Regolamento per l'utilizzo delle risorse informatiche e di rete dell' Azienda per i Servizi Sanitari n° 1 Triestina

Premessa

Questo Regolamento stabilisce le disposizioni alle quali gli utilizzatori di risorse informatiche dell'ASS1, intese in apparecchiature, programmi e servizi, devono attenersi per un uso tecnicamente corretto quindi efficace, legittimo ed economicamente efficiente, dell'intero sistema informatico aziendale.
S'intendono per risorse informatiche:

- personal computers, computers portatili, stampanti, dispositivi di ogni tipo collegati ai computers ed utilizzati presso le sedi dell'Azienda per i Servizi Sanitari n° 1 Triestina o, al di fuori di queste, ovunque sia possibile utilizzare servizi aziendali in internet o in rete dedicata;
- server, NAS, Network Attached Storage, SAN, Storage Area Network, e computers installati nelle aree riservate a SCSI presso la sede centrale o in ogni altra sede periferica dell'Azienda;
- ogni apparato di rete, strumento di misura o di test collegato alla rete aziendale;
- tutto il software e i dati disponibili nei sistemi o attraverso di essi, per l'utilizzo da parte degli utenti o di terzi autorizzati.

Un elenco non esaustivo delle categorie di utilizzatori che possono accedere alle risorse del sistema aziendale può essere così dettagliato:

- Dipendenti e assimilati in comando
- Componenti della Direzione Strategica e del Collegio dei Sindaci
- Medici di medicina generale, Pediatri di Libera scelta e collaboratori operanti presso i loro ambulatori
- Amministratori
- Personale delle farmacie in convenzione CUP
- Personale e collaboratori con incarichi professionali
- Personale interinale
- Stagisti
- Tirocinanti
- Eventuali ospiti.

ART. 1

Autorizzazione all'accesso

L'accesso alle risorse del sistema aziendale è riservato agli utilizzatori autorizzati ed esplicitamente incaricati.

L'incarico avviene con la sottoscrizione della relativa richiesta a SCSI da parte del responsabile di struttura complessa o assimilata, per conto di quel suo collaboratore che deve essere abilitato.

La richiesta è prodotta su apposita modulistica, e il responsabile di struttura, inteso come responsabile del trattamento, individua il proprio collaboratore come incaricato del trattamento.

L'autorizzazione e il relativo rilascio delle credenziali avviene a seguito di autorizzazione della richiesta da parte del responsabile SCSI e di conseguente procedura di rilascio, registrazione e comunicazione delle modalità di impiego e amministrazione.

Questa, prodotta da funzionari SCSI incaricati, prevede anche la registrazione e la tenuta degli archivi degli autorizzati.

Le credenziali vengono fornite nominalmente al soggetto autorizzato, in busta chiusa, direttamente da SCSI, o se necessario, da soggetti terzi gestori come Insiel S.p.A. su indicazione di SCSI, assieme alle informazioni sulla tenuta, l'amministrazione e il comportamento relativo.

ART. 2

Accesso alle risorse aziendali

Per ottenere l'accesso, l'utilizzatore deve fornire le proprie credenziali di autenticazione previste per il tipo di account assegnato come parole chiave, codici identificativi, carte a microprocessore, token, certificati digitali, o dispositivi che riconoscono le caratteristiche biometriche.

Le credenziali sono strettamente personali e non possono essere cedute o condivise.

In caso di credenziali costituite da parola chiave (password) associata al nome utente, la legge definisce i criteri con cui le credenziali devono essere prodotte, rilasciate e utilizzate.

L'accesso alle risorse avviene solitamente per mezzo di un computer aziendale collegato alla rete dell'Azienda, amministrata da SCSI e che costituisce un sottosistema dell'infrastruttura del SISSR, Sistema Informativo Socio Sanitario Regionale.

La totalità delle macchine aziendali è a dominio sul dominio aziendale amministrato da SCSI e quindi l'accesso e l'autenticazione avvengono di norma attraverso le credenziali di dominio.

Queste consentono l'accesso a tutte le altre procedure amministrate direttamente da SCSI, come la posta elettronica e altri servizi, mentre per altre procedure amministrate da fonitori terzi come Insiel S.p.A., l'utilizzo delle

procedure avviene, dopo l'accesso al dominio, tramite altre credenziali specifiche per la procedura.

Nel caso di computers portatili vi possono essere diversità di comportamento perché, qualora le macchine non vengano impiegate in rete, può essere utile impiegare credenziali specifiche diverse da quelle di dominio per attivare la macchina.

Le credenziali di dominio divengono nuovamente necessarie se si deve accedere dall'esterno della rete aziendale, ad esempio via internet, a servizi aziendali quali la posta elettronica.

Le credenziali di dominio sono costituite da un'identità composta dalla sequenza cognome-nome o da nomi specifici istituzionali, a seconda dei casi, e da una parola chiave modificabile dall'utilizzatore, di otto lettere e cifre contenente obbligatoriamente maiuscole e minuscole, che va rinnovata ogni tre mesi.

Per ottemperare alle norme di legge, la parola chiave usata deve essere di lunghezza predefinita oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non dovrebbe contenere riferimenti agevolmente riconducibili all'incaricato quali nome, cognome, nomi di figli, coniugi o simili,, deve essere modificata da questi al primo utilizzo, e successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e personali, e comunque in tutte le situazioni che SCSI riterrà opportune, come ad esempio per l'autenticazione al dominio aziendale e al sistema di posta elettronica, la parola chiave dovrà essere modificata almeno ogni tre mesi.

Per compiti di monitoraggio, controllo, aggiornamento dei sistemi e nel pieno rispetto del DLG 196/2003, art. 616 CP e art. 4 Statuto dei Lavoratori il personale del Sistema Informativo può accedere, direttamente oppure utilizzando appositi strumenti hardware e/o software, a qualsiasi risorsa informatica.

ART. 3

Utilizzo delle risorse informatiche

Le risorse informatiche dell'Azienda possono essere utilizzate esclusivamente per le attività istituzionali e non è consentito l'uso per fini personali.

Non è consentita la conservazione di dati personali o sensibili di soggetti terzi sul computer di lavoro senza che questo sia comunicato a SCSI e da questa debitamente autorizzato dopo la verifica dell'ottemperanza alle esigenze tecniche e di legge.

Non è consentita per nessun motivo, soprattutto sanitario, la creazioneautonoma di archivi di dati personali, sensibili, clinici, sociali o di salute sui singoli computers di lavoro.

Qualora questo risultase necessario a seguito di verifiche di SCSI, alla quale l'esigenza dovrà essere rappresentata, l'archivio verrà conservato su apposite macchine server nelle condizioni di sicurezza, accessibilità e garanzia

di riservatezza stabilite e garantite da SCSI in ottemperanza dello stato dell'arte tecnico, delle leggi e dei regolamenti.

In particolare sono poi tassativamente vietate e perseguibili per via amministrativa, civile e penale le seguenti attività :

- diffondere prodotti informativi lesivi dell'onorabilità, individuale o collettiva;
- diffondere prodotti informativi di natura politica al di fuori di quelli consentiti dalla legge e dai regolamenti;
- diffondere, in rete o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura;
- svolgere ogni tipo di attività commerciale non prevista dai fini istituzionali dell'azienda;
- compiere attività che possano rappresentare una violazione della legge in materia di Copyright, come la copia non autorizzata di software, CD e DVD audio e video, clonazione o programmazione di smart card;
- compiere attività che compromettono in qualsiasi modo la sicurezza delle risorse informatiche e della rete aziendale;
- accedere a siti ed acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
- ogni altra attività illegale qui non elencata.

Il furto, il danneggiamento o lo smarrimento di strumenti informatici aziendali devono essere tempestivamente denunciati all'Azienda.

ART. 4

Responsabilità degli utenti

L'utente impiega solitamente una configurazione di rete ottimizzata che non può in alcun caso modificare, così come non può effettuare manomissioni o interventi sulle apparecchiature o sui programmi non formalmente autorizzati dal servizio tecnico del Sistema Informativo, al quale deve comunicare tempestivamente le necessità di interventi su apparecchiature e programmi in ordine alla corretta fornitura del servizio.

Gli utilizzatori sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso, è fatto loro divieto di accedere direttamente o indirettamente a directory, files e servizi non espressamente e preventivamente autorizzati dal Sistema Informativo.

E' fatto divieto a ciascun utente di divulgare, per fatto imputabile a lui direttamente o indirettamente, password, login e comunque chiavi di accesso riservate.

Qualora queste venissero smarrite, va fatta immediata segnalazione e dell'accaduto e richiesta di sostituzione al Sistema Informativo.

Gli utilizzatori sono obbligati a segnalare immediatamente al Sistema Informativo ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza**.**

Gli utenti che si assentano dal lavoro per un periodo uguale o superiore a 6 mesi, per aspettativa di ogni genere, maternità, malattia, quiescenza o altro, sono tenuti ad informare attraverso il proprio responsabile il Sistema Informativo per le vie formali, al fine di provvedere alla corretta amministrazione dell'account.

Gli utilizzatori sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive del Sistema Informativo divulgate tramite i canali istituzionali.

In caso di violazione o inadempimento di quanto riportato ai precedenti punti, il Sistema Informativo procederà a disabilitare l'accesso dell'utente e ne darà comunicazione agli uffici competenti per l'eventuale accertamento di responsabilità disciplinari del personale interessato**.**

ART. 5

Software e copyright

L'utente risponde del software installato sul computer che gli è affidato.

Il Sistema Informativo provvede all'acquisto, o alla regolarizzazione, delle licenze necessarie per l'uso del software presente sui computer dell'Azienda.

Ogni qual volta si presenti la necessità di acquisire nuovo software per esigenze degli utenti, l'acquisto deve essere preventivamente concordato con il Sistema Informativo che ne valuterà la praticabilità di volta in volta.

E' vietato distribuire software soggetto a Copyright acquistato dall'Azienda, al di fuori dei termini delle licenze.

E' vietato distribuire software che possa danneggiare le risorse informatiche.

E' vietato accedere a dati e/o programmi per i quali non vi è autorizzazione o esplicito consenso scritto da parte dell'intestatario.

ART. 6

Apparecchiature

Il Sistema Informativo provvede direttamente o indirettamente all'acquisto di tutte le dotazioni informatiche quali computer, stampanti apparecchiature di rete, accessori e altro, ad eccezione dei prodotti consumabili come toner, cartucce e simili, e ne cura la distribuzione, l'installazione, la manutenzione e l'aggiornamento tecnologico.

L'amministrazione del parco macchine aziendale, l'aumento o la razionalizzazione delle dotazioni, le scelte di sistema, tecnologia e distribuzione, sono di esclusiva competenza di SCSI, come da Atto Aziendale, e

di conseguenza ogni operazione o intervento sui singoli elemento del sistema informativo aziendale è di competenza di SCSI.

Ogni necessità non contemplata negli acquisti programmati deve essere preventivamente concordata con il Sistema Informativo che ne valuterà di volta in volta l'opportunità.

ART. 7

Le seguenti attività sono tassativamente vietate:

- utilizzare strumenti che potenzialmente sono in grado di consentire l'accesso non autorizzato alle risorse informatiche come ad esempio cracker, programmi di condivisione quali IRC, ICQ, o software di monitoraggio della rete in genere;
- configurare servizi già messi a disposizione in modo centralizzato, quali DNS , DHCP o server di qualsiasi natura , Web o E-mail;
- intercettare pacchetti sulla rete, utilizzare sniffer o software di analisi del traffico come *Spyware,* dedicati a carpire, in maniera invisibile, dati personali, password e ID dell'utente oppure a controllare ogni attività, ivi inclusa la corrispondenza e i dati personali, del dipendente;
- accedere ai locali e ai *box* riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi;
- cablare o collegare apparecchiature alle prese di rete senza l'autorizzazione del Sistema Informativo, di conseguenza ogni sostituzione o aggiunta di schede di rete deve essere preventivamente segnalata agli addetti del Sistema Informativo, per la registrazione degli indirizzi ethernet univoci come *MAC address,*
- installare hub per sottoreti di PC e stampanti;
- utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente;
- installare modem per chiamate su linee analogiche, digitali o xDSL;
- installare modem configurati in *call-back;*
- 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 informatiche, sia dell'Ente che di terze parti, violandone le misure di sicurezza;
- accedere ai file di configurazione del sistema, farne delle copie e trasmetterle ad altri;
- svelare le password altrui, nonché trasmettere in chiaro, pubblicare o mandare in stampa liste di account utenti o nomi host e corrispondenti indirizzi IP delle macchine;
- utilizzare programmi gratuiti tipo *shareware*, prelevati da siti Internet o in allegato a riviste o libri senza la formale autorizzazione del Sistema Informativo;

Ogni azione che non sia comunque conforme allo spirito di questo Regolamento, verrà considerata una violazione della sicurezza, e come tale comporterà la segnalazione al Dirigente responsabile del Servizio.

ART. 8

Amministratori di sistema

Si definisce amministratore di sistema il soggetto a cui è conferito il compito di sovraintendere a una o più risorse informatiche dell'Azienda (L. 318/99, art. 1, comma 1.c)

Gli amministratori di sistema sono obbligati ad operare nel rispetto delle politiche dell'Ente in materia di sicurezza, a garantire la massima riservatezza nella trattazione dei dati personali anche desunti dal software di analisi del traffico, a mantenere riservate le informazioni relative al collegamento degli utenti fatti salvi i casi di interessamento della Magistratura a fronte di ipotesi di reato.

Forniscono ai dirigenti dei settori, report contenenti dati aggregati relativi all'andamento del traffico, ai picchi anomali settoriali, alla statistica generale di accesso ai siti più frequentati.

Il Sistema Informativo revoca l'accesso temporaneo alla risorsa informatica e di rete, sentito il Dirigente preposto, qualora questo sia utilizzato impropriamente o in violazione delle leggi vigenti; potrà altresì interrompere temporaneamente la prestazione del servizio in presenza di motivati problemi di sicurezza, riservatezza o guasto tecnico, dandone tempestiva comunicazione all'utente.

Il personale del Sistema Informativo può accedere in qualsiasi momento, anche senza preavviso, ai locali e alle risorse informatiche dell'Ente sia in caso di emergenza, sia per effettuare gli interventi di assistenza, verifica e supporto.

ART. 9

Posta Elettronica

Gli utenti possono richiedere che venga loro assegnata una casella di posta elettronica configurata secondo uno dei seguenti profili

- Standard
- Avanzato
- Privilegiato
- Illimitato

Le caratteristiche dei profili sono riassunte nella seguente tabella.

Profilo	Dim. Max	Dim. blocco ricezione	Dim. di avviso	Dim. Max Allegati
Standard	40 Mb	35 Mb	30 Mb	10 Mb
Avanzato	80 Mb	75 Mb	60 Mb	10 Mb
Privilegiato	120 Mb	110 Mb	100 Mb	10 Mb
Illimitato	1 Gb	970 Mb	800 Mb	20 Mb

Una volta raggiunto il limite di dimensione della casella configurato per l'avviso, all'utente viene inviata una notifica senza che il sistema intraprenda

alcuna azione.

Al raggiungimento del limite di dimensione configurato per il blocco della ricezione, il sistema invia una notifica all'utente e inibisce la possibilità di ricevere messaggi fino al ripristino della dimensione sotto il limite configurato.

In nessun caso gli allegati potranno superare le dimensioni massime configurate.

Il profilo predefinito è il profilo Standard.

Qualora l'utente riscontrasse la necessità di passare ad un profilo, fra quelli configurabili, dalle caratteristiche superiori, dovrà inoltrare una richiesta al Sistema Informativo che provvederà a valutarne la fattibilità.

Le caselle di posta che non verranno usate per un periodo superiore ai 3 mesi verranno segnalate per le vie formali ai responsabili.

Trascorso un periodo di 5 giorni senza avere ottenuto alcuna risposta da parte dell'interessato, la casella verra temporaneamente disabilitata.

Trascorsi ulteriori 30 giorni dalla disabilitazione verrà emessa una segnalazione al responsabile, e passati 5 giorni senza aver ottenuto risposta, la casella sarà definitivamente eliminata.

La posta elettronica, come ogni altro strumento aziendale, va utilizzata nel rispetto delle regole della pubblica amministrazione, adottando comportamenti conseguenti sia nei confronti dell'ente che dei singoli utilizzatori e colleghi.

Saranno dunque da evitare gli impieghi impropri per questioni personali, la condivisione dei messaggi con più soggetti di quelli ragionevolmente necessari, l'invio a tutta l'azienda o a gruppi consistenti di essa di comunicazioni che non abbiano valenza istituzionale.

Pur risultando oramai acquisito l'uso colloquiale dello strumento, sarà opportuna un'attenzione alla forma quando ciò risulterà opportuno, e la tendenza a non impiegare linguaggi, epiteti o espressioni che possano risultare ambigui o offensivi.

Sarà inoltre considerato particolarmente inopportuno utilizzare lo strumento, per la sua facilità di impiego, in polemiche più o meno personali che coinvolgano uditorii inutilmente ampi.

È inoltre da evitare con la massima attenzione lo scambio tremite posta elettronica di documenti riservati, dati personali, sensibili o clinici, come assolutamente da evitare è la creazione di archivi impropri di dati personali, sensibili o sanitari, sulle caselle di posta elettronica, ache se per scopi di salute.

Le responsabilità penali e civili di simili comportamenti, qualora gli archivi venissero violati e o le informazioni di soggetti terzi venissero alterate o smarrite, saranno di coloro che risulteranno titolari della procedura o delle caselle interessate.

Qualunque configurazione di servizio o prestazione al di fuori del presente regolamento dovrà essere concordata di volta in volta con il Sistema Informativo.

ART. 10

Medici di Medicina Generale in convenzione.

I Medici di medicina generale in convenzione con l'Azienda, sono collegati alla rete ASS1 sfruttando linee di trasmissione dati ADSL a totale carico dell'Azienda.

L'Azienda cura la manutenzione e l'aggiornamento tecnologico delle linee secondo le indicazioni del Servizio Informativo.

Non è consentito, se non espressamente autorizzato dal Sistema Informativo, il collegamento alle linee di qualsiasi apparecchiatura come Modem, Telefono e altro, nè direttamente né tramite i dispositivi di accesso quali Router, Hub o Modem.

Il Sistema Informativo cura l'installazione e la manutenzione esclusivamente in merito al computer, agli accessori nonché ai dispositivi di rete di proprietà dell'Azienda.

Previa autorizzazione il medico può installare sul computer programmi di sua proprietà e destinati alla gestione dell'ambulatorio.

In ogni caso il medico è responsabile dell'integrità e congruenza dei dati personali registrati sul computer di proprietà dell'Azienda.

Ove si renda necessario installare, sul computer di proprietà dell'Azienda, dispositivi per la salvaguardia dei dati quali masterizzatori, unità di backup, e altro, il medico provvederà alla fornitura dell'apparecchiatura mentre l'installazione sarà curata dal Sistema Informativo.

Ogni altra installazione dovrà essere concordata con il Sistema Informativo che ne valuterà di volta in volta la fattibilità.

Ove i programmi richiedano che l'utente disponga dei privilegi amministrativi, questi saranno assegnati su richiesta del medico, e potranno essere sospesi in qualunque momento qualora si riscontrassero violazioni al presente regolamento.

Per quanto non specificatamente dichiarato, valgono le regole generali precedentemente descritte in questo regolamento.

Prescrizioni generali

A margine del presente Regolamento vanno sottolineati altri tre comportamenti generali da considerare obbligatori per tutti gli utilizzatori di risorse informatiche aziendali e che riguardono, non tanto l'uso delle risorse informatiche, quanto l'adeguamento dei comportamenti in sintonia con esigenze organizzative aziendali, e normative del settore:

1. la segnalazione per richiesta d'intervento in caso di guasti o anomalie su apparecchiature informatiche o applicativi va fatta attraverso l'utilizzo dell'helpdesk, strumento utilizzabile in rete, documentabile e tracciabile;

2. qualora lo strumento di helpdesk non fosse utilizzabile o raggiungibile da postazioni contigue a quelle interessate, la segnalazione potrà essere fatta al numero telefonico 040 3995441, ove esiste l'apposito servizio di appoggio, e non cercando contatti diretti con tecnici e uffici ai vari numeri telefonici di SCSI;

3. in ottemperanza al Dlgs. 196/2003 e quindi a garanzia dell'integrità dei dati gestiti dagli utilizzatori, il comportamento a riguardo va concordato con SCSI, Struttura Complessa del Sistema Informativo.

Nelle more e ad integrazione di quanto previsto dal presente regolamento fanno fede i comportamenti prescritti dalla normativa vigente in tema di utilizzo di beni materiali e di dati informatici di proprietà o gestiti per competenza dell'A.S.S. n° 1 Triestina.

In caso di violazione accertata del presente regolamento, si applica il procedimento disciplinare previsto nel contratto di lavoro e negli accordi sindacali. Qualsiasi violazione alla normativa italiana vigente da parte degli utenti sarà segnalata alle Autorità competenti.

Il presente regolamento è soggetto a revisione periodica.