Ai Collaboratori
dell'ASP Giovanni XXIII
Sede

Oggetto: disciplina aziendale in materia di utilizzo degli strumenti informatici

La presente per informare che l'Azienda ha approvato con atto n. 361 del 29.10.2008 la disciplina aziendale in materia di utilizzo degli strumenti informatici, che si allega.

La disciplina, adottata sulla base e secondo le indicazioni contenute nella deliberazione 1.3.2007 n. 13 del Garante per la protezione dei dati personali, ha l'obiettivo di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e collaboratori fornendo informazioni utili per comprendere cosa può fare ogni dipendente/collaboratore per contribuire a garantire la sicurezza informatica di tutta l'Azienda.

La S.V. è pregata di compilare la dichiarazione di assunzione di responsabilità per l'accesso a Internet dalle postazioni aziendali, che si allega, e riconsegnarla al Servizio Risorse Umane.

Distinti saluti.

La Responsabile del Servizio Risorse Umane
Elisabetta Calzolari

All.ti n. 2:
- disciplina aziendale relativa all'utilizzo degli strumenti informatici;
- dichiarazione di assunzione di responsabilità.

40139 Bologna • Viale Roma, 21 • tel. +39 051 6201 322 • fax +39 051 6201325 • e-mail m.cuppini@aspgiovanni23.it

ASP GIOVANNI XXIII
Bologna

DISCIPLINA AZIENDALE RELATIVA ALL'UTILIZZO DEGLI STRUMENTI INFORMATICI

INDICE

PREMESSA

1. Il presente Disciplinare, adottato sulla base e secondo le indicazioni contenute nella deliberazione 1 marzo 2007 n. 13 del Garante per la protezione dei dati personali, recante "Linee guida del Garante per posta elettronica ed internet", ha per oggetto i criteri e le modalità operative di accesso ed utilizzo di internet e della posta elettronica da parte dei dipendenti dell'ASP Giovanni XXIII e di tutti gli altri soggetti che a vario titolo prestano servizio o attività per conto e nelle strutture dell'ASP.
2. Tali indicazioni integrano le specifiche istruzioni operative fornite a tutti gli incaricati in attuazione del D.lgs 196/03 – Testo Unico in materia di protezione dei dati personali.
3. Esso ha l'obiettivo di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e collaboratori fornendo informazioni utili per comprendere cosa può fare ogni dipendente/collaboratore per contribuire a garantire la sicurezza informatica di tutta l'Azienda.

NORME DI COMPORTAMENTO

1. Utilizzo del Personal Computer

1. Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile di servizio.
2. L'accesso all'elaboratore è protetto da password di accesso al dominio che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Le password devono essere utilizzate per l'accesso alla rete, per l'accesso a qualsiasi applicazione che lo preveda e per lo screen saver.
3. Non è consentita l'attivazione o la modificazione della password di accensione (bios).
4. Il Responsabile del Sistema Informativo, per l'espletamento delle funzioni e mansioni assegnate, ha la facoltà di monitorare lo spazio occupato dalle caselle di posta elettronica sul server e informare gli utilizzatori circa l'opportunità di liberare spazio, cancellando alcuni messaggi, quando lo spazio libero si approssima a zero.
5. Non è consentito installare autonomamente programmi provenienti dall'esterno senza la preventiva autorizzazione del Responsabile del Sistema Informativo ed una richiesta scritta da parte del responsabile dell'unità organizzativa cui è assegnato il PC. In caso di necessità di acquisto o dotazione di software applicativi e/o procedure pertinenti esclusivamente alcune Aree/Servizi ed i relativi dirigenti/responsabili, deve essere comunque sempre richiesta per iscritto l'autorizzazione preventiva da parte del Responsabile del Sistema Informativo, per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti. Sussiste infatti il grave pericolo di introdurre involontariamente virus informatici o di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi.
6. Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dal Responsabile del S.I. (d.lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 su nuove norme di tutela del diritto d'autore).
7. Non è consentito all'utente ed ai dirigenti/responsabili modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso, le configurazioni delle reti LAN/WAN presenti nelle sedi e la configurazione del Browser per la navigazione, salvo autorizzazione esplicita del Responsabile del Sistema Informativo.

8. È responsabilità del dirigente/responsabile di Servizio verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.
9. Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Si sottolinea che, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere sempre attivato lo screen saver e la relativa password.
10. Non è consentita l'installazione sul proprio PC o il collegamento sulla rete LAN di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, PC portatili, telefoni cellulari, PDA ed apparati in genere), se non con l'autorizzazione espressa del Responsabile del Sistema Informativo, previa richiesta scritta da parte del dirigente/responsabile dell'unità organizzativa cui è assegnato il PC o il segmento di rete LAN.
11. Agli utenti incaricati del trattamento dei dati sensibili è fatto obbligo di distruggere eventuali copie di sicurezza o supporti di tipo removibile (floppy, CD-Rom, Nastri) qualora non sia possibile rendere irrecuperabili i dati in essi contenuti. Ai sensi del Dlgs 196/03 e successive modificazioni ed integrazioni, è fatto divieto di divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati dell'ente se non disciplinate da appositi protocolli di intesa.
12. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile del Sistema Informativo nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 9 relativo alle procedure di protezione antivirus.
13. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
14. È vietato rimuovere, danneggiare deliberatamente o asportare componenti hardware.
15. È vietato accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici.
16. Il personale è tenuto ad osservare le direttive del Responsabile del Sistema Informativo volte a garantire il corretto funzionamento delle procedure di backup. I dati, documenti o file creati o modificati attraverso le applicazioni di produzione individuale (– es. office o open-office - devono essere salvati solo sui supporti appositamente destinati sui servers (unità di rete con cartelle dedicate agli uffici). Tale disposizione può essere derogata, su disposizione del dirigente/responsabile di servizio, solo per motivi tecnici.
17. È vietato utilizzare gli strumenti informatici dell'ente al fine di custodire, far circolare o promuovere materiale pubblicitario personale, codice maligno (virus, trojan horses, programmi pirata o altre porzioni di codice maligno e/o altro materiale non autorizzato).
18. È vietato copiare o mettere a disposizione di altri materiale protetto dalla legge sul diritto d'autore (documenti, files musicali, immagini, filmati e simili) di cui l'Azienda non abbia acquisito i diritti.

2. Utilizzo della rete

1. Hanno diritto ad accedere alla rete dell'Azienda tutti i dipendenti, le ditte fornitrici di software e/o servizi per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.
2. 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 potranno essere svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore del Sistema. Al fine di garantire la corretta gestione delle politiche di sicurezza delle informazioni è fatto divieto di replicare su dischi locali dei PC dati aziendali, banche dati e documenti sensibili senza esplicita autorizzazione del Responsabile del Sistema Informativo e senza l'adozione di adeguate politiche di sicurezza, quali la criptazione dei dati stessi e l'adozione di politiche di backup comprensive della dotazione di idonei archivi protetti.

3. Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con nomi utente diversi dal proprio.
4. Il Responsabile del Sistema Informativo può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
5. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
6. Non è consentito ai Dirigenti/Responsabili collegare reti di PC od altri dispositivi alla rete aziendale senza la preventiva autorizzazione scritta dell'Amministratore di Sistema ed una verifica della conformità agli standard tecnici presenti.
7. È vietato agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.
8. È vietato agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori).
9. È vietato fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.).
10. È vietato installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (per esempio, virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p).
11. È vietato monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere, copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita.
12. È vietato usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete.

3. Gestione delle Password

1. Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal Responsabile del Sistema Informativo. É consentita comunque l'autonoma modifica da parte degli utenti.
2. Occorre adottare le necessarie cautele per mantenere segrete le password. Esse sono infatti strettamente personali, non devono in nessun caso essere comunicate ad altri (per es. non devono essere scritte su post-it affissi al monitor o sotto la tastiera, non devono essere date a colleghi prima di assenze o periodi di ferie, salvo quanto disposto al successivo paragrafo 7 comma 8) in quanto ogni utente è responsabile della sicurezza della propria password.
3. Le password devono essere lunghe almeno 8 caratteri, (salvo impedimenti tecnici delle applicazioni), formate da lettere (maiuscole e/o minuscole), numeri e caratteri speciali quali & % ^ # $, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (per es. nomi/date di nascita e simili).
4. Le password utilizzate dagli incaricati al trattamento hanno una durata massima di 3 mesi, trascorsi i quali le password devono essere sostituite.
5. La password deve essere immediatamente sostituita nel caso si sospetti che la stessa abbia perso la segretezza.
6. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile Sistema Informativo o all'Amministratore del Sistema.
7. È dato incarico ai dirigenti/responsabili di comunicare tempestivamente e in forma scritta eventuali cambi di mansione di loro collaboratori che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia al Servizio Risorse Umane che al Responsabile del Sistema Informativo, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password ove necessario.

4. Utilizzo di supporti dati esterni

1. Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) o unità disco rimovibili (chiavi usb o dischi esterni portatili) o supporti ottici (CD e DVD) contenenti dati sensibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
2. I supporti contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.
3. Non è consentito scaricare files, contenuti in supporti esterni, non aventi alcuna attinenza con la propria prestazione lavorativa.
4. Tutti i files di provenienza incerta, ancorché potenzialmente attinenti all'attività lavorativa, non devono essere utilizzati/installati/testati. Nel caso di effettiva necessità di impiego devono essere sottoposti ad un preventivo controllo ed alla relativa autorizzazione all'utilizzo da parte del Responsabile del Sistema Informativo.

5. Utilizzo delle stampanti

1. È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.
2. È buon a regola evitare di stampare documenti o file molto lunghi o ad alto contenuto grafico su stampanti comuni.

6. Utilizzo di PC portatili

1. L'utente è responsabile del PC portatile eventualmente assegnatogli dall'Amministratore del Sistema e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
3. I PC portatili utilizzati all'esterno (convegni etc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.
4. Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente dal Responsabile del Sistema Informativo. È vietato utilizzare le suddette connessioni all'interno delle sedi dell'Azienda se contemporaneamente connessi alla rete LAN.

7. Uso della posta elettronica

1. La casella di posta elettronica .....@aspgiovanni23.it, di tipo web-mail usufruibile accedendo al sito web dell'Azienda, assegnata all'ufficio e/o all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Si rammenta che i sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse; si raccomanda pertanto agli utenti di non inoltrare dati ed informazioni classificabili "sensibili" o "riservate" con questo mezzo.
2. È fatto assoluto divieto di utilizzare le caselle di posta elettronica .....@aspgiovanni23.it per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti la propria attività o funzione svolta per l'Azienda, salvo diversa ed esplicita autorizzazione.
3. È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
4. È obbligatorio controllare con il software antivirus i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

5. È vietato inviare catene telematiche (o di "Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore del Sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.
6. Vista l'enorme diffusione su internet di messaggi Spam e/o contenenti allegati potenzialmente pericolosi, è richiesto agli utenti di utilizzare il buon senso nell'apertura di messaggi e allegati. Messaggi in altre lingue, o provenienti da mittenti sconosciuti, o provenienti da mittenti conosciuti ma del tutto fuori luogo o totalmente inattesi, devono essere trattati come "pericolosi" e vanno eliminati o sottoposti all'attenzione del Responsabile del Sistema Informativo prima di essere aperti.
7. In caso di assenza programmata dal servizio, l'utente deve utilizzare l'apposita funzionalità del sistema che consente di inviare automaticamente un messaggio di risposta che avvisa il mittente dell'assenza del destinatario, indicando eventualmente, in accordo con il dirigente/responsabile dell'Ufficio, altre modalità di contatto.
8. In caso di previsione di assenza prolungata, oltre alla possibilità di attivare la procedura di cui sopra, l'utente, in accordo con il dirigente/responsabile dell'Ufficio, può delegare formalmente altro dipendente (fiduciario) a verificare il contenuto dei messaggi e ad inoltrare al dirigente/responsabile quelli ritenuti più rilevanti per lo svolgimento dell'attività lavorativa.
9. In caso di assenza prolungata o di assenza non programmata di un utente, il dirigente/responsabile dell'Ufficio può contattare il Responsabile del Sistema Informativo per far modificare l'autorizzazione di accesso sulla casella di posta dell'utente, per gestire la posta in entrata e garantire così il buon funzionamento e il proseguimento dell'attività aziendale.

8. Uso della rete Internet e dei relativi servizi

1. Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad Internet effettuato tramite elaboratori connessi alla rete è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (firewall, viruswall, antivirus, proxy server, etc.).
2. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
3. È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile del Sistema Informativo.
4. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dalla Direzione Generale o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.
5. È vietata ogni forma di registrazione a siti, mailing-list i cui contenuti non siano legati all'attività lavorativa.
6. È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta.
7. La Direzione Generale si riserva di applicare, per singoli e gruppi di utenti, politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
8. Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.

9. Protezione antivirus

1. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
2. Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.
3. Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:
   - sospendere ogni elaborazione in corso senza spegnere il computer
   - segnalare l'accaduto al Responsabile del Sistema Informativo.
4. Non è consentito l'utilizzo di floppy disk, CD-Rom, CD riscrivibili, nastri magnetici di provenienza ignota.
5. Ogni dispositivo magnetico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere consegnato all'Amministratore di Sistema.

MONITORAGGIO E CONTROLLI

1. L'Azienda ritiene che l'attività di prevenzione debba essere prevalente rispetto all'attività di controllo. Per questo si impegna a promuovere azioni di sensibilizzazione e di diffusione dei principi e delle regole corrette per l'utilizzo degli strumenti informatici (ad esempio tramite comunicazioni interne e la predisposizione di opuscoli informativi) e con attività formative mirate.
2. L'Azienda si avvale di sistemi di controllo che hanno la finalità di:
   - garantire la sicurezza nel trattamento dei dati e nell'uso della dotazione informatica e non mirano ad un controllo a distanza nei confronti dei lavoratori.
   - rilevare eventuali danni patrimoniali già posti in essere, ma anche agire quale deterrente rispetto a comportamenti impropri e potenzialmente dannosi che, se non sottoposti a controlli, potrebbero comportare responsabilità patrimoniali dirette a carico dell'Ente.
3. I controlli predisposti saranno comunque improntati al rispetto dei principi di necessità, proporzionalità, imparzialità, trasparenza e protezione dei dati.
4. I controlli potranno essere di due tipi: periodico casuale e puntuale.
   - **Periodico casuale:** a verifica dell' efficacia delle misure di sicurezza saranno effettuati controlli a campione con cadenza trimestrale. La scelta del/dei clients su cui effettuare i controlli si basa sul numero che identifica univocamente ogni client inserito nel database dell'hardware aziendale, selezionato tramite un generatore di numeri casuale.
   - **Puntuale:** a seguito di problemi di sicurezza riscontrati sulla rete interna, potranno essere effettuati controlli su specifici clients, con lo scopo di isolare velocemente la causa del problema e ripristinare la funzionalità del client, salvaguardando i dati in esso contenuti.
5. Le attività sull'uso del servizio di accesso ad internet vengano automaticamente registrate in forma elettronica attraverso il firewall, nel rispetto delle disposizioni di legge in materia e automaticamente cancellate dopo sei mesi.
6. Le registrazioni sono mantenute presso il Servizio Informatico dell'Azienda.
7. I dati delle registrazioni possono essere trattati in forma anonima per esecuzione di statistiche sull'utilizzo dei servizi.
8. Il trattamento dei dati contenuti nei LOG può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.
9. I dati anonimi aggregati, riferibili all'intera Azienda e/o a sue Aree, sono a disposizione del Direttore Generale per le valutazioni di competenza e riguardano:
   - per ciascun sito/dominio visitato le seguenti informazioni: il numero di accessi, il traffico generato suddiviso per fasce orarie ed il numero di utenti che lo visitano.
10. Nel caso sia riscontrato un utilizzo anomalo di internet, quali ad esempio a titolo meramente esemplificativo:

- l'utilizzo in orario non compatibile con gli orari di servizio,
- la consultazione di siti ritenuti non attinenti con l'attività lavorativa in relazione al loro contenuto o perché la modalità o la frequenza di consultazione lasci presumere un utilizzo a fini personali

l'Azienda provvederà a:

- diffondere un avviso 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 all'Ufficio/Settore/Servizio/Reparto in cui è stata rilevata l'anomalia;
- effettuare controlli circoscritti su singole postazioni di lavoro, in caso di successivo permanere di una situazione non conforme.

11. I controlli sulla navigazione Internet potranno estendersi al massimo ai dati relativi ai tre mesi precedenti quello dell'effettuazione del controllo.
12. I dati personali contenuti nei LOG possono essere trattati in via eccezionale e tassativamente nelle seguenti ipotesi:
    - per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria.
    - su richiesta del Direttore Generale quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento.
13. I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a tre mesi e sono periodicamente cancellati automaticamente dal sistema.
14. I dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi e per il controllo del rispetto delle licenze regolarmente acquistate.
15. Le comunicazioni effettuate attraverso il servizio di posta elettronica sono riservate. Il contenuto di tali comunicazioni non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte dell'Azienda o da parte di altri soggetti.

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

1. È obbligatorio attenersi alle Istruzioni Operative allegate alla lettera di nomina ad "incaricato" consegnate ad ogni dipendente e al Documento Programmatico sulla sicurezza (DPS) adottato dall'ASP e aggiornato con cadenza annuale che è possibile consultare collegandosi a Pubblica\Privacy\DPS regolamento dati sensibili

VIOLAZIONI

1. Il mancato rispetto o la violazione delle regole contenute nel presente Disciplinare è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.
2. Il dipendente e l'utilizzatore deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche, ai principi e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni" D.M. 28.11.2000 allegato al CCNL 22.01.2004.

Il presente disciplinare viene consegnato a ciascun dipendente/utilizzatore dell'ASP Giovanni XXIII, che firma per ricevuta.

Sarà affisso nelle bacheche aziendali in formato cartaceo ed inserita in formato elettronico nella rete intranet.

Dichiarazione di assunzione di responsabilità per l'accesso a Internet dalle postazioni aziendali

(Dichiarazione da sottoscrivere e trasmettere al Servizio Risorse Umane)

Il sottoscritto, firmando il presente documento, riconosce di aver letto, compreso ed accettato integralmente la Disciplina Aziendale in materia di Utilizzo degli Strumenti Informatici consegnata;

Nome e Cognome: _____

Servizio/Settore/ Struttura/ Reparto: _____

Firma: _____

- o Acconsente al trattamento dei dati personali (D. Lgs n. 196/2003)
- o Non acconsente al trattamento dei dati personali
  (in caso di rifiuto al trattamento dei dati personali, il collegamento a Internet sarà disabilitato, con esclusione del sito aziendale, della posta elettronica se prevista)

Firma: _____

Data : _____