REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI E TELEMATICI DEL COMUNE DI MANTOVA

CAPO I:
PREMESSA - FINALITA' - AMBITO DI APPLICAZIONE - PRINCIPI GENERALI
Art. 1 - Premessa

Il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali"e l'Allegato Disciplinare Tecnico impongono comportamenti tali da assicurare a chiunque il diritto alla protezione dei dati personali che lo riguardano, e l'adozione di misure di sicurezza minime e di misure di sicurezza idonee a garantire tale diritto, rispettivamente disciplinate dall'art. 33 e dall'art. 31 del Codice.
Il Garante per la protezione dei dati personali ha inoltre emanato, in data 01/03/2007, un provvedimento in materia di lavoro ("Lavoro: le linee guida del Garante per Posta Elettronica e Internet") con il quale prescrive ai datori di lavoro di adottare la "misura necessaria", a garanzia degli interessati, riguardante l'onere di specificare le modalità di utilizzo della Posta Elettronica e della rete Internet da parte dei lavoratori, come successivamente indicato anche nella Direttiva n. 02/2009 della Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica.

Il Comune di Mantova, come Ente e in qualità di Datore di Lavoro, in un'ottica di trasparenza e correttezza, per il corretto utilizzo delle attrezzature informatiche (Hardware e Software) e sulle misure minime di sicurezza per il trattamento dei dati, approvato con D.G. n. 456 del 16/08/2000 e modificato con D.G. n. 89 del 26/08/2008 di approvazione del Documento Programmatico sulla Sicurezza (DPS), adotta il presente Regolamento per disciplinare il corretto utilizzo degli strumenti di lavoro e soprattutto delle risorse informatiche in dotazione a dipendenti e collaboratori così come le misure di sicurezza idonee a garantire la protezione dei dati da esso trattati, in aggiunta alle misure di sicurezza minime, al fine di assicurare il corretto espletamento delle funzioni dell'Ente e la liceità dell'attività svolta da dipendenti e collaboratori.
Il sistema informativo del Comune di Mantova è costituito dall'insieme del patrimonio informativo digitale e delle risorse tecnologiche ed organizzative che acquisiscono, elaborano, rendono disponibile ed utilizzano tale patrimonio informativo.
Le risorse tecnologiche sono l'insieme degli strumenti hardware e software che permettono di accedere al patrimonio informativo digitale dell'ente, nonché alle risorse informative esterne collegate alla rete dell'ente tramite reti pubbliche o private.

Art. 2 - Finalità

Il presente regolamento disciplina:

a) le modalità di accesso ed utilizzo degli strumenti informatici, della rete informatica e dei servizi che tramite la stessa rete è possibile ricevere ed offrire all'interno e all'esterno dell'Amministrazione, nell'ambito dello svolgimento delle proprie mansioni ed attività di ufficio da parte degli amministratori, dipendenti e collaboratori del Comune di Mantova;
b) l'individuazione del complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, al fine di garantire l'aderenza e la rispondenza alle vigenti normative in materia, nonché gli adeguati livelli di sicurezza ed integrità del patrimonio informativo dell'Amministrazione Comunale.

Art. 3 - Ambito di applicazione

1) Il presente regolamento si applica a tutti gli utenti interni che sono autorizzati ad accedere alle risorse tecnologiche del sistema informatico del Comune.

2) Per utenti interni (di seguito: utenti) si intendono gli amministratori, i dirigenti, i dipendenti a tempo indeterminato e determinato, il personale con altre forme di rapporto contrattuale ed i collaboratori esterni impegnati in attività istituzionali limitatamente al periodo di collaborazione.

3) Il presente regolamento è richiamato quale parte integrante nel contratto individuale di lavoro per i dipendenti o nell'atto di instaurazione della collaborazione a vario titolo con il Comune, ed è consegnato all'interessato, alla sottoscrizione del contratto stesso.

Per meglio specificare, ai fini del presente regolamento:

a) per "TITOLARE" si intende l'Ente Comune di Mantova cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati, ivi compreso il profilo della sicurezza;

b) per "STRUTTURA" si intende un'Area, Coordinamento Intersettoriale, Centro di Responsabilità del Comune di Mantova, diretta da un Dirigente.

c) per "AMMINISTRATORE DI SISTEMA" si intende il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema informatico;

d) per "RESPONSABILE" si intende il soggetto che, per collocazione funzionale, esperienza, capacità e affidabilità assume il compito di garantire il rispetto delle vigenti disposizioni in materia di trattamento dati, ivi compreso il profilo relativo alla sicurezza;

e) per "INCARICATO DEL TRATTAMENTO" si intende il soggetto che è stato autorizzato dal titolare o dal responsabile a compiere operazioni sui dati cui ha accesso.

Art. 4 - Principi generali

1. Il Comune di Mantova promuove l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, in accordo con le linee guida e i principi delineati dalla normativa vigente.

2. I dati e le informazioni gestite ed archiviate in modalità informatica costituiscono patrimonio dell'Ente finalizzato all'erogazione di servizi istituzionali. Di conseguenza,allo scopo di consentire la piena disponibilità di tale patrimonio, la gestione informatizzata dei dati, deve privilegiare l'utilizzo di sistemi gestionali accentrati, indipendenti dalla singola postazione di lavoro, governati da livelli di autorizzazione predeterminati (user-password, ruolo). Pertanto la gestione con memorizzazione delle informazioni in locale, sul proprio personal computer, deve essere ridotta al minimo e limitata ai soli casi di estrema necessità.
In quest'ultima ipotesi, qualora il dipendente debba assentarsi per un periodo prolungato e programmato, deve concordare con il proprio dirigente, le modalità per mettere a disposizione le informazioni d'ufficio memorizzate all'interno del proprio personal computer.

3. Il Comune di Mantova promuove, all'interno del piano annuale della formazione, anche tramite supporti documentali pubblicati nella intranet comunale, l'aggiornamento e la formazione dei propri dipendenti in merito al corretto utilizzo delle strumentazioni informatiche e telematiche.

4. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi e dei programmi a cui ha accesso, nonché dei dati trattati a fini istituzionali.

5. Ogni utente è altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali, anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.

6. Sono vietati comportamenti che possono creare un danno, anche di immagine, all'Ente.

7. Gli strumenti di lavoro e in particolare le risorse informatiche e telematiche, messi a disposizione dall'Ente ai dipendenti e ai collaboratori, devono essere utilizzati in modo responsabile e ispirato ai principi di diligenza e correttezza. Essendo di proprietà dell'Ente, devono essere utilizzati per il conseguimento dei suoi fini istituzionali e non per scopi diversi. Non vengono rilasciate copie o autorizzazioni di utilizzo di applicazioni o componenti software, licenziati a nome dell'Ente, per scopi privati, ed è inoltre fatto divieto di utilizzare le risorse informatiche comunali per comunicare in modo anonimo o modificando la reale identità del mittente.

8. Per l'Ente l'utilizzo improprio, da parte di dipendenti e collaboratori, di Posta Elettronica, Internet e telefoni aziendali, può pregiudicare il regolare funzionamento delle installazioni tecniche o altri beni o interessi meritevoli di tutela e/o giuridicamente protetti, tra cui:

a) economie dei costi;
b) la capacità di memoria utilizzabile dei server o l'ampiezza di banda disponibile per il collegamento in rete;
c) sicurezza delle applicazioni e dei dati (disponibilità, integrità, cd. confidenzialità);
d) produttività sul lavoro;
e) la reputazione o l'immagine dell'Amministrazione comunale;
f) responsabilità oggettiva dell'Amministrazione comunale, ex art. 2049 c.c., per comportamenti illeciti dei propri dipendenti.

9. Per dipendenti e collaboratori dell'Ente, i rischi derivanti dall'utilizzo di Posta Elettronica, Internet e telefoni e fax aziendali, riguardano:

a) la protezione dei dati personali, propri e di terzi, poiché i predetti strumenti lasciano "tracce" del loro uso;

b) la possibilità che l'Ente, in fase di eventuale legittimo controllo, venga a conoscenza di dati od opinioni personali di dipendenti e collaboratori;

c) relativamente all'uso di Posta Elettronica, di Internet, e di supporti rimovibili l'introduzione di virus, worm, cavalli di Troia o installazioni di programmi estranei nel computer utilizzato da dipendenti e collaboratori, con conseguente perdita di tutti o parte dei file salvati sul medesimo computer.

CAPO II
CRITERI DI UTILIZZO DELLE RISORSE TECNOLOGICHE

Art. 5 - Utilizzo del personal computer

1. Il personal computer è uno strumento di lavoro e il suo utilizzo deve essere finalizzato esclusivamente allo svolgimento delle attività professionali e istituzionali dell'Amministrazione. Il personal computer viene assegnato all'utente in relazione alle funzioni svolte, previa autorizzazione del Capo Settore della struttura di appartenenza.
Ciascuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione.
Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

2. Ogni utente deve tenere comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e tali da ridurre i rischi per la sicurezza del sistema informatico. E' vietato l'utilizzo di supporti per la memorizzazione dei dati (CD, DVD, memorie USB, etc.) non sicuri e/o provenienti dall'esterno, al fine di non diffondere eventuali virus.

3. E' necessario spegnere il personal computer al termine dell'attività lavorativa o in caso di assenza prolungata dal proprio ufficio, al fine di evitare l'accesso, anche fortuito, ai dati ivi contenuti, nonché al fine di prevenire utilizzi indebiti da parte di terzi che possono essere fonte di responsabilità. In presenza di dati personali e/o sensibili il PC dovrà essere bloccato ogni qualvolta rimanga incustodito.

4. Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte di ASTER SRL , e in tal caso la suddetta password dovrà essere depositata in busta chiusa presso la segreteria di Settore o presso il referente informatico del settore.

5. I dati archiviati informaticamente devono essere esclusivamente quelli attinenti alle proprie attività lavorative.

6. Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, è infatti assolutamente da evitare un'archiviazione ridondante.

8. La tutela dei dati archiviati su personal computer che gestiscono localmente documenti e/o dati è demandata all'utente finale, il quale dovrà effettuare, con frequenza opportuna, i salvataggi su supporti dedicati ed idonei, nonché la conservazione degli stessi in luoghi adatti. Si consiglia di utilizzare i dischi di rete opportunamente configurati come luogo ove salvare i documenti di lavoro, ed utilizzare i dischi locali del PC solo per lavorazioni e/o bozze.

9. Non è possibile modificare le configurazioni hardware e software predefinite dagli amministratori di sistema ed installare autonomamente programmi o applicativi senza preventiva autorizzazione di ASTER SRL.

10. E' vietata l'installazione non autorizzata di sistemi che sfruttino il sistema telefonico o reti wireless per l'accesso a internet o ad altre reti esterne.

11. I sistemisti e i tecnici (personale interno di ASTER SRL e/o di ditte affidatarie del servizio) che hanno in gestione le componenti del sistema informatico comunale, possono, previo accordo con l'utente, procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza, sia sui singoli personal computer sia sulle cartelle di rete.

12. I sistemisti e i tecnici (personale interno di ASTER SRL e/o di ditte affidatarie del servizio) incaricati della gestione e della manutenzione del sistema informatico possono, in qualsiasi momento, accedere al personal computer per attività di manutenzione preventiva e correttiva, previo accordo con l'utente. In caso di intervento manutentivo da remoto (anche con strumenti di supporto, assistenza e diagnostica remota), per il quale verrà richiesta preventivamente all'utente l'abilitazione telematica, l'utente potrà verificare le operazioni eseguite che vengono tutte visualizzate sul monitor durante la connessione.

13. Tutti i dati sensibili riprodotti su supporti magnetici devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da terzi. Altrettanta cautela deve essere riposta in fase di stampa dei documenti contenenti dati sensibili: la stampa va effettuata su stampanti presidiate dall'addetto e, ove le attrezzature (stampanti di rete, fotocopiatrici con funzione di stampa, etc.) lo consentano, avviare la fase di stampa solo dopo aver inserito un apposito codice.

14. L'eventuale malfunzionamento o danneggiamento del personal computer deve essere tempestivamente comunicato al servizio Help-Desk delle ditte affidatarie del servizio.

15. In caso di furto è onere dell'utente, o del responsabile del settore di appartenenza, effettuare denuncia all'autorità di polizia e far pervenire al Settore SOPI copia della denuncia.

16. Oltre a quanto sopra detto, particolare diligenza deve essere posta dall'utente di PC portatile utilizzato in ambienti esterni all'Amministrazione, sia sotto il profilo della protezione dell'apparecchiatura, sia sotto il profilo della sicurezza dei dati in essa contenuti.

17. E' responsabilità del Dirigente di Settore compartecipare al processo di gestione della sicurezza informatica e collaborare alla verifica del coerente utilizzo delle risorse assegnate e ad evitarne sia l'uso improprio, che l'accesso da parte di personale non autorizzato.

NON È CONSENTITA:

1. l'installazione e la duplicazione di software non coperto da regolare licenza fornita dalla STRUTTURA di appartenenza;
2. l'installazione di software libero non soggetto a licenza d'uso, non autorizzato dalla STRUTTURA di appartenenza o dall'AMMINISTRATORE DI SISTEMA;
3. l'installazione di software non autorizzato, finalizzato ad alterare la funzionalità del collegamento in rete della stazione di lavoro;
4. l'alterazione degli indirizzi e dei protocolli di rete assegnati dall'AMMINISTRATORE DI SISTEMA;
5. l'inibizione o la sospensione, anche temporanea, del funzionamento del software ANTIVIRUS installato dall'AMMINISTRATORE DI SISTEMA;
6. l'utilizzazione di funzioni e tecniche di condivisione di archivi gestiti dalla propria postazione di lavoro senza la contemporanea adozione di opportune parole chiave di accesso (password) da fornire ai colleghi che ne debbano fare uso;
7. il trasferimento di dati non autorizzato da e verso l'esterno alla Amministrazione Comunale in qualsiasi forma (supporti dati rimovibili, collegamento linee dati con o senza fili, utilizzo di reti telematiche private o pubbliche, ecc.).

Art. 6 - Gestione utenti

L'abilitazione all'utilizzo delle risorse informatiche avverrà a seguito di esplicita richiesta da inoltrare ad ASTER SRL da parte del Dirigente di Settore.
Analogamente, qualsiasi variazione nell'anagrafica dei Dipendenti e/o di risorse esterne che collaborano deve essere tempestivamente comunicata ad ASTER SRL che provvedereà ad effettuare le variazioni nel sistema Informatico dell'Ente, al fine di salvaguardare i diritti di accesso alle informazioni, derivanti dal gruppo di appartenenza e/o dal ruolo che la risorsa aveva precedentemente.

Per gli stagisti, collaboratori esterni o altre figure simili, sarà cura di ogni Settore inoltrare richiesta ad ASTER SRL specificando gli estremi della persona interessata, nonché le date di inizio e fine dell'account richiesto.

Art. 7 - Gestione degli account e delle password

1. L'account è costituito da un codice identificativo personale (username o user id) e da una parola chiave (password).

2. Gli account possono essere numerosi, ciascuno con una specifica password, si distinguono, in particolare:
a) di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete,
b) gestionali, per l'accesso alle applicazioni gestionali a utenti che, per motivi di servizio, ne devono fare uso.

4. La password che viene associata a ciascun utente è personale, non cedibile e non divulgabile.

5. Le password dovranno avere le seguenti caratteristiche:
- lunghezza minima 8 caratteri.
- caratteri di tipo alfanumerico, una lettera minuscola e una lettera maiuscola ed un carattere speciale (? / ! - _ ecc.).

• Si consiglia di utilizzare password non riconducibili a:
- nome o cognome proprio o di un collega o di un famigliare
- identificativi di ufficio, di area, di servizio o del Comune, in modo parziale o completo
- date di nascita, codici fiscali o altri elementi che ne facilitino l'individuazione • validità di 90 giorni.

6. Va inoltre tenuto conto che:
- dopo la scadenza, potrà essere riutilizzata la medesima password solo dopo sei (6) rinnovi consecutivi,
- la password non potrà essere rinnovata prima che siano trascorse 24 ore dall'ultimo rinnovo,
- in caso di inserimento di una password errata è possibile effettuare fino a tre tentativi dopodiché l'utenza viene bloccata.

Art. 8 - Utilizzo dell e cartelle di rete

1. Le cartelle di rete sono aree di disco su server a disposizione dei vari Settori ed Uffici. Ogni Settore avrà uno spazio la cui dimensione è limitata e determinata da ASTER SRL, in funzione delle esigenze del settore, della disponibilità dell'intero sistema di memorizzazione, del numero di utenti, dei volumi e tipologia di documenti trattati.

2. Le cartelle di rete sono periodicamente salvate da ASTER SRL con cadenza minima di un giorno ed i corrispondenti salvataggi sono disponibili per un arco temporale massimo di 45 giorni.

3. Le cartelle di rete, sono aree di condivisione di documenti strettamente istituzionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia correlato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.

4. L'organizzazione e la gestione dell'albero delle sottocartelle è demandata al Referente informatico di settore di cui all'art. 12 del presente Regolamento. Questi ha anche il compito di effettuare una pulizia periodica degli archivi, con cancellazione dei file obsoleti, duplicati o inutili. Nel caso di un'organizzazione di settore distribuita, il referente informatico ha il compito di monitorare che la suddetta buona pratica venga messa in atto.

5. ASTER SRL, nel caso si prefiguri un uso improprio o che metta a repentaglio la sicurezza del sistema informatico dell'Ente, ha la facoltà, previ accordi con il Referente Informatico, di procedere alla rimozione di ogni file o applicazione, nonché inibire temporaneamente l'accesso alle cartelle di rete interessate.

Art. 9 - Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente all'espletamento dei compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi, privilegiando altresì soluzioni operative che mirino al risparmio, privilegiando innanzitutto l'utilizzo di carta riciclata con stampa fronte retro, nonché soluzioni operative che mirino ad evitare l'utilizzo di carta (memorizzazione di documenti scansionati e comunicazione via mail) nell'ottica delle direttive inerenti alla digitalizzazione della Pubblica Amministrazione.

CAPO III:
GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 10 - Utilizzo di Internet

1. L'utilizzo di Internet deve essere limitato a scopi inerenti l'attività lavorativa.

2. L'Amministrazione adotta misure di filtraggio, che permettono di inibire o restringere l'accesso a siti i cui contenuti siano classificati pericolosi o non attinenti agli scopi istituzionali.

3. Sono vietate tutte le azioni atte ad eludere tali politiche di filtraggio di cui al precedente comma.

4. ASTER SRL, nel caso si prefiguri un uso improprio o che metta a repentaglio la sicurezza del sistema informatico dell'Ente, ha la facoltà di inibire temporaneamente anche senza preavviso la navigazione in internet alle postazioni di lavoro interessate.

5. Ai soli fini di gestione e di salvaguardia giuridica degli interessi dell'Ente e dei propri dipendenti, il sistema di gestione della navigazione in internet provvede alla tracciatura secondo norma vigente, che prevede esclusivamente la registrazione delle URL senza entrare nel merito delle attività svolte (compilazione form, contenuti web-mail, etc.). Il tempo di mantenimento di tali dati viene stabilito in 12 mesi, in analogia a quanto richiamato nel provvedimento del 24/7/2008 del Garante per la protezione di dati personali.

Art. 11 - Gestione e u tilizzo della posta elettronica

1. Le caselle di posta elettronica rilasciate sono di due tipi:
   - casella di posta elettronica istituzionale – riconducibile ad un'unità organizzativa (segreteria di Settore, servizio al pubblico, etc.)
   - casella di posta elettronica individuale: casella assegnata al singolo utente interno.

2. Il Capo Settore o il responsabile dell'Unità di progetto stabilisce quali utenti hanno accesso alle caselle di posta elettronica istituzionali assegnate al Settore.

3. La casella di posta elettronica assegnata è uno strumento di lavoro ed il suo utilizzo è consentito solo per finalità connesse allo svolgimento della propria attività lavorativa. Le persone assegnatarie sono responsabili del corretto utilizzo della stessa.

4. Non è consentito l'invio o la ricezione di messaggi con allegati di dimensione superiori a 15 Mb e con estensione uguali a .lnk .bat .exe .scr ed in generale file di tipo eseguibile o di applicazione. Si precisa che il

sistema di sicurezza e antivirus installato a protezione del server di posta elettronica del Comune non consente la ricezione e l'invio di messaggi di posta che contengono allegati con le caratteristiche sopra elencate. Eventuali esigenze particolari potranno essere segnalate ASTER SRL che individuerà la soluzione tecnica più appropriata.

5. In caso di cessazione del rapporto di lavoro o collaborazione o di mandato degli amministratori, l'indirizzo di posta elettronica individuale dell'interessato viene immediatamente cessato, a seguito comunicazione scritta ad ASTER SRL.

6. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e con allegati di grandi dimensioni.

7. E' vietato utilizzare l'indirizzo delle caselle di posta elettronica istituzionale e personale per l'invio o la ricezione di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione.

8. Ai soli fini di gestione e di salvaguardia giuridica degli interessi dell'Ente e dei propri dipendenti, il sistema di gestione della posta elettronica provvede alla tracciatura della corrispondenza in entrata e in uscita, secondo norma vigente, che prevede esclusivamente la registrazione dell'identificativo della postazione di lavoro, del mittente e del destinatario. Il tempo di mantenimento di tali dati viene stabilito in 12 mesi, in analogia a quanto richiamato nel provvedimento del 24/7/2008 del Garante per la protezione di dati personali.

CAPO IV:
MODALITA' di UTILIZZO DEGLI STRUMENTI DI TELEFONIA MOBILE E DI CONNETTIVITA' IN MOBILITA'

Le modalità d'uso regolamentate nel presente capitolo si applicano a tutti gli incaricati, a tutti i dipendenti senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell' Ente, a prescindere dal rapporto contrattuale con la stessa intrattenuto.

Art. 12 - Principi di utilizzo dei telefoni cellulari e degli altri strumenti di connettività

Per motivate esigenze di servizio il personale dell'Ente può essere dotato di telefono cellulare e di altri strumenti di connettività in mobilità, secondo le procedure e nel rispetto delle norme di utilizzo di seguito indicate.
La violazione del presente regolamento potrà comportare l'applicazione delle sanzioni disciplinari contemplate dal Contratto Collettivo Nazionale di Lavoro applicabile, nel rispetto dei principi di gradualità e proporzionalità, nonché delle altre misure di tutela del caso.

Art. 13 - Esigenze di servizio

L'uso del telefono cellulare e di altri strumenti per la connettività in mobilità può essere concesso quando la natura delle prestazioni e dell'incarico richiedano pronta e costante reperibilità e disponibilità in luoghi diversi dalla sede di lavoro o quando sussistano particolari ed indifferibili esigenze di comunicazione che non possono essere soddisfatte con gli strumenti di telefonia e posta elettronica da postazione permanente.

Art. 14 - Concessione

La concessione del telefono cellulare o di altro strumento di connettività in mobilità è richiesta dai Dirigenti dell'Ente per i dipendenti di rispettiva afferenza.
La richiesta deve essere prioritariamente finalizzata, ove possibile in relazione alla natura delle esigenze da

assolvere, alla concessione di apparati di telefonia destinati ad un utilizzo collettivo da parte dei collaboratori della struttura in caso di svolgimento di servizi fuori sede.

In ogni caso, la richiesta deve essere esaustivamente motivata con la precisa e puntuale indicazione delle condizioni che determinano la concessione del telefono.

Il Segretario Generale e i Dirigenti dell'Ente sono dotati di un telefono cellulare di servizio e Tablet, per tutta la durata dell'incarico, in relazione ai compiti ed alle particolari esigenze di servizio connesse all'espletamento dell'incarico.

Sia il terminale sia la relativa utenza sono concessi in uso al dipendente fino ad esplicita revoca.

Pertanto, al venire meno dei requisiti indicati o in caso di cessazione del rapporto di lavoro, il Dirigente del Settore interessato dovrà dare immediata comunicazione al Settore di competenza che provvederà al ritiro del materiale fornito ed al conseguente riutilizzo dell'utenza. Nell'ipotesi di trasferimento ad un diverso settore dell'Ente, il permanere delle condizioni per l'uso del telefono di servizio dovrà essere attestato dal Dirigente del Settore di destinazione.

La concessione del telefono cellulare può essere disposta anche per periodi di tempo limitati, in relazione ad esigenze contingenti (eventi, missioni, servizi straordinari).

Art. 15 - Norme di utilizzo

L'assegnatario del dispositivo di comunicazione mobile è responsabile del suo corretto utilizzo dal momento della presa in consegna fino alla restituzione e/o revoca e dovrà porre ogni cura nella sua conservazione, per evitare danni, smarrimenti o sottrazioni.

Nel caso in cui un apparecchio sia concesso a più utilizzatori, l'assegnatario è la persona che il Dirigente ha individuato nella lettera di richiesta. In ogni caso, il Settore dovrà tenere nota degli effettivi utilizzatori per tutta la durata della concessione.

In caso di furto o smarrimento dell'apparecchio il dipendente dovrà darne immediata comunicazione al proprio Settore e, ai fini dell'immediato blocco dell'utenza.

Se il furto o lo smarrimento si verificano in circostanze o in tempi in cui non è possibile comunicare con il Settore di competenza, il dipendente dovrà provvedere personalmente al blocco della Sim contattando il gestore di telefonia mobile.

Il dipendente dovrà quindi presentare la formale denuncia di furto o smarrimento e farne pervenire copia al Settore di competenza per gli adempimenti successivi.

I telefoni cellulari ed i dispositivi tablet possono essere utilizzati soltanto per ragioni di servizio.

I dipendenti dovranno comunque utilizzare i dispositivi nei casi di effettiva necessità, ponendo la massima attenzione al contenimento della spesa.

E' obbligatorio l'uso del PIN di sicurezza della SIM.

E' esclusa la possibilità di qualsiasi utilizzo per fini privati.

Gli assegnatari di dispositivi di comunicazione mobile a titolo esclusivamente nominativo possono utilizzare il telefono di servizio o/o dispositivo mobile per usi personali, solo digitando l'apposito codice che comporta l'addebito della chiamata direttamente all'utilizzatore.

L'utilizzo all'estero dei dispositivi dovrà essere preventivamente comunicato ed autorizzato.

Nel caso di utilizzo dei dispositivi all'estero per traffico dati , dovrà essere effettuato solo ed esclusivamente utilizzando eventuali reti wifi e non tramite lutilizzo della SIM in modalità RAOMING.

Pertanto sarà cura dell'utilizzatore procedere alla disattivazione del traffico dati in modalità roaming.

TUTTO IL TRAFFICO DATI GENERATO IN MODALITA' ROAMING VERRA' ADDEBITATO ALL'UTILIZZATORE.

Al dipendente verranno applicate le stesse condizioni tariffarie previste per l'Ente.

In caso di malfunzionamento o di guasto dell'apparecchio o della Sim il dipendente dovrà rivolgersi al Settore di competenza.

Art. 16 - Sistema di verifiche

Il Settore di competenza in attuazione dell'art. 2, comma 594 della Legge finanziaria 2008, nel rispetto della normativa sulla tutela e riservatezza dei dati personali, applica un sistema di verifiche sull'utilizzo corretto delle utenze telefoniche.

Il Settore di competenza effettua i controlli su tutti gli strumenti di telefonia mobile messi a disposizione dall'Ente al fine di verificarne il corretto utilizzo.

I controlli sono effettuati sulle base delle informazioni trasmesse dagli operatori telefonici alla struttura competente.

Le informazioni contengono: il volume complessivo del traffico telefonico (relativo sia ai tempi sia all'importo) delle chiamate in uscita addebitate all'Ente con riferimento ai servizi voce/dati per ciascuna singola utenze, il dettaglio del traffico telefonico, comprensivo di data/ora/durata chiamata, numero chiamato (ultime tre cifre oscurate) per ciascuna singola utenza, volume dati scambiato per quanto riguarda il traffico dati / Internet.

Le informazioni inerenti alle spese relative alle singole utenze sono periodicamente trasmesse ai Responsabili del settore a cui risultano assegnate le utenze stesse.

Sono escluse dal controllo le chiamate private effettuate previa digitazione di un apposito codice che comporta l'addebito della chiamata direttamente all'utilizzatore.

I controlli effettuati dal Settore di competenza devono in ogni caso rispettare i seguenti principi:

a) necessità: i dati trattati durante l'attività di controllo devono essere sempre e soltanto quelli strettamente necessari a perseguire le finalità di consentire di monitorare e mirano a ridurre la spesa pubblica, sia rilevando eventuali danni patrimoniali già posti in essere, sia agendo quale deterrente rispetto a comportamenti impropri e potenzialmente dannosi, per cui la loro omissione potrebbe comportare responsabilità patrimoniali dirette a carico dell'Ente;

b) proporzionalità: i controlli devono sempre essere effettuati con modalità tali da garantire, nei singoli casi concreti, la pertinenza e non eccedenza delle informazioni rilevate rispetto alle finalità perseguite e specificate;

c) imparzialità: i controlli devono essere effettuati su tutte le strumentazioni telefoniche messe a disposizione dall'Ente e conseguentemente possono coinvolgere tutti gli utilizzatori delle stesse, a qualunque titolo abbiano assegnata la strumentazione. L'imparzialità inoltre deve essere garantita

mediante sistemi di estrazione casuale per l'effettuazione dei controlli a campione ed in nessun caso possono essere effettuati controlli mirati e ripetuti nei confronti di soggetti specifici con finalità discriminatorie o persecutorie o volutamente sanzionatorie. I controlli puntuali possono essere effettuati soltanto sulla base di specifiche, oggettive e circostanziate segnalazioni;

d) trasparenza e correttezza: in base a tale principio l'amministrazione deve mettere in atto tutte le azioni necessarie per garantire la preventiva conoscenza da parte di tutti i soggetti potenzialmente sottoposti ai controlli del presente disciplinare. Devono pertanto essere informati dei possibili controlli
tutti i soggetti che operano, a qualunque titolo e con qualunque rapporto, per l'Ente . A tal fine l'Ente deve in particolare consegnare l'informativa ex art. 13 del Codice per la protezione dei dati personali all'atto della sottoscrizione del contratto e tale informativa deve contenere espresso riferimento al presente disciplinare;

e) protezione dei dati personali: i controlli devono in ogni caso essere effettuati rispettando la dignità e la libertà personale dei soggetti sottoposti a controllo garantendo altresì la riservatezza dei dati personali raccolti durante la procedura di controllo. I dati devono essere gestiti soltanto dai soggetti preventivamente designati quali responsabili e incaricati del trattamento. I controlli devono essere effettuati rispettando la normativa vigente in materia di protezione dei dati personali ed in particolare le prescrizioni di cui all'art. 11 del Codice.

Modalità dei controlli sull'utilizzo delle strumentazioni telefoniche

Il controllo sull'utilizzo delle strumentazioni telefoniche, effettuato in forma anonima, è di tre tipologie:

a) puntuale;

b) a campione;

c) controllo occasionale a seguito di "screening generale" dei tabulati in presenza di evidenti anomalie;

e si effettuano nel modo di seguito indicato.

a) Controllo puntuale

Il controllo puntuale è effettuato su utenze telefoniche determinate, a seguito di specifica segnalazione effettuata da un soggetto terzo. Si considera terzo anche l'operatore telefonico.
Nel caso in cui la segnalazione del soggetto terzo si riferisca a una persona nominativamente individuata, la struttura competente all'effettuazione dei controlli deve dare informazione del controllo in corso al soggetto cui si riferisce la segnalazione, specificando che può essere presentata richiesta di accesso ai relativi documenti amministrativi a norma della Legge n. 241/1990 e ss. mod. e int.

b) Controllo a campione

Estrazione del campione

Il campione è costituito, in via alternativa:

b.1) da una percentuale pari al 2% del totale delle utenze assegnate, con esclusione di quelle dati;
b.2) da tutte le utenze assegnate ad un determinato Settore.

L'identificativo univoco delle utenze è dato dalla posizione dell'utenza nella lista utenze complessiva, ordinata per numero utenza crescente, indipendentemente dall'operatore telefonico.

c) Controllo occasionale a seguito di “screening generale” dei tabulati in presenza di evidenti anomalie Suddetta tipologia di controllo viene attivata a seguito di un esame di carattere generale, in corrispondenza del processo di copiatura dei dati forniti, mediante CD, dall’operatore telefonico nel computer degli incaricati e in cui emerga una palese e immediata anomalia nei tabulati del traffico telefonico.

Le anomalie che possono emergere sono:

- orario chiamate precedente alle ore 07:30 e successivo alle ore 18:30 in considerazione del normale orario di servizio; l’elenco del personale che abitualmente, per ragioni di servizio, deve effettuare telefonate in una fascia oraria diversa da quella indicata, sarà debitamente segnalato al Responsabile del Settore;

- numero di telefonate, compresi i messaggi di testo, che superano del 50% la media complessiva delle telefonate effettuate;

- durata delle telefonate superiore al 50% della durata media complessiva ;

- alta ripetitività delle comunicazioni telefoniche ad utenze extra aziendali.

CAPO V:
REFERENTI INFORMATICI E FORMAZIONE

Art. 17 - Referente informatico di settore

1. Ogni settore dovrà nominare un referente informatico. Nel caso di strutture complesse potranno essere nominati più referenti informatici in accordo con ASTER SRL .

2. Al Referente sarà assegnato il compito di:
- verificare le esigenze di strumentazione informatica e segnalarle ad ASTER SRL,
- collaborazione con ASTER SRL nella supervisione sul corretto utilizzo delle risorse informatiche,
- assolvere a quanto previsto nell'art. “Utilizzo delle cartelle di rete”.

3. I referenti dovranno avere conoscenze idonee al ruolo.

CAPO V:
CONTROLLI

Art. 18 - Controlli e r esponsabilità

1. L’Amministrazione si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e del presente regolamento, nonché nel rispetto dello Statuto dei Lavoratori.

2. Per esigenze organizzative, produttive e di sicurezza l’Amministrazione effettuerà controlli automatizzati generali con l'obiettivo di individuare potenziali rischi per la sicurezza o usi impropri del sistema informatico. Il Capo Settore SOPI ha la facoltà, nell'ambito di quanto previsto dalla normativa vigente, di effettuare eventuali ulteriori approfondimenti
con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, qualora i controlli automatici riscontrino potenziali rischi o problemi. I suddetti procedimenti di controllo saranno opportunamente documentati (tipo di controlli, nome del sistemista che opera i controlli, log di accesso ai sistemi, riscontri dei controlli).

3. Qualora la tipologia dei controlli automatizzati adottati contempli la possibilità di controllo dell'attività dei lavoratori, l'attivazione sarà preceduta da un accordo con le rappresentanze sindacali aziendali, le quali inoltre vengono informate delle iniziative adottate in sede di prima applicazione del presente Regolamento.

4. Il mancato rispetto o la violazione delle norme contenute nel presente regolamento è perseguibile con provvedimenti disciplinari, nonché con le azioni civili e penali consentite.