Regolamento per l'utilizzo dei sistemi informatici e di telecomunicazioni del Comune di Zola Predosa

Approvato con deliberazione della Giunta Comunale n. 98 del 16.11.2011

Il Segretario generale
Dr.ssa Daniela Olivi

Il Sindaco
Stefano Fiorini

Disposizioni Generali
Art. 1
Premessa

1.1 Il presente regolamento disciplina le modalità di accesso e di utilizzo dei sistemi informatici e di telecomunicazioni del Comune di Zola Predosa. Il regolamento si applica a tutti gli utenti che accedono alla rete comunale o che utilizzano i sistemi di telecomunicazione. Scopo di questo regolamento è quello di evitare comportamenti che possano creare problemi o minacce alla sicurezza nel trattamento dei dati , malfunzionamenti, interruzione di servizi, danni patrimoniali e d'immagine all'Amministrazione Comunale, violazioni di copyright e di altre norme di legge.

1.2 Per l'accesso ad internet da postazioni pubbliche è presente un apposito regolamento pubblicato sul sito internet dell'Amministrazione Comunale. Il cittadino, al momento della richiesta di attivazione del servizio, dovrà fornire le proprie generalità e sottoscrivere l'accettazione delle norme riportate in tale regolamento. Il traffico internet delle postazioni pubbliche è registrato associando i siti visitati all'identificativo del cittadino. I dati sono trattati e conservati in base alle leggi vigenti e nel rispetto delle norme sulla privacy. La rete di accesso pubblica deve essere fisicamente o logicamente separata da quella usata dall'Amministrazione per le attività istituzionali.

Art. 2
Definizioni

2.1 Nel presente Regolamento si intende per:

a) Amministrazione o Ente: Il Comune di Zola Predosa.

b) Utente:

- Tutti i dipendenti, senza distinzione di livello e/o ruolo.
- Tutti i collaboratori dell'amministrazione a prescindere dal rapporto contrattuale con la stessa intrattenuto (Consulenti, Collaboratori a progetto, In stage, ecc.).
- Tutti gli amministratori (Assessori, Consiglieri comunali, ecc.).
- Tutti i fornitori e manutentori (hardware e software) nonché il personale di enti esterni autorizzati che abbiano accesso alla rete del Comune di Zola Predosa e ai sistemi di telecomunicazioni.

c) Internet: il sistema di interconnessione tra computer e reti locali, ad accesso pubblico, che consente la trasmissione di informazioni in tutto il mondo.

d) Intranet: il sistema di collegamento in rete realizzato con i protocolli di Internet ma riservato alle comunicazioni all'interno dell'Ente.

e) Amministratore di sistema: il personale del Comune di Zola Predosa a cui è conferito il compito di sovraintendere alle risorse del sistema informativo dell'Ente e di consentirne l'utilizzazione.

2.2 Per ogni altra definizione si rimanda a quanto previsto dal **Codice dell'Amministrazione Digitale** attualmente in vigore.

Art. 3
Pubblicazione del Regolamento e comunicazione agli utenti

3.1 Il regolamento è pubblicato sul sito web della Intranet comunale nella sezione Atti e Documenti / Regolamenti.

3.2 Gli utenti sono tenuti a prendere visione e a rispettare le disposizioni contenute nel regolamento sull'utilizzo dei sistemi informatici e di telecomunicazioni del Comune di Zola Predosa.

Art. 4
Riferimenti

4.1 Al fine di garantire l' osservanza delle disposizioni in materia di riservatezza dei dati l' utente è tenuto a seguire le disposizioni riportate nei seguenti documenti:

1. Breve vademecum per il dipendente pubblico in tema di Privacy;
2. Documento Programmatico per la sicurezza del Comune di Zola Predosa;

Questi documenti sono pubblicati sul sito web della Intranet comunale nella sezione Atti e Documenti / Privacy e sono tenuti separati dal regolamento in quanto sottoposti a revisione periodica.

4.2 Gli utenti devono inoltre rispettare le disposizioni contenute nella normativa nazionale vigente in materia.

4.3 Il presente regolamento annulla e sostituisce le norme definite dai seguenti regolamenti ed atti:

- disposizioni per l'utilizzo di internet e della posta elettronica sul luogo di lavoro [allegato alla Delibera di G.C 13/09]
- Disciplinare per l'utilizzo degli apparecchi cellulari [Delibera di G.C 69/2008]

Art. 5
Help Desk

5.1 Le richieste di assistenza tecnica ai servizi informatici vanno inviate tramite il programma di help desk. Il programma di help desk è da utilizzare in via prioritaria per richiedere interventi dei servizi informatici al fine di garantire un tracciamento delle segnalazioni a fini statistici, la possibilità di monitorare lo stato avanzamento lavori e la gestione della coda delle richieste.

5.2 E' possibile contattare, in caso di urgenza, il personale addetto all'assistenza tecnica al numero interno dedicato o tramite il cellulare di servizio . In ogni caso l'utente deve poi compilare la richiesta di assistenza tramite il programma di help desk.

5.3 L'intervento tecnico può essere effettuato in teleassistenza fornendo all'operatore, quando richiesto, l'indirizzo di rete della postazione di lavoro (Indirizzo IP) e consentendo l'accesso alla comparsa della richiesta di conferma. Informazioni sull'utilizzo dei computers, dei programmi e delle stampanti di rete sono pubblicate sul sito web della Intranet comunale nella sezione Aiuto.

Disposizioni sulla Sicurezza

Il Segretario generale
Dr.ssa Daniela Olivi

Il Sindaco
Stefano Fiorini

Art. 6
Autorizzazioni e Password

6.1 Le autorizzazioni all'accesso al sistema informatico e ai sistemi di telecomunicazione sono assegnate in funzione del ruolo e della collocazione di ogni utente nell'organigramma dell'ente e delle esigenze operative comunicate ai servizi informatici dalla dirigenza dell'ente.

6.2 Il personale delle società ospitate nei locali dell'ente, dei carabinieri e polizia, di altri enti o di società esterne, può accedere ai servizi del sistema informativo comunale previa apposita convenzione con l'ente come stabilito dal Documento Programmatico per la Sicurezza.

6.3 L'amministratore di sistema, viste le informazioni inerenti gli utenti, assegna, sospende o revoca le autorizzazioni all'accesso ai servizi erogati con l'eccezione di particolari funzioni le cui autorizzazioni sono delegate ai responsabili dei servizi:

- Anagrafe – Il responsabile dei servizi demografici;
- Contabilità – Il responsabile dei servizi finanziari;

6.4 L'amministratore di sistema (o il responsabile, nei casi precedentemente citati) assegna agli utenti credenziali di accesso personali ed univoche. Le credenziali di un utente vengono disattivate nel caso in cui egli perda le qualità che gli consentono l'accesso alle risorse del sistema informatico.

6.5 L'utente deve provvedere a modificare la password di accesso al dominio immediatamente, non appena la riceve per la prima volta. (si ricorda che maiuscole e minuscole sono considerati caratteri differenti)

6.6 Le credenziali di accesso personali non vanno comunicate ad altre persone.
Le credenziali di accesso non vanno annotate su supporti cartacei o informatici che siano accessibili ad altre persone.

6.7 Non devono essere comunicati a terzi ne annotati in posizioni accessibili i codici delle fotocopiatrici/stampanti.

6.8 I requisiti di complessità delle password sono:

- redazione con caratteri maiuscoli e/o minuscoli (almeno una maiuscola);
- composizione con inclusione di simboli, numeri, punteggiatura e lettere;
- lunghezza non inferiore ad 8 caratteri ;
- password non agevolmente riconducibile all'identità del soggetto che la gestisce. La password non deve essere basata su informazioni personali, familiari o informazioni direttamente riferibili al soggetto titolare della password stessa.
- La password non deve essere composta ne contenere parole di senso compiuto anche straniere.

6.9 L'utente è informato del fatto che la conoscenza delle credenziali di

autenticazione da parte di terzi consentirebbe a questi ultimi l'utilizzo del sistema e dei servizi erogati attraverso di esso.

6.10 Qualora l'utente ritenga che un soggetto non autorizzato possa essere venuto a conoscenza della propria password, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione al direttore di area e all'amministratore di sistema.

6.11 Non debbono essere utilizzate nella configurazione dei browser o in altre applicazioni le opzioni di memorizzazione della password.

6.12 L'utente deve modificare la password periodicamente e non deve alterare la funzione "cambio password" che obbliga a modificare la password periodicamente. Il periodo massimo di validità della password di accesso alla rete è di 3 mesi.

6.13 L'utente è tenuto a impedire l'accesso al proprio sistema tramite attivazione del blocco del desktop con password o tramite disconnessione ogni qualvolta sia costretto ad assentarsi dal locale o nel caso ritenga di non essere in grado di presidiare l'accesso al sistema.

6.14 Non è consentita l'attivazione delle password del bios (configurazione e avvio sistema), senza preventiva autorizzazione da parte dell'amministratore di sistema.

6.15 Il personale dei servizi informatici può cambiare le credenziali di accesso di un utente per effettuare un accesso ai dati o alle risorse hardware in dotazione nel caso di una sua prolungata assenza o impedimento e nei casi in cui l'intervento sia indispensabile ed indifferibile per operatività, sicurezza e necessaria manutenzione del sistema.

Art. 7
Cessazione del servizio e trasferimento

7.1 L'utente che cessa il servizio presso l'amministrazione o viene trasferito è tenuto preventivamente ad eliminare i propri dati personali dai sistemi dell'amministrazione e concordare preventivamente con il proprio responsabile la gestione dei dati relativi al servizio svolto.

7.2 I dirigenti e/o responsabili devono comunicare all'amministratore di sistema le necessità di modifica dei permessi di accesso per quanto riguarda i servizi di propria competenza.

Art. 8
Utilizzo della rete

8.1 L'accesso alla rete è protetto da password. Per l'accesso deve essere utilizzato il proprio profilo personale (username e password) ricordando di indicare anche il corretto nome di domino (ZOLADOM).

8.2 L'accesso da sedi esterne è consentito previa autorizzazione dell'amministratore di sistema e nel rispetto delle disposizioni riportate nel Documento Programmatico per la sicurezza del Comune di Zola Predosa.

Il Segretario generale
Dr.ssa Daniela Olivi

Il Sindaco
Stefano Fiorini

8.3 Inoltre valgono le seguenti limitazioni:

- E' vietato modificare la configurazione degli apparati di rete;
- E' vietato l'utilizzo della rete comunale per fini non espressamente autorizzati;
- E' vietato monitorare ciò che transita in rete. Solo l'amministratore di sistema per ragioni di manutenzione e sicurezza è autorizzato a verifiche sul traffico di rete in forma anonima ed in ogni caso in osservanza delle norme vigenti sulla riservatezza dei dati;
- E' vietata l'installazione non autorizzata di modem o altri apparati che sfruttino il sistema di comunicazione telefonico per l'accesso a sistemi informatici esterni o interni all'ente;

Art. 9
Salvataggio dei Dati, Disaster Recovery

9.1 I dati presenti sui server di rete sono salvati a cura dei servizi informatici.

9.2 Per quanto riguarda i dati salvati sui PC locali vengono solo effettuate occasionali immagini dei dischi di sistema al fine di velocizzare un eventuale ripristino dei computers. L' utente è quindi tenuto ad utilizzare le unità di rete per l'espletamento delle proprie mansioni.

9.3 L' utilizzo di crittografia per i dati presenti all'interno dell'ente deve essere preventivamente valutato e autorizzato dall'amministratore di sistema che definirà la gestione delle password e dei certificati. Lo smarrimento di password e certificati per l'accesso a dati crittografati può comportare la perdita dei dati.

Art. 10
Firma digitale

10.1 Il dispositivo di firma digitale è personale e va custodito con cura tenendolo sempre separato dal codice PIN.

10.2 L'utente è tenuto a conservare con diligenza i dati forniti dall'Ente Certificatore al rilascio del dispositivo di firma. Tali dati sono necessari per poter effettuare attività amministrative relative al certificato di firma.

10.3 L'utente è tenuto a controllare la data di scadenza e ad attivarsi preventivamente per il rinnovo al fine di garantire la continuità del servizio.

10.4 In caso di smarrimento o sottrazione l' utente deve provvedere alla revoca del certificato.

Disposizioni sull'utilizzo delle attrezzature

Art. 11
Utilizzo di hardware e software

11.1 Ogni utente assegnatario di hardware e software è tenuto all’uso appropriato e

alla sua diligente conservazione. E' inoltre tenuto all'autonoma conservazione della relativa documentazione, della licenza d'uso, dei supporti magnetici, ottici e di qualsiasi altro materiale consegnato contestualmente all'hardware o al software. Tale materiale potrà essere richiesto per esigenze di servizio quali, ad esempio, il ripristino del funzionamento dell'hardware o del software.

11.2 E' vietato ogni utilizzo non inerente all'attività lavorativa in quanto può contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza.

11.3 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte dell'amministratore di sistema.

11.4 L'utente non deve rimuovere o alterare etichette riportanti codici prodotto, numeri di serie, codici di licenza, numeri di inventario e codici identificativi utilizzati dai servizi informatici per la gestione del parco macchine.

11.5 Ogni dispositivo hardware deve essere spento ogni sera prima di lasciare l'ufficio o in caso di assenza prolungata, salvo casi motivati ed autorizzati dal dirigente competente.

11.6 I dati di lavoro devono essere salvati sui dischi di rete al fine di garantire la possibilità di effettuare copie di sicurezza.

11.7 Il profilo locale dell'utente (desktop e cartelle documenti) deve essere mantenuto alle minime dimensioni possibili in quanto soggetto a sincronizzazione col server di dominio ad ogni avvio e arresto del sistema.

11.8 Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'amministratore di sistema.

11.9 Non è consentito modificare le impostazioni predefinite dei browser e relativi plugin.

11.10 Non è consentito memorizzare sui sistemi dell'ente rilevanti quantità di dati personali non inerenti le attività lavorative e amministrative (esempio: foto, musica, filmati) senza l'approvazione dell'amministratore di sistema.

11.11 Non è consentita la riproduzione o la duplicazione di dati e/o programmi informatici protetti da copyright tranne nei casi esplicitamente autorizzati dalla licenza.

11.12 Gli operatori dei servizi informatici possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza o che violino norme di legge, sia sui PC degli utenti sia sulle unità di rete.

11.13 Le stampanti di rete messe a disposizione sono da utilizzarsi in via prioritaria rispetto alle stampanti personali. Tutte le stampanti di rete messe a disposizione dal sistema informatico comunale, indipendentemente dalla collocazione geografica, sono

accessibili a tutti gli utenti con l' eccezione di alcuni casi in cui occorre essere autorizzati dall'amministrazione.

11.14 E' vietato l' utilizzo di apparecchiature elettriche non autorizzate sulle linee di alimentazione dei sistemi informatici provenienti dal gruppo di continuità (UPS).

Art. 12
Dischi di rete

12.1 Ad ogni utente comunale dotato di una postazione di lavoro fornita dall'ente è normalmente riservato uno spazio sul disco locale ed eventualmente una cartella personale ed una o più cartelle condivise sui dischi accessibili attraverso la rete. L'utilizzo di tali risorse è strettamente riservato all'archiviazione ed alla condivisione dei file necessari alla normale attività lavorativa.

12.2 Per lo scambio e la condivisione temporanea di files viene messa a disposizione un'area dei dischi di rete denominata "Tutti".

12.3 Particolare attenzione deve essere prestata alla duplicazione degli archivi al fine di evitare possibili disallineamenti e perdite dei dati.

12.4 In caso di necessità di spazio sui dischi di rete l' amministratore di sistema ha facoltà di intervenire senza preavviso spostando i dati su altre unità al fine di garantire continuità dei servizi.

12.5 L'utente è tenuto alla periodica pulizia di tutti gli spazi assegnati, con cancellazione dei files obsoleti o inutili.

12.6 I dati contenuti nelle cartelle condivise dei dischi di rete vengono salvati quotidianamente su supporto magnetico a cura del personale dei servizi informatici.
Sui dati presenti nei dischi dei computer locali non viene garantito un salvataggio periodico.

12.7 Le richieste di recupero dei dati vanno inoltrate, non appena se ne manifesti la necessità, al personale dei servizi informatici, che provvederà a verificare la possibilità ed i tempi di recupero dei dati compatibilmente con le esigenze di servizio.

Art. 13
Utilizzo di pc portatili

13.1 L'utente è responsabile del PC portatile assegnatogli dall'amministrazione e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

13.2 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. L' utente deve inoltre porre attenzione ad evitare lo smarrimento degli accessori come manualistica, alimentatore, mouse, cavi vari e unità di memorizzazione rimovibili.

13.3 I PC portatili utilizzati all'esterno (convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto.

13.4 Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari facendo particolare attenzione alla presenza di dati sensibili e/o giudiziari anche su supporti rimovibili.

13.5 Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus e degli altri software installati.

Art. 14
Utilizzo e conservazione dei supporti di memorizzazione rimovibili

14.1 Tutti gli utenti devono porre particolare attenzione ai supporti di origine esterna adottando tutti gli accorgimenti finalizzati a prevenire l'esecuzione di programmi non autorizzati ad esempio virus, trojan e altro malaware. Effettuare una scansione antivirus prima di aprire o importare dati provenienti da origini esterne.

14.2 Tutti i supporti di memorizzazione rimovibili, contenenti dati sensibili e giudiziari, devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati, furti inclusi, e trattamenti non consentiti (armadio chiuso a chiave o cassaforte).

14.3 La conservazione dei supporti avviene fino alla cessazione degli obblighi o delle necessità di custodia. Gli utenti devono successivamente adottare tutti gli accorgimenti necessari per rendere inintelleggibile e non ricostruibili tecnicamente i dati contenuti nei supporti, ovvero distruggere fisicamente tali supporti in modo da impedire che essi possano essere recuperati da persone non autorizzate al trattamento. Contattare i servizi informatici per ricevere opportune istruzioni in merito alla cancellazione e/o distruzione dei supporti.

Art. 15
Utilizzo dei materiali di consumo

15.1 L'utilizzo dei sistemi di stampa, copia e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, CD, DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi. Quando possibile utilizzare stampa fronte/retro e riciclare carta utilizzata. E' buona regola evitare di stampare documenti molto lunghi o non strettamente necessari. Utilizzare documenti elettronici per quanto possibile.
In caso di necessità la stampa in corso può essere cancellata dalla coda di stampa.

15.2 In caso di grandi volumi di stampa occorre valutare economicamente l'opzione di appoggiarsi a fornitori esterni che, disponendo di attrezzature idonee a produrre grossi volumi, possono garantire costi inferiori.

Art. 16
Utilizzo di videoproiettori

16.1 Alcuni ambienti sono dotati di videoproiettori fissati al soffitto. Occorre informare con adeguato anticipo il personale che deve predisporre gli apparecchi

prenotando anche il locale dove verrà effettuata la proiezione.

16.2 L' utente deve porre attenzione al corretto uso dei proiettori ed evitare lo smarrimento o il danneggiamento di accessori in dotazione come cavi e telecomandi.

Art. 17
Utilizzo stampanti, fotocopiatrici e scanner rete

17.1 Non è consentito stampare o effettuare copie di documenti personali su qualsivoglia stampante e/o fotocopiatrice.

17.2 Per l' utilizzo di alcuni apparati può essere richiesto un codice di accesso legato al servizio al fine di monitorare i consumi.

17.3 Le stampe inviate alle stampanti comuni vanno ritirate prontamente dai vassoi al fine di evitare sia interferenze tra i vari lavori di stampa che la possibilità che persone non autorizzate possano acquisire informazioni classificate come dati sensibili. Analoghe considerazioni valgono per l' utilizzo delle fotocopiatrici.

17.4 Per l'eliminazione di documenti con dati sensibili utilizzare gli appositi distruggi documenti posizionati in prossimità delle fotocopiatrici.

17.5 I documenti sottoposti a scansione su scanner di rete debbono essere copiati prontamente dall'utente nella apposita directory ed eliminate dal disco dello scanner sia per evitare l' accumulo di documenti che per impedire che le informazioni contenute rimangano accessibili a persone non autorizzate. Utilizzare postazioni di lavoro dotate di scanner locale per acquisire dati sensibili.

Art. 18
Utilizzo dei telefoni cellulari

18.1 I cellulari forniti dall'amministrazione si suddividono in:
1) Cellulari personali: comprendono i cellulari assegnati in via permanente ed esclusiva al consegnatario in relazione della funzione ovvero della mansione svolta;
2) Cellulari di servizio: comprendono i cellulari assegnati temporaneamente al personale dell'ente per il periodo necessario allo svolgimento delle attività che ne richiedono l'uso.

18.2 Principi
L'acquisizione e l'utilizzo degli apparecchi cellulari deve essere improntato a principi di razionalizzazione delle risorse strumentali e della progressiva riduzione delle spese di esercizio.
L'utilizzo dei cellulari, in particolare, deve assicurare la razionalizzazione dell'uso dei cellulari nei soli casi di effettiva necessità e quando esigenze di servizio richiedano pronta e costante reperibilità. È fatto salvo quanto previsto al successivo punto, riguardante l'uso di cellulari personali.
18.3 Acquisizione dei cellulari e attivazione di nuove utenze
Le acquisizioni ovvero le sostituzioni degli apparecchi cellulari sono effettuate dall'economo, su richiesta del servizio interessato, compatibilmente con il fabbisogno.
All'atto dell'attivazione di nuove utenze deve essere effettuata una valutazione circa la

configurazione da attribuire a ciascun cellulare richiesto, scegliendo tra le tipologie di utenza prepagata e utenza in concessione.

18.4 Destinazione dei cellulari

Gli apparecchi cellulari di proprietà ovvero che rientrano nella disponibilità dell'Ente sono presi in carico dall'economo mediante iscrizione negli inventari.
Ogni apparecchio cellulare comunale è assegnato, con apposito atto:
- all'utilizzatore, qualora l'uso del cellulare sia riservato in via esclusiva al medesimo;
- all'economo comunale per i cellulari di uso generale a disposizione di più utilizzatori.

18.5 Cellulari personali

Il cellulare personale viene concesso a fronte dell'insediamento in cariche istituzionali di particolare rilevanza ovvero per particolari posizioni nell'organizzazione del lavoro. In particolare possono usufruire del cellulare personale:
- Sindaco e vice-sindaco;
- Segretario comunale e direttore generale;
- Direttori di Area.

Gli apparecchi cellulari assegnati ad uso personale non possono essere ceduti a terzi a nessun titolo. Al cessare delle condizioni che hanno condotto all'assegnazione del telefono cellulare ad uso personale e, comunque, al venir meno dell'incarico in virtù del quale era stata disposta l'assegnazione, la relativa utenza viene tempestivamente cessata e l'assegnatario è tenuto alla immediata restituzione dell'apparecchio.
Opzione per telefonate diverse da quelle di servizio:
Agli assegnatari di telefoni cellulari ad uso personale è consentito di utilizzare gli stessi per chiamate personali o comunque diverse da quelle di servizio solamente nel caso in cui sia stata attivata l'opzione "dual billing" o similari, che consente di addebitare i relativi costi direttamente all'utilizzatore o alla persona giuridica da questo individuata in sede di attivazione dell'opzione.
Al di fuori dei casi sopra individuati, è fatto divieto di utilizzare l'apparecchio per chiamate diverse da quelle di servizio.

18.6 Cellulari di servizio

Al di fuori dei casi di cui al punto precedente, riguardante l'uso di cellulari personali, l'assegnazione del cellulare è limitata ai soli casi in cui il personale dipendente debba assicurare, per esigenze di servizio, pronta e costante reperibilità.
L'utilizzo del cellulare è disposto previa autorizzazione del responsabile del servizio interessato contenente anche l'indicazione delle esigenze di servizio che ne rendono necessario l'uso nonché la durata delle stesse. La richiesta di assegnazione deve essere indirizzata all'economo comunale. Il provvedimento di assegnazione deve specificare i motivi della stessa, gli obblighi, i divieti e le modalità di utilizzo dell'apparecchio. All'atto della consegna l'utilizzatore deve sottoscrivere apposito verbale.
È fatto obbligo all'economo di compilare un registro delle assegnazioni degli apparecchi cellulari di uso generale in cui dovranno essere annotati:
- gli estremi del provvedimento di assegnazione, ove esistente;
- data e ora di consegna dell'apparecchio;
- esigenze di servizio;
- data e ora di riconsegna dell'apparecchio;
- ogni notizia sullo stato di funzionamento dell'apparecchio.

18.7 Utilizzo dei cellulari

Tutti i telefoni cellulari che l'ente mette a disposizione per lo svolgimento dell'attività lavorativa o delle cariche istituzionali devono essere utilizzati, da parte di coloro che vi operano:

- in modo strettamente pertinente alla propria attività lavorativa o carica istituzionale ed impegnandosi ad un utilizzo appropriato, efficiente, corretto e razionale. Nella definizione di attività lavorativa devono essere ricomprese anche le attività che siano strumentali e connesse alla stessa quali, ad esempio, i rapporti con le organizzazioni sindacali;
- tenendo sempre presente l'interesse collettivo al risparmio delle risorse pubbliche.

L'effettuazione delle chiamate da e verso telefoni cellulari dell'ente deve rispondere a criteri di effettiva necessità ed urgenza. La durata delle chiamate deve essere la più breve possibile in relazione alle esigenze di servizio, dando preferenza all'invio di messaggi di testo in caso di brevi comunicazioni.
Qualora l'assegnatario del telefono cellulare si trovi negli uffici comunali, è fatto obbligo di utilizzare gli apparecchi della rete fissa per comunicare con altri apparecchi di rete fissa.
Al fine di garantire l'immediata rintracciabilità nei casi di necessità, gli utilizzatori dei telefoni cellulari hanno l'obbligo di mantenere in funzione il telefono cellulare durante le ore di servizio, durante le ore di reperibilità, ove previste ed in tutti i casi in cui le circostanze concrete lo rendano opportuno.

18.8 Doveri e responsabilità degli utilizzatori

Ogni assegnatario di apparecchio cellulare è tenuto all'uso appropriato ed alla diligente conservazione dell'apparecchio e dei suoi accessori, nonché alla piena conoscenza di tutte le funzioni e modalità di utilizzo previsto ed alla tenuta della prescritta documentazione.
È fatto divieto:

- di abbandonare o lasciare incustodito l'apparecchio cellulare;
- di utilizzare l'apparecchio cellulare per chiamate personali, nel caso in cui non sia stata

attivata l'opzione "dual billing".

18.9 Gestione degli apparecchi cellulari e del servizio di telefonia mobile

L'Ufficio economato, oltre a quanto altro indicato nel presente documento, provvede alla gestione degli apparecchi cellulari e del servizio di telefonia mobile ed in particolare:
a) presta la necessaria assistenza tecnica, disponendo la riparazione degli apparecchi cellulari in caso di guasto o la sostituzione in caso di furto o di smarrimento;
b) provvede alla adeguata diffusione dei numeri di telefono, comprese le eventuali variazioni;
c) provvede alla individuazione di forme contrattuali e gestionali più convenienti, alla gestione del contratto con la società telefonica, alla liquidazione delle relative fatture;
d) effettua verifiche a campione circa il corretto utilizzo degli apparecchi cellulari secondo le modalità indicate nell'Art. 37.

18.10 Rilevazione annuale delle informazioni e dei costi di esercizio

Al termine di ogni esercizio il Servizio Economato riepiloga su appositi tabulati tutti i dati concernenti i cellulari personali e di servizio. Le informazioni vengono utilizzate dallo stesso Servizio per provvedere al raffronto ed alla valutazione degli stessi in modo

tale che possa essere rilevato il volume di traffico, il costo medio e complessivo annuo. In tale sede viene altresì effettuata una valutazione circa la convenienza di mantenere attive le utenze cellulari nonché di ridefinirne le configurazioni in relazione alle esigenze.

Art. 19
Utilizzo dei telefoni fissi

19.1 Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non inerenti l'attività lavorativa stessa fatti salvi casi eccezionali e di emergenza. Non sono comunque ammesse telefonate private verso :

- interurbane su rete fissa;
- chiamate internazionali sia su rete fissa che cellulari;
- telefoni satellitari.

Art. 20
Utilizzo dei fax

20.1 E' vietato l'utilizzo dei Fax per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

20.2 Particolare attenzione deve essere posta all'inserimento del numero del destinatario al fine di evitare che informazioni sensibili possano essere inviate a destinatari non pertinenti.

20.3 I fax debbono essere posizionati e gestiti in modo tale che eventuali documenti trasmessi o ricevuti non siano accessibili a persone non autorizzate. I rapporti di ricezione, che possono contenere anch'essi dati sensibili, vanno raccolti e gestiti opportunamente.

Art. 21
Utilizzo di hardware di proprietà personale

21.1 L'utente può connettere postazioni di lavoro o apparati personali alla rete comunale solo con l'autorizzazione dell'amministratore di sistema.

21.2 Nel caso in cui l'hardware di proprietà personale non sia dotato di un software antivirus regolarmente aggiornato, potrà essere negato l'accesso alla rete comunale.

Art. 22
Utilizzo di software di proprietà personale

22.1 L'utente può utilizzare software di proprietà personale, solo con l'autorizzazione ed il coordinamento dell'amministratore di sistema, per fini di manutenzione, assistenza tecnica, dimostrazioni di prodotti , rappresentazioni pubbliche e altre condizioni in cui si manifesti la necessità di tale utilizzo.

22.2 Per quanto riguarda il software di proprietà personale, l'utente è il solo responsabile della rispondenza alle norme sulla proprietà intellettuale e della validità

delle licenze.

22.3 Il software dovrà essere verificato in merito alla presenza di malaware prima dell'utilizzo nella rete comunale.

22.4 L'utente sarà responsabile del funzionamento del software, della sua manutenzione e della integrità degli archivi gestiti.

Art. 23
Rispetto della proprietà intellettuale e delle licenze

23.1 Tutto il software in uso nel sistema informatico comunale deve essere ottenuto seguendo le procedure di acquisizione definite dai servizi informatici e deve essere registrato a nome dell'amministrazione comunale.

23.2 Tutto il software deve essere valutato preventivamente dall'amministratore di sistema al fine di verificarne l'idoneità tecnica ad operare sui sistemi informatici comunali.

23.3 Non è possibile installare, duplicare o utilizzare software o dati acquisiti al di fuori di quanto consentito dagli accordi di licenza. Tutti gli utenti sono tenuti al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright).

Art. 24
Utilizzo del Software sviluppato dagli utenti

24.1 I dipendenti comunali sono autorizzati a sviluppare procedure software basate sugli strumenti di automazione messi a disposizione dagli applicativi installati a bordo delle stazioni di lavoro (per esempio Microsoft Office). Le procedure software realizzate devono soddisfare particolari esigenze d'ufficio, non risolvibili ricorrendo agli applicativi resi disponibili dall'amministrazione.

24.2 L'utente realizzatore delle procedure software è il diretto responsabile della loro manutenzione e della integrità degli archivi gestiti.

24.3 L' utente è tenuto ad informare l'amministratore di sistema delle applicazioni sviluppate al fine di pianificare un opportuna politica di backup e di un eventuale integrazione con le applicazioni sviluppate dai servizi informatici.

Art. 25
Antivirus

25.1 L'utente non è autorizzato a modificare le impostazioni del software antivirus o ad interrompere le scansioni pianificate.

25.2 Ogni utente deve tenere comportamenti tali da proteggere i dati personali contro il rischio di intrusione e dall'azione di programmi aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.

25.3 Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato, secondo le procedure previste.

25.4 Nel caso che il software antivirus rilevi la presenza di un virus, l'utente dovrà segnalare immediatamente l'accaduto all'Amministratore di Sistema prendendo nota dei messaggi riportati dal software antivirus.

25.5 Ogni dispositivo rimovibile di provenienza esterna o dubbia 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.

Art. 26
Internet

26.1 Tutti gli utenti a cui è assegnata una postazione informatica di lavoro possono utilizzare Internet a meno di particolari restrizioni disposte dalla dirigenza dell'ente.

26.2 Ogni utente è direttamente e totalmente responsabile dell'uso di Internet, dei contenuti ricercati, dei siti contattati, delle informazioni recuperate e delle modalità con cui opera.

26.3 All'utente non è consentito:
- la navigazione su siti con contenuti di natura oltraggiosa o discriminatoria per sesso, lingua, religione, origine etnica, opinione e appartenenza politica o sindacale;
- servirsi della postazione di accesso ad internet per attività poste in essere in violazione del diritto di autore o altri diritti tutelati dalla normativa vigente
- effettuare transazioni finanziarie e/o acquisti on line se non attinenti l'attività lavorativa o espressamente autorizzati dal Responsabile;
- utilizzare per interesse personale sistemi Peer to Peer, di file sharing, podcasting, webcasting , istant messaging o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio, o TV via web);
- scaricare software, filmati o file musicali anche se gratuiti dalla rete, salvo casi di comprovata utilità lavorativa e comunque previa autorizzazione da parte del Responsabile dei Servizi Informatici;
- registrarsi a siti i cui contenuti non siano attinenti con l'attività lavorativa, partecipare a forum o utilizzare chat per motivi diversi da quelli lavorativi, registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Per evitare un uso non corretto della rete Internet, possono essere applicati appositi filtri per non accedere alle seguenti tipologie di siti:
- principali social-network italiani ed internazionali;
- siti peer to peer;
- siti di download di musiche e filmati.

26.4 E' consentito l'utilizzo di Internet per assolvere incombenze amministrative o burocratiche (rapporti con le banche, le assicurazioni, i gestori di servizi pubblici) purché contenuto nei tempi strettamente necessari alla svolgimento di tali transazioni.

Art. 27
Hot Spot WiFi

27.1 L'installazione di ogni dispositivo di collegamento radio deve essere sottoposto

alla preventiva valutazione dei servizi informatici al fine di valutare i possibili rischi di accessi non autorizzati alle risorse informatiche che tali sistemi presentano.

27.2 L'Amministrazione si riserva di modificare , sospendere o implementare il servizio senza nessun preavviso agli utenti in relazione alle esigenze di sicurezza della rete e alla conformità alle norme di legge dell'utilizzo della medesima.

27.3 La funzionalità degli accessi pubblici non è garantita H24, eventuali disservizi saranno risolti nel più breve tempo possibile compatibilmente con le priorità dei servizi informatici.

27.4 Sono possibili filtraggi in base all'indirizzo hardware dei dispositivi collegati. L'utente è tenuto alla scrupolosa custodia delle credenziali di accesso e dei certificati di autenticazione.

Art. 28
Posta elettronica

28.1 La casella di posta, assegnata dall'Amministrazione Comunale al dipendente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

28.2 La casella di posta elettronica deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto ingombranti. Alla casella di posta potranno essere applicate delle limitazioni alla dimensione della casella stessa.

28.3 Tutti i messaggi di posta elettronica sono soggetti a scansione antivirus. Il sistema procederà alla rimozione di eventuali allegati sospetti.

28.4 L'assegnazione dell'indirizzo di posta elettronica avviene contestualmente all'assegnazione delle credenziali di autenticazione dell'utente ed è riconducibile alla forma ncognome@comune.zolapredosa.bo.it dove ncognome è l'iniziale del nome seguita dal cognome. I casi di omonimia saranno gestiti di volta in volta e concordati con l'utente.

28.5 L'accesso al servizio di posta elettronica da parte di un utente avviene mediante le credenziali di autenticazione (user-id e password) di accesso al sistema informativo. L'accesso alla posta elettronica è possibile anche da internet.

28.6 Al dipendente non è consentito:
- utilizzare la casella di posta elettronica comunale assegnata per la partecipazione a dibattiti, forum e mailing list ad eccezione dei casi in cui queste operazioni siano strettamente attinenti la propria attività lavorativa;
- diffondere messaggi di posta elettronica di dubbia provenienza od aprire od inviare catene telematiche ;
- aprire allegati di non comprovata origine
- effettuare il download di file con estensioni: .vbs, .bat, .exe
- effettuare tecniche di mail spamming, cioè inviare un numero massiccio di comunicazioni a liste di distribuzione extra aziendali o azioni equivalenti.
- Inviare dati sensibili o giudiziari in chiaro.

I messaggi di posta elettronica in chiaro diretti all'esterno possono essere intercettati durante il recapito, pertanto, nel caso di invio di dati sensibili, giudiziari o estremamente riservati, occorre prevedere l' utilizzo di procedure di crittografia nei messaggi inviati. Tali procedure debbono comunque fare riferimento alle norme vigenti in materia.

28.7 Deve essere posta attenzione ad evitare l' invio di informazioni a destinatari non pertinenti.

28.8 Per evitare la diffusione a tutti di indirizzi di posta in messaggi con destinatari multipli utilizzare il modo Bcc.

28.9 Nel caso di ricezione di messaggi non pertinenti segnalare al mittente il problema e distruggere il messaggio.

28.10 L' utente deve verificare il corretto funzionamento del filtro antispam, provvedendo a fornire al sistema le indicazioni riguardo i falsi positivi e i falsi negativi.

28.11 Ciascun utente, titolare di una casella di posta, può utilizzare specifiche funzionalità di posta elettronica per inviare automaticamente, in caso di assenza, messaggi di risposta che informino il mittente della propria indisponibilità, e funzioni di inoltro automatico dei messaggi ricevuti verso indirizzi di altro utente, sempre considerando gli aspetti relativi alla gestione dei dati sensibili.

28.12 Nel caso in cui un utente si assenti senza aver provveduto ad attivare i suddetti sistemi di inoltro e da questo derivasse un interruzione del servizio l'amministratore di sistema, dietro richiesta del responsabile/direttore, provvederà all'accesso della casella di posta al fine di garantire la continuità dell'attività lavorativa.

Art. 29
Intranet

29.1 L'utente può trovare sul sito web della intranet comunale numerose informazioni riguardanti l' organizzazione del Comune di Zola Predosa, norme e regolamenti, procedure e informazioni, guide e manuali sull'utilizzo delle risorse informatiche messe a disposizione dall'amministrazione. Indicazioni su miglioramento e modifiche delle informazioni pubblicate vanno inviati ai Servizi Informatici. Il sito web della intranet è all'indirizzo **http://intranet.zola.net/ezpublish**

Art. 30
Groupware

30.1 Si intende per groupware un programma atto a facilitare e rendere più efficace il lavoro cooperativo da parte di gruppi di persone. E' compito dell'utente mantenere aggiornate le informazioni relative al servizio, al numero di telefono e dell'eventuale cellulare di servizio. L'utente deve modificare questi dati ogni volta che variano in modo da garantire la consistenza della rubrica o , nel caso non possa operare direttamente, informare i servizi informatici delle variazioni.

Il Segretario generale
Dr.ssa Daniela Olivi

Il Sindaco
Stefano Fiorini

30.2 Il groupware va inoltre utilizzato per gestire le prenotazioni delle sale, degli appuntamenti e per condividere informazioni e documenti.

30.3 Il groupware è accessibile da internet, le informazioni sul modo di accesso sono disponibili sul sito web della intranet.

Art. 31
Messaggi SMS

31.1 Il sistema di invio SMS va utilizzato esclusivamente per ragioni di servizio. I responsabili debbono attribuire agli operatori gli opportuni privilegi necessari allo svolgimento dei compiti.

31.2 Il database dei numeri telefonici contiene dati riservati e va quindi trattato opportunamente.

Art. 32
Videosorveglianza

32.1 Le attività di videosorveglianza sono normate da apposito regolamento comunale e dalla normativa nazionale vigente in materia.

Art. 33
Altri servizi

33.1 I numerosi servizi messi a disposizione dall'amministrazione sono raggruppati in un portale di accesso posizionato nella intranet comunale all'indirizzo: http://pafweb.zola.net

Art. 34
Disponibilità dei servizi

34.1 I servizi forniti sono disponibili tutti i giorni con la limitazione delle ore notturne in cui possono verificarsi arresti di alcuni servizi per effettuare le copie di backup dei dati. Eventuali operazioni di manutenzione vengono preannunciate tramite posta elettronica , sul portale delle applicazioni e mediante messaggistica di rete. Per maggiori dettagli contattare i servizi informatici.

Disposizioni sui Controlli

Art. 35
Controlli e Tracciamento navigazione

35.1 In caso di anomalie dei sistemi rilevate dal personale dei servizi informatici sono effettuati controlli anonimi che si concludono con avvisi generalizzati, diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzia l'utilizzo irregolare degli strumenti aziendali e si invitano gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

35.2 In presenza del perdurare delle anomalie riscontrate sarà invece possibile un'intensificazione dei controlli che possono giungere fino alla verifica dell'identificativo del terminale utilizzatore e del codice identificativo con il quale è stato utilizzato Tali controlli su base individuale possono essere autorizzati dal dirigente competente dietro richiesta motivata e non generica, in ogni caso solo dopo ripetute anomalie, delle quali deve essere tempestivamente data informazione al dirigente

competente. Tali procedure saranno gestite nel massimo rispetto delle disposizioni in materia di tutela della privacy.

35.3 Il traffico internet della rete comunale è registrato.
I dati registrati potranno essere aggregati per svolgere controlli finalizzati ad evitare abusi nell'uso di Internet o per determinare le cause di eventuali malfunzionamenti del sistema.

35.4 I computers e le stampanti connessi alla rete comunale sono monitorati per quanto riguarda le caratteristiche hardware, software e nome utente utilizzatore al fine di mantenere un censimento continuamente aggiornato del parco macchine installato.

35.5 Sulle fotocopiatrici viene controllato il volume di copie e stampe tramite codice di accesso legato all'ufficio.

35.6 La quasi totalità dei server e apparati di rete è sotto continuo monitoraggio funzionale al fine di evidenziare in modo precoce l' emergere di problemi di funzionamento.

35.7 L'amministratore di sistema, su richiesta dell'autorità giudiziaria potrà in ogni momento fornire i dati registrati dal sistema.

Art. 36

Controlli relativi all'utilizzo dei telefoni cellulari

36.1 Finalità dei controlli. Esclusioni

L'ente effettua controlli sull'utilizzo degli apparecchi cellulari messi a disposizione al fine di:
• verificarne il corretto utilizzo;
• monitorare e ridurre la spesa pubblica, sia rilevando eventuali danni patrimoniali già posti in essere sia agendo quale deterrente rispetto a comportamenti impropri, per cui la loro omissione potrebbe comportare responsabilità patrimoniali dirette;
• tutelare l'immagine dell'ente e di coloro che vi prestano la propria attività.
I controlli effettuati dall'ente devono rispettare i principi di necessità, proporzionalità, imparzialità, trasparenza e protezione dei dati personali.
Al fine di preservare il libero esercizio delle funzioni politiche, sono esclusi dai controlli gli apparecchi cellulari messi a disposizione degli organi politici.

36.2 Tipologia dei controlli

I controlli sull'utilizzo degli apparecchi cellulari sono di due tipologie:
• controlli semestrali;
• controlli puntuali.

36.3 Controlli semestrali

Semestralmente il Servizio Economato procede alla verifica dei costi sostenuti per la telefonia mobile al fine di monitorare e razionalizzarne la spesa così come previsto dall'art. 2, c. 294 della legge finanziaria per il 2008 (L. 244/07) e ai fini della redazione della Rilevazione annuale citata in precedenza.

36.4 Controlli puntuali

Il controllo puntuale sull'utilizzo degli apparecchi cellulari viene effettuato:
a) su segnalazione nominativa del diretto superiore (Responsabile di Servizio / Direttore di Area);
b) nel caso in cui, in sede di controllo semestrale, vengano riscontrate evidenti anomalie o rilevanti scostamenti di oltre il 30% nel volume complessivo di traffico relativo alla singola utenza rispetto alla media registrata nei sei mesi precedenti.
Nel valutare l'attivazione del controllo puntuale indicato alla lettera b), si dovrà tenere in considerazione eventuali necessità, anche temporalmente limitate, connesse a particolari finalità istituzionali o di servizio, a conoscenza del responsabile del servizio.

36.5 Svolgimento delle verifiche
L'avvio del controllo puntuale deve essere comunicato per iscritto all'interessato e, per conoscenza, al responsabile del servizio competente. Nel caso in cui il controllo venga effettuato su segnalazione del Responsabile di Servizio / Direttore di Area, deve essere specificato che può essere presentata richiesta di accesso ai relativi documenti amministrativi a norma della Legge n. 241/1990. Il termine per la conclusione del procedimento è di 30 giorni.
Il controllo viene effettuato sulle informazioni rese disponibili dall'operatore telefonico inerenti il volume complessivo di traffico relativo, contenenti:
• indicazione analitica delle chiamate in uscita addebitate all'ente, comprensiva dei numeri di telefono (con oscuramento almeno delle ultime tre cifre) dei tempi e del relativo importo
• i dati del costo complessivo di collegamenti a internet effettuati con apparecchi cellulari.
La documentazione analitica sarà controllata preventivamente dal Servizio Economato e successivamente inviata al Responsabile del Servizio/Direttore di Area competente per un esame congiunto con l'utilizzatore, al fine di verificarne in particolare la pertinenza con l'attività lavorativa svolta.

36.6 Esito delle verifiche
Sulla base delle verifiche svolte, il Responsabile del Servizio/Direttore di Area competente comunica immediatamente per iscritto all'utilizzatore l'esito del controllo ed avvia, nel caso in cui ritenga che vi sia stato un utilizzo improprio dell'apparecchio, i procedimenti conseguenti.

Art. 37
Disposizioni finali

37.1 Per tutto quanto non previsto e disciplinato dal presente Regolamento si rimanda alla normativa vigente in materia con particolare riferimento al Codice dell'Amministrazione Digitale.

Il Segretario generale
Dr.ssa Daniela Olivi

Il Sindaco
Stefano Fiorini