c) MISURE MINIME DI SICUREZZA PER IL TRATTAMENTO DI DATI SENSIBILI MEDIANTE UTILIZZO DELLA POSTA ELETTRONICA E ACCESSO ALLA RETE (INTERNET E INTRANET)

Premesso che il provvedimento del Garante per la protezione dei dati personali 1° marzo 2007 (in GU n. 58 del 10 marzo 2007) raccomanda l'adozione da parte dei datori di lavoro di un Disciplinare Interno per L'uso di Internet e della Posta Elettronica e che tale indicazione è presente nella la Direttiva n. 2/2009 del Ministro Brunetta sull'utilizzo di internet e della posta elettronica istituzionale sul luogo di lavoro nella Pubblica Amministrazione, L'Azienda Ospedaliera Istituto Ortopedico Gaetano Pini (di seguito Azienda Ospedaliera) ha deciso di emanare il seguente regolamento sull'utilizzo della posta elettronica aziendale e dell'accesso alla rete (intranet e internet). Il presente regolamento ha l'obiettivo di fornire indicazioni a tutto il personale abilitato all'utilizzo della rete aziendale su:

- tutela dei beni patrimoniali aziendali;
- garanzia del regolare svolgimento del servizio interno ed esterno di posta elettronica;
- garanzia di un accesso alla rete aziendale e a internet per tutti i fruitori, in condizioni di regolarità, sicurezza e tutela dei dati personali e sensibili propri e delle persone eventualmente oggetto delle comunicazioni.

Articolo 1: **Norme di comportamento**

A norma del vigente Codice di comportamento per i dipendenti delle Pubbliche Amministrazioni, durante l'orario di lavoro il dipendente dedica la propria attività allo svolgimento delle mansioni affidategli nel rispetto dei principi di diligenza e correttezza.
Il dipendente è altresì responsabile del diligente e corretto uso dei beni aziendali che gli sono stati affidati per lo svolgimento delle proprie mansioni.
Il mancato rispetto delle regole contenute nel presente regolamento, ferma la responsabilità civile, penale e amministrativa, è perseguibile con provvedimenti disciplinari ai sensi dei contratti nazionali vigenti per il personale del SSN.

Articolo 2: **Controlli**

L' Azienda Ospedaliera si riserva la facoltà di verificare a livello informatico, per finalità di sicurezza e tutela del proprio patrimonio, l'esistenza di un comportamento illecito del dipendente nell'uso degli strumenti elettronici, accesso a internet e uso della posta elettronica.
Le verifiche si svolgeranno, con le modalità indicate negli articoli successivi, nel rispetto della libertà, della segretezza delle comunicazioni e delle garanzie previste dai CCNL, dallo Statuto dei lavoratori e dal Codice Privacy.
A seguito delle verifiche informatiche potranno essere raccolti dati personali che saranno trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza della finalità di tutela della sicurezza e del patrimonio.
Eventuali informazioni di natura sensibile potranno essere trattate dall'Azienda Ospedaliera se necessario per far valere o difendere un diritto in sede giudiziaria.

Articolo 3: **Tutela della rete aziendale**

L'utilizzo dei PC, 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) strettamente personali e non cedibili a terzi che possono essere richieste attraverso il MOD/16 RA/01.

Il codice per l'identificazione dell'utente può avere le seguenti caratteristiche:

- per i dipendenti cognome–matricola aziendale;
- per gli studenti e i frequentatori medici cognome -666666;
- per i dipendenti universitari cognome -777777;
- per i soggetti esterni che hanno un'attività continuativa di presidio cognome-999999.

Gli utenti sono responsabili delle postazioni di lavoro a loro assegnate pertanto non devono lasciarle incustodite e accessibili durante una sessione di lavoro.
Per garantire la riservatezza e la sicurezza dei dati personali trattati, l'utente deve inoltre:

- utilizzare password lunghe almeno otto caratteri;
- modificare la password al primo utilizzo e, successivamente, ogni tre mesi. Il sistema avviserà comunque l'utente dell'approssimarsi della data di scadenza della password;
- evitare di utilizzare riferimenti banali nella costruzione delle password (ad esempio è sconsigliato usare il proprio nome, la propria data di nascita , il nome del coniuge, ecc...);
- adottare le necessarie cautele per assicurare la segretezza e l'esclusività della password (ad esempio non scrivere la password su promemoria da attaccare al computer, non adottare procedure di memorizzazione automatiche);
- modificare immediatamente la password nel caso ritenga che la stessa abbia perso le necessarie caratteristiche di riservatezza.

Inoltre, a scopo difensivo della strumentazione, della rete aziendale e delle informazioni possedute e gestite, è:

- vietato installare modem o altri apparecchi non autorizzati;
- vietato collegare alla rete PC non autorizzati;
- vietato installare programmi non autorizzati.

Qualora il singolo utente abbia necessità specifiche provvede ad inoltrare richiesta di supporto tecnico ai Sistemi Informativi Aziendali attraverso la debita compilazione del MOD/17 RA/01.

Articolo 4: **Accesso a internet**

L'accesso a internet è consentito nel rispetto dei principi di correttezza e diligenza per perseguire finalità di tipo istituzionale e/o previste dalla legge.
L'utente non può accedere a internet per perseguire scopi privati e/o vietati dalla legge ma solo per ragioni di lavoro al fine di raggiungere obiettivi di studio, ricerca e documentazione. E' fatto divieto di scaricare e riprodurre, anche su supporti differenti, il materiale soggetto a proprietà intellettuale o protetto da copyright, il cui utilizzo possa ledere la normativa vigente sul diritto d'autore.

Pertanto:

- non è consentito navigare in siti o registrarsi a siti non attinenti allo svolgimento delle mansioni;

- non è consentito il download di programmi, di file musicali, di file multimediali anche se gratuiti, salvo autorizzazione preventiva ed espressa;
- è vietato scaricare o immettere nella rete aziendale materiale di qualsiasi genere non attinente all'attività lavorativa o comunque di provenienza illecita.
- è vietato partecipare a forum non autorizzati ed utilizzare chat line

L'utente è considerato direttamente responsabile per un eventuale accesso illecito, per l'appropriazione indebita del materiale cartaceo utilizzato per stampare i risultati della navigazione e per il danneggiamento della rete aziendale a causa dei virus informatici introdottisi in seguito ad un uso non accorto degli strumenti informatici messi a disposizione.
E' fatto salvo il diritto dell' Azienda Ospedaliera di chiedere l'ulteriore risarcimento del danno.

La Azienda Ospedaliera si riserva, a scopo difensivo della strumentazione, della rete aziendale e delle informazioni possedute e gestite, di filtrare, inibendone l'accesso, i siti ritenuti non idonei a garantire la sicurezza ovvero la pertinenza agli scopi istituzionali, mediante l'utilizzo di parole chiave o di appositi filtri informatici ovvero di controlli successivi random non associabili all'utente diretto.
La Azienda Ospedaliera si riserva altresì la facoltà di bloccare eventuali download di file multimediali, musicali o comunque non pertinenti con gli scopi aziendali.

La Azienda Ospedaliera si riserva controlli anonimi, in accordo con il Codice Privacy, tramite utilizzo di file di log, sul corretto utilizzo di internet basandosi su dati aggregati riferiti all'intera struttura aziendale o a sue aree o a gruppi di utenti. Solo in seguito al verificarsi di ripetute anomalie possono essere eseguiti controlli a livello individuale.

Nel caso in cui si presentasse l'esigenza di accedere a siti che risultassero bloccati, l'utente provvede a richiedere il supporto tecnico dei Sistemi Informativi Aziendali attraverso la casella di posta elettronica segreteria.sia@gpini.it

***Articolo 5:* Casella di posta elettronica**
La Azienda Ospedaliera si impegna a fornire, ove richiesta con le opportune procedure, una casella di posta elettronica a tutto il personale dipendente, ad uso esclusivamente istituzionale, al seguente indirizzo:

nome.cognome@gpini.it

La casella di posta, assegnata all'utente o al gruppo di utenti, è uno strumento di lavoro e come tale deve essere utilizzata ai fini istituzionali. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Fermo restando quanto sopra, è tollerato un uso personale limitato, tale da non intralciare o danneggiare o interferire in alcun modo con l'attività istituzionale né in termini di tempo dedicato né in termini di quantità/qualità delle informazioni e dei messaggi scambiati.
In ogni caso:

- è vietato inviare o memorizzare messaggi a contenuto offensivo, discriminatorio;
- è vietato usare la posta elettronica per documenti riservati o confidenziali;
- per non correre il rischio di essere infettati da virus, dovranno essere cancellati, senza aprirli, messaggi insoliti o provenienti da mittenti sconosciuti, inoltre dovrà essere disattivare la funzione anteprima automatica e il riquadro di anteprima;

- in caso di assenza del dipendente, l'utente deve attivare il sistema di risposta automatica ai messaggi di posta elettronica ricevuti;
- è dovere del dipendente, che si assenta dal servizio, rendere possibile l'accesso ai files e alla casella di posta elettronica da parte del responsabile dell'ufficio; a tal fine il dipendente è tenuto a indicare un fiduciario prontamente reperibile per la lettura dei messaggi di posta elettronica; in questo caso verrà riportata l'indicazione dell'utente – diverso dal titolare – che ha aperto o inviato il messaggio.

E' fatto divieto di utilizzare nome utente e password di un altro utente per accedere in sua assenza alla sua casella di posta elettronica.
L'utente dovrà provvedere alla manutenzione della propria casella di posta al fine di evitare una eccessiva espansione della stessa che comporterebbe spreco di risorse aziendali. Pertanto è cura dell'utente archiviare o cancellare periodicamente documenti inutili, superati, ingombranti.

A scopo difensivo della strumentazione, della rete aziendale e delle informazioni possedute e gestite, la AO si riserva di filtrare la corrispondenza in entrata mediante appositi filtri *antispam e antivirus* come ritenuti idonei con rispetto al livello tecnologico raggiunto dai prodotti specifici presenti sul mercato.
Inoltre sono filtrati messaggi in ricezione, provenienti anche da utenti conosciuti, con allegati aventi particolari estensioni (es: exe, bat, cmd, com, mdb,dll etc...)
L'Azienda Ospedaliera promuove l'utilizzo della posta elettronica nei seguenti casi:

- richieste o concessioni di ferie e permessi;
- richieste o comunicazione di designazione in comitati, commissioni, gruppi di lavoro o altri organismi;
- convocazione per riunioni;
- comunicazioni di servizio al singolo dipendete;
- diffusione di circolari;
- invio documenti redatti su supporto cartaceo.

***Articolo 6:* Divieti e limitazioni dell'uso della posta elettronica**
Al fine di assicurare la fruibilità del servizio per tutti gli utenti della Azienda Ospedaliera, la dimensione massima consentita per l'invio o la ricezione di messaggi di posta elettronica è di 30MByte.

E' fatto divieto di inoltro di mail non pertinenti l'attività istituzionale, quali, a mero titolo di esempio:

- che possano violare, per il loro contenuto o per il destinatario, disposizioni di legge o linee guida aziendali o possano compromettere l'immagine dell'Azienda;
- auguri di festività varie;
- pubblicità varie;
- partecipazione a mailing list salvo diversa ed esplicita autorizzazione.

E' altresì vietato rispondere o partecipare alle cosiddette "catene di S.Antonio" qualunque sia il contenuto.
Poiché la posta elettronica è in chiaro, è vietato veicolare tramite *e-mail* dati personali ovvero sensibili relativi a persone o pazienti. Qualora ciò sia necessario per motivi istituzionali, i dati stessi devono essere veicolati in forma anonima o crittografata ovvero secondo i protocolli e le procedure di sicurezza indicate dai competenti uffici dei Sistemi Informativi Aziendali.

Articolo 7: **Disclaimer e firma**

Costituisce obbligo dell'utilizzatore autorizzato, di collaborare in modo diligente con il datore di lavoro apponendo su tutte le mail obbligatoriamente in uscita verso l'esterno *il testo ufficiale disclaimer* quale rilasciato dall'Ente tramite gli uffici competenti dei Sistemi Informativi Aziendali.

Articolo 8: **Importazione di files**

L'Azienda Ospedaliera autorizza l'importazione di file di provenienza esterna, alle condizioni tecnico operative e di sicurezza specificate in appositi protocolli operativi rilasciati dai competenti uffici dei Sistemi Informativi Aziendali.

Articolo 9: **Supporti rimovibili di dati**

Gli utenti sono responsabili dei dati memorizzati sui supporti rimovibili (chiavetta USB, floppy disk, CD-ROM, DVD, ecc...).

Per i supporti contenenti dati sensibili, con riferimento alle vigenti norme sul Codice Privacy, l'utente provvederà alla loro custodia in luoghi sicuri al fine di evitare accessi non autorizzati o trattamenti non consentiti o alternativamente provvederà alla crittografia dei dati in essi contenuti.

I supporti contenenti dati sensibili se non più utilizzati devono essere distrutti o resi inutilizzabili in maniera definitiva. Un eventuale riutilizzo è possibile solo previa cancellazione definitiva dei dati precedentemente contenuti.