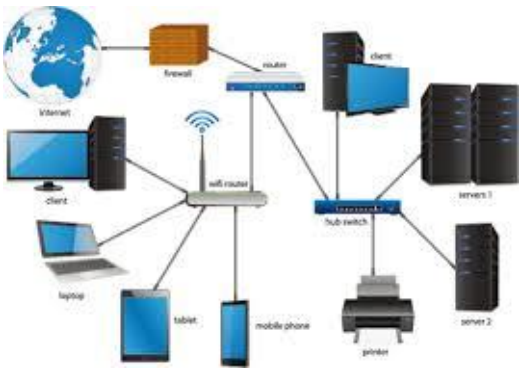
COMUNE DI
MONTEPRANDONE

REGOLAMENTO PER L'UTILIZZO DI STRUMENTI INFORMATICI E SULLA SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI ELETTRONICI



Approvato con DGC n. 66 del 17.06.2021

Premessa

Il presente Regolamento raccoglie norme e linee guida da seguire per eliminare o ridurre i rischi derivanti da un uso scarsamente corretto ed a volte poco consapevole dell'utilizzo degli strumenti elettronici.

Un uso degli strumenti elettronici, difforme dalle regole contenute nel presente regolamento, può esporre il Comune di Monteprandone a rischi di accessi non autorizzati o alla divulgazione di informazioni relative al sistema informatico interno.

L'utilizzatore è la prima "vittima" della violazione della riservatezza e della sicurezza e per tale motivo il presente documento vuole innanzi tutto tutelare e salvaguardare chi con la propria attività lavorativa utilizza questi strumenti. I dati trattati per mezzo dei sistemi del Comune di Monteprandone rimangono di proprietà dello stesso.

Quadro normativo di riferimento

- Regolamento Europeo 2016/679. Regolamento generale per la protezione dei dati personali.
- Decreto Legislativo 30 giugno 2003, n. 196. Codice in materia di protezione dei dati personali (recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE).
- Legge 20 maggio 1970 n. 300. Norme sulla tutela della libertà e dignità del lavoratori, della libertà sindacale e dell'attivita' sindacale nei luoghi di lavoro e norme sul collocamento (*Statuto dei lavoratori*).
- Legge 18 agosto 2000 n. 248. Nuove norme di tutela del diritto d'autore.
- Legge 7 agosto 1990 n. 241. Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

Adozione

Il presente Regolamento è formalmente adottato con le forme e le modalità di cui all'art. 26 del vigente Regolamento Comunale sull'ordinamento degli uffici e servizi.

INDICE

Capo I - Disposizioni generali

Art. 1 - Oggetto e ambito di applicazione

1. Il presente regolamento disciplina:
    a) le modalità di utilizzo degli strumenti informatici nell'ambito dello svolgimento dell'attività lavorativa;
    b) le modalità di utilizzo della posta elettronica, di internet, della rete aziendale, delle password assegnate, dei telefoni aziendali, sia fissi che mobili;
    c) le misure tecniche, informatiche, organizzative e logistiche necessarie per garantire il livello minimo di protezione per il trattamento dei dati personali dei lavoratori e di terzi e tutela della dignità sul luogo di lavoro, ai sensi delle vigenti norme in materia, nonché per assicurare gli adeguati livelli di sicurezza ed integrità del patrimonio informativo dell'Amministrazione Comunale;
    d) le modalità di effettuazione dei controlli e le conseguenze della violazione delle disposizioni del presente regolamento.
2. Il presente documento si applica a tutti i soggetti che utilizzano le risorse informatiche (strumentazioni informatiche, apparecchi telefonici e posta elettronica ecc.) del Comune di Monteprandone presso qualunque sede o ufficio riconducibile alla struttura, siano essi dipendenti a tempo pieno o parziale, collaboratori, consulenti, dipendenti di aziende esterne legate da contratti di fornitura di servizi, amministratori o altri soggetti a cui ne è concesso l'uso presso qualunque sede o ufficio riconducibile alla struttura. Ai collaboratori non si applicano le disposizioni relative alle sanzioni disciplinari che rimangono in capo al soggetto che ne ha autorizzto l'uso.

Art. 2 - Indicazioni generali

1. Le apparecchiature informatiche, i programmi e, in generale, la strumentazione che l'Amministrazione Comunale di Monteprandone mette a disposizione dei soggetti di cui all'art. 1, comma 2, possono essere utilizzate, nel pieno rispetto delle norme del presente Regolamento, solo per scopi strettamente professionali ed istituzionali. Ciò vale sia per le risorse condivise (risorse di rete, stampanti di rete, fax, servizi di tipo Internet/posta elettronica ecc.), sia per quelle affidate al singolo dipendente (Personal Computer, periferiche, stampanti locali, ecc.). Le risorse informatiche affidate al singolo Incaricato sono strumenti di lavoro appartenenti al patrimonio del Comune di Monteprandone e pertanto vanno custoditi in modo appropriato; il furto, il danneggiamento o lo smarrimento di tali strumenti debbono essere prontamente segnalati all'Ente.
2. L'Amministrazione comunale è titolare di tutte le risorse informatiche dell'Ente. Il personale dipendente e/o assimilato, per mezzo del presente regolamento, é preventivamente informato su quali siano gli usi consentiti e proibiti di tali risorse.
3. I Personal Computer, sia fissi che mobili, che vengono consegnati all'Incaricato sono comprensivi del software certificato e necessario a svolgere correttamente le mansioni affidate. Non è consentito modificare le configurazioni impostate sul proprio PC.
4. L'Amministrazione, nel rispetto dei principi di cui alle premesse, può memorizzare e conservare i dati relativi alla navigazione in internet e al traffico telematico dei dipendenti e collaboratori per il tempo strettamente necessario agli adempimenti di natura tecnica o relativi alla sicurezza e comunque giustificati dall'adempimento da precise disposizioni normative, e in ogni caso per un periodo non superiore a due anni. Tali dati sono detenuti e custoditi dal Servizio Informatica.
5. Nel rispetto del principio della prevenzione degli abusi, l'Ente si riserva il diritto di eliminare o sospendere in qualsiasi momento l'accesso a determinati siti Internet, mediante sistemi di blocco automatico o simili, ovvero a limitare l'accesso ai soli siti istituzionali riconducibili all'attività lavorativa, così come di bloccare la ricezione di files sospetti allegati a messaggi di posta elettronica aziendale.
6. Ogni infrazione alle regole dell'Ente per un uso corretto del Sistema Informatico Comunale costituirà una violazione della sicurezza ed esporrà l'utente alle conseguenze di cui al capo V del presente regolamento.
7. Tutti i soggetti interessati dalle disposizioni del presente Regolamento sono tenuti a contattare il Responsabile dell'unità organizzativa di cui fanno parte 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.

Art. 3 - Soggetti, competenze e responsabilità

1. Le competenze e le responsabilità del personale dell'Amministrazione comunale per ciò che concerne l'utilizzo dei servizi informatici, sono definite nei commi seguenti del presente Regolamento.
2. I responsabile di settore 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 a tutti gli obblighi inerenti la titolarità loro affidata in materia di trattamento di dati personali gestiti dall'Amministrazione Comunale, in applicazione del Regolamento Europeo 2016/679.

3. L'amministratore di Sistema, incaricato della sicurezza informatica, o le persone o ditte esterne all'uopo incaricate, sono tenuti a svolgere le seguenti attività:
   a) monitorare i sistemi per individuare un eventuale uso scorretto degli stessi e/o gni eventuale attività non auto-rizzata sui sistemi.nel rispetto della privacy degli utenti e secondo le previsioni del presente regolamento;
   b) adottare tutte le misure atte a garantire la sicurezza del Sistema Informatico Comunale;
   c) implementare le policy di sicurezza sul Sistema Informatico Comunale;
   d) dare informazioni in materia di sicurezza informatica, e tutte le necessarie istruzioni per un utilizzo ragionevolmente sicuro del sistema informative.
4. Ciascun dipendente comunale e collaboratore è personalmente e direttamente responsabile per ciò che concerne:
   a) il rispetto delle regole di cui al presente regolamento;
   b) ogni uso che venga fatto delle attrezzature informatiche e delle credenziali (account, passwords, user Id) assegnategli, fatto salvo l'eventuale uso improprio degli stessi derivante da fatto non imputabile al dipendente.

Art. 4 - Definizioni

1. 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"**

Capo II – Disposizioni sull'utilizzo della strumentazione in dotazione

Art. 5 – Assegnazione di hardware e software al personale e regole per l'utilizzo

1. Per prevenire l'introduzione di virus e/o altri programmi dannosi e per proteggere l'integrità del Sistema Informatico Comunale, tutto l'hardware ed il software in dotazione agli uffici deve essere registrato a nome dell'Amministrazione Comunale ed assegnato ai dipendenti esclusivamente dal Servizio Informatica, competente in materia.
2. Al fine di proteggere l'integrità del Sistema Informatico Comunale, non possono essere utilizzati eventuali software di proprietà personale, tra cui rientrano anche i programmi regolarmente acquistati e registrati, programmi shareware e/o freeware, eventuali software scaricati da Internet o provenienti da CD/DVD allegati a riviste e/o giornali o altri software posseduti a qualsiasi titolo. Nel caso in cui tali software dovessero essere utili per lavoro, l'utente deve contattare il Servizio Informatica, previa autorizzazione scritta del proprio Responsabile. Il Servizio Informatica, esaminata la richiesta, può consentire lo "sblocco" per l'installazione.
3. Non possono essere installati e/o utilizzati supporti hardware diversi da quelli assegnati (es. modem, masterizzatori, webcam, microfoni e in generale qualsiasi tipo di supporto informatico). E' consentito l'utilizzo di personal computers e altro hardware di proprietà del dipendente/collaboratore solo previa autorizzazione del Responsabile di riferimento, ed in conformità delle disposizioni del presente regolamento.
4. Il personale è tenuto al rispetto delle leggi in materia di tutela della proprietà intellettuale (copyright) e non può installare, duplicare o utilizzare i software al di fuori di quanto consentito dagli accordi di licenza.
5. L'assistenza tecnica per malfunzionamenti ordinari o diagnosi di sistema attraverso strumenti di controllo remoto deve avvenire solo previa autorizzazione dell'utilizzatore e di norma in presenza dell'utilizzatore stesso.
6. In caso di malfunzionamenti straordinari e in situazioni di emergenza il Responsabile della sicurezza ha la facoltà in qualunque momento di accedere a qualunque sistema informatico del Comune di Monteprandone per l'espletamento delle proprie funzioni

Art. 6 – Utilizzo del personal computer assegnato al singolo utente

1. Il personal computer, fisso o portatile, assegnato al dipendente è uno strumento di lavoro e deve essere utilizzato secondo criteri di diligenza e correttezza, nonché sulla base delle prescrizioni del presente articolo.
2. Il dipendente non può spostare il pc di proprietà dell'Ente in altro ufficio o fuori dai locali comunali, salvo autorizzazione del Responsabile di Settore, sentito il Servizio Informatica, ed è tenuto a custodire il pc con la massima diligenza, curando di spegnerlo sia al termine della giornata lavorativa, che nel caso di assenze prolungate dall'ufficio, al fine di evitare accessi da parte di terzi non autorizzati. Il pc in dotazione può essere lasciato acceso esclusivamente nel caso di utilizzo dello stesso mediante desktop remoto appositamente autorizzato. In questo caso il dipendente deve assicurarsi di aver attivato lo stand-by protetto da password.
3. Il dipendente non può modificare le impostazioni del pc assegnato e non può installare qualsiasi soft- ware senza l'autorizzazione di cui al precedente articolo 5, comma 2.

4. A ciascun dipendente è assegnata una password per l'accesso al proprio personal computer, la quale deve essere custodita con la massima cura e non divulgata.
5. I dipendenti sono tenuti a variare la password con cadenza periodica, in conformità a quanto previsto dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Codice in materia di protezione dei dati personali); di ciò verranno previamente avvisati dal Servizio Informatica.
6. I dipendenti possono utilizzare il personal computer di un collega assente solo ed esclusivamente per improrogabili necessità di lavoro (quale, ad esempio, la temporanea impossibilità di utilizzo del proprio personal computer per cause tecniche), previa autorizzazione del Responsabile di Settore. Di tale evento deve essere redatto verbale, sottoscritto dal Responsabile di Settore e dall'utilizzatore, da cui risultino il soggetto utilizzatore, le ragioni che hanno reso necessario l'utilizzo di altro personal computer, la durata dell'utilizzo e ogni altra indicazione utile.
7. L'uso del personal computer del Comune è consentito per motivi personali solo se ricorrono tutte le condizioni tassativamente indicate di seguito:
    a) il computer non deve essere utilizzato a scopi di profitto (es. affari commerciali per un'altra attività professionale);
    b) non devono essere visionati e/o salvati contenuti che possono creare un danno, anche di immagine, all'Ente, ovvero contenuti illeciti e contenuti pornografici;
    c) non è in ogni caso consentito il salvataggio o l'archiviazione di dati non riconducibili all'attività lavorativa;
    d) l'uso delle attrezzature per scopi diversi dal lavoro è tollerato solo al di fuori degli orari di lavoro.

Art. 7 - Rete del Comune di Monteprandone

1. La possibilità di accedere alla rete interna da parte di ogni utilizzatore, rappresenta lo strumento più rilevante per il trattamento dei dati e per l'utilizzo dei servizi di accesso e condivisione delle risorse. L'utilizzo della complessa e diversificata gamma dei servizi erogati deve aderire ai compiti e alle attività assegnate per il raggiungimento del fine istituzionale del Comune di Monteprandone.
2. Le modalità di accesso richiedono sempre l'assegnazione di Credenziali di autenticazione, corredate da precise norme di attivazione, controllo e disattivazione.
3. Il corretto utilizzo delle risorse di rete è strettamente correlato a scopi strettamente lavorativi, per tale motivo ogni attività deve essere adeguata a questi vincoli. Sono vietate all'utilizzatore le seguenti attività:
    - Trasgressione della riservatezza di altri utilizzatori o dell'integrità di dati personali.
    - Compromissione dell'integrità dei sistemi e dei servizi.
    - Consumo di risorse in misura tale da compromettere l'efficienza di altri servizi di rete.
4. Il Comune di Monteprandone si riserva la facoltà di procedere alla verifica ed alla eventuale rimozione di qualsiasi file o applicazione memorizzato sulle cartelle di rete se ritenuto rischioso per la sicurezza dei sistemi, od anche acquisito e installato in violazione delle norme contenute nel presente documento.

Art. 8 - Spazio disponibile sul server dell'ente

1. Lo spazio disponibile sul server è finalizzato a garantire la sicurezza dei dati, attraverso il salvataggio dei dati su uno spazio protetto, oltre che sul personal computer assegnato, nonché a consentire a più utenti di lavorare con maggiore efficacia su files condivisi. Ciascun utente può memorizzare dati (esclusi quelli estranei all'attività lavorativa) solo all'interno della directory del proprio servizio o directory personale.
2. Sul server aziendale possono essere archiviati e salvati solo dati relativi all'attività lavorativa. Poiché i dati salvati sul server aziendale sono in linea generale visibili per tutti coloro che hanno accesso alla rete comunale, ciascun Responsabile di Settore stabilisce per la propria area o servizio quali dati possono essere salvati sul server, nel rispetto delle disposizioni vigenti anche a livello di ente in tema di privacy. I files contenenti dati personali e riservati saranno ospitati in apposite directory accessibili solo a livello di servizio o, comunque, ad un numero limitato di utenti, su indicazione del Responsabile di Settore competente.
3. Il Servizio Informatica può in qualsiasi momento rimuovere dal server qualsiasi file ritenuto pericoloso per l'integrità del sistema e non conforme alle prescrizioni del regolamento, previa comunicazione al dipendente/collaboratore. Inoltre, il Servizio Informatica può diramare in qualsiasi momento avvisi rivolti alla generalità dei dipendenti, o a gruppi più ristretti, a seconda dei casi, per segnalare la presenza di files non consentiti, ma non pericolosi per l'integrità del sistema, con l'invito a rimuoverli autonomamente entro un breve termine perentorio. Decorso inutilmente il termine, i files sono rimossi dal Servizio Informatica,con conseguente segnalazione al Responsabile di Settore nella cui area o servizio è avvenuta la violazione per i necessari provvedimenti.

Art. 9 – Assegnazione delle credenziali di autenticazione

1. Ad ogni utilizzatore, previa richiesta da parte del proprio responsabile, vengono assegnate le Credenziali di autenticazione e i relativi profili di autorizzazione necessari e sufficienti all'attività che sarà tenuto a svolgere.
2. Tipicamente viene assegnata la Credenziale di accesso alla rete dell'Ente e le Credenziali necessarie all'utilizzo

dei prodotti software utilizzati dal Comune di Monteprandone.

3. Il Codice di identificazione personale, associato alla Credenziale, non può venir assegnato ad altri incaricati, neppure in tempi diversi.
4. La Parola chiave della credenziale di autenticazione di accesso alla rete del Comune di Monteprandone deve venir cambiata almeno ogni 3 mesi.
5. La comunicazione del Codice di identificazione e della Parola chiave avviene mediante l'invio in busta chiusa e sigillata al richiedente che provvederà ad inoltrarla all'utilizzatore.

Art. 10 – Cancellazione e disattivazione

1. Le Credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate dagli Amministratori di sistema, salvo quelle autorizzate per soli scopi di gestione tecnica. Vengono ugualmente disattivate anche in caso del venir meno delle condizioni che consentono all'utilizzatore l'accesso ai dati personali.
2. Il Codice per l'identificazione non può venir assegnato ad altri incaricati, neppure in tempi diversi.
3. La cancellazione definitiva di una Credenziale viene effettuata qualora non venga più verificata la sussistenza delle condizioni per la sua conservazione. Ciò avviene periodicamente, e comunque a cadenza annuale, ed è a carico degli Amministratori di sistema.

Capo III – Disposizioni Utilizzo Posta elettronica - Intranet - Internet – Telefonia

Art. 11 - Posta elettronica

1. La posta elettronica è uno strumento di lavoro e, come tale, va utilizzato secondo criteri di diligenza e correttezza, nonché sulla base delle prescrizioni del presente articolo.
2. L'assegnazione degli account di posta elettronica implica l'obbligo di utilizzo di tale mezzo di comunicazione solo per lo svolgimento della propria attività lavorativa.
3. È concesso l'uso della posta elettronica del Comune anche per motivi privati e/o per contatti interpersonali (es. per inviare o ricevere mail da un amico), ma solo se sussistono le seguenti condizioni tassativamente indicate:
   a) le mail non devono essere utilizzate per scopi di profitto (es. scambio di dati commerciali per un'altra attività);
   b) le mail non devono comprendere contenuti che possono creare un danno, anche di immagine, all'Ente, ovvero contenuti illeciti e contenuti pornografici;
   c) l'uso della posta elettronica per scopi diversi dal lavoro è tollerato solo al di fuori degli orari di lavoro.
4. È' vietato installare ed utilizzare sistemi client di posta elettronica non conformi agli standard adottati dall'Ente.
5. Il dipendente non deve rivelare ad alcuno le proprie credenziali per l'accesso ai servizi di posta elettronica e/o di rete, nè utilizzare il nome utente e la password di altri utenti.
6. La formula "**everyone (tutti)**", ovvero un elenco contenente tutti gli indirizzi mail del personale e non, come destinatario di posta elettronica può essere utilizzata solo dai Responsabili o da persone specificamente autorizzate dai Responsabili per una specifica tipologia di "everyone" (*Esempio: un comunicato stampa può essere inviato con everyone dal responsabile del'Ufficio Stampa e relazioni esterne o da personale da lui stabilmente delegato per questa specifica tipologia di invio. Altro esempio: una mail relativa a un'interruzione dei servizi informatici per manutenzione può essere inviata con everyone dal Resonsabile del Servizio Informatica o da personale da lui stabilmente delegato per questa specifica tipologia di invio*). È espressamente vietato l'utilizzo della formula "**everyone**" per l'invio di mail di scherzi, l'invio di auguri di qualsiasi tipo (Natale, ecc.), catene telematiche ed ogni altra tipologia di messaggio non espressamente prevista in questo disciplinare. Si ribadisce che lo strumento della posta elettronica non è equiparabile ad un forum per ospitare discussioni, commenti, considerazioni di varia natura, ecc.. **La formula "everyone" può essere utilizzata per comunicazioni di carattere sindacale da parte dei rappresentanti sindacali interni, nonché delle organizzazioni sindacali che, in possesso dei requisiti previsti per fruire delle prerogative sindacali previste dalla normativa di riferimento, abbiano preventivamente comunicato all'ente il nominativo del dipendente autorizzato ad inoltrare comunicazioni attraverso la posta elettronica aziendale.**
7. 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.
8. In caso di assenza prolungata o comunque programmata, nel caso in cui fosse eccezionalmente necessario accedere alla posta elettronica di un dipendente assente per improrogabili necessità di lavoro, il Responsabile della Sicurezza Informatica, previa apposite richiesta del Responsabile di Settore interessato, ne può abilitare l'accesso ad altro utilizzatore. Di tale evento deve essere redatto verbale, sottoscritto dal Responsabile e dall'utilizzatore, da cui risultino il soggetto utilizzatore, le ragioni che hanno reso necessario l'utilizzo di altro personal computer, la durata dell'utilizzo e ogni altra indicazione utile.
9. **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**.

Art. 12 – Riservatezza della Posta elettronica

1. Si rammenta che la confidenzialità della posta elettronica è limitata in quanto i messaggi transitano nella rete pubblica di Internet e possono essere quindi visionati da terzi non autorizzati. Il livello di riservatezza di una email si avvicina di più a quello di una lettera aperta (cartolina), piuttosto che a quello di una lettera chiusa, a meno che non si sia utilizzato un sistema di cifratura.
2. L'invio di comunicazioni elettroniche con informazioni personali, si ricorda, è sottoposto alla disciplina prevista dal Regolamento Europeo 2016/679. Regolamento generale per la protezione dei dati personali.
3. Si raccomandano gli utenti a prestare la massima attenzione nella stampa di messaggi di posta elettronica, soprattutto nel caso si utilizzino delle stampanti di gruppo o accessibili a più persone.
4. Si raccomanda di inserire la firma in calce all'email nonché, nei casi in cui non sia già inserita automaticamente, un'adeguata avvertenza sulla privacy e sulla riservatezza dei messaggi inviati, come nell'esempio successivo:
   "Questo messaggio ed i suoi allegati è di carattere riservato ed è indirizzato esclusivamente al destinatario specificato. L'accesso, la divulgazione, la copia o la diffusione sono vietate a chiunque altro ai sensi delle normative vigenti, e possono costituire una violazione penale. In caso di errore nella ricezione, il ricevente è tenuto a cancellare immediatamente il messaggio, dandone conferma al mittente a mezzo email. "
   "This message and its attachments (if any) may contain confidential, proprietary or legally privileged information and it is intended only for the use of the addressee named above. No confidentiality or privilegi is waived or lost by any mistransmission. If you are not the intended recipient of this message you are hereby notified that you must not use, disseminate, copy it in any form or take any action in reliance on it. If you have received this message in error, please, delete it (and any copies of it) and kindly inform the sender, of this email."

Art. 13 – Internet

1. Gli utenti sono tenuti ad utilizzare il collegamento ad Internet per motivi legati all'esecuzione della prestazione lavorativa
2. **Sono pertanto vietati**:
   a) 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;
   b) l'utilizzo di qualsiasi mezzo alternativo (modem, chiavette sim o altro) al collegamento predisposto dall'Ente per connettersi ad Internet;
   c) l'accesso alla rete dall'esterno con qualsiasi altro mezzo di accesso remoto senza apposita autorizzazione del Responsabile di Settore competene e del Responsabile della sicurezza informatica;
   d) 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.
   e) disabilitare i sistemi adottati per bloccare l'accesso ad alcuni siti.
   f) Partecipare a forum non professionali, l'utilizzo di chat line (escluso gli strumenti autorizzati), di bacheche elettroniche e la registrazione in guestbook anche utilizzando pseudomini, con la sola esclusione di quelli espressamente autorizzati per iscritto.
   g) Gli utilizzatori sono invitati a limitare il rilascio di informazioni personali durante la navigazione via Web. L'utilizzatore è tenuto nel corso della navigazione a leggere con attenzione qualsiasi finestra, pop-up o avvertenza prima di proseguire nella navigazione e in particolare prima di accettare delle condizioni contrattuali o di aderire a delle iniziative online.
   h) Nel caso di comunicazione di dati sensibili o informazioni riservate via Web è necessario accertarsi che vi sia la protezione della comunicazione attraverso un opportuno protocollo di sicurezza. Ad esempio nel caso di Microsoft Explorer ciò può essere verificato controllando che nel bordo inferiore destro del browser appaia il disegno di un piccolo lucchetto chiuso di colore giallo.
3. È concesso l'uso del collegamento Internet del Comune anche per motivi personali (es. vedere il sito di un luogo di vacanza), ma è vincolato a tre condizioni:
   a) l'uso di Internet non deve essere per scopi di profitto;
   b) l'uso di Internet non deve comprendere contenuti che possono creare un danno, anche di immagine, all'Ente, ovvero contenuti illeciti e contenuti pornografici;
   c) l'uso di Internet per scopi diversi dal lavoro è tollerato solo al di fuori degli orari di lavoro.
4. Ai sensi del presente regolamento, l'uso corretto e responsabile delle risorse Internet innanzitutto comporta:
   a) l'astensione da usi illegali e non etici;
   b) l'astensione dall'invio, ricezione o mostra di testi o immagini che possano essere offensivi per i destinatari o per le persone presenti in ufficio;
   c) il rispetto dei diritti di proprietà intellettuale facendo solo copie autorizzate di programmi o dati soggetti a copyright;

d) il rispetto della riservatezza di persone e/o siti, non spacciandosi per un altro utente, non tentando di raggiungere o modificare l'accesso a file, password o dati che appartengono ad altri, non cercando di disattivare o sabotare l'accesso o l'utilizzo di qualunque sistema o rete di computer tramite Internet.

Art. 14 – Disciplina ed addebito delle telefonate effettuate in casi eccezionali

1. I Telefoni aziendali sia fissi che mobili devono essere utilizzati esclusivamente per motivi di lavoro.
2. Sono consentite ai dipendenti comunali, limitatamente a casi eccezionali, telefonate personali, e l'utilizzazione dei dispositivi mobili in dotazione con addebito delle relative spese.

Capo IV – Disposizioni per il trattamento di dati personali

Art. 15 – Elementi di sicurezza dei dati personali

1. Per proteggere le informazioni è necessario tutelarne tre qualità fondamentali: la riservatezza, l'integrità e la disponibilità.
2. Quando si parla di tutela delle informazioni vanno considerate quindi tutte le "forme" in cui esse si possono oggettivare.
3. Da questo punto di vista le informazioni possono trovarsi nelle seguenti tipologie di "contenitori":
   - Cartaceo
   - Informatico
   - Verbale
   - Altri supporti materiali (microfilm, prototipi e plastici, video, cassette, pellicole, informazioni riportate su lavagne o tabelloni, campioni di nuovi materiali, ecc.).
4. Per ciascun tipo di "contenitore" esistono specifiche modalità di interazione tra soggetto e informazione (lettura, scrittura, visione, ascolto, diffusione, ecc.) ed eventualmente sistemi di interazione specifici che consentano ad una pluralità di soggetti di trasmettere, ricevere, conservare, ecc. le informazioni.
5. Quando una stessa informazione risiede in più di un "contenitore", occorre proteggerla adottando contromisure adeguate alle diverse caratteristiche dei "contenitori" e del "sistema di interazione" utilizzato.

Art. 16 – Conservazione

1. Conservare le informazioni negli archivi rispettando le misure previste per i diversi livelli di classificazione, i tempi di permanenza determinati dagli obblighi di legge, dal Titolare o dal Responsabile al trattamento e le correlate procedure in vigore.
2. Assicurare l'adeguata conservazione delle informazioni riservate presso terzi esterni attraverso apposite clausole contrattuali o accordi di riservatezza concordati, caso per caso, con le funzioni interne competenti.
3. Applicare, alla conservazione delle copie e ai duplicati di qualsiasi contenitore di informazioni, le stesse misure di sicurezza applicate agli originali.
4. In caso di conservazione di documenti cartacei contenenti dati personali, selezionare l'accesso agli archivi attraverso un sistema di autorizzazione stabilito dal Responsabile dei relativi trattamenti.
5. Utilizzare armadi, cassetti, ecc. chiusi a chiave, qualunque sia il contenitore dell'informazione (documento cartaceo, CD-ROM, DVD, videocassette, ecc.)
6. In caso di conservazione su sistemi informatici:
   a) Se si tratta di server web comunali, configurare l'accesso ai dati con Sistema di logging degli accessi.
   b) Se si tratta di server web esterni:
      b1. Richiedere esplicitamente al gestore l'utilizzo di strumenti software e hardware in grado di prevenire accessi illeciti e l'aggiornamento costante della configurazione attraverso la consultazione delle segnalazioni emesse dalla Funzione Sicurezza aziendale, nelle modalita' da convenire.
      b2. Proteggere i dati sul server con strumenti in grado di garantirne un adeguato livello di sicurezza.
   c) Se si tratta di Personal computer in rete è necessario eliminare tutte le possibilità di accesso a cartelle condivise. Abilitare all'accesso solo utilizzatori che siano stati formalmente incaricati del trattamento ai sensi Regolamento Europeo 2016/679 (Regolamento generale per la protezione dei dati personali), fornendo loro Codice di Accesso Personale e Parola chiave.Le ditte esterne che si occupano della manutenzione dei PC (o parti di essi) che contengono informazioni esclusive devono avere sottoscritto contratti contenenti apposite clausole di riservatezza. Tali contratti dovranno prevedere, dove possibile, l'effettuazione delle operazioni presso i locali comunali, senza l'asportazione di parti contenenti informazioni esclusive.
7. In caso di trasporto fuori dalla sede di lavoro, custodire le informazioni in contenitori (borse, valigette portadocumenti, plichi, ecc.) idonei ad evitare perdite, acquisizioni indebite o manomissioni.

8. Per archivi cartacei contenenti dati sensibili il Responsabile del trattamento deve prevedere un sistema di controllo degli accessi ai locali o ai singoli armadi o cassetti. In funzione dei casi specifici, del layout degli ambienti, della quantità dei dati ecc. tale sistema può essere manuale (es: registro cartaceo su cui riportare i dati relativi ai soggetti autorizzati e agli accessi) o elettronico. Il sistema prescelto deve consentire di selezionare e controllare gli accessi e registrarli fuori orario di lavoro. Se affidati agli incaricati autorizzati i documenti dovranno essere conservati, fino alla loro restituzione in contenitori muniti di serratura.
9. Non è consentita la trasmissione di dati personali sensibili (D.Lgs 196/2003) via email o tramite Internet/Intranet (tranne nei casi esplicitamente autorizzati).

Capo V – Violazioni, controlli e disposizioni finali

Art. 17 – Violazioni

1. Qualsiasi utilizzo non conforme alle disposizioni del presente Regolamento e/o alle leggi vigenti è riconducibile ad esclusiva responsabilità dell'utente, salvo che la violazione non dipenda da fatto non imputabile all'utente medesimo.
2. L'utente è direttamente responsabile, civilmente e penalmente, per l'uso improprio di Internet, per la violazione di accessi protetti, per il mancato rispetto delle norme sul copyright e sulle licenze d'uso.
3. Il Comune di Monteprandone si riserva di denunciare alle autorità competenti l'utente trovato ad utilizzare il servizio per attività illegali.
4. Le violazioni del presente regolamento comportano altresì responsabilità disciplinare del dipendente.

Art. 18 – Modalità dei controlli

1. Nonostante l'Amministrazione comunale non intenda monitorare l'utilizzo della rete in sé da parte dell'utente di postazione, si riserva il diritto di monitorare e verificare l'attuazione delle disposizioni del presente regolamento, nonché di effettuare tutti i necessari controlli per verificare la funzionalità e sicurezza del sistema, nel pieno rispetto della normativa vigente in tema di privacy, di tutela della dignità del lavorato re, nonché del principio di c.d. gradualità dei controlli di cui alle Linee Guida del Garante in materia.
2. A tal fine, i controlli normalmente effettuati dal Servizio Informatica, avranno carattere anonimo ed avranno ad oggetto dati aggregati, riferiti ad aree e/o servizi e/o unitá.
3. Nei casi di sospetta violazione delle norme di cui al presente regolamento, il Responsabile del Servizio Informatica provvederà ad informare il Segretario Genarale, che diramerà comunicati e avvisi generalizzati, contenenti indicazioni e istruzioni, sentito il Servizio Informatica, da osservare scrupolosamente.
4. In presenza di persistenti anomalie, possono essere inviati avvisi a singoli gruppi di lavoratori ovvero a singoli utenti. In difetto di rispetto delle previsioni di cui agli avvisi, sono consentiti controlli e ispezioni su postazioni individuali.

Art. 19 – Revisione periodica

1. Il presente regolamento entra in vigore con la sua formale adozione ed è soggetto a revisione ed aggiornamento quando necessario.

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. 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 Mozilla Firefox e Microsoft Internet Explorer. Ne esistono altri meno diffusi, 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 pro- pri a tutti i presenti) o privati (ospitati in "stanze" virtuali).

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. Es. Zimbra, Outlook Express.

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.

Crittosistema – Programma che consente di comunicare in maniera comprensibile, escludendo chi non è in possesso della chiave di lettura.

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 com-posta 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 - La madre di tulle le reti di computer. 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) - 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 adia-centi) 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 argo-mento. 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 MHz) 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 di file 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 del-l'immagine molto migliore. Lo standard MPEG- 2 è stato adottato dalla televisione digitale, terrestre e via satelli- te, 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, a un servizio telematico o a un sito Internet. E' necessario digitarla esattamente, assieme alla user-id. Alcuni software distinguono fra lettere maiu-scole e mi- nuscole. E' consigliabile non scriverla su bigliettini o 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 colleghi con lo stesso computer ha libero accesso.

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…

Sistema Informativo del Comune. 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.

Server - 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) o a contenere i file di un sito web (web server). Utilizza un sistema operativo di rete. I computer collegati e che utilizzano il servizio del server si chiamano client. A volte lo stesso computer svolge diverse funzioni di server (es: sia file server che print 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 (dai 10 ai 50 dollari), 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 di suoni ed immagini) per i computer.

UserId - Nome utente

Utente (User) - Chiunque utilizzi un elaboratore collegato alla rete del Sistema Informatico Comunale, sia che il collegamento avvenga in rete locale, come avviene all'interno delle sedi provinciali, 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.