REGOLAMENTO PER L'UTILIZZO DEI SERVIZI ICT AZIENDALI

REGOLAMENTO PER L'ACCESSO E L'USO DELLA RETE INFORMATICA E TELEMATICA DELL'INRCA

INDICE

Art.1 Introduzione e ambito di applicazione
Art.2 Soggetti che possono avere accesso alla Rete
Art.3 Modalità di accesso alla Rete e agli applicativi
Art.4 Regole che riguardano le password di accesso alla Rete Informatica
Art.5 Attività non consentite nell'uso della Rete
Art.6 Posta Elettronica
Art.7 Internet
Art.8 Amministrazione delle Risorse Informatiche
Art.9 Regole per la gestione di strumenti Elettronico/Informatico (tutti gli Utenti della Rete)
Art.10 Regole di comportamento per minimizzare i rischi da virus
Art.11 L'affidamento di dati personali all'esterno
Art.12 Incident Response e Ripristino
Art.13 Violazioni al presente Regolamento
Art.14 Sanzioni
Art.15. Modifiche del Regolamento

ART.1. INTRODUZIONE E AMBITO DI APPLICAZIONE

Il presente regolamento, da ora detto anche documento, disciplina le modalità di accesso e di uso della Rete Informatica e telematica e dei servizi che, tramite la Rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'Ente.

Per Rete dell'INRCA si intende l'insieme delle Risorse informatiche, cioè delle Risorse Infrastrutturali e del Patrimonio informativo digitale.

Le Risorse infrastrutturali sono costituite dalle componenti hardware/software e dagli apparati elettronici collegati alla Rete Telematica. "Patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Il presente regolamento si applica a tutti gli utenti Interni ed Esterni che sono autorizzati ad accedere alla Rete, dove per utenti Interni si intendono tutti gli Amministratori, i Dirigenti, i dipendenti a tempo indeterminato e a tempo determinato e i collaboratori interni occasionali, mentre per utenti Esterni si intendono: le ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse, collaboratori esterni.

Ai fini del Regolamento si considerano le definizioni:

- **Servizi:** l'insieme di funzionalità che il sistema informativo ICT aziendale mette a disposizione degli utenti;
- **Utenti:** tutti coloro che sono autorizzati all'uso dei Servizi (dipendenti, collaboratori, personale esterno, etc…),
- **Risorse Tecnologiche**: tutti i server, le workstation, i personal computer, le periferiche (come ad esempio le stampanti, i sistemi di archiviazione, etc.) gestite sotto la responsabilità dell'Ente, unitamente ad ogni dispositivo di rete sia attivo che passivo a cui tali sistemi possono essere interconnessi, compresi i sistemi per l'accesso ad Internet. A quanto sopra indicato si aggiungano software, applicazioni, librerie di supporto, documenti o servizi informatici connessi con i sistemi o le reti sopra indicate, così come la posta elettronica ed ogni altro servizio Internet;
- **Spazio Disco Utente**: porzione delle Risorse Tecnologiche riservata agli Utenti di specifici Servizi per l'archiviazione di materiale in formato elettronico (file);
- **Account Utente**: le credenziali composte dalla coppia "Username" e "Password" tramite le quali un Utente è identificato univocamente dai sistemi e per mezzo delle quali ha l'autorizzazione ad accedere ai Servizi erogati dalle Risorse Tecnologiche;
- **Indirizzo e-mail**: l'indirizzo di posta elettronica eventualmente associato all'Account Utente,
- **Amministratori di Sistema**: l'insieme del personale incaricato di provvedere alla gestione e al regolare funzionamento delle Risorse Tecnologiche.

Sicurezza

La sicurezza deve essere considerata da tutti gli utenti una componente essenziale nell'attività quotidiana, finalizzata alla protezione dei dati, delle informazioni e delle apparecchiature, da manomissioni, uso improprio o distruzione. La sicurezza delle informazioni dipende principalmente dai seguenti aspetti:

- il controllo degli accessi alle informazioni,
- il mantenimento della loro integrità e riservatezza,
- la sicurezza nella trasmissione e nella comunicazione sia all'interno dell'Ente che all'esterno (ad es. Internet),
- la sicurezza delle postazioni di lavoro e dei personal computer,
- la tempestiva rivelazione e segnalazione di eventuali problemi di sicurezza.

Tutti gli utenti devono concorrere alla realizzazione della sicurezza, pertanto devono proteggere le informazioni loro assegnate per lo svolgimento delle proprie attività lavorative in termini di:

- utilizzo delle risorse informatiche,
- accesso ai sistemi e ai dati,
- uso delle password.

Principi generali

- L'INRCA promuove l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire le proprie finalità istituzionali.
- L'utilizzazione dei Servizi da parte dell'Utente, è condizionato all'accettazione integrale del presente Regolamento.
- I Servizi sono erogati nel rispetto delle finalità dell'INRCA.
- Ogni utente è responsabile civilmente e penalmente del corretto uso delle Risorse informatiche e dei Servizi/programmi ai quali ha accesso, compresi i propri dati, quindi, consapevole delle potenzialità offerte dagli strumenti informatici e telematici, si impegna ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
- Gli Utenti sono i soli responsabili dell'accuratezza dei dati ottenuti tramite l'utilizzo dei Servizi. L'Ente, dunque, non è responsabile dei risultati derivanti dall'utilizzazione dei Servizi, né tanto meno del loro successivo impiego.
- L'Ente non è responsabile dell'integrità delle Risorse Tecnologiche e dello Spazio Disco Utente;
- Il posto di lavoro costituito da personal computer, viene consegnato completo di quanto necessario per svolgere le proprie funzioni, software applicativo compreso, è pertanto vietato modificarne la configurazione.
- L'uso delle risorse tecnologiche è limitato ai fini lavorativi ed istituzionali dell'Ente.
- L'uso dei Servizi deve essere effettuato in conformità alle norme vigenti e senza provocare alcun danno morale o materiale all'Ente od a terzi;
- Un uso dei Servizi in maniera non conforme al Regolamento può comportare la sospensione all'Utente dell'erogazione dei medesimi ed un'eventuale azione legale al fine di tutelare gli interessi dell'Ente.
- L'accesso alla rete ed ai servizi/programmi è assicurato compatibilmente con le potenzialità delle attrezzature. Gli accessi di determinate categorie di utenti, potranno essere regolamentate quando questo è richiesto da ragioni tecniche.

ART.2 SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete dell'ISTITUTO tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Per consentire l'obiettivo di garantire la sicurezza e il miglior funzionamento delle risorse disponibili, l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

In generale l'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

Accesso alla rete dall'esterno. Questa modalità di accesso è riferibile essenzialmente alle ditte che svolgono attività di manutenzione sui propri sistemi (hardware e software applicativi) inseriti nella rete dell'INRCA. Questo problema va affrontato rivolgendosi agli Amministratori di Sistema i quali stabiliranno le modalità per l'accesso di soggetti esterni.

Integrazione con altre reti. Chiunque abbia la necessità di integrare le proprie risorse informatiche inserite nella rete dell'INRCA con altre reti, deve rivolgersi agli Amministratori di Sistema che dovranno farsi carico del

problema e portarlo a soluzione salvaguardando comunque prioritariamente la sicurezza complessiva della nostra rete.

ART.3 MODALITÀ DI ACCESSO ALLA RETE E AGLI APPLICATIVI

Principi generali

- Qualsiasi accesso alla rete e agli applicativi deve essere associato alle credenziali di una persona fisica, cui saranno collegate tutte le attività svolte.
- L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
- L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte sulla rete tramite le proprie credenziali (Username – Password).
- Al primo collegamento alla rete e agli applicativi, l'utente (Interno od Esterno) deve modificare la password (parola chiave) comunicatagli dal custode delle password, che gliela concederà se sarà rispettato quanto di seguito descritto.

Utenti Interni

Per essere autorizzati all'uso delle risorse informatiche e dei relativi servizi, è necessario che gli utenti Interni presentino richiesta scritta e firmata dal responsabile dell'U.O. da cui dipendono. Per facilitare la pratica è stato predisposto e reso disponibile sul Portale Intranet dell'INRCA, il modello "**Modulo Attivazione/Disattivazione Utenti rete Inrca**". Tale modello deve essere compilato in ogni sua parte e quindi fatto pervenire agli Amministratori della rete. Con le stesse modalità, cioè scaricando dal Portale Intranet dell'INRCA il modulo "**Modulo per Richiesta Mail",** l'utente può richiedere, per motivi di servizio, all'Amministratore della rete la creazione di una casella di posta elettronica e dei relativi servizi/programmi.

Nel caso fosse evidenziata dal Dirigente la necessità per l'utente di accedere ai dati di competenza di un altro servizio, la richiesta di accesso dovrà essere approvata e sottoscritta anche dal Dirigente del servizio responsabile del trattamento dei dati.

Gli Amministratori di Sistema provvedono ad assegnare ad ogni utente un Account di rete secondo le modalità più avanti descritte.

Utenti Esterni

Per essere autorizzati all'uso delle risorse informatiche e dei relativi servizi, è necessario che gli utenti Esterni inoltrino formale richiesta al responsabile dell'Unità Operativa interessata che a sua volta la inoltrerà agli Amministratori di Sistema. L'Amministratore di Sistema, provvederà ad inviare al Legale Rappresentante dell'Azienda una lettera di incarico, in cui sarà specificatamente richiesto di elencare i nominativi di tutti coloro cui dovrà essere concesso l'accesso ai trattamenti di loro competenza.

La lettera di incarico, firmata dal Legale Rappresentante dell'Azienda, dovrà ritornare all'Amministratore di Sistema, affinché quest'ultimo possa rilasciare le credenziali di accesso alla rete ai soggetti elencati nella lettera di incarico.

ART.4 REGOLE CHE RIGUARDANO LE PASSWORD DI ACCESSO ALLA RETE INFORMATICA

Chiunque intende accedere alla rete informatica e/o agli strumenti elettronici dell'INRCA, deve soddisfare una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa

sia in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico. L'utente deve gestire le proprie credenziali di autenticazione secondo le seguenti regole:

- Sulla base del modulo reperibile sulla Intranet aziendale, correttamente compilato e fatto pervenire agli amministratori di sistema, gli stessi creano le credenziali di autenticazione associando un codice per l'identificazione dell'incaricato (*username)*, ad una parola chiave riservata (*password*), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla periodicamente con un procedimento imposto dal sistema stesso.
- Ad ogni utente vengono assegnate e associate individualmente, per cui non è ammesso che due o più utenti possano accedere agli strumenti elettronici utilizzando la medesima credenziale.
- E' invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.
- Lo User-Name deve essere associato in maniera univoca e non può essere riassegnato neanche in tempi successivi ad altro utente.
- La disattivazione delle credenziali di autenticazione è immediata:
  - nel caso in cui l'incaricato perda la qualità, che gli consentiva di accedere allo strumento,
  - dopo tre mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica*,* il cui utilizzo è quindi sporadico,
  - dopo cinque tentativi falliti di accesso.
- Elaborare in modo appropriato la password e conservarla con segretezza. Agli incaricati è imposto l'obbligo, automatizzato dal sistema, di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema
  - successivamente, almeno ogni tre mesi.
- La password deve essere costituita da una sequenza di almeno otto caratteri alfanumerici di cui almeno un carattere alfabetico maiuscolo, almeno un carattere alfabetico minuscolo ed almeno un numero, e non deve essere facilmente individuabile; nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.
- La password non deve contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), né consistere in nomi noti, anche di fantasia (pippo, pluto, paperino, ecc..).
- Nel proprio interesse, l'utente deve immediatamente richiedere la sostituzione delle credenziali, qualora ne accertasse la perdita o ne verificasse una rivelazione surrettizia. Infatti tutte le azioni riferibili ad una password saranno addebitate all'utente cui appartiene, che di conseguenza se ne dovrà assumere le responsabilità.
- La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare).
- Se l'utente inserisce una password su un dispositivo hardware/software che gli amministratori di sistema non sono in grado di disattivare, nell'eventualità che si renda necessario accedere per indispensabili e indifferibili motivi, ad esempio in caso di sua prolungata assenza o impedimento, occorre che l'incaricato stesso provveda:
  - a scrivere la parola chiave su un foglio di carta, a inserirla in una busta che deve essere chiusa e sigillata
  - consegni la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato dal Responsabile al momento dell'attribuzione della password.
- Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

ART.5 ATTIVITÀ NON CONSENTITE NELL'USO DELLA RETE

Agli utenti è assolutamente fatto divieto di collegare alla Rete, causa gli enormi rischi per la sicurezza della rete stessa, client dotati di Sistemi Operativi non preventivamente autorizzati dagli amministratori di Sistema.

Agli utenti è assolutamente fatto divieto altresì di collegare alla rete qualsiasi strumento elettronico non facente parte del patrimonio INRCA. PC o hardware di terze parti non possono cioè essere collegati alla rete senza previa autorizzazione degli Amministratori di Sistema.

Non sono inoltre consentite le seguenti attività:

- utilizzare le Risorse Tecnologiche per usare, archiviare, detenere, duplicare o diffondere in qualunque forma materiali tutelati da diritti d'autore o diritti connessi o sui quali terzi vantino diritti morali e patrimoniali (D.Lgs. n. 68/2003, Legge 22 Aprire 1941 n.633 e successive modificazioni);
- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la Rete e in generale le risorse informatiche dell'Istituto per scopi incompatibili con l'attività istituzionale dell'INRCA;
- conseguire l'accesso non autorizzato a risorse di rete interne;
- conseguire l'accesso non autorizzato a risorse di rete esterne alla Rete, tramite la stessa Rete Informatica;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- effettuare o permettere ad altri trasferimenti non autorizzati di informazioni (software, dati, ecc);
- installare qualsiasi programma da parte dell'utente o di altri operatori, se non previa autorizzazione degli amministratori di sistema;
- installare applicativi non compatibili con l'attività istituzionale:
- disinstallare, cancellare, copiare o asportare programmi software per scopi personali;
- installare componenti hardware senza preventiva autorizzazione degli Amministratori di Sistema;
- rimuovere, danneggiare o asportare componenti hardware;
- utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti;
- utilizzare software visualizzatori di pacchetti TCP/IP, software di intercettazione di tastiera, software di decodifica password e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
- inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non prima da questi espressamente autorizzate e ad essi comunicate;
- abbandonare il posto di lavoro lasciandolo senza protezione da accessi non autorizzati.

ART.6 POSTA ELETTRONICA

Il servizio di posta elettronica è concesso esclusivamente agli Utenti abilitati come supporto per il raggiungimento dei fini lavorativi e istituzionali dell'Ente. Ogni Direttore di Unità Operativa può richiedere l'assegnazione di una casella di posta elettronica per motivi di servizio per i propri collaboratori, compilando l'apposito modulo scaricabile dalla Intranet aziendale.

Ogni utente cui è concesso un indirizzo di Posta Elettronica, deve rispettare le seguenti regole e i divieti che seguono.

Regole

- La dimensione di base assegnata ad ogni casella è pari a 50 MB, per cui l'utente è tenuto ad esercitare una corretta gestione dello spazio assegnatogli. L'utente può comunque ottenere dagli amministratori di sistema, se le motivazioni saranno ritenute giustificate, un aumento dello spazio assegnato.

- E’ fatto espressamente obbligo agli utenti di Posta Elettronica di esercitare un corretta gestione sulla propria casella di posta. Pertanto ogni utente è tenuto ad eliminare regolarmente i messaggi da cancellare, e a salvare in una propria cartella i messaggi da conservare, evitando così la saturazione della casella. A questo fine sono state pubblicate sulla intranet aziendale le istruzioni per attivare l’applicativo OutLook che prevede questa funzione.
- Ogni utente si impegna a consultare con regolarità la propria casella di posta elettronica.
- Gli amministratori di sistema, cui è demandato il compito di gestire le risorse assegnate al servizio di Posta Elettronica, disattiveranno automaticamente la caselle di posta non consultate da oltre 90 giorni, a meno che l’utente non abbia comunicato agli stessi, la giustificata impossibilità di consultarla per un periodo così lungo.

Attivita' non consentite

- l’utilizzo della posta elettronica per fini diversi da quelli istituzionali,
- un uso che possa in qualche modo recare qualsiasi danno all’INRCA o a terzi, come l'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente,
- inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici,
- inoltrare "catene" di posta elettronica (catene di S.Antonio e simili), anche se afferenti a presunti problemi di sicurezza,
- la trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (D.lgs. 196/03).

ART.7 INTERNET

Attivita' non consentite

- l’installazione sul proprio computer di browser diversi da Internet Explorer
- l'uso di Internet per motivi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati dagli amministratori di sistema e per particolari motivi tecnici;
- l'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);
- lo scaricamento (download) di software e di file non necessari all'attività istituzionale;
- utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer;
- accedere a flussi in streaming audio/video da Internet per scopi non istituzionali (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse Internet).

ART.8 AMMINISTRAZIONE DELLE RISORSE INFORMATICHE

Agli Amministratori di Sistema sono consentite in maniera esclusiva le seguenti attività:

- Gestire hardware/software di tutte le strutture tecniche informatiche di appartenenza dell’INRCA, collegate in rete o meno.
- Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
- Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
- Rimuovere programmi software dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle

normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

- Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.
- Utilizzare le credenziali di accesso di amministratore del sistema, o l'account di un utente, tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di sua prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Dirigente di struttura dell'utente assente o impedito e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.
- In caso di Incident Response e Ripristino gli amministratori di sistema sono tenuti come primo atto ad avviare tutte le misure di isolamento, contenimento e raccolta delle informazioni e Computer Forensic Analysis dell'incidente. Successivamente, devono avviare le procedure di Disaster Recovery per il ripristino dei dati e dei servizi.

Per motivi di sicurezza e protezione dei dati, è in programma l'attivazione di un sistema che consenta la memorizzazione in appositi supporti informatici, di ogni attività compiuta nella Rete Informatica da ogni account di rete. Detti supporti potranno essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo, e potranno essere messi a disposizione dell'Autorità Giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D.Lgs. n. 196/2003.

ART.9 REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICO/INFORMATICO

Per tutti gli utenti cui è concesso l'accesso alla rete e agli strumenti elettronici dell'Ente, devono essere adottate le seguenti misure:

- ogni utente è responsabile dei dati memorizzati nel proprio profilo utente. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo quanto previsto dal codice Privacy;
- l'accesso agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- tutte le operazioni di manutenzione effettuate on-site, sia che siano svolte da personale interno che esterno, devono avvenire con la supervisione dell'incaricato del trattamento;
- tutti i supporti estraibili in cui sono realizzate le copie di backup, vanno conservate in armadio chiuso a chiave;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, deve essere adottato uno screensaver automatico che si attiva dopo non oltre i 10 minuti di non utilizzo. Si precisa che l'utente in caso di allontanamento può bloccare immediatamente il computer, (Ad esempio nei sistemi Windows digitando i tasti "Ctrl-Alt+Canc");
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo;
- la stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato;
- gli apparecchi fax devono essere installati in locali ad accesso controllato e l'utilizzo deve essere regolato dagli incaricati del trattamento;
- la manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, va autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di

sicurezza previste dal disciplinare;

- nei casi in cui, a causa di prolungata assenza o impedimento dell'incaricato, fosse indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe essere necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine, ogni incaricato deve:
  - scrivere la parola chiave su un foglio di carta e inserirlo in una busta che deve essere chiusa e sigillata,
  - consegnare la busta a chi custodisce le copie delle parole chiave, il cui nominativo viene loro indicato al momento dell'attribuzione della password;
- i supporti che contengono dati sensibili 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 armadi o cassetti chiusi a chiave e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati;
- 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 definitivamente;
- gli archivi contenenti dati sensibili devono essere organizzati in modo che il loro collegamento con il nominativo del paziente sia temporaneamente inintelleggibile. Pertanto tali archivi dovranno essere strutturati su distinte tabelle e/o crittografati;
- è fatto divieto assoluto di memorizzare dati personali e/o sensibili sulla propria postazione di lavoro;
- è fatto divieto assoluto di effettuare copie di dati personali e/o sensibili su supporti rimovibili, a meno che questi, non siano prima adeguatamente crittografati;

ART.10 REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS

Premesso che l'Ente ha dotato il proprio sistema ICT di Sistema Antivirus gestito centralmente dagli Amministratori di Sistema, e che su ogni client il software antivirus si aggiorna automaticamente ad ogni accensione, ogni utente è tenuto a rispettare le seguenti regole di comportamento:

- verificare che l'aggiornamento antivirus avvenga regolarmente, in caso contrario deve avvisare gli amministratori di sistema;
- divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd/dvd, pendrive) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS, ecc...;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete Internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, in quanto potrebbe essere falso e portare a un sito-truffa;
- non utilizzare le chat, il messenger e software analoghi;
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui abbia scoperto un il virus (nella maggior parte dei casi esso è in grado di risolvere il problema. Nei restanti chiederà di

eliminare il file infetto);

- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC;
- i dischi di ripristino del proprio PC, la copia di backup del sistema operativo consentita per legge, i driver delle periferiche (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC) vanno consegnati ad un incaricato che li custodirà per un loro successivo utilizzo.

Nel caso di sistemi danneggiati seriamente da malware l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; sulla base della seguente procedura:

1. formattare l'Hard Disk, definire le partizioni e reinstallare il Sistema Operativo;
2. installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;
3. reinstallare i programmi applicativi a partire dai supporti originali;
4. effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
5. effettuare il RESTORE dei soli dati a partire da una copia di backup recente. "*NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP*": potrebbe essere infetto;
6. ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

ART.11 L'AFFIDAMENTO DI DATI PERSONALI ALL'ESTERNO

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno, si devono adottare i seguenti criteri atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime previste dagli articoli da 33 a 35 del Dlgs 196/03 e dal disciplinare tecnico, allegato sub b) del codice.

Per la generalità dei casi in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno, devono essere impartite istruzioni per iscritto al terzo destinatario di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano
- dalla direttiva 95/46/CE, se il terzo destinatario non è italiano.

Qualora il trasferimento avvenga verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 Dlgs 196/03, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.

Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **sensibili e/o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico.

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati mediante apposita lettera scritta.

ART.12 INCIDENT RESPONSE E RIPRISTINO

Gli utenti della rete informatica devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso delle credenziali;

- modifica e sparizione di dati;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. avvisare immediatamente gli amministratori di sistema e isolare la scena dell'incidente.

ART.13 VIOLAZIONI AL PRESENTE REGOLAMENTO

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente comporta l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigenti.

ART.14 SANZIONI

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti dell'ISTITUTO.

ART.15. MODIFICHE DEL REGOLAMENTO

- L'Utente accetta ogni modifica del Regolamento resa necessaria da disposizioni di legge e/o regolamenti e/o provvedimenti delle competenti Autorità.
- L'Utente accetta altresì ogni modifica del Regolamento introdotta con provvedimenti adottati dall'Istituto.
- Le eventuali modifiche introdotte al presente regolamento, diventeranno immediatamente esecutive, e saranno comunicate a tutti gli utenti utilizzando gli strumenti a disposizione, posta elettronica e/o fax o per mezzo della intranet aziendale, e all'interno dei corsi di aggiornamento che si terranno regolarmente ogni anno.