si definisce Amministratore di sistema il soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un computer (L. 318/99, art. 1, comma 1.c). L'Amministratore di sistema è un incaricato con autorizzazioni speciali; egli esercita le sue funzioni eseguendo le operazioni necessarie per la corretta elaborazione dei trattamenti informatizzati, di archiviazione e movimentazione degli archivi informatizzati, di monitoraggio della rete telematica, oppure eseguendo le attività necessarie ad assicurare il corretto funzionamento delle risorse informatiche nonché l'ordinaria gestione e manutenzione dei programmi richiesti per l'esecuzione dei trattamenti informatizzati.

L'Incaricato Amministratore di sistema sovrintende, nei limiti dell'incarico assegnato, alle risorse del sistema operativo di un elaboratore o di un sistema di base dati, al fine di porre in essere le operazioni che comportano il trattamento e l'archiviazione dei dati

COMPITI

- Rilascio del codice identificativo (user-id) e della "password iniziale" per l'utilizzazione dell'elaboratore da parte degli utenti/incaricati di trattamenti, su richiesta del Responsabile. Disattivazione di tali credenziali di autenticazione dopo 6 mesi di inutilizzo;
- gli amministratori di sistema sono obbligati ad operare nel rispetto delle politiche dell'Azienda in materia di sicurezza, garantendo la massima riservatezza nel trattamento dei dati personali; il loro operato deve essere monitorato nel rispetto della normativa vigente anche tramite l'utilizzo di log.
- Al Servizio Informatico Aziendale per mezzo degli amministratori di sistema e' riservato il diritto di revocare l'accesso alle risorse di calcolo e di rete senza preavviso, qualora essi siano utilizzati impropriamente o in violazione delle leggi vigenti;
- eventuali utilizzi abusivi delle risorse di calcolo devono essere immediatamente segnalati all'Amministratore di Sistema;
- il personale del Servizio e/o i referenti locali (amministratori di sistema) devono essere in grado, in caso di emergenza, di poter accedere in qualsiasi momento ai locali e alle risorse di calcolo a loro affidati.

Ulteriori compiti specifici dell'Amministratore di Sistema sono:

- ✓ Creare e all' occorrenza modificare il profilo di accesso ed autorizzazione di ciascun utente, sulla macchina a questi assegnata per l'uso delle sue mansioni, secondo le specifiche dettate dall'incarico dell'utilizzatore. Ricadono in questo compito la creazione di un Account con autorizzazioni limitate nel sistema operativo che permetta l'accesso alle sole risorse informatiche per le quali all' utente e' concesso l'utilizzo.
- ✓ Assegnare la prima password di accesso al sistema operativo ed assicurarsi che questa venga sostituita dall'utente al primo accesso.
- ✓ Effettuare gli aggiornamenti relativi ai software di sicurezza , per gli utenti non collegati alla rete, almeno ogni sei mesi.

Individuazione dell' Amministratore di sistema

Data l'operatività intrinseca alla funzione di Amministratore di sistema si propone di creare, a seconda delle esigenze di servizio, uno o più amministratori per ciascuna struttura aziendale.
La persona adatta a svolgere tale ruolo verrà individuata a cura dei responsabili di verifica e di controllo della struttura. Le funzioni rivestite dai responsabili di verifica e controllo della struttura non coincidono con le funzioni assunte dai responsabili del trattamento dei dati.
In caso di omessa individuazione di uno o più amministratori di sistema è abilitato il Coordinamento privacy aziendale, individuato nel regolamento aziendale sulla tutela della privacy, a proporre l'incarico di Amministratore di sistema al Responsabile del Servizio Informatico Aziendale

Nomina dell' Amministratore di sistema
La procedura di nomina di Amministratore di sistema viene formalizzata dal Responsabile del Servizio Informatico Aziendale che ha le competenze per valutare i requisiti funzionali e tecnici richiesti alle persone individuate per assolvere la funzione di Amministratore di Sistema.

Criteri e Procedure di rilascio di user-id e password
E' compito dell'Amministratore di Sistema, definire gli identificativi e le password iniziali, gestire i profili di abilitazione con le relative assegnazioni.
Il Responsabile che ha richiesto le autorizzazioni ha l'obbligo di provvedere prontamente alla richiesta di ritiro o modifica delle autorizzazioni assegnate qualora, a seguito di modifiche organizzative o procedurali, le mansioni effettivamente svolte dall'incaricato non siano più coerenti con i trattamenti autorizzati. L'amministratore di sistema renderà operative queste modifiche.

Criteri e Procedure per assicurare l'integrità dei dati
I dati contenuti negli archivi informatici sono protetti contro il rischio di perdita, anche accidentale, attraverso apposite procedure che consentono il veloce ripristino delle informazioni perdute o danneggiate.
In linea di massima, le suddette procedure prevedono l'esecuzione almeno ogni sei mesi di una prova di ripristino.

Aspetti della sicurezza riguardo il trattamento dei dati e la detenzione degli archivi.
Norme comportamentali degli utenti (Responsabili ed incaricati)

SICUREZZA FISICA

Gli Incaricati evitano comportamenti che possano pregiudicare la riservatezza dei dati. Per esigenze specifiche chiedono indicazioni e direttive al Responsabile del trattamento dei dati

Uso e conservazione dei supporti Magnetici

Tutti i supporti rimovibili (dischetti, cd-rom, ecc..) utilizzati dagli addetti presso le stazioni di lavoro devono sempre riportare un etichetta che ne indichi il contenuto (ad esempio backup del gg/mm/aaaa) e l' ufficio di provenienza del supporto.

Le copie di backup di dati contenenti dati personali e sensibili vanno conservate in luogo sicuro non accessibile al pubblico ed a personale non incaricato del trattamento dei dati.

L'utilizzo di supporti rimovibili anonimi non è consentito.

SICUREZZA LOGICA

La sicurezza logica si realizza principalmente assicurando che tutti gli accessi ai diversi componenti del sistema informativo avvengano esclusivamente secondo modalità prestabilite. Per tale motivo, ogni qual volta si rende necessario l'utilizzo di una risorsa deve essere previsto un meccanismo che consenta all'utente di autenticarsi, ossia a dimostrare la propria identità, tipicamente mediante l'utilizzo di un *codice identificativo personale* (USERID) ed una *parola chiave* (PASSWORD).

Nell'ambito delle presenti misure minime, sono individuati i seguenti livelli di protezione:

- Password di accensione del PC (password di BIOS)
- Userid e password per l'accesso al S.O.;
- Userid, password e profili di abilitazione per le applicazioni informatiche centralizzate.
- Password di salvaschermo (screensaver)
- Password di accesso agli applicativi del Sistema informatico tramite Single Sign On.

Istruzioni sull'utilizzo delle password e dei codici identificativi personali

Password di accensione del PC (password di BIOS)

Tutti gli utenti che utilizzano un Pc, anche non collegato in rete, possono identificarsi con una password, al momento dell' accensione del Pc, utilizzando una funzionalità del BIOS del PC;
L'utilizzo della password di BIOS deve comunque essere concordato ed autorizzato dall' amministratore di sistema che ne detterà le regole specifiche.

Codice identificativo personale (userid) e password per l'accesso al S.O.

Oltre all'identificazione appena descritta, tutti gli utenti che utilizzano PC collegati alla rete dell' AO. A. Cardarelli, per poter accedere alle risorse presenti nella propria rete (stampanti e cartelle), dovranno identificarsi con userid e password al momento del collegamento. Questa verifica dell' identità dell'utente si aggiunge all'identificazione descritta in precedenza, nel senso che e' operativa a prescindere dal fatto che l'utente sia o meno utilizzatore di una o più delle applicazioni informatiche prima elencate.

REGOLE VALIDE PER LA PASSWORD DEL S.O.

La password del S.O. può essere modificata dall'utente	SI
Durata della password del S.O.	Da un minimo di 3 mesi ad un massimo di 6 mesi
Lunghezza minima della Password	8 caratteri alfanumerici

Linee guida per il corretto utilizzo delle password

Vi sono diverse categorie di password, ognuna con il proprio ruolo preciso:

I. **la password di accensione del pc** (password di BIOS) impedisce l'utilizzo improprio della propria postazione di lavoro, quando per un motivo qualsiasi non ci si trova in ufficio. La password di accensione ha una lunghezza non inferiore a **8 caratteri** e deve essere aggiornata almeno ogni **3 mesi/6 mesi.**
II. **la password di accesso al S.O.** impedisce che l'eventuale accesso non autorizzato ad un pc renda disponibili le risorse dell'ufficio (cartelle condivise e stampanti). La password di S.O. ha una lunghezza non inferiore a **8 caratteri** e deve essere aggiornata da due a preferiobilmente 4 volte l'anno (ogni 3/6 mesi);
III. **la Password delle applicazioni informatiche centralizzate (Software client)** permette di restringere l'accesso alle funzioni e ai dati al solo personale autorizzato.
IV. **La password del salvaschermo** impedisce che un'assenza momentanea permetta ad una persona non autorizzata di visualizzare il lavoro in corso e/o accedere ai documenti residenti sulla postazione di lavoro.

Ad ogni codice identificativo (user-id) è associata una parola chiave (password) rilasciata inizialmente in accordo con le regole definite dal Servizio Informatico Aziendale. Al primo utilizzo, l'Incaricato ha l'obbligo di modificarla tenendo presenti le seguenti regole minime:

- deve essere di tipo alfanumerico, di non meno di 8 caratteri;
- non deve essere composta utilizzando lo user-id;
- non deve essere ottenuta anagrammando la precedente;
- deve essere sostituita almeno ogni sei mesi. Ogni tre mesi se il trattamento riguarda dati sensibili.

La scelta della password da parte dell'utente deve essere oculata in quanto il modo più semplice e più utilizzato per realizzare un accesso illecito ad un sistema e/o ad un' applicazione, consiste

nell'ottenere le credenziali identificative di un utente autorizzato, ossia la sua coppia userid e password.
Considerato che per molte applicazioni informatiche centralizzate, lo userid coincide o contiene la matricola del dipendente ed è quindi un dato noto, l'intera sicurezza si basa sulla conoscenza della password. La scelta, quindi, di password "forti" rappresenta un aspetto essenziale della sicurezza informatica.
É pertanto necessario che le password non contengano riferimenti conducibili all' utente.
Nella Gestione delle password è necessario attenersi alle indicazioni di seguito riportate:

Cosa NON fare .

1) NON comunicare a nessuno le proprie password, qualunque sia il mezzo che viene utilizzato per inoltrare la richiesta (telefono, messaggio di posta elettronica, ecc.).
2) Ricordare che nessuno è autorizzato a richiedere le password, nemmeno il personale tecnico di supporto, e che lo scopo principale per cui sono utilizzate le password è di assicurare che nessun altro possa utilizzare le risorse a cui si è abilitati;
3) NON scrivere le password su supporti che possano essere trovati facilmente e/o soprattutto in prossimità della postazione di lavoro utilizzata;
4) NON scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana che di lingue straniere. Esistono programmi che permettono di provare come password tutte quelle contenute in dizionari elettronici estremamente ampi, in termini di numero di lemmi, e in diverse lingue, scritte sia in senso normale che in senso inverso;
5) NON usare come password il nome utente o parole che possano essere facilmente riconducibili all'identità dell'utente, come, ad esempio, il codice fiscale, il nome del coniuge, il nome dei figli, la data di nascita, il numero di telefono, la targa della propria auto, il nome della strada in cui si abita, il nome della squadra di calcio per cui si tifa, ecc.;
6) NON usare come password parole ottenute da una combinazione di tasti vicini sulla tastiera o sequenze di caratteri (esempio: qwerty, asdfgh, 123321, aaabbb, ecc.);
7) NON usare la stessa password per le diverse tipologie di password prima individuate;
8) NON rendere note password vecchie e non più in uso, in quanto da questi dati è possibile ricavare informazioni su ciclicità e/o regole empiriche e personali che l'utente utilizza per generare le proprie password.

Cosa fare .

1) Cambiare le password frequentemente ricordando che il limite massimo di validità di una password stabilito dalle presenti misure minime è di 6 mesi;
2) Utilizzare password lunghe almeno *otto* caratteri con un misto di lettere, numeri e segni di interpunzione;
3) Nella digitazione delle password assicurarsi che non ci sia nessuno che osservi ciò che si digita sulla tastiera del PC;
4) Utilizzare password distinte per le diverse tipologie di password prima descritte.

Come scegliere le password .

Le password migliori sono quelle facili da ricordare ma, allo stesso tempo, difficili da individuare. Questo genere di password può essere ottenuto, ad esempio, comprimendo frasi lunghe in pochi caratteri presenti nella frase, utilizzando anche segni di interpunzione e caratteri maiuscoli e

minuscoli. La frase "Nel 1969 l'uomo è andato sulla luna" può, ad esempio, fornire tra le tante possibilità la seguente "N69UèAsL".
Accanto a questa tecnica, per ottenere password ancora più "forti", si possono sostituire le lettere risultanti dalla compressione della frase, con cifre o caratteri che assomiglino alle lettere; ad esempio la frase "Questo può essere un modo per ricordare la password" diventa "Qp&lmpRP".
Un altro modo per ottenere password "forti" consiste nel combinare date o numeri che si ricordano facilmente con pezzi di parole che sono in qualche modo abituali e quindi semplici da ricordare; ad esempio la combinazione "felice1983", che utilizzata direttamente potrebbe essere una password "debole" (combinazione del nome del figlio e della data di nascita), può diventare una password migliore in questo modo "FeLi83ce", o una password "forte" così "F&Li83cE".
N.B. Non utilizzare come password gli esempi riportati nel presente manuale.

Tutti gli utenti si atterranno alle seguenti disposizioni:

- l'utente è responsabile della corretta tenuta della password di accensione del PC che gli è stato assegnato e delle password di accesso alla rete e alle applicazioni;
- L'utente a cui è stata assegnata una userid per l'accesso alla rete e/o per l'utilizzo di applicazioni informatiche centralizzate, è responsabile di tutto quanto accade a seguito di transazioni ed elaborazioni abilitate dal proprio codice identificativo personale. Per le applicazioni informatiche centralizzate, tale responsabilità si riferisce ai privilegi associati al suo profilo di abilitazione;
- L' utente cambia le proprie password secondo le disposizioni riportate nelle misure minime e nel presente manuale;
- L'Amministratore di Sistema gestisce le password secondo le disposizioni riportate nel presente manuale;
- L'utente attiverà tutte le misure in suo potere per evitare che terzi abbiano accesso al suo PC mentre si allontana durante una sessione di lavoro. A tal fine uscirà sempre dall' applicazione in uso (logoff) ed eventualmente blocca il Pc con la password di un salvaschermo;

SICUREZZA DEL SOFTWARE E DELL'HARDWARE .

Se nell'utilizzo del PC e/o dell'applicazione informatica a cui si è abilitati, viene rilevato un problema che può compromettere la sicurezza dei dati, l'utente ne dà immediata comunicazione all'Amministratore di sistema, in mancanza al suo diretto Responsabile dei trattamenti.
Il Servizio Informatico Aziendale, a cui andra' poi effettuata la segnalazione della problematica riscontrata provvedera' ad analizzare e risolvere la problematica adottando tutte le misure tecniche necessarie.
All'utente è vietato installare programmi non attinenti le normali attività d'ufficio, né nuovi programmi necessari, senza il preventivo parere tecnico dell' Amministratore di sistema. Gli utenti non possono modificare le configurazioni hardware e software delle apparecchiature senza il preventivo parere tecnico dell'Amministratore.
Tutti gli utenti evitano qualsiasi tipo di azione teso a superare le protezioni applicate ai sistemi e alle applicazioni. Gli interventi di installazione, configurazione, riparazione ed avviamento dei sistemi sono effettuabili esclusivamente dal personale tecnico del Servizio Informatico Aziendale o della ditta a cui sia affidata la manutenzione delle apparecchiature informatiche.
In quest'ultimo caso, il Responsabile del trattamento è tenuto a verificare che al termine dell'intervento il PC sia riportato nella situazione originaria per quanto riguarda le *misure* minime

(password di accensione, presenza del programma antivirus). E' espressamente vietata qualsiasi azione volta a superare il blocco con password all'accensione del Pc.

Inoltre:

- è *vietato* l'accesso ai locali e/o ai *box* riservati alle apparecchiature informatiche e di rete, o apportare qualsiasi modifica agli stessi senza l'autorizzazione del Servizio Informatico Aziendale;
- è *vietato* cablare o collegare apparecchiature alle prese di rete senza l'autorizzazione del Servizio Informatico Aziendale;
- è *vietato* utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente dal Servizio Informatico Aziendale;
- è *vietato* installare modem configurati per l' accesso remoto dall' esterno;
- è *vietato* intraprendere azioni allo scopo di:
    - degradare le risorse del sistema,
    - impedire ad utenti autorizzati l'accesso alle risorse,
    - ottenere risorse superiori a quelle già allocate ed autorizzate,
    - accedere a risorse di calcolo, sia dell'Azienda che di terze parti, violandone le misure di sicurezza;
- è *vietato* effettuare copie di file di configurazione del sistema.

PROTEZIONE DA VIRUS INFORMATICI .

I virus informatici rappresentano una delle minacce principali per la sicurezza dei sistemi informativi e dei dati in essi presenti. Un virus informatico può danneggiare un PC, può modificare e/o cancellare i dati in esso contenuti, può compromettere la sicurezza e la riservatezza di un intero sistema informativo, può rendere indisponibile parti di esso, ivi compresa la rete di trasmissione dati.
I seguenti comportamenti inducono un aumento del livello di rischio di contaminazione da virus informatici:

- installazione di software gratuito (freeware o shareware) prelevato da siti internet o allegato a riviste e/o libri;
- scambio di file eseguibili allegati a messaggi di posta elettronica;
- ricezione ed esecuzione di file eseguibili allegati a messaggi di posta elettronica;
- collegamenti ad internet con esecuzione di file eseguibili, applets Java, ActiveX;
- utilizzo della condivisione, senza password, di cartelle fra computer in rete;
- utilizzo di floppy disk già utilizzati e la cui provenienza sia dubbia.

Al fine di evitare i problemi correlati alla diffusione di virus informatici, gli utenti devono rispettare, come misure minime, le seguenti norme:

1) accertarsi che sul proprio computer sia sempre operativo il programma antivirus previsto dal Servizio Informatico Aziendale;
2) accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati. Nel caso che il mittente del messaggio di posta elettronica dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati;

3) sottoporre a controllo, con il programma antivirus installato sul proprio PC, tutti i supporti di provenienza esterna prima di eseguire una qualsiasi operazione di trasferimento dei files in esso contenuti;
4) non condividere con altri computer il proprio disco rigido o una cartella di files senza password di protezione in lettura/ scrittura;
5) proteggere in scrittura i propri floppy disk contenenti programmi eseguibili e/o files di dati;
6) limitare la trasmissione fra computer in rete di files eseguibili e di sistema;
7) non intraprendere azioni di modifica sui sistemi utilizzati a seguito di diffusione di messaggi e segnalazioni di virus informatici da qualsiasi fonte provengano. Le uniche azioni eventualmente necessarie sono comunicate esclusivamente dall' Amministratore di sistema o dal Servizio Informatico Aziendale.
8) non scaricare dalla rete internet programmi o files non inerenti l'attività dell'ufficio o comunque sospetti.

Dal punto di vista operativo, occorre considerare che:

A. Il programma antivirus, per i PC collegati in rete, viene aggiornato automaticamente. Per i PC non collegati in rete l'aggiornamento del programma antivirus verrà effettuato da parte del personale tecnico (Amministratore di sistema locale);
B. Al momento dell'individuazione di un virus informatico sul PC da parte del programma antivirus, l'utente segue le istruzioni riportate sullo schermo dal programma ed avverte contestualmente il Responsabile del trattamento dei dati dell'evento. Quest'ultimo, dopo aver verificato che siano state rispettate le misure minime di protezione da virus informatici, provvede a segnalare al Servizio Informatico Aziendale l'evento per eventuali e successivi interventi tecnici;
C. la distribuzione di documenti in formato elettronico avverrà tramite formati standard, compatibili e possibilmente compressi (p.e. PDF).

UTILIZZO DELLA RETE INTERNET .

Il sistema informatico dell'Azienda ed i dati in esso contenuti possono subire gravi danneggiamenti per effetto di un utilizzo improprio della connessione alla rete internet; inoltre, attraverso tale rete possono penetrare nel sistema virus informatici ed utenti non autorizzati. Allo scopo di evitare questi pericoli, gli utenti ottemperano alle seguenti regole:

1. utilizzano la connessione ad internet esclusivamente per lo svolgimento dei compiti istituzionali dell' ufficio;
2. non diffondono messaggi di posta elettronica di provenienza dubbia, non partecipano a sequenze di invii di messaggi e non inoltrano o diffondono messaggi che annunciano nuovi virus;
3. le caselle di posta elettronica rilasciate dall'Amministrazione non vengono utilizzate dagli utenti per fini privati o personali. Gli utenti sono responsabili dell'uso della casella di posta elettronica istituzionale loro assegnata;
4. gli utenti limitano allo stretto indispensabile l'invio di messaggi di posta elettronica con allegati,scegliendo, ove necessario, il formato degli allegati che occupa meno spazio;

5. è vietato l'utilizzo di servizi di comunicazione e condivisione files che esulino dalle ordinarie funzioni di browsing internet (http), posta elettronica e trasferimento files;
6. gli utenti devono essere a conoscenza dei seguenti 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.