REGOLAMENTO ORGANIZZATIVO PER L'UTILIZZO DEI SERVIZI DI RETE INTRANET, INTERNET, POSTA ELETTRONICA, SOFTWARE E HARDWARE.

Motivazioni:

Negli ultimi tempi il Comune di Ospedaletti ha visto aumentare il numero dei servizi informatizzati, con la conseguente necessità di maggiori accessi ad Internet ed in ultimo la realizzazione dell'interconnessione di tutti i personal computers e quindi l'accesso alla rete Intranet interna.

Tutto questo ha avuto importanti ricadute sui problemi di sicurezza.
Si rende quindi necessario attivare una serie di norme, restrizioni e controlli per garantire la sicurezza dei sistemi e definire le responsabilità degli utilizzatori delle risorse nel rispetto del testo unico sulla privacy e del documento programmatico sulla sicurezza (DPS). L'adozione di queste politiche viene fatta nell'intento di:

- garantire la massima efficienza delle risorse informatiche e del loro utilizzo;
- garantire la riservatezza delle informazioni e dei dati;
- provvedere ad un servizio continuativo nell'interesse dell'Ente;
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche;
- garantire la massima sicurezza nello scambio di dati ed informazioni tra il Comune di Ospedaletti e le altre istituzioni.

E' compito dell'Ente:

- adottare tutti i dispositivi di sicurezza necessari a difendere i propri sistemi informatici;
- implementare meccanismi di controllo e monitoraggio per evitare intrusioni o abusi, anche mediante installazione di firewall, capaci di monitorare, impedire ed interrompere, se del caso, accessi e uscite sulle porte aperte del sistema durante la connessione ad una rete oppure on-line;
- responsabilizzare e formare gli utenti circa i rischi penali, civili, amministrativi connessi all'uso indebito dei mezzi informatici o alla riproduzione non autorizzata di software;
- evitare che i propri utenti, utilizzando gli strumenti informatici dell'Ente, compiano abusi legati all'utilizzo improprio delle risorse della Rete Internet ed Intranet e dei dati ivi contenuti.

Definizioni:

1) Ai fini dell'applicazione del presente Regolamento deve intendersi:

   a) Per Codice della Privacy (CP)
   Decreto Legislativo 30 giugno 2003 n. 196 e successive modifiche ed integrazioni

   b) Per Codice dell'Amministrazione Digitale (CAD)
   Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche ed integrazioni

   c) per Sistema Informatico del Comune di Ospedaletti (SIC)
   "L'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, computers, stampanti utilizzate dai dipendenti e dagli amministratori comunali, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in do-

tazione ed uso all'Amministrazione Comunale di Ospedaletti";

d) per utente:
"Chiunque, dipendente o amministratore, utilizzi un elaboratore collegato alla rete intranet del Comune di Ospedaletti, sia che il collegamento avvenga in rete locale, come avviene all'interno dell'edificio comunale, sia che si tratti di un accesso remoto, come avviene nei collegamenti via modem e/o ADSL (uffici esterni)."

f) Amministratore di sistema:
vedi art. 5);

e) per Amministratore di rete:
vedi art. 6);

g) Amministratore di Banche Dati (database):
vedi art. 7);

h) Webmaster o Amministratore di siti web
"soggetto" incaricato della manutenzione e dello sviluppo del sito web. Al webmaster non sono attribuite funzioni di carattere editoriale.

2) Al fine di consentire una più agevole comprensione dei termini prettamente tecnici e/o informatici contenuti nel presente Regolamento, si rinvia al glossario di cui all'allegato A.

Finalità:

1) Le apparecchiature informatiche, i programmi, e tutte le varie funzionalità che l'Amministrazione Comunale di Ospedaletti mette a disposizione dei suoi utenti al fine di usufruire dei servizi di rete, e in particolar modo dei servizi di tipo Internet/Intranet/Posta elettronica sia esterna che interna, devono essere utilizzate nel pieno rispetto delle norme del presente Regolamento al fine di evitare possibili danni erariali, finanziari e di immagine all'Ente stesso.

2) Tutto il personale interessato dalle disposizioni del presente Regolamento, è tenuto a contattare l'amministratore di sistema prima di intraprendere qualsiasi attività non esplicitamente compresa nelle disposizioni che seguono, al fine di garantire che tali attività non siano in contrasto con gli standard di sicurezza informatica stabiliti dall'Ente.

Capo I - Criteri di carattere generale

Art. 1 - Accesso alle risorse del sistema informatico comunale (SIC).

1) l'accesso alle risorse della Rete aziendale è riservato agli utenti;

2) ogni risorsa informatica collegata alla Rete è affidata ad un utente che acquisisce lo status di responsabile per la gestione e l'utilizzo della risorsa stessa. Qualora l'utente debba accedere a Internet ed Intranet tramite la rete dell'Ente o utilizzare una risorsa informatica, deve adeguarsi alle prescrizioni del presente regolamento;

3) L'amministratore di sistema potrà accedere alla risorsa informatica dell'utente per compiti di monitoraggio, controllo e/o aggiornamenti della configurazione di rete, ai fini della sicurezza del sistema e della rete, nel rispetto della presente politica di gestione e della riservatezza dei dati personali (ai sensi del Codice della Privacy), sentito il Direttore Generale ed il Responsabile del servizio Internet/Intranet/Sito Internet. Gli accessi effettuati dall'amministratore di sistema sono registrati in appositi logs a disposizione dell'Amministrazione Comunale per gli scopi consentiti dalla vigente normativa in materia.

Art. 2 - Utilizzo delle risorse informatiche e reti

1) Le risorse informatiche del Comune di Ospedaletti devono essere utilizzate esclusivamente per le attività istituzionali. Non è consentito l'uso per fini personali (art. 10, comma 3, del Codice di comportamento dei dipendenti di cui al Decreto del Ministro della Funzione Pubblica del 28.11.2000).

2) Sono tassativamente vietate e perseguibili amministrativamente, civilmente ed in taluni casi, anche penalmente le seguenti attività:
   - accedere a siti ed acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
   - 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
   - compiere attività che possono rappresentare una violazione della legge in materia di Copyright;
   - effettuare copie non autorizzate di software, CD 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;
   - ogni altra attività illegale per norma di legge.

Art. 3 - Responsabilità degli utenti.

1) L'utente non può in alcun caso modificare la configurazione di rete, non può effettuare manomissioni o interventi sulle apparecchiature di rete o sui programmi gestionali di rete, non formalmente autorizzati dall'amministratore di sistema, al quale deve comunicare tempestivamente le necessità di interventi su apparecchiature e programmi in ordine alla corretta prestazione dei servizi;

2) deve prestare attenzione nel caso in cui intenda installare o rimuovere software che lo stesso non vada ad influire sulle prestazioni della rete;

3) Ai sensi del Codice della Privacy e del CAD e delle normative e disposizioni legistrative ad essi collegati, l'accesso alla risorsa informatica è personale e vi si accede tramite nome utente e password di identificazione. L'accesso non può essere condiviso o ceduto. I tenutari del nome utente e della password devono comunque comunicare all'Amministratore di Sistema il nominativo degli Amministratori, Responsabili di Servizio o altri dipendenti che ne vengono messi a conoscenza per motivi di servizio. L'utente può accedere alle risorse informatiche dell'Ente condivise nell'ambito del servizio di appartenenza, anche da altre postazioni purché per la connessione utilizzi le credenziali a lui attribuite;

4) la password è personale e non cedibile o trasmissibile a terzi, ad eccezione di quanto riportato al precedente punto 3). E' fatto divieto a ciascun utente di divulgare, per fatto imputabile a lui direttamente o indirettamente, password, login e comunque chiavi di accesso riservate, le quali vanno conservate in luogo sicuro e non accessibile ad altri. Se smarrite, va fatta immediata segnalazione al segretario comunale e richiesta di sostituzione all'amministratore di sistema;

5) gli utenti 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;

6) gli utenti sono obbligati a segnalare immediatamente al Segretario Comunale, al proprio Responsabile del servizio ed all'amministratore di sistema ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza. Al quinto tentativo di violazione o inadempimento di quanto riportato ai precedenti punti, il sistema automatico di sicurezza della rete, procederà al distacco temporaneo dell'utente dal collegamento ad internet ed intranet. L'Amministratore di Sistema ne darà comunicazione al Segretario Comunale ed al Responsabile del Servizio Intranet/Internet per l'eventuale accertamento di responsabilità disciplinari da parte dell'utente.;

7) gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive dell'amministratore di sistema divulgate tramite e-mail o bollettini.

8) I Responsabili dei servizi sono tenuti a:
   a) informare il personale sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo dell'Ente;
   b) assicurare che il personale a loro assegnato si uniformi alle regole ed alle procedure descritte nel presente Regolamento;
   c) adempiere, qualora assumano lo "status" di responsabili del trattamento dei dati, a tutti gli obblighi inerenti la titolarità loro affidata in materia di trattamento di dati personali gestiti dal Comune, come previsto dal Codice della Privacy) e quant'altro in materia.

Art. 5 - Amministratore di sistema: competenze, nomina e responsabilità

a) Definizione

Per amministratore di sistema si intende , in ambito informatico, la figura professionale finalizzata alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti. Sono equiparate ad amministratore di sistema le figure professionali incaricate della gestione dei rischi concernenti la protezione dei dati, quali amministratori di basi di dati, amministratori di rete e di apparati di sicurezza e gli ammini-

stratori di sistemi software complessi.

b) Requisiti per la nomina

L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice della Privacy, il titolare e il responsabile devono attenersi comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29 del predetto Codice della Privacy.

c) Designazione

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Viene designato direttamente dal Sindaco mediante proprio provvedimento. La nomina ha carattere di assunzione di responsabilità ed è valida fino a revoca e/o decadenza del Sindaco per cessazione della carica o altri motivi indicati nello Statuto Comunale.

d) Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza redatto ai sensi dell'allegato B) al D. Lgs. 196/2003 (Codice della Privacy).

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, il titolare del trattamento dei dati, identificato nella figura del Sindaco, nella qualità di datore di lavoro è tenuto a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito del Comune di Ospedaletti, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell'informativa resa agli interessati ai sensi dell'art. 13 del Codice della Privacy nell'ambito del rapporto di lavoro che li lega al titolare utilizzando strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un'eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

e) Verifica delle attività

L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

f) Registrazione degli accessi

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'e-

vento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

g) **Responsabilità**
L'Amministratore di sistema è direttamente responsabile dei sistemi a lui affidati ed individuati come quelli installati nei locali adibiti a CED del Comune di Ospedaletti. Per le macchine non ubicate nei locali CED la responsabilità di amministratore di sistema ricade totalmente in capo al responsabile di posizione organizzativa in cui le risorse hardware e software sono installate.

Art. 6 - Amministratore di rete

L'Amministratore di rete ha il compito di sorvegliare l'attività della rete, di intervenire rapidamente in caso di congestione o di problemi di accesso. Deve inoltre avere una conoscenza approfondita di tutte le apparecchiature di rete, dei diversi protocolli di comunicazione e delle differenti architetture di rete.
E' inoltre incaricato della gestione degli account degli utenti, dalla loro creazione all'arrivo di nuovo personale fino alla loro distruzione alla loro partenza. In più, tenendo conto della rapida evoluzione delle tecnologie e dei supporti di trasmissione, l'amministratore di rete deve assicurare un controllo permanente per far evolvere l'infrastruttura di rete dell'Ente.
In collaborazione con il responsabile della sicurezza informatica (se nominato), l'amministratore di rete è incaricato di attuare i dispositivi di protezioni appropriati, di sorvegliare i log delle attività e controllare le allerte di sicurezza. Per anticipare tutti i potenziali rischi, dovrà mettere a punto un piano di recupero che definisca le azioni da intraprendere per ristabilire l'accesso il prima possibile, nel rispetto della politica di sicurezza informatica dell'Ente.

In dettaglio l'amministratore di rete ha il compito di:

a) monitorare i sistemi per individuare un eventuale uso scorretto degli stessi, nel rispetto della privacy degli utenti;
b) segnalare prontamente al Segretario Comunale ed al proprio Responsabile del servizio, ogni eventuale attività non autorizzata sui sistemi.
c) Segnalare al proprio responsabile del servizio, nel caso in cui l'amministratore di rete non sia nominato responsabile di posizione organizzativa, la necessità di eventuali acquisti di hardware e/o software occorrenti al funzionamento della rete.
d) L'amministratore di sistema è obbligato a 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 e dell'Amministrazione Comunale a fronte di ipotesi di reato;
e) fornire periodicamente report contenenti dati aggregati relativi all'andamento del traffico, ai picchi anomali settoriali, alla statistica generale di accesso ai siti più frequentati;
f) può revocare l'accesso temporaneo alla risorsa informatica e di rete, sentito il Segretario Comunale e al Responsabile del Servizio Intranet/Internet qualora questo sia utilizzato impropriamente o in violazione delle leggi vigenti;
g) potrà altresì interrompere temporaneamente la prestazione del servizio in presenza di motivati problemi di sicurezza, riservatezza o guasto tecnico, dandone tempestiva comunicazione all'utente.
h) L'amministratore di rete 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, supporto – qualora richiesto – e controllo, quest'ultimo quando richiesto dall'Amministrazione Comunale o dal Responsabile del servizio.
i) può essere tenuto alle prestazioni lavorative anche in ore notturne e durante i giorni

festivi, con i trattamenti retributivi ed i turni previsti dai contratti collettivi (art. 11, c. 3, D. Lgs n. 39/1993).

Art. 7 - Amministratore di database

L'amministratore di database detto anche responsabile di database o amministratore di banche di dati è incaricato della manutenzione e lo sviluppo dei database che costituiscono il sistema informatico aziendale.

a) Competenze

Tenendo in considerazione l'importanza dei dati di cui è incaricato, l'amministratore di database deve possedere una solida esperienza in Informatica con una buona conoscenza dei principali DB (sistemi di gestione di database), del linguaggio SQL, che permetta la loro consultazione e allo stesso tempo di conoscere alcuni linguaggi di programmazione, affinché possa essere capace di automatizzare determinati compiti.

La sua responsabilità lo rendono garante dell'integrità del sistema informatico della Ente. Inoltre, le conoscenze specializzate del DB potranno essere necessarie per ottimizzare le richieste, i parametri del DB o per mettere a punto degli strumenti di supervisione di accesso alle basi.

L'Amministratore di database potrà anche operare a supporto degli utenti delle applicazioni clienti o ai gruppi di sviluppo per risolvere situazioni di blocco, consigliarli o aiutarli all'elaborazione di richieste complesse.

In collaborazione con il Responsabile di sicurezza, l'amministratore di database dovrà predisporre delle strategie e delle procedure di salvataggio e ripristino dei dati per assicurare la perennità dei dati di cui è incaricato.

Oltre alle competenze di natura tecnica, l'amministratore di database deve avere una buona conoscenza delle applicazioni della società e essere capace di capire i bisogni degli utenti per realizzare o modificare un database. In linea di principio, possiede una capacità in materia di progettazione di sistemi informatici e di modelli UML..

Art. 8 - Titolarità

1) L'Amministrazione Comunale è titolare di tutte le risorse informatiche dell'Ente. Il personale dipendente e/o assimilato dovrà essere informato su quali siano gli usi consentiti e proibiti di tali risorse.

2) Ogni infrazione alle regole dell'Ente per un uso corretto del sistema informatico. costituirà una violazione della sicurezza ed esporrà l'utente ai provvedimenti previsti in tali casi, come meglio esplicitato all'articolo 33 del presente regolamento.

Art. 9 - Responsabile della sicurezza informatica - del backup e ripristino dati

Al responsabile della sicurezza informatica, del backup e ripristino dati sono affidati i compiti di:

a) elaborazione delle regole per un utilizzo ragionevolmente sicuro del sistema informativo;
b) implementazione delle policy di sicurezza sul sistema informatico;
c) predisposizione del materiale informativo e divulgativo in materia di sicurezza informatica.
d) segnalare prontamente al segretario comunale/direttore generale ogni eventuale attività non autorizzata sui sistemi.
e) Effettuare le copie dei dati contenuti sui sistemi di rete verificando il corretto ripristino in caso di necessità

Art. 10 - Nomine cumulative

In considerazione delle dimensioni dell'Ente, valutati i benefici e le politiche di sicurezza informatica e gestionali, è possibile nominare un'unica persona amministratore di sistema, di rete, di basi di dati e responsabile della sicurezza informatica.

I suddetti incarichi possono essere affidati in toto od in parte a ditte specializzate o tecnici esterni secondo la vigente normativa in materia di incarichi esterni e di rispetto della sicurezza informatica e del trattamento dei dati.

Art. 11 - Centralizzazione delle risorse

Al fine di razionalizzare la gestione delle risorse hardware e software, nonché umane, viene stabilito che i server di rete, le banche dati e le procedure operative deputate alla gestione, vengano unificate in un unico locale.

Art. 12 - Diritto di accesso.

1) Hanno diritto di accesso ai servizi di rete erogati dal Comune di Ospedaletti, il personale dipendente dell'Ente, Amministratori e Consiglieri Comunali;

2) Le modalità di accesso ai servizi variano a seconda del tipo di utente. Richiedono in ogni caso l'assegnazione di password personali e segrete di accesso;

3) l'autorizzazione di accesso viene rilasciata dall'Amministratore di Sistema;

4) l'accesso ai servizi di rete deve essere compatibile con le direttive di sicurezza;

5) sono consentite le attività non in contrasto con l'attività istituzionale dell'Ente.

Art. 13 - Intervento di tecnici esterni

1) I tecnici di ditte esterni, incaricati dai singoli responsabili di servizio, diinterventi hardware o software sulle macchine in dotazione, prima di procedere alla configurazione delle macchine od installazione di software, devono informarsi presso l'Amministratore di sistema riguardo la compatibilità degli interventi con le risorse hardware e software della rete..

2) In caso di interventi che comportino l'eventuale sostituzione di cavi, connessioni o apparati di rete è necessario il preventivo benestare dell'Amministratore di Sistema che provvederà alla sconnessione fisica del tratto di rete interessato dagli interventi fino alla conclusione degli interventi stessi.

Art. 14 - Copie di backup

1) Il sistema di rete è predisposto per la copia automatizzata, ad orari prestabiliti, dei dati contenuti nel server principale. Tale copia viene effettuata su idoneo supporto informatico in formato criptato e conservata in armadi idonei alla conservazione di supporti informatici. Un'ulteriore copia dei dati può essere conservata, all'esterno dell'ente, a cura del responsabile del backup

2) L'utente, ove non utilizzi il sistema automatico di archiviazione di rete, si impegna ad effettuare backups periodici del proprio lavoro su supporti magnetici e/o su dispositivi di proprietà dell'Amministrazione. Non è consentito effettuare backups aggiuntivi su dispositivi e/o punti di memorizzazione diversi da quelli di cui sopra. Periodicamente potranno essere disposti, dal titolare del trattamento, verifiche campione della corretta esecuzione delle copie dei dati. In caso di inadempienza si procederà con l'applicazioni di sanzioni disciplinari o amministrative secondo la gravità del caso.

3) E’ ammessa la conservazione di sicurezza delle copie di backups, protette con idonei sistemi di crittografia, a cura del Responsabile del Servizio interessato all’esterno dell’ente, previa comunicazione scritta, al Segretario Comunale/Direttore Generale e per conoscenza all’Amministratore di Sistema, del luogo e delle modalità di conservazione. In caso di smarrimento e/o furto deve procedere ad immediata denuncia presso l’Autorità Giudiziaria al Sindaco ed al Segretario Comunale/Direttore Generale.

4) Nel caso di uso improprio delle copie di backups, conservate all’esterno, o di discordanza dei dati in esse contenuti, l’Amministrazione Comunale si riserva di adottare i necessari provvedimenti..

5) Per la sicurezza dei dati informatici gli uffici redigono il Documento Programmatico sulla Sicurezza di cui al D. Lgs. 30.06.2003 n. 196.

6) Il responsabile della sicurezza dei dati non è imputabile per la perdita o danneggiamento di dati ospitati sui singoli pc o i cui archivi non sono ospitati sui server di rete e per i quali non è stato effettuato il backup o le procedure di ripristino non funzionino.

Capo II - Internet

Art. 15 - Finalità e obiettivi

1) Il servizio internet ha l'obiettivo primario di favorire la comunicazione verso l'esterno, oltre che favorire il reperimento e la divulgazione di informazioni utili per lo svolgimento della propria professione.

2) In particolare il servizio internet si articola nelle seguenti finalità:
   a) consentire l'accesso alla rete internet World Wide Web da parte degli utenti del Comune di Ospedaletti preventivamente autorizzati;
   b) consentire l'utilizzo di posta elettronica verso l'esterno da parte degli utenti del Comune di Ospedaletti;
   c) permettere la gestione di un sito ufficiale del Comune, rivolto al pubblico, cui possono accedere gli utenti di internet;
   d) permettere la pubblicazione sul sito ufficiale del Comune di raccolte di informazioni, documenti e dati;

Art. 16 - Accesso ad internet

1) L'accesso ai siti pubblici disponibili su Internet, a consultazione gratuita, è consentito per consultare documenti, informazioni e dati che risultino utili ai fini della propria attività istituzionale;

2) Il sistema informatico di gestione all'accesso internet è configurato in modo tale che l'accesso sia ristretto ai soli utenti autorizzati alla navigazione, e possa avvenire soltanto da postazioni di lavoro abilitate alla navigazione.

3) All'interno dell'edificio comunale l'accesso è consentito esclusivamente tramite i personal computers regolarmente collegati alle prese di rete. L'uso di sistemi wireless è consentito esclusivamente dietro autorizzazione dell'Amministratore di Sistema che fornirà le password di accesso dopo aver verificato le effettive necessità di collegamento alla rete;

4) Al fine di garantire l'accesso ad internet ad utenti esterni in occasione di eventi, riunioni, ecc., presso il palazzo comunale e la biblioteca civica è installato un sistema di connessione wireless mediante rilascio di ticket di accesso di durata variabile comunque non oltre le nove ore giornaliere.

5) Gli utenti sono tenuti ad utilizzare il collegamento ad Internet unicamente per motivi legati ai propri doveri di ufficio. Sono pertanto vietati
   - l'uso di Internet per lo scarico di file del tipo MP3, AVI, MPG, Quicktime, e/o altri tipi di files o programmi per la fruizione di contenuto audio/video non legati ad un uso d'ufficio se non per motivate esigenze istituzionali e per particolari servizi;
   - l'uso e la navigazione su siti non legati ad esigenze esclusivamente di tipo lavorativo. A tal fine l'Amministratore di Sistema, su richiesta dell'Amministrazione Comunale, verificate le effettive condizioni, provvederà ad inibire la consultazione dei siti web non utili alla produttività dell'Ente e, soprattutto, potenzialmente lesivi per l'infrastruttura;
   - l'accesso a siti di social networking, voip o chat di qualunque natura, il cui accesso non sia richiesto da precise disposizioni legislative e solo dietro motivata richiesta all'amministratore di rete da parte del responsabile del servizio interessato;
   - l'accesso alla rete internet è disponibile tutti i giorni lavorativi dalle ore 7 alle ore 20. In caso di necessità il responsabile della sicurezza informatica, d'accordo con i re-

sponsabili di servizio, indicherà un orario alternativo per la concessione del servizio di accesso ad internet;

- l'utilizzo di qualsiasi mezzo alternativo (modem o altro) al collegamento Lan dell'Ente per connettersi ad Internet;
- l'accesso alla rete dall'esterno via modem o con qualsiasi altro mezzo di accesso remoto senza l'autorizzazione del responsabile della sicurezza informatica;
- lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo.
- Effettuazione di collegamenti ad Internet ed attivazione di caselle di posta elettronica, avvalendosi di attrezzature e/o abbonamenti personali, da qualsiasi postazione all'interno dell'Ente. Per la consultazione della posta personale è ammesso l'utilizzo di servizi di web mailing o analoghi;

Art. 17 - Autorizzazioni

1) Sono autorizzati all'uso del servizio Internet tramite le connessioni di rete interne:
   - il personale amministrativo adibito all'uso di un personal computer;
   - il Segretario Comunale;
   - tutti i componenti dell'Amministrazione Comunale;
   - l'amministratore di sistema;
   - consulenti esterni previa autorizzazione del Responsabile del Servizio Intranet/Internet/Sito e a seguito di autenticazione nel sistema a cura dell'Amministratore di Sistema;

Art. 17 - Documentazione dell'attività di navigazione

3) l'accesso ai siti internet da parte di un qualsiasi utente è documentato, per gli scopi previsti dalla Legge, automaticamente in un log, che riporta i dettagli della navigazione, che elenca i siti e i documenti che l'utente ha consultato;

4) i log sono memorizzati in modo protetto sul server di sistema e potranno eventualmente essere visionati da:
   - Segretario Comunale;
   - Titolare del trattamento dei dati (Sindaco);
   - Amministratore di sistema (solo per fini legati alla sicurezza informatica ed al miglioramento dell'efficienza della rete) ed esclusivamente in forma anonima aggregata e solo per scopi statistici;
   - Autorità giudiziaria.

5) I logs sono conservati per il periodo minimo di sei mesi e non sono assolutamente modificabili o accessibili da parte degli utenti.

6) Della presenza dei logs vengono informate le rappresentanze sindacali unitarie.

Capo III - Intranet

Art. 18 - Finalità

1) Le finalità del servizio intranet sono:
   a) semplificazione e potenziamento delle modalità di comunicazione ed informazione interna su oggetti, temi ed attività la cui conoscenza sia funzionale al miglior svolgimento dell'attività dell'Amministrazione Comunale nel caso sia utile dare notizia interna e soprattutto sull'attività dei singoli servizi con particolare riguardo sia alle procedure concernenti l'elaborazione di atti normativi e di indirizzo, sia alle procedure concernenti l'attività amministrativa e gestionale. Pertanto, lo scopo della rete intranet è quello di rendere più facile il reperimento di informazioni utili per lo svolgimento dei compiti istituzionali mediante l'attivazione di un unico "serbatoio di informazioni" dove viene semplificato, in virtù di un sistema digitale di gestione degli stessi, l'accesso ai dati e documenti di interesse comune;
   b) semplificare il coordinamento e gestione dell'iter formativo degli atti normativi e dei provvedimenti amministrativi di competenza del Comune, assicurando ad essi la massima trasparenza interna;
   c) favorire l'efficienza e l'economicità dell'attività amministrativa e della gestione, attraverso la semplificazione dei processi organizzativi interni, il rafforzamento della cooperazione tra gli uffici e la condivisione delle esperienze lavorative;
   d) creare e sviluppare sinergie e scambi di informazioni con il sito internet, agevolando il flusso di informazioni, al fine di offrire ai cittadini l'accesso ai documenti pubblici nonché l'interscambio di informazioni e dati con altre Pubbliche Amministrazioni;
   e) rappresentare il portale della comunicazione interna dell'ente.

Art. 19 - Autorizzazioni e accesso

1) Sono autorizzati all'uso del servizio intranet tramite le connessioni di rete interne:
   - tutto il personale amministrativo adibito all'uso di un personal computer;
   - il Segretario Comunale;
   - tutti i componenti dell'Amministrazione Comunale (Sindaco, Assessori e Consiglieri);

2) L'accesso avviene tramite password personale e nome utente. Gli utenti sono suddivisi per gruppi rispecchiando il servizio di appartenenza;

3) L'utente può accedere:
   - alla directory relativa al proprio servizio;
   - ai servizi condivisi di rete intranet;
   - alla directory di intescambio informazioni tra utenti.

4) La registrazione di un utente nel sistema è effettuata dall'Amministratore di Sistema contestualmente all'assegnazione della relativa casella di posta elettronica interna;

5) l'accesso alla rete intranet è disponibile tutti i giorni lavorativi dalle ore 7 alle ore 20.. In caso di necessità l'Amministratore di Sistema, d'accordo con i responsabili di servizio, indicherà un orario alternativo per la concessione del servizio;

Art. 20 - Documentazione dell'attività di navigazione

1) l'accesso alla rete intranet da parte di un qualsiasi utente è documentato automaticamente in un log, che riporta i dettagli della navigazione, che elenca tutte le operazioni e i documenti che l'utente ha consultato;

2) i log sono memorizzati in modo protetto sul server di sistema e potranno eventualmente essere visionati da:
   - Segretario Comunale;
   - servizio Titolare del trattamento dei dati (Sindaco);
   - Amministratore di sistema (solo per fini legati alla sicurezza informatica ed al miglioramento dell'efficienza della rete) ed esclusivamente in forma anonima aggregata e solo per scopi statistici;
   - Autorità giudiziaria.

3) I logs sono conservati per il periodo minimo di sei mesi e non sono assolutamente modificabili o accessibili da parte degli utenti.

4) Della presenza dei logs vengono informate le rappresentanze sindacali unitarie.

Art. 21 - Accesso dall'esterno alla rete intranet

1) L'accesso alle risorse del sistema intranet dall'esterno è consentito tramite VPN (virtual private network).

2) Su richiesta scritta ed assunzione di responsabilità, l'Amministratore di Sistema può, verificati i requisiti di sicurezza, concedere le credenziali di accesso alla rete VPN.

Capo IV - Posta elettronica

Art. 22 - Posta elettronica – utilizzo

1) L'invio e la ricezione di messaggi di posta elettronica (email) è consentito per lo scambio di comunicazioni e dati utili all'esercizio della propria attività sia all'interno che all'esterno dell'Ente;

2) Ai sensi della direttiva PCM 27 novembre 2003 "Impiego della posta elettronica nelle pubbliche amministrazioni", è istituita la casella di posta elettronica istituzionale avente per indirizzo: comune@comune.ospedaletti.im.it oppure comune @comune.ospedaletti.im.gov.it) la cui gestione è affidata al servizio protocollo;

Art. 23 - Posta elettronica – autorizzazioni

1) Sono autorizzati all'uso della posta elettronica con indirizzi riconducenti al dominio ufficiale dell'Ente :
   - i dipendenti del Comune;
   - il Segretario Comunale;
   - gli amministratori comunali in carica;

Art. 24 - Posta elettronica - attribuzione

1) Ai sensi della direttiva PCM 27 novembre 2003 "Impiego della posta elettronica nelle pubbliche amministrazioni" a tutti i dipendenti ed amministratori è attribuita una casella di posta elettronica ordinaria (anche quelli per i quali non sia prevista la dotazione di un personal computer) nel formato cognome.nome@comune.ospedaletti.im.it.

2) La casella di posta elettronica nominativa può essere utilizzata per:
   a. per richiedere o concedere ferie o permessi, richiedere o comunicare designazioni in comitati, commissioni, gruppi di lavoro o altri organismi, convocare riunioni, inviare comunicazioni di servizio ovvero notizie dirette al singolo dipendente (in merito alla distribuzione di buoni pasto, al pagamento delle competenze, a convenzioni stipulate dall'amministrazione ecc...), diffondere circolari o ordini di servizio;
   b. scopi istituzionali la comunicazione tramite email deve avvenire sulla casella istituzionale dell'ente o quella destinata alla gestione della posta elettronica certificata.

3) L'accesso alla casella di posta elettronica nominativa viene rilasciata dall'amministratore di sistema il quale attribuisce inizialmente una password (strettamente personale) assegnata in modo casuale e consegnata in busta chiusa ad ogni singolo dipendente.

4) La consultazione della casella è permessa, anche al di fuori dell'ente, mediante ricorso a sistemi di web mailing.

5) L'Amministrazione Comunale non può in alcun modo accedere al contenuto della posta elettronica nominativa e pertanto non si assume alcuna responsabilità penale o amministrativa per l'uso improprio di tali caselle il cui corretto utilizzo è di esclusiva competenza dell'assegnatario.

6) La casella di posta elettronica nominativa viene revocata, dall'Amministratore di sistema, alla cessazione, per qualsiasi motivo del dipendente o dell'amministratore. Verrà in ogni caso emesso un preavviso di sette giorni di cessazione della casella alla scadenza del quale ogni messaggio non letto verrà cancellato. Nel caso di cancellazione di una casella di

posta elettronica nominativa, gli eventuali messaggi in arrivo, per la durata di un anno, verranno dirottati automaticamente su una casella di posta elettronica di deposito, gestita dal responsabile del servizio informatico, il quale provvederà a stamparli ed inviarli al recapito del dipendente o amministratore cessato dal lavoro o dalla carica.

Art. 25 - Casella di posta elettronica certificata

1) Per la trasmissione telematica di comunicazioni (art. 14, commi 1 e 2 del DPR 445/2000) che necessitano di una ricevuta di invio e di una ricevuta di consegna, ai sensi del CAD e del DPR 11 febbraio 2005, n. 68 è istituita una casella di posta elettronica certificata per ciascun registro di protocollo

2) La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

3) Le modalità di gestione della casella di posta elettronica certificata e l'invio e ricezione dei messaggi sono indicate nel manuale del servizio di protocollo e flussi documentali.

4) La gestione tecnica e l'attivazione delle caselle di posta elettronica certificata sono demandate all'Amministratore di Sistema.

Art. 26 - Responsabilità

1) L'assegnazione degli account di posta elettronica implica l'obbligo di utilizzo di tale mezzo di comunicazione per lo svolgimento dei propri doveri di ufficio, ciò significa che sono vietati tutti gli utilizzi di detto strumento non in conformità con gli scopi dell'Ente. Per questo motivo sono vietati:
   - l'utilizzo di posta elettronica per motivi privati e/o per contatti interpersonali tra i dipendenti non inerenti l'uso d'ufficio, nonché l'iscrizione a catene di Sant'Antonio elettroniche, mailing list pubblicitarie e simili;
   - l'accesso al sevizio di posta elettronica internet attraverso mezzi (modem o altro) diversi dal collegamento alla rete informatica dell'Ente;
   - l'accesso alla posta elettronica in orari differenti da quello di lavoro. A tal fine l'amministratore di sistema concorderà con i responsabili di Servizio un orario di massima per l'erogazione del servizio di posta elettronica.

2) L'utente si impegna:
   - a non modificare, per nessun motivo, la configurazione hardware e software della sua macchina; a non utilizzare sistemi client di posta elettronica non conformi agli standard adottati dall'Ente;
   - a non rivelare ad alcuno le proprie credenziali per l'accesso ai servizi di posta elettronica e/o di rete, e a non utilizzare il nome utente e la password di altri utenti, ed a non rivelare notizie, dati o informazioni legate al segreto d'ufficio.

3) Non è consentito l'utilizzo di crittosistemi o di qualsiasi altro programma di sicurezza e/o crittografia non previsto esplicitamente dal responsabile della sicurezza informatica.

4) E' vietata l'apertura di allegati di posta elettronica senza il previo accertamento dell'identità del mittente e una verifica a mezzo di software antivirus.

5) Non è consentita la trasmissione, a mezzo posta elettronica, di dati sensibili, personali e/o commerciali di alcun genere.

Capo V - Sito Internet del Comune

Art. 27 - Accesso alla struttura del sito internet.

1) L'accesso alla struttura del sito, al programma di gestione dello stesso, ai codici sorgenti delle pagine stesse è riservato esclusivamente al responsabile tecnico del sito.
   In ogni caso non è possibile rendere noto ad altri la password di accesso al programma di trasferimento delle pagine dal computer della webmaster al computer del provider internet.

2) I codici sorgenti delle pagine saranno custoditi a cura del responsabile del procedimento tecnico in luogo sicuro e protetto.

3) Il responsabile tecnico (webmaster) del sito può coincidere con l'Amministratore di Sistema.

Art. 28 - Contenuti

1) Il sito conterrà informazioni utili a pubblicizzare la cittadina a livello turistico/culturale. Non presenterà carattere pubblicistico per associazioni o ditte private. Inoltre il contenuto dovrà essere strettamente attinente con la vocazione turistica di Ospedaletti e/o con l'attività amministrativa ed organizzativa del comune.

2) Non verranno pubblicate notizie a carattere politico, sindacale, contrarie alle istituzioni o che offendano il buon gusto.

3) In particolare sul sito internet troverà collocazione obbligatoriamente:
   a) l'organigramma, l'articolazione degli uffici, le attribuzioni e l'organizzazione di ciascun ufficio di livello dirigenziale non generale, nonché il settore dell'ordinamento giuridico riferibile all'attività da essi svolta, corredati dai documenti anche normativi di riferimento;
   b) l'elenco dei procedimenti svolti da ciascun ufficio di livello dirigenziale non generale, la durata di ciascun procedimento, ed il nome del responsabile del procedimento secondo quanto stabilito dalla legge 7 agosto 1990, n. 241 e secondo quanto previsto dai singoli ordinamenti corredati dalla normativa di riferimento;
   c) le scadenze e le modalità di adempimento dei procedimenti individuati ai sensi degli articoli 2 e 4 della legge 8 agosto 1990, n. 241;
   d) l'elenco completo delle caselle di posta elettronica istituzionali attive, specificando anche se si tratta di una casella di posta elettronica certificata di cui alla vigente normativa in materia;
   e) le pubblicazioni di cui all'articolo 26 della legge 7 agosto 1990, n. 241, nonché ogni altra pubblicazione prevista dalla legge 7 giugno 2000, n. 150;
   f) l'elenco di tutti i bandi di gara;
   g) l'elenco degli eventuali servizi forniti in rete.
   h) Tutta la modulistica e formulati in uso nell'Ente validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.
   i) Ogni documentazione il cui obbligo di pubblicazione è previsto da disposizioni di legge.

Art. 29 - Collaborazione

1) Alla realizzazione del sito dovranno collaborare tutti gli uffici facendo pervenire al webmaster, il testo che deve essere pubblicato, corredato eventualmente di immagini rispettando i seguenti parametri:

- il testo potrà essere scritto a macchina, con carattere nitido e senza correzioni su fogli di colore bianco;
- nel caso venga utilizzato un personal computer il testo dovrà essere redatto con Word e salvato con formato RTF senza formattazione di carattere o di paragrafo (cioè senza grassetto, corsivo o sottolineato e giustificato al margine sinistro), carattere tipo Arial altezza 10 .
- le immagini (fotografie) dovranno essere nitide sia a colori che in bianco e nero;
- nel caso in cui le immagini vengano trasmesse tramite supporto magnetico esse dovranno essere salvate in formato JPEG ad alta risoluzione (16 milioni di colori) o se si tratta di disegni in formato GIF 89a con sfondo trasparente;

Art. 30 - Realizzazione e pubblicazione

1) Il sito internet del Comune deve essere realizzato secondo le direttive impartite dalla vigente normativa in materia con particolare riguardo alla L. 4/2004 ed alle linee guida di progettazione e sviluppo per i siti delle pubbliche amministrazioni.

2) Il Comune di Ospedaletti individua ai sensi dell'art. 5 della direttiva del Ministro per la Pubblica Amministrazione e l'Innovazione n. 8/2009, un responsabile del procedimento di pubblicazione di contenuti sui siti internet di propria competenza.

3) Il responsabile del procedimento prima di procedere alla pubblicazione delle pagine sul sito provvederà a vagliare i contenuti dei testi pervenuti dagli altri uffici, procedendo alle opportune correzioni e/o rettifiche anche di concerto con il responsabile del servizio che ha prodotto i testi da pubblicare, eliminando i testi o le immagini non ritenute pubblicabili.

Capo VI - Software e hardware

Art. 31 - Acquisto di software e hardware

1) Per prevenire l'introduzione di virus e/o altri programmi dannosi e per proteggere l'integrità del sistema informatico tutto l'hardware ed il software in dotazione agli uffici deve essere acquistato dal Comune di Ospedaletti.

2) E' istituito con decorrenza 1 Gennaio 2010, un registro dell'hardware e software acquistato la cui gestione è affidata all'Amministratore di Sistema..

3) Per il software comune a tutti gli uffici (antivirus, utility, elaboratori testi, fogli elettronici, ecc.) è auspicabile ricorrere ai programmi multilicenze offerti da tutti i produttori.

4) È ammesso in casi particolari l'utilizzo di hardware di provenienza esterna (ad esempio notebook) di proprietà degli utenti della rete e/o ditte di assistenza. In tal caso l'Amministratore di Sistema provvederà a seguito degli opportuni controlli a configurare l'uso temporaneo della risorsa in rete;

5) L'Amministrazione Comunale, in casi particolari, può concedere l'uso esterno dei software di proprietà per attività strettamente connesse all'attività istituzionale;

6) il Servizio Intranet/Internet provvede all'acquisto, allo sviluppo ed alla regolarizzazione delle licenze necessarie per il software ed hardware necessario al corretto funzionamento della rete;

Art. 32 - Rispetto della proprietà intellettuale e delle licenze

1) Tutto il software in uso sul sistema informatico deve essere ottenuto seguendo le procedure e le linee guida in materia e deve essere registrato a nome dell'Amministrazione Comunale.

2) Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright), e non possono installare, duplicare o utilizzare i vari software al di fuori di quanto consentito dagli accordi di licenza.

Art. 33 - Utilizzo del software di proprietà personale

1) Al fine di proteggere l'integrità del sistema informatico, il personale non può utilizzare eventuale software di proprietà personale. Tutto ciò comprende anche le applicazioni regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo.

Art. 34 – Utilizzo di software OpenSource o a codice riutilizzabile

L'Amministrazione Comunale si impegna a diffondere all'interno dell'Ente l'utilizzo di software autoprodotto, open source, a codice libero, o riutilizzabile. Nel caso in cui il software sia prodotto in proprio mediante strutture interne o ricorso a ditte esterne (nel qual caso il proprietario del codice sorgente rimane il Comune di Ospedaletti), il software può essere distribuito ad altre amministrazioni secondo le modalità del riuso previste dal Capo VI - articoli da 67 a 70 del CAD

Capo VII - Disposizioni finali

Art. 35 - Precauzioni e prescrizioni

1) l'uso di CD anche musicali in formato MP3 o similari, con fotografie o ed in particolare duplicati o creati con personal computer può, in alcuni casi, essere veicolo di infezioni da virus. Pertanto occorre prestare attenzione al loro ascolto sui personal computer del sistema informatico comunale, accertandone preventivamente la provenienza.

2) E' ammesso l'uso di supporti di memorizzazione quali floppy disc, cdrom o memory pen per lo scambio di dati tra gli uffici. Nel caso tali supporti abbiamo provenienza esterna sarà cura dell'utente verificare il corretto rispetto per l'attuazione delle politiche di sicurezza e antivirus.

Art. 36 – Violazioni e controlli

1) Qualsiasi utilizzo non conforme alle disposizioni del presente Capo e/o alle leggi vigenti è ad esclusiva responsabilità dell'utente.

2) Le seguenti attività sono tassativamente vietate:
   a) utilizzare strumenti che potenzialmente siano in grado di consentire l'accesso non autorizzato alle risorse informatiche (ad esempio cracker, programmi di condivisione quali IRC, ICQ, AudioGalaxy o software di monitoraggio della rete in genere);
   b) configurare servizi già messi a disposizione in modo centralizzato, quali DNS , DHCP o server internet (Web o E-mail);
   c) intercettare pacchetti sulla rete, utilizzare sniffer o software di analisi del traffico (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;
   d) accedere ai locali e ai box riservati alle apparecchiature di rete, o apportare qualsiasi modifica agli stessi;
   e) cablare o collegare apparecchiature alle prese di rete senza l'autorizzazione dell'Amministratore di sistema ed, in particolare, ogni sostituzione o aggiunta di schede di rete deve essere preventivamente segnalata all'amministratore di sistema, per la registrazione degli indirizzi ethernet univoci (MAC address);
   f) installare hub per sottoreti di PC e stampanti;
   g) utilizzare indirizzi di rete e nomi non espressamente assegnati all'utente;
   h) installare modem per chiamate su linee analogiche, digitali o xDSL;
   i) installare modem configurati in call-back;
   j) 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.
      - è vietato utilizzare programmi gratuiti (shareware) prelevati da siti Internet o in allegato a riviste o libri senza la formale autorizzazione dell'Amministratore di sistema;

3) Ogni azione che non sia comunque conforme allo spirito del presente Regolamento, verrà considerata una violazione della sicurezza, e come tale comporterà la segnalazione al Direttore Generale/Segretario Comunale e al Responsabile del servizio Intranet/Internet/Sito;

4) l'utente risponde del software installato sul computer che gli è affidato;

5) è vietato distribuire software soggetto a Copyright acquistato dall'Ente, al di fuori dei termini delle licenze;

6) è vietato distribuire software che possa danneggiare le risorse informatiche, anche via e-mail;

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

8) L'Amministrazione Comunale si riserva il diritto di monitorare e verificare, nel pieno rispetto della normativa vigente in tema di privacy, del vigente CCNL e della normativa in materia, l'attuazione delle disposizioni del presente regolamento. Nei casi di accertata violazione di tali norme, è demandata ai rispettivi Responsabili di servizio l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituente reato.

Art. 37 – Locali apparecchiature di rete

1) Le apparecchiature di rete: server, switch e router sono ospitati in un ufficio sito all'interno dell'edificio comunale dotato delle caratteristiche climatiche idonee al funzionamento delle macchine;

2) Le suddette apparecchiature sono ospitate in apposito armadio metallico chiuso a chiave. Una copia delle chiavi è conservata dall'Amministratore di Sistema, l'altra conservata a cura del responsabile del servizio.

3) Per ovvi motivi di sicurezza l'accesso alle attrezzature è consentito esclusivamente all'Amministratore di Sistema ed al Responsabile del Servizio Intranet/Internet/Sito;

4) In caso di assenza del personale dell'ufficio, e/o al di fuori dell'orario di apertura al pubblico, che ospita le attrezzature di rete, la stanza deve essere resa inaccessibile mediante chiusura a chiave delle porte. Inoltre deve essere dotata dei necessari dispositivi di sicurezza meccanici ed elettronici eventualmente anche di videosorveglianza.

5) Copia dei files di configurazione della rete è conservata a cura dell'amministratore di sistema

Art. 38 – Postazione internet pubblica – terminali di accesso per il pubblico.

1) E' possibile attivare una o più postazione pubblica di accesso ad internet.
Tale postazione collegata alle linee di trasmissione dati condivide dell'Ente non dovrà consentire l'accesso agli archivi informatici dell'Ente.

2) Il collegamento alle linee telefoniche dovrà avvenire mediante apparecchiature e connessioni dedicate.

3) E' possibile attivare l'installazione all'interno dell'Ente a disposizione del pubblico di uno o più terminali di accesso ai servizi telematici offerti dall'Ente;

4) Le modalità tecniche di attivazione, nel rispetto della L. n. 241/1990 e del D. Lgs. 196/2003, saranno oggetto di apposito regolamento la cui approvazione è demandata alla Giunta Comunale

Art. 39 – Entrata in vigore

1) Il presente regolamento entra in vigore ad avvenuta pubblicazione all'albo pretorio.

Allegato “A”

GLOSSARIO DEI TERMINI TECNICI E/O INFORMATICI

Account	Iscrizione registrata su un server e che, tramite l'inserimento di una userId e di una password, consente l'accesso alla rete e/o ai servizi. Ad esempio, un account (ottenuto con un abbonamento ad un ISP) ci permette di entrare in Internet, un altro account (spesso con un altro server, gratuito) ci serve per ricevere e spedire posta elettronica. Un account ci consente di accedere alle risorse di una rete locale, come server, file server, stampanti.. Altri account servono per accedere a server e servizi quali enciclopedie, notiziari, shareware...
Antivirus	Tipo di software che cerca e distrugge gli eventuali programmi virus e cerca di rimediare ai danni che hanno compiuto.
Attachment/Allegato di posta elettronica	File o Documento di qualunque genere agganciato ad un messaggio di posta elettronica per essere inviato a distanza.
AVI (Audio Video Interleaved)	Formato per file video in Windows '9x. I dati del video e dell'audio sono memorizzati in pacchetti alternati. I video AVI hanno un'ottima qualità di riproduzione, ma i suoi file sono molto più grossi degli altri formati video.
Backup	Copia di riserva di un disco, di una parte del disco o di uno o più file.
Browser	Software che consente la visualizzazione della pagine di Internet e/o Intranet. Spesso deve essere affiancato da plug-in per rendere attive determinate funzionalità come il suono ed i filmati. I due browser più importanti sono Nescape Navigator e Microsoft Internet Explorer. Ne esistono altri minori, quali Mosaic e Opera. Può essere utilizzato anche per la consultazione di pagine HTML in locale.
Chat (webchat)	Sistema che consente il dialogo (tramite digitazione sulla tastiera) di più utenti contemporaneamente tramite Internet. I chat possono essere pubblici (ognuno legge i messaggi di tutti gli altri ed invia i propri a tutti i presenti) o privati (ospitati in “stanze” virtuali). Non sono ammessi sulla rete intranet del Comune di Ospedaletti.

Client Personal	collegato ad un server tramite rete locale o geografica, ed al quale richiede uno o più servizi. Alcuni software, come i database, sono divisi in una parte client (residente ed in esecuzione sul personal per la consultazione o la modifica del database) ed una parte server (residente ed in esecuzione sul server per gestire il database e rispondere alle interrogazioni dei client).
Client di posta elettronica	Software che, collegandosi ad un server, consente lo scambio di messaggi e di file attraverso il servizio di posta elettronica. I Client ammessi sul sistema informatico sono: Ms Outlook, Ms Entourage e Apple Mail.
Crittografia	Invio di dati resi incomprensibili e che è possibile decodificare solamente tramite apposito hardware e/o software. Esistono diversi tipi di

	crittografia e la decodifica dipende, comunque, da una parola chiave o da una smart card. Il metodo più utilizzato è quello a chiave pubblica.

Database (Base di Dati)	Qualsiasi aggregato di dati organizzato in campi (colonne) e record (righe).
Download	Registrare sul proprio disco rigido un file richiamandolo, tramite modem o rete, da un computer, da un server o da un host (tramite Internet, rete locale o geografica).
E-mail Electronic mail, posta elettronica.	Scambio di messaggi e di file attraverso una rete locale o Internet. Avviene in tempo reale ed è indipendente dalla posizione fisica dei computer mittente e destinatario. I messaggi e file vengono conservati da un server che provvede a inoltrarli al destinatario quando questo si collega
Firewall	Insieme di software/hardware usato per filtrare i dati in scambio fra reti diverse, al fine di proteggere un server da attacchi pervenuti via rete locale o via Internet. Consente il passaggio solamente di determinati tipi di dati, da determinati terminali e determinati utenti.
Freeware	Software realizzato e distribuito da privati o piccole società, attraverso Internet od i CD-ROM allegati alle pubblicazioni in edicola. Il programma è pienamente funzionante e non è necessario pagare nulla, anche se a volte si tratta di software molto utile. A volte l'autore chiede l'invio di una cartolina di ringraziamento (cardware), altre volte un versamento per beneficenza ad ospedali od altri organismi.
Hardware	letteralmente ferramenta, in informatica si intende l'insieme dei componenti (CPU, HARD DISK, ecc.) che costituiscono un computer.
HTML	Linguaggio di programmazione utilizzato in Internet e pubblicato nel 1991. Serve a creare documenti di testo e grafica che siano visualizzabili da qualsiasi sistema, tramite comandi incorporati nel documento stesso. Rispetto ai precedenti GML e SGML ha dei comandi che rendono 'attive' parti del testo o della grafica: cliccando su uno di questi punti, il link, viene richiamato sullo schermo un altro documento. Il documento, quando viene visualizzato, viene chiamato pagina. Una pagina, se divisa in frame, può essere composta da più di un documento, uno per ciascuna frame. Per visualizzare le pagine Internet è necessario un software apposito chiamato browser, e visualizzare una serie di pagine viene chiamato navigare. Un gruppo di pagine registrate sullo stesso server ed aventi, in genere, lo stesso argomento, si chiama sito.
Internet	E' l'insieme mondiale delle reti di computer interconnesse mediante il protocollo TCP/IP
Intranet	Rete locale che, pur non essendo necessariamente accessibile dall'esterno, fa uso di tecnologie Internet.
Lan (Local Area Network)	Una rete che collega computer e periferiche (es. stampanti, fax, scanner...) installate nella stessa sede (es. stesso palazzo, anche a piani diversi) oppure in sedi vicine (es. due palazzi adiacenti) in modo che non serva ricorrere a servizi di trasmissione dati esterni, cittadini, regionali,

	nazionali od internazionali.
Mailing list	Lista di distribuzione automatica di messaggi di posta elettronica, riguardanti un determinato argomento. I messaggi sono inviati ad un list server, che li archivia e provvede ad inviarli automaticamente agli iscritti.
Modem (modulatore/demodulatore)	Apparecchiatura che consente di inviare e ricevere i dati digitali dei computer tramite le linee analogiche del telefono oppure le linee digitali ISDN.
MP3 ((MPEG-4 Audio Layer III)	Tecnologia, emessa nel 1998 dal comitato MPEG, per la compressione/decompressione di file audio che consente di mantenere una perfetta fedeltà e qualità anche riducendo il file audio (ripreso da un Cd audio) di ben 11 volte la lunghezza originale. Un file che contiene 5 minuti di musica stereo (in due canali da 16 bit a 44.100 KHz) passa dai 60 Mb del file originale, ai soli 5 Mb del file MP3, pur mantenendo la stessa qualità che si otterrebbe da un CD audio. La compressione può variare da un minimo di 5 volte (con un brano da CD audio a 32 Kb al secondo) ad un massimo di 176 volte (audio solo vocale, senza musica a 1 Kb al secondo). L'MP3 ha infatti fatto sviluppare la pirateria musicale sul fronte di Internet: un file MP3 viene trasferito dal server al computer in circa 20 minuti. Da molti siti è possibile scaricare file audio di canzoni, anche le più recenti; dotandosi di un masterizzatore CD (compatibile con i CD audio) è possibile riprodurre un CD audio pirata perfetto, oppure prepararsi un CD personalizzato con canzoni di cantanti diversi. Alla base del MP3 c'è il Layer III, elaborato dal IIS.
MPG (Motion Picture Experts Group)	Comitato formato nel 1988 da membri ISO e IEC che stabilisce gli standard digitali per audio e video. Ha emesso gli standard JPEG e MPEG.
Ricordiamo, tra gli altri:	
MPEG-1	Standard, emesso nel 1993 dal comitato MPEG, per la registrazione difile audio e video su VideoCD con qualità simile ai nastri VHS e risoluzione di 360x288 pixel ed un bit rate costante di 1,5 Mbit al secondo. Contrassegnato dalla sigla ISO 11172.
MPEG-2	Evoluzione del formato MPEG-1, che consente una risoluzione di 720x576 pixel in PAL (25 quadri al secondo) o di 720x480 in SECAM (30 quadri al secondo) ed un bit rate più elevato, quindi una riproduzione dell'immagine molto migliore. Lo standard MPEG-2 è stato adottato dalla televisione digitale, terrestre e via satellite, e dai produttori di DVD, in quanto riesce a combinare velocità e qualità
Password	Parola che consente l'accesso di un utente ad una rete, ad un servizio telematico o ad un sito Internet. E' necessario digitarla esattamente, assieme alla user-id. Alcuni software distinguono fra lettere maiuscole e minuscole. E' consigliabile non scriverla su bigliettini od agende, né utilizzare parole troppo semplici da indovinare (es: il proprio nome, il numero di telefono o la data di nascita). Se l'accesso è ad alta protezione, la password deve avere un numero minimo di caratteri, deve essere alfanumerica, e può essere previsto un intervallo regolare per la sua modifica (es: ogni mese). Occorre anche fare attenzione alle finestre di dialogo che richiedono la password: spesso è possibile istruire il programma od il sistema a ricordare ed immettere automaticamente la password,

	ma allora chiunque si collega con lo stesso computer ha libero accesso. Il sistema informatico del Comune non prevede il cambio delle password di rete da parte dell'utente, compito demandato all'amministratore di sistema.
Plug-in	Software accessorio che aggiunge determinate funzioni ai programmi, ad esempio ai programmi di grafica od ai browser. Nei programmi di grafica i plug-in possono consentire l'uso di determinate periferiche, oppure l'esecuzione sull'immagine di effetti e di elaborazioni, di applicazioni di filtri. Ad un browser consentono funzioni come la visualizzazione di video, il collegamento con telecamere in diretta, l'ascolto di musica, il dialogo a voce fra più utenti, ed altro durante la visualizzazione delle pagine Internet.
Policy	Insieme di regole che determina quali contenuti possano passare attraverso una rete. Ad esempio, in una accesso Internet, possono essere bloccati contenuti di tipi erotico, sessuale, commerciale, di gioco…
Quicktime	Standard definito dalla Apple e utilizzata da tutti i computer per la riproduzione fedele dei filmati video. E' previsto un plug-in QuickTime per i programmi di navigazione in Internet.
Sistema Informatico del Comune di Ospedaletti.	E' l'insieme coordinato dell'infrastruttura di rete telematica e degli apparati, elaboratori, software, archivi dati e/o risorse informative a qualsiasi titolo archiviate in modo digitale, in dotazione ed uso all'Amministrazione Comunale di Ospedaletti
Server di rete	Computer dedicato allo svolgimento di un servizio preciso, come la gestione di una rete locale o geografica, alla gestione delle periferiche di stampa (print server), allo scambio e condivisione di dati fra i computer (file server, database server), all'invio o inoltro di posta elettronica (mail server) od a contenere i file di un sito web (webserver). Utilizza un sistema operativo di rete. I computer collegati e che utilizzano il servizio del server, si chiamano client. A volte lo stesso computer, come nel caso della rete del Comune di Ospedaletti svolge diverse funzioni di server (es: file server, mail server, web server).
Shareware	Software realizzato e distribuito da privati o piccole società, attraverso Internet od i CD-ROM allegati alle pubblicazioni in edicola. L'utilizzatore può provare il programma prima di acquistarlo, nel caso basta inviare un messaggio di posta elettronica all'autore con i dati della propria carta di credito (o direttamente inviare i soldi via posta ordinaria)per ricevere un codice che, inserito nel programma, ne consente l'uso completo. Infatti certe funzionalità importanti, o i livelli finali nei giochi, sono spesso bloccati e disponibili sono dopo la registrazione dell'acquisto. Il costo, comunque, è molto inferiore a quello dei prodotti commerciali, anche se certi programmi shareware non hanno nulla da invidiare a quelli commerciali. Visto che il prezzo è molto basso, è sempre conveniente registrarsi e pagare, così si potranno ricevere gli aggiornamenti ed altri programmi dello stesso autore, nonché dare un contributo allo sviluppo di software a prezzo contenuto.
Software	sono i programmi (professionali, ludici, video, musicali, raccolte disuoni

	ed immagini) per i computer.
Spyware / maleware	Programmi simili a virus che installati inconsapevolemente trasmettono dati ed informazioni a siti internet o indirizzi di posta elettronica ad insaputa dell'utente
UserId	Nome utente
Utente (User)	Chiunque utilizzi un elaboratore collegato alla rete, sia che il collegamento avvenga in rete locale, come avviene all'interno del palazzo comunale sia che si tratti di un accesso remoto, come avviene nei collegamenti via modem.
Virus	Un programma creato per diffondersi da computer a computer, spesso danneggiando i dati e gli altri programmi registrati.

Allegato “B”

NETIQUETTE
Etica e norme di buon uso dei servizi di rete

Fra gli utenti dei servizi telematici di rete, prima fra tutte la rete Internet, ed in particolare fra i lettori dei servizi di “news” Usenet, si sono sviluppati nel corso del tempo una serie di “tradizioni” e di “principi di buon comportamento” (galateo) che vanno collettivamente sotto il nome di “netiquette”. Tenendo ben a mente che la entità che fornisce l'accesso ai servizi di rete (provider, istituzione pubblica, datore di lavoro, etc.) può regolamentare in modo ancora piu' preciso i doveri dei propri utente, riportiamo in questo documento un breve sunto dei principi fondamentali della “netiquette”, a cui tutti sono tenuti ad adeguarsi.

1) Quando si arriva in un nuovo newsgroup o in una nuova lista di distribuzione via posta elettronica, e' bene leggere i messaggi che vi circolano per almeno due settimane prima di inviare propri messaggi in giro per il mondo: in tale modo ci si rende conto dell'argomento e del metodo con cui lo si tratta in tale comunità.

2) Se si manda un messaggio, e' bene che esso sia sintetico e descriva in modo chiaro e diretto il problema.

3) Non divagare rispetto all'argomento del newsgroup o della lista di distribuzione.

4) Se si risponde ad un messaggio, evidenziare i passaggi rilevanti del messaggio originario, allo scopo di facilitare la comprensione da parte di coloro che non lo hanno letto, ma non riportare mai sistematicamente l'intero messaggio originale.

5) Non condurre “guerre di opinione” sulla rete a colpi di messaggi e contromessaggi: se ci sono diatribe personali, e' meglio risolverle via posta elettronica in corrispondenza privata tra gli interssati.

6) Non pubblicare mai, senza l'esplicito permesso dell'autore, il contenuto di messaggi di posta elettronica.

7) Non pubblicare messaggi stupidi o che semplicemente prendono le parti dell'uno o dell'altro fra i contendenti in una discussione. Leggere sempre le FAQ (Frequently Asked Questions) relative all'argomento trattato prima di inviare nuove domande.

8) Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano stati sollecitati in modo esplicito.

9) Non essere intolleranti con chi commette errori sintattici o grammaticali. Chi scrive, è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività.

10) Alle regole precedenti, vanno aggiunti altri criteri che derivano direttamente dal buon senso:
    A La rete è utilizzata come strumento di lavoro da molti degli utenti.

    B Nessuno di costoro ha tempo per leggere messaggi inutili o frivoli o di carattere personale, e dunque non di interesse generale.

    C Qualunque attività che appesantisca il traffico sulla rete, quale per esempio il trasferimento di archivi voluminosi, deteriora il rendimento complessivo della re-

te. Si raccomanda pertanto di effettuare queste operazioni in orari diversi da quelli di massima operatività (per esempio di notte), tenendo presenti le eventuali differenze di fuso orario.

D Vi sono sulla rete una serie di siti server (file server) che contengono in copia aggiornata documentazione, software ed altri oggetti disponibili sulla rete. Informatevi preventivamente su quale sia il nodo server più accessibile per voi. Se un file è disponibile su di esso o localmente, non vi è alcuna ragione per prenderlo dalla rete, impegnando inutilmente la linea e impiegando un tempo sicuramente maggiore per il trasferimento.

E Il software reperibile sulla rete può essere coperto da brevetti e/o vincoli di utilizzo di varia natura. Leggere sempre attentamente la documentazione di accompagnamento prima di utilizzarlo, modificarlo o re-distribuirlo in qualunque modo e sotto qualunque forma.

F Comportamenti palesemente scorretti da parte di un utente, quali:
- violare la sicurezza di archivi e computers della rete;
- violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata;
- compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, ecc.) costruiti appositamente;

costituiscono dei veri e propri crimini elettronici e come tali sono punibili dalla legge.

Per chi desiderasse approfondire i punti qui trattati, il documento di riferimento è RFC1855 "Netiquette Guidelines", ed anche RFC2635 "A Set of Guidelines for Mass Unsolicited Mailings and Postings" disponibili sulla rete presso:

ftp://ftp.nic.it/rfc/rfc1855.txt
ftp://ftp.nic.it/rfc/rfc2635.txt

Questo documento è tratto dal sito del Registro Nazionale dei domini internet presso il Consiglio Nazionale delle Ricerche

Contratti_Doc:Documenti:Regolamenti:regolamento intranet 2009.doc