Azienda Ospedaliera San Gerardo U.O. Affari Generali e Legali	**DOCUMENTO PRESCRITTIVO** **REGOLAMENTO SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI AZIENDALI E PER L'ACCESSO E L'UTILIZZO DEI SERVIZI INTERNET E DI POSTA ELETTRONICA AZIENDALI**	Rev. 00	Pag. 1 / 12
		AGL-DA-006	

REGOLAMENTO SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI AZIENDALI E PER L'ACCESSO E L'UTILIZZO DEI SERVIZI INTERNET E DI POSTA ELETTRONICA AZIENDALI

Data	**Descrizione**	Redatto	Verificato	Approvato
24-11-2010	Prima emissione	M. Meroni	E. Parravicini	V.Colao

Regolamento sull'utilizzo degli strumenti informatici aziendali e per l'accesso e l'utilizzo dei servizi Internet e di Posta Elettronica

1. Finalità del presente regolamento

Il presente regolamento:

- disciplina l'utilizzo degli strumenti informatici aziendali e l'accesso e l'utilizzo dei servizi Internet e di Posta Elettronica (e-mail) da parte dei dipendenti e/o dei collaboratori dell'Azienda Ospedaliera San Gerardo;
- detta linee guida da seguire per l'utilizzo sicuro dei servizi Internet e di Posta Elettronica (e-mail) aziendali;
- definisce le modalità di controllo sull'utilizzo degli strumenti informatici aziendali e dei servizi Internet e di Posta Elettronica (email) aziendali da parte dell'ente datoriale, sottolineando che tale controllo viene effettuato nel pieno rispetto dello Statuto dei lavoratori e degli accordi sindacali;
- specifica le sanzioni che l'Azienda Ospedaliera può adottare in caso di mancato rispetto delle disposizioni contenute nel presente Regolamento.

2. Definizioni

Amministratore del sistema: soggetto a cui è conferito il compito di sovrintendere alle risorse del sistema informativo, di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Sistemi Informativi Aziendali: la struttura aziendale cui fa capo la responsabilità della gestione dei sistemi informatici.

Internet Service Provider (ISP): la società che fornisce all'Azienda Ospedaliera la connettività alla rete Internet.

Log: l'archivio delle attività di consultazione in rete.

Regolamento: il documento che ha ad oggetto la regolazione di una determinata funzione dell'Ente. Può contenere delle linee guida e dei suggerimenti per una migliore fruizione dei servizi aziendali.

Postazione di lavoro: lo strumento collegato alla rete aziendale tramite la quale l'incaricato autorizzato accede anche ai servizi Internet e di Posta Elettronica (e-mail).

Risorse informatiche aziendali: qualsiasi combinazione di apparati tecnologici dell'Azienda Ospedaliera, hardware o software, telefoni abilitati all'uso di Internet e della Posta Elettronica, utilizzati per le comunicazioni elettroniche ed elaborazione dei dati.

Utente: il dipendente e/o il collaboratore autorizzato dall'Azienda Ospedaliera ad utilizzare le risorse informatiche aziendali.

3. Norme nazionali vigenti e disposizioni che regolano l'utilizzo delle risorse informatiche aziendali, l'uso di Internet e della Posta Elettronica e il trattamento dei dati

Per quanto concerne l'utilizzo delle risorse informatiche aziendali, gli incaricati devono attenersi, oltre che alle disposizioni contenute nel presente Regolamento e alle istruzioni sul trattamento dei dati già impartite dall'Azienda Ospedaliera, alle leggi, regolamenti e direttive elencati di seguito:

- Codice sulla protezione dei dati personali emanato con D.Lgs. 196/2003;
- Direttive del Garante per la protezione dei dati personali, in particolare la deliberazione n.13 del 1 marzo 2007 e Direttive del Dipartimento della Funzione Pubblica con particolare riguardo alla Direttiva n.2 del 25 maggio 2009;
- Codice disciplinare contenuto nei Contratti Collettivi del Comparto;
- Codice di comportamento dei dipendenti delle pubbliche amministrazioni di cui al Decreto del Ministro per la funzione pubblica del 28 novembre 2000;
- Codice etico-comportamentale dell'A.O. San Gerardo approvato con delibera n. 368 del 28/6/2007.

4. Regole generali sull'uso delle risorse informatiche

4.1 Gestione della password

L'utilizzo delle risorse informatiche aziendali, della rete aziendale, delle informazioni in essa contenute, dei programmi applicativi e il trattamento dei dati personali con strumenti elettronici è consentito agli utenti in possesso di credenziali di autenticazione (nome utente e password), di regola, strettamente personali e non cedibili a terzi.

Le password di ingresso alle risorse informatiche e alla rete sono attribuite dall'Amministratore del Sistema e possono essere formate da lettere (maiuscole o minuscole) e/o numeri.

Nel caso di fondato sospetto che la propria password abbia perso la segretezza, questa deve essere immediatamente sostituita, dandone comunicazione al predetto Amministratore del Sistema.

Qualora l'utente venga a conoscenza della password di altro utente, è tenuto a darne immediata notizia alla persona interessata e all'Amministratore del Sistema.

Le password utilizzate dagli incaricati al trattamento hanno una durata massima di 3 mesi, trascorsi i quali devono essere sostituite con le modalità indicate dall'Amministratore del Sistema visionabili nel sito Intranet aziendale.

4.2 Gestione delle risorse informatiche

Ogni utente deve trattare le risorse informatiche a sua disposizione con cura e diligenza.

Ogni utente deve, altresì, utilizzare dette risorse in modo da non compromettere la sicurezza e la riservatezza del Sistema Informativo e da non pregiudicare ed ostacolare le attività dell'Azienda Ospedaliera.

Non è consentito all'utente, senza autorizzazione espressa dell'Amministratore del Sistema:

- installare autonomamente sul Personal Computer programmi provenienti dall'esterno;
- modificare le caratteristiche impostate sul proprio personal computer;
- installare dispositivi di comunicazione (come ad esempio modem, router, ecc).

Il Personal Computer deve essere spento ogni sera prima di lasciare l'ufficio, o in caso di assenze prolungate dall'ufficio. L'utente deve altresì evitare indebiti utilizzi da parte di terzi dei mezzi informatici a sua disposizione.

E' fatto obbligo interpellare il personale del Sistema Informativo Aziendale prima di ogni spostamento di Personal Computer per valutarne l'impatto, la fattibilità e predisporre le configurazioni adatte.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna (cd- rom, chiavette USB, ecc). Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus installato su ogni Personal Computer.

Nel caso in cui il Personal Computer non risulti dotato di antivirus (identificabile immediatamente dall'assenza di messaggi specifici) è fatto obbligo all'utente di segnalare immediatamente la carenza al Sistema Informativo Aziendale.

Ogni utente deve controllare il regolare funzionamento e l'aggiornamento periodico del software antivirus installato, segnalando eventuali anomalie al Sistema Informativo Aziendale.

Qualora venga rilevata la presenza di virus l'utente deve adottare le seguenti misure:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare immediatamente l'accaduto al Sistema Informativo Aziendale.

4.3 Utilizzo dei supporti magnetici

Tutti i supporti riutilizzabili (cd-rom, chiavette USB, ecc.) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da persone non autorizzate. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti contenenti dati sensibili devono essere contenuti in armadi chiusi a chiave. Tutti i files di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione da parte dell'Amministratore del Sistema.

4.4 Utilizzo della rete fisica

Gli armadi di rete contengono apparati fondamentali che distribuiscono le informazioni alla rete informatica fisica dell'Ospedale. E' vietato a chiunque l'accesso agli armadi di rete, la

modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto.
In caso di malfunzionamenti è necessario per il personale tecnico potere accedere agli apparati tempestivamente. E' quindi vietato depositare materiale nelle vicinanze degli armadi di rete o in modo che possano impedire o costituire ostacolo all'apertura della porta di accesso all'armadio, con particolare riferimento a sostanze infiammabili.
È responsabilità di ogni utente prestare attenzione a non alterare le connessioni a muro e i cavi che le collegano ai Personal Computer, con sedie o arredi. E' utile segnalare al personale preposto alla pulizia dei locali la loro posizione per evitarne il danneggiamento.

4.5 Utilizzo della rete logica

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema.
Le unità di rete presenti sul server possono essere comuni a gruppi omogenei di lavoro o strettamente personali e non visibili ad altri utenti. .
E' cura dell'utente informarsi sulla natura delle condivisioni in uso alla sua connessione.
I server di rete sono le uniche entità preposte alla condivisione di risorse. E' vietato condividere localmente dischi, cartelle o risorse (es. cartelle di scambi), ad eccezione delle stampanti comuni. Per esigenze di scambio di file tra uffici sono disponibili strutture adeguate presso i server del Sistema Informativo Aziendale.
L'Amministratore del Sistema può in qualunque momento procedere alla rimozione di file o applicazioni pericolosi per la sicurezza, sia sui Personal Computer che sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni 6 mesi) pulizia degli archivi, con la cancellazione di file obsoleti o inutili.

5 Disposizioni comuni all'accesso e all'utilizzo dei Servizi Internet e di Posta Elettronica aziendale

5.1 Utilizzatori

L'accesso ai servizi Internet e di Posta Elettronica aziendali e il loro utilizzo sono riservati ai dipendenti e ai collaboratori dell'Azienda appositamente autorizzati.

I servizi Internet e di Posta Elettronica aziendali non possono quindi essere utilizzati da altre persone, salvo esplicita autorizzazione dell'Amministratore di sistema.

5.2 Utilizzi consentiti dei servizi Internet e di Posta Elettronica aziendali

I servizi Internet e di Posta Elettronica aziendali sono uno strumento di lavoro. I dipendenti e i collaboratori autorizzati ad accedere alla rete Internet e alla Posta Elettronica tramite le risorse informatiche messe a disposizione dall'Azienda Ospedaliera (Personal Computer, telefoni, ecc.) devono, pertanto, utilizzare tali strumenti solo per scopi attinenti alla propria attività lavorativa e nel rispetto delle disposizioni in materia di diritto d'autore e delle altre disposizioni di legge vigenti.

La configurazione dei servizi viene effettuata esclusivamente dall'Amministratore del Sistema. All'utente non è concesso modificare tale configurazione.

6. Misure da adottare per tutelare la sicurezza e la privacy nella navigazione in Internet

6.1 Navigazione sicura

L'abilitazione alla navigazione in Internet può costituire uno strumento aziendale necessario allo svolgimento della propria attività di lavoro. E' quindi proibita la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa.

Data la vasta gamma di attività aziendali, non può definirsi a priori un elenco di siti aziendali autorizzati: l'Azienda Ospedaliera si riserva tuttavia la facoltà di utilizzare appositi strumenti di filtraggio, mediante i quali può essere bloccata la navigazione su categorie di siti i cui contenuti sono da considerarsi oggettivamente estranei agli interessi e alle attività aziendali (black list).

Il divieto di accesso ad un sito appartenente a quelli ricompresi nella black. list aziendale viene visualizzato esplicitamente sul video.

Tali siti, oltre naturalmente a quelli pedopornografici o pornografici, sono tutti quelli di "Social Networking" (Twitter, Youtube, Facebook, ecc.) o di altro genere, ove il loro utilizzo non sia motivatamente connesso all'attività lavorativa.

Su questi siti e senza reali esigenze lavorative, anche in assenza di "blocchi informatici all'accesso", è vietato "navigare".

Nel corso della navigazione l'utente è tenuto a leggere con attenzione qualsiasi finestra, pop up o avvertenza, prima di proseguire nella navigazione.

Non è consentito installare autonomamente programmi provenienti dall'esterno senza la esplicita autorizzazione dell'Amministratore del Sistema.

6.2 Rilascio di informazioni personali o dell'Azienda Ospedaliera S. Gerardo durante la navigazione

Gli utenti sono invitati a limitare il rilascio di informazioni personali durante la navigazione via Web.

Qualsiasi informazione aziendale può essere comunicata via Web, se strettamente necessaria, nel rispetto dei doveri stabiliti dalle leggi vigenti del Codice disciplinare dei CCNL e del Codice Etico-comportamentale.

Nel caso di comunicazione di dati personali sensiblli o informazioni riservate via Web, nei casi consentiti dalla normativa vigente, è necessario accertarsi che vi sia la protezione della comunicazione attraverso un idoneo sistema di sicurezza, quale, ad esempio Secure Sockets Layer (SSL).

E' opportuno quindi lasciare abilitato l'avviso di accesso a pagine protette.

6.3 Altre prescrizioni per la navigazione in Internet

Gli utenti sono invitati ad organizzare in modo ordinato la propria cartella dei siti Preferiti.

Si consiglia agli utenti di salvare sul proprio spazio disco in locale i file .pdf e .doc scaricati dalla rete, prima di aprirli.

7. Misure da adottare per tutelare la sicurezza e la privacy nell'utilizzo della posta elettronica

7.1 Indirizzi di posta elettronica

Sono attivati indirizzi di posta elettronica per le strutture aziendali condivisi dagli operatori assegnati a ciascuna di esse (es. denominazione.ufficio@hsgerardo.org). Al singolo lavoratore dipendente può essere assegnato un indirizzo e-mail personale del tipo: nominativo@hsgerardo.org.

7.2 Confidenzialità

La confidenzialità della posta elettronica e della comunicazione attraverso il Web è limitata in quanto i messaggi, transitando nella rete pubblica di Internet, possono essere visionati da terzi non autorizzati. Per questa ragione si deve porre la massima attenzione accertandosi che vi sia la protezione di cui al punto 6.2, comunicare informazioni classificate come riservate o dati sensibili attraverso l'e-mail o attraverso il Web.

7.3 Attendibilità del mittente

L'utente è tenuto a prestare particolare attenzione nell'apertura di e-mail il cui mittente non sia conosciuto.

7.4 Gestione delle liste di destinatari

Gli utenti devono organizzare l'agenda del proprio programma di Posta Elettronica in modo che non vi possano essere degli errori nella selezione dei destinatari dei messaggi.

7.5 Contenuto dei messaggi

Gli utenti devono assicurarsi che nei loro messaggi elettronici non siano inserite inconsapevolmente informazioni su User e Password utilizzate per accedere ad altre applicazioni. In particolare va usata la massima cautela nell'invio a mezzo Posta Elettronica di pagine internet che potrebbero contenere nell'indirizzo informazioni utili a risalire alla User/Password utilizzata.

Gli utenti sono invitati a nominare correttamente i nomi dei file allegati alle e-mail, specificando, nel caso si procedesse ad inviare documenti soggetti a modifiche e revisioni, la versione corrente del file con dei numeri progressivi.

E' esplicitamente vietato l'invio di messaggi in risposta a richieste di adesione a programmi di catene telematiche (c.d. di Sant'Antonio), indipendentemente dalle finalità presunte.

Gli utenti sono invitati a prestare attenzione nell'utilizzo della funzione "Rispondi" e "Rispondi a tutti", nel caso il messaggio originario sia stato inviato ad un numero elevato di destinatari.

7.6 Altre prescrizioni per l'utilizzo della posta elettronica

Gli utenti sono invitati a leggere quotidianamente la posta elettronica e a rispondere in tempi ragionevoli alle e-mail ricevute.

Gli utenti sono tenuti sempre ad accertarsi che gli eventuali allegati dei propri messaggi non eccedano la dimensione massima di 5 Mb. Qualora si riscontrasse la necessità di allegare un file di dimensioni superiori è buona norma che il mittente si assicuri previamente con il destinatario sulla possibilità di ricevere un messaggio di tali dimensioni.

La funzione che permette di metterli in coda per un successivo invio è caratterizzata da un'alta percentuale di casi di mancato o ritardato invio.

Si invitano gli utenti che hanno selezionato l'opzione di completamento automatico dell'indirizzo di prestare molta attenzione nella selezione dei destinatari.

Gli utenti devono periodicamente cancellare o organizzare in opportune cartelle la posta già letta; una quantità troppo elevata di e-mail nella cartella predefinita di arrivo della nuova posta può compromettere sensibilmente la stabilità del programma di posta.

Gli utenti devono sempre indicare con chiarezza (nel campo oggetto) l'argomento del proprio messaggio. E' possibile richiedere una ricevuta di corretto ricevimento della propria mail. A tale ricevuta va tuttavia assegnata una importanza relativa, poiché talvolta la conferma della ricezione avviene ad opera del mail server centrale e non del destinatario ultimo del messaggio, salvo ovviamente il caso dell'utilizzo di posta elettronica certificata (PEC).

Gli utenti sono invitati a segnalare al Servizio Informativo Aziendale l'arrivo sistematico di messaggi non sollecitati (spam) da determinati indirizzi e-mail.

Gli utenti sono invitati a prestare la massima attenzione nell'utilizzo delle funzioni avanzate di filtro che consentono di inoltrare automaticamente determinati messaggi in arrivo ad altri destinatari.

Posta elettronica certificata (PEC)

La PEC (Posta Elettronica Certificata) è un sistema di una e-mail con valore legale. Una mail trasmessa da una casella di PEC e ricevuta da una casella PEC ha il medesimo valore legale della tradizionale raccomandata postale con ricevuta di ritorno.

Perchè tutto questo avvenga è necessario che anche il mittente abbia un indirizzo PEC. Il termine "certificata" si riferisce al fatto che al mittente viene rilasciata una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e di eventuali allegati ed al mittente la ricevuta di avvenuta consegna.

La PEC attesta, quindi, che il messaggio è stato spedito, consegnato e che non è stato modificato.

L'email inviata da un dominio non certificato, ovvero non PEC (p.e. da un normale programma di posta elettronica) ad un indirizzo di PEC non assume, invece, valore formale e legale, e pertanto non crea vincoli di alcun genere per l'ente.

L'Azienda Ospedaliera S. Gerardo ha attivato le caselle di Posta Elettronica Certificata per diverse strutture aziendali.

8. Sistemi di risposta automatica, nomina del fiduciario e disclaimer in calce alle email

8.1 Sistemi di risposta automatica

Per prevenire l'apertura della posta elettronica dei dipendenti e per rispettare il principio di necessità e non eccedenza del trattamento di dati personali, l'Azienda Ospedaliera mette a disposizione di ciascun lavoratore apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze (ad es. per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.

Il dipendente è tenuto ad avvalersi di tali modalità in caso di assenze prolungate

In caso di eventuali assenze non programmate (ad es. per malattia), qualora il lavoratore non abbia provveduto ad attivare la procedura descritta (anche avvalendosi di servizi web mail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, semprechè sia necessario e mediante personale appositamente incaricato (ad es., l'Amministratore di Sistema), può disporre lecitamente l'attivazione di un analogo accorgimento, avvertendo gli interessati.

Ciascun lavoratore, a tal fine, è tenuto a nominare un fiduciario che, nel caso di assenza improvvisa o prolungata, sussistendo improrogabili necessità legate all'attività lavorativa, possa essere individuato quale destinatario dei messaggi di posta elettronica del lavoratore assente.

La nomina del fiduciario deve essere redatta in forma scritta, riportare la sottoscrizione del fiduciante e del fiduciario e consegnata al Responsabile della Struttura.

8.2 Disclaimer da porre in calce ai messaggi email dell'Azienda Ospedaliera

I messaggi di posta elettronica inviati tramite il sistema di posta elettronica aziendale devono contenere un avvertimento ai destinatari, nel quale viene dichiarata l'eventuale natura non personale dei messaggi stessi, precisando che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente, con le modalità di cui al presente Regolamento aziendale.

L'utente potrà adottare il seguente testo: "Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute da persone appartenenti all'organizzazione lavorativa del mittente secondo le modalità previste dal regolamento aziendale adottato in materia. Se per un disguido avete ricevuto questa mail senza essere i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo del mittente".

9. Responsabilità

9.1 Responsabilità nell'utilizzo dei servizi Internet e di Posta Elettronica aziendali

L'utente è direttamente e totalmente responsabile dell'uso delle risorse informatiche assegnategli e del servizio di Posta Elettronica e di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

L'utente sarà pertanto responsabile di qualsiasi danno arrecato all'Azienda Ospedaliera, all'Internet Provider o terzi, in dipendenza della mancata osservanza di quanto previsto dal presente Regolamento.

La violazione delle prescrizioni del presente regolamento può configurare un illecito civile, penale, amministrativo e/o disciplinare, quest'ultimo perseguibile secondo le procedure previste nei CCNL vigenti.

In conformità alle disposizioni generali e civili vigenti l'utente è obbligato a tenere indenne l'Azienda Ospedaliera da tutte le perdite, danni, responsabilità, costi, oneri e spese, ivi comprese le eventuali spese legali, che dovesse subire o sostenere quali conseguenze di qualsiasi violazione degli obblighi e garanzie previste nel presente regolamento e/o comunque correlate all'uso improprio degli strumenti messi a disposizione dall'ente datoriale.

10. Controlli dell'Azienda Ospedaliera sull'accesso e l'utilizzo dei servizi Internet e di Posta Elettronica tramite le risorse informatiche da parte degli utenti

10.1 Registrazione delle attività sull'uso dei servizi

Le attività sull'uso dei servizi Internet e di Posta Elettronica dell'utente vengono registrate elettronicamente sotto forma di file di log.

L'attività di registrazione viene effettuata a cura dell'Amministratore del Sistema, che garantisce anche la custodia dei file di log, in base alle normative vigenti.

10.2 Memorizzazione files di log della navigazione ad internet

Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento internet, memorizzano un giornale (file di log) contenente le informazioni relative ai siti che i gli strumenti informatici hanno visitato. Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'utente, garantendo in tal modo il suo anonimato.

L'accesso a questi dati è consentito all'Amministratore del Sistema o, su autorizzazione di quest'ultimo, al personale del Sistema Informativo Aziendale.

I sistemi softtware sono programmati e configurati in modo da cancellare perioedicamente i dati relativi agli accessi ad Internet ed al traffico telematico.

L'eventuale prolungamento dei tempi di conservazione è eccezionale e può aver luogo solo rispetto ad esigenze tecniche e di sicurezza del tutto particolari, in relazione all'indispensabilità del dato per l'esercizio o la difesa di un diritto in sede giudiziaria, oppure in ragione dell'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta della Polizia Giudiziaria o dell''Autorità Giudiziaria.

10.3 Controlli

Nel rispetto del divieto di controllo a distanza del lavoratore e dello Statuto dei Lavoratori nel quale tale divieto è contenuto, l'Azienda Ospedaliera effettua controlli sull'uso degli strumenti elettronici da parte degli utenti tramite consultazione dei file di log solo in relazione:

- ad esigenze di sicurezza e finalità di tutela del proprio patrimonio (ad es. nel caso in cui l'integrità del sistema sia minata da un problema di sicurezza e sia necessaria la consultazione dei file di log per individuare e eliminare l'anomalia);
- all'indispensabilità dei dati di log rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di rispondere ad una specifica richiesta dell'Autorità Giudiziaria o dell'Autorità di Pubblica Sicurezza.

10.4 Graduazione dei controlli

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'Azienda effettua per le finalità di tutela di cui all'articolo precedente, con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

- controllo preliminare su dati aggregati (riferiti all'intera struttura lavorativa o a una sua area e rilevazione della tipologia di utilizzo, e-mail, file audio, accesso a risorse estranee alle mansioni);
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;
- solo in caso di successivo permanere dell'anomalia l'Azienda Ospedaliera si riserva la facoltà di procedere ad effettuare controlli circoscritti su singole postazioni di lavoro.

Sono in ogni caso vietati controlli prolungati, costanti o indiscriminati.

11. Pubblicità del regolamento

Il presente regolamento verrà diffuso attraverso la rete interna e l'affissione in luogo accessibile a tutti, e verrà consegnato ai dirigenti nominati responsabili per il trattamento dei dati, ai fini della diffusione a tutto il personale nominato incaricato del trattamento dei dati.