comune di
PRATO

REGOLAMENTO SULL'UTILIZZO DELLE RISORSE INFORMATICHE E TELEFONICHE

Approvato con Delibera di Giunta
n. 545 del 2 dicembre 2008

INDICE

Articolo 1: Definizioni
Articolo 2: Oggetto e finalità
Articolo 3: Risorse informatiche e telefoniche
Articolo 4: Credenziali di autenticazione
Articolo 5: Modalità di manutenzione delle risorse
Articolo 6: Modalità di utilizzo delle Risorse
Articolo 7: Comportamenti vietati
Articolo 8: Misure di prevenzione
Articolo 9: Monitoraggi
Articolo 10: Misure a garanzia degli utenti
Articolo 11: Controlli relativi all’utilizzo delle risorse
Articolo 12: Pubblicità e Decorrenza

Articolo 1: Definizioni

1. Ai fini del presente regolamento si intendono per:
   a) Amministrazione (denominata anche Ente): il Comune di Prato, con sede in Piazza del Comune, considerata anche la sua articolazione territoriale in Circoscrizioni di Decentramento.
   b) D.lgs. 30.06.2003 n. 196: Codice in materia di protezione dati personali (detto anche "Codice").
   c) Misure di Sicurezza: Misure obbligatorie disciplinate dal "Codice" volte ad assicurare la sicurezza dei dati e dei sistemi per ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
   d) DPS: Documento Programmatico sulla Sicurezza dei dati e dei sistemi aggiornato almeno annualmente e deliberato dalla Giunta Comunale di Prato.
   e) Hardware (HW): è l'insieme delle risorse fisiche informatiche.
   f) Software (SW): usato in ambito informatico, indica un programma o un insieme di programmi in grado di funzionare su un elaboratore.
   g) Backup: è la copia di riserva di un disco, di una parte del disco o di uno o più file o programmi su supporti di memorizzazione diversi da quello in uso. È creata per scopi di archiviazione o per salvaguardare file di valore da eventuali perdite qualora la copia originale dovesse venire danneggiata o distrutta. È detta anche copia di backup o file di backup.
   h) Risorse informatiche: sono i dispositivi Hardware e Software nonché i servizi di collegamento e comunicazione in rete.
   i) Risorse Telefoniche: sono i dispositivi di telefonia fissa e mobile.
   j) FILE: è un agglomerato di dati disponibile per gli utenti del sistema.
   k) LOG: è una raccolta di dati automaticamente prodotti per la gestione dei telefoni derivati dai centralini, della navigazione internet e delle comunicazioni via posta elettronica.
   l) FILE di LOG (o LOG FILE): File nel quale vengono registrate le operazioni che l'utente compie durante la sua sessione di attività riferite sia alle risorse utilizzate che all'accesso ai dati ed alle banche dati dell'Ente.
   m) RETE: è l'insieme di mezzi connessi tra di loro allo scopo di condividere le risorse hardware e software, nonché consentire lo scambio di dati.
   n) Corrispondenza aperta: quella accessibile da parte di tutti coloro che legittimamente dispongano della "chiave informatica di accesso".
   o) Utenti: Tutti coloro ai quali è assegnato dal Comune di Prato un sistema di autorizzazione che hanno titolo ad accedere ed utilizzare le risorse informatiche e telefoniche per svolgere

attività all'interno dell'Ente nonché i servizi di comunicazione elettronica non accessibili al pubblico. Ai fini del presente regolamento si intendono per "utenti" i soggetti che svolgono attività lavorativa.

p) Servizi di comunicazione elettronica non accessibili al pubblico: servizi di comunicazione elettronica forniti a gruppi delimitati di soggetti per esigenze aziendali.
q) Sistema di autorizzazione: è l'ambito di accesso alle risorse, allo scopo di limitare l'accesso ai soli dati e servizi necessari all'attività dell'utente.
r) SPAM: è la diffusione massiccia di un messaggio via Internet.
s) Banche dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Articolo 2: Oggetto e finalità

1. L'Amministrazione definisce le modalità di comportamento, monitoraggio e controllo per l'utilizzo delle risorse informatiche e telefoniche messe a disposizione degli utenti allo scopo di garantire:
   a. Il corretto utilizzo delle stesse;
   b. La sicurezza, la disponibilità e l'integrità dei sistemi informativi e dei dati anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
   c. La continuità' dei servizi dell'Amministrazione.

Articolo 3: Risorse informatiche e telefoniche

1. L'amministrazione, ove necessario, mette a disposizione degli utenti un elaboratore di tipologia e capacità correlate all'attività da svolgere. L'elaboratore è dotato di opportuno software in modo da offrire la corretta integrazione con il restante sistema informativo e permettere all'utente di ottenere il massimo delle prestazioni dall'hardware disponibile. L'elaboratore può essere dotato di collegamento ad uno spazio disco condiviso, accessibile in rete, sottoposto a regolare backup e del quale è garantita l'affidabilità e la disponibilità nel tempo.
2. Il personal computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
3. L'amministrazione, ove necessario, assegna all'utente, ovvero a gruppi di utenti, l'accesso alla rete Internet, uno o più indirizzi di posta elettronica, l'uso di una o più stampanti di rete e/o locali e l'uso della rete telefonica nei modi necessari allo svolgimento della sua attività.

Articolo 4: Credenziali di autenticazione

1. L'Amministrazione Comunale fornisce all'utente le "credenziali di autenticazione", ad esso univocamente correlate, al fine di consentire l'accesso ai dati ed alle risorse necessarie allo svolgimento della propria prestazione lavorativa.
2. Le credenziali di autenticazione sono esclusivamente personali ed è fatto obbligo di conservarle secondo le procedure e le cautele descritte nel Documento Programmatico per la Sicurezza aziendale.
3. La custodia da parte dell'Amministrazione delle copie delle credenziali è organizzata garantendo la relativa segretezza secondo le procedure e le cautele descritte nel Documento Programmatico per la Sicurezza (DPS) aziendale.
4. E assolutamente proibito entrare nella rete e nei programmi con credenziali di identificazione utente diverso da quelle assegnate. La parola chiave d'ingresso alla rete ed ai programmi ed ogni altro codice riservato personale sono segrete e vanno conservate e gestite secondo le procedure impartite.
5. La responsabilità del salvataggio dei eventuali dati contenuti nei dischi fissi o rimovibili o altre unità di memorizzazione locali (quali a titolo esemplificativo e non esaustivo: il desktop, i dischi a:, b: e c: o altre lettere identificative di dispositivi rimovibili), è a carico del singolo utente. Per garantire maggiore flessibilità vengono create su richiesta del dirigente del settore cartelle di lavoro condivise in rete a seconda del gruppo di lavoro o del progetto.
6. Il personale del Servizio "Sistema informativo", o altro personale esterno all'uopo incaricato, può in qualunque momento procedere alla rimozione di ogni file o applicazione che ritiene essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.
7. Ciascun utente deve provvedere alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili con cadenza almeno trimestrale.
8. Nel caso di cessazione del servizio e/o trasferimento per mobilità, il Dirigente o Responsabile del servizio è tenuto ad impartire idonee istruzioni al fine di garantire la continuità del servizio e il rispetto della privacy, pertanto, i documenti di interesse per l'interno ufficio devono essere trasferiti in opportune aree accessibili dai colleghi. È vietata la semplice distruzione indiscriminata di documenti dal proprio computer dato che i file archiviati sono documentazione amministrativa di proprietà del Comune.

Articolo 5: Modalità di manutenzione delle risorse

1. Il Sistema informativo, per l'assistenza e la manutenzione, utilizza strumenti che permettano agli operatori del servizio stesso di prendere il controllo dell'elaboratore in sede d'utente.

2. Per impedire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati agli utenti, le attività di cui al precedente comma potranno essere condotte esclusivamente nei seguenti casi:
   a. L'attivazione del controllo comporta l'automatica disconnessione dell'utente e chiusura forzata di ogni applicativo aperto;
   b. I sistemi di controllo remoto sono installati e configurati in modo da richiedere all'utente una cosciente e volontaria azione di abilitazione sul proprio computer. Tale abilitazione dovrà essere obbligatoriamente temporanea e valere esclusivamente per il tempo strettamente necessario all'esecuzione dell'intervento;
3. In ogni caso l'utente può verificare la durata dell'intervento e la disconnessione dal proprio computer, anche per interventi effettuati presso la postazione dell'utente.
4. Il personale dal servizio "Sistema informativo" incaricato può compiere interventi per garantire la sicurezza e la salvaguardia del sistema informativo comunale che possono comportare anche l'accesso ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà si applica anche in caso di assenza prolungata od impedimento dell'utente.
5. Il personale incaricato dal servizio "Sistema informativo" ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento è effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, è data comunicazione della necessità dell'intervento stesso.

Articolo 6: Modalità di utilizzo delle Risorse

1. L'utente, nell'utilizzo delle risorse assegnate, è tenuto a:
   a. Memorizzare, ove non sia diversamente ed automaticamente disposto da parte dello specifico software utilizzato, i documenti inerenti alla propria attività esclusivamente nelle quote di spazio disco condiviso accessibile in rete (utilizzando, a titolo esemplificativo, i dischi identificati con le lettere I:, N: Q: R: S: e T:);
   b. Aggiornare i documenti archiviati sia eliminando quelli non più necessari sia chiedendone la masterizzazione su supporti rimovibili, nel caso in cui debbano essere conservati in sicurezza;
   c. Prestare attenzione alla duplicazione dei dati in modo da evitare un'archiviazione ridondante e un conseguente spreco di risorsa disco;

d. Utilizzare l’indirizzo di posta elettronica solo per lo svolgimento della propria attività. La relativa corrispondenza ha natura di “corrispondenza aperta” ed è conoscibile da parte del Comune di Prato;
e. Aggiornare costantemente la casella di posta elettronica conservando solo la corrispondenza strettamente necessaria alla propria attività;
f. Utilizzare la rete internet in relazione alla propria attività, prestando particolare attenzione alla disciplina in materia di diritto di autore e altri diritti connessi e di utilizzo della rete;
g. Non utilizzare le risorse telefoniche per esigenze personali, salvo i casi di urgenza;
h. Stampare i soli documenti inerenti alla propria attività.

2. L’utente che viene a conoscenza di un software in grado di migliorare la propria attività, deve segnalarlo al personale del servizio “Sistema informativo” la struttura competente che valuterà la sua possibile installazione in modo da garantire la compatibilità funzionale-tecnica e normativa, il mantenimento dell’efficienza dei sistemi operativi e delle reti, prevenire il pericolo di introdurre involontariamente virus informatici, di alterare la stabilità delle applicazioni degli elaboratori e dei sistemi operativi ed evitare le responsabilità civili e penali derivanti da un uso non consentito di software coperto da licenza d’uso.
3. Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall’ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l’indebito uso.
4. Nel caso in cui l’utente si avvalga di una postazione portatile è responsabile della custodia della stessa sia durante gli spostamenti che durante l’utilizzo nel luogo di lavoro.

Articolo 7: Comportamenti vietati

1. È vietata la modifica e la personalizzazione della configurazione dell’elaboratore utilizzato dall’utente per lo svolgimento della propria attività.
2. L’utente non può, in ogni caso, installare materiale (immagini, sfondi, software in genere) diverso da quello già configurato dal sistema informativo dell’Ente; ciò per prevenire l’attacco del sistema da parte di virus informatici.
3. È vietato agli utenti di installare autonomamente software anche se necessari alla propria attività. Eventuale software installato dall’utente in violazione del presente comma potrà essere rimosso dai tecnici competenti senza autorizzazione dell’utente stesso.
4. L’utente deve evitare l’uso di qualsiasi spazio disco, fisso o rimovibile (quali a titolo esemplificativo e non esaustivo: il desktop, i dischi a:, b: e c: o altre lettere identificative di dispositivi rimovibili), presente sulla propria postazione se non in via temporanea e per il tempo strettamente necessario.

5. È vietata la registrazione a mailing list che abbiano contenuti non attinenti alla propria attività e la creazione di un indirizzo di posta elettronica diverso e/o ulteriore rispetto a quello fornito dal Comune di Prato o l'utilizzo delle caselle di posta elettronica personali per motivi diversi da quelli strettamente legati all'attività lavorativa.
6. È proibita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
7. Nel caso in cui al dipendente venisse assegnato un cellulare aziendale, egli rimane responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le stesse regole previste per l'utilizzo del telefono fisso. In particolare, è vietato l'utilizzo del telefono cellulare per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile solo se previsto dal contratto in vigore con il relativo gestore e solo dopo aver definito questo tipo di utilizzo con l'assistenza del Servizio "Sistema Informativo".
8. È, altresì, vietato l'utilizzo delle fotocopiatrici aziendali per fini personali.
9. In materia di responsabilità e sanzioni si rimanda al sistema generale previsto dalle normative vigenti.

Articolo 8: Misure di prevenzione

1. Per ridurre il rischio di usi impropri della "navigazione in Internet", vengono implementate misure di accesso filtrato mediante un software che inibisca l'accesso a specifici siti o pagine ritenuti non correlabili con alcuna attività. Gli eventuali controlli possono avvenire mediante un sistema di controllo dei contenuti (proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo e sistematico, ma viene effettuato soltanto dietro motivata richiesta del responsabile del Servizio a cui il lavoratore è assegnato In ogni caso, i file vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità dell'Ente.
2. Per ridurre il rischio di usi impropri della "Posta elettronica" sono emanate direttive da parte dei soggetti competenti circa l'utilizzo prioritario di indirizzi di posta elettronica condivisi tra più utenti eventualmente affiancati a quelli individuali.
3. Per combattere lo "SPAM" è utilizzato apposito software per i messaggi di posta in transito. Questa attività è svolta in modo autonomo dal software che non mantiene memoria dei messaggi analizzati.

Articolo 9: Monitoraggi

1. Per finalità tecniche, economiche o statistiche è effettuato, nel rispetto dell'obbligo di adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati e per prevenire utilizzi indebiti, il monitoraggio:
   a. Dei dati di traffico telefonico derivati dai centralini dell'Amministrazione, della navigazione internet e delle comunicazioni via posta elettronica. Tale monitoraggio mediante "file di log" è disciplinato, nei suoi aspetti tecnici, da un documento tecnico denominato "Norme per la raccolta, gestione, conservazione e distruzione dei file di log" predisposto ed costantemente aggiornato dal Sistema Informativo dell'Ente ed adottato con atto del Dirigente di tale servizio. Di tale documento è assicurata idonea pubblicità;
   b. Dei dati di traffico relativo alle attività di accesso ai dati ed alle banche dati del Comune di Prato
   c. Dell'Hardware e del software degli elaboratori in rete;
   d. Dell'uso delle stampanti, sia in modo indiretto, tramite il conteggio dei ricambi consumati, sia in modo diretto, tramite contatori attivati per stampante.

Articolo 10: Misure a garanzia degli utenti

1. Allo scopo di garantire i diritti degli utenti sono adottate le seguenti misure:
   a. I dati prodotti dai monitoraggi effettuati non possono essere oggetto di elaborazioni volte a definire il profilo o la personalità dell'utente ovvero ad individuarne dati sensibili e giudiziari;
   b. I documenti elettronici e/o cartacei funzionali alla rilevazione di eventuali anomalie sull'utilizzo delle risorse, ivi compresi quelli formati dall'elaborazione dei dati estratti dai "files di log", sono prodotti, di norma, a cadenza bimestrale rispettando i principi di finalità, pertinenza e non eccedenza di cui al "Codice protezione dati personali", sono forniti ai soggetti che esercitano la funzione di controllo per ciascuna tipologia di utenti e sono conservati, di norma, per il tempo strettamente necessario all'espletamento delle relative procedure.
   c. L'accesso da parte dell'Amministrazione ai dati e agli strumenti elettronici, ivi compresa la corrispondenza elettronica, è limitato ai soli casi nei quali sia indispensabile ed indifferibile intervenire per assicurare il regolare svolgimento dei servizi ovvero la manutenzione, la sicurezza, la disponibilità e l'integrità di sistemi informativi e di dati. Le relative procedure sono descritte nel Documento Programmatico per la Sicurezza aziendale. L'utente deve essere informato, anche successivamente, dell'intervento effettuato del quale è redatto apposito verbale;
2. Le procedure di cui al precedente comma 1 lett. c. si applicano, anche senza informare l'utente, in caso di cessazione dal servizio per dimissioni o altra causa, se l'utente non ha provveduto o

non può provvedere all'applicazione delle procedure previste per questi casi nel Documento Programmatico per la Sicurezza (DPS) aziendale.

Articolo 11: Controlli relativi all'utilizzo delle risorse

1. I controlli sono attivati:
   a. nel caso in cui si verifichino anomalie dal confronto dei documenti di cui al precedente articolo 10, comma 1, lettera b.;
   b. nel caso in cui si verifichi un evento dannoso o una situazione di pericolo ovvero un segnale od un messaggio di avviso, allarme e avvertimento nel sistema informativo (alert) che rendano necessarie misure di verifica di comportamenti anomali;
   c. nel caso in cui, da un'analisi non correlata agli utenti ed effettuata per motivi tecnici, economici, statistici siano rilevate anomalie;
   d. Nel caso previsto dall'art. 8, comma 1, secondo capoverso.
2. I controlli devono essere svolti nel rispetto dei seguenti criteri:
   a. Deve essere, per quanto possibile, preferito un controllo preliminare su dati aggregati anonimi riferiti alle strutture apicali;
   b. Il controllo anonimo produce in prima istanza, in presenza di anomalie, un avviso generalizzato con l'invito ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite;
   c. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale;
   d. 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;
3. I soggetti che esercitano la funzione di controllo sono: il direttore generale, i dirigenti apicali per le risorse umane che operano nella loro struttura organizzativa, i responsabili del Servizio di cui all'art. 8, comma 1, secondo capoverso.
4. I controlli sono effettuati nel rispetto delle disposizioni in materia di privacy e di misure minime di sicurezza, come indicato dai Responsabili di Servizio in materia di trattamento dei dati ai sensi del disciplinare tecnico allegato al decreto legislativo 30 giugno 2003, n.196.

Articolo 12: Pubblicità e Decorrenza

1. Il presente regolamento verrà adeguatamente pubblicizzato verso i singoli utenti attraverso i normali strumenti di comunicazione interna all'Amministrazione.
2. Il presente regolamento costituisce informativa agli utenti ai sensi dell'art. 13 del Dlgs. 196/2003 "Codice Protezione Dati Personali".

Il presente Regolamento del Comune di Prato avrà decorrenza dal primo giorno del mese successivo al termine della procedura di cui all’art. 4 della Legge 300/1970 “Statuto dei Lavoratori” nonché delle normali procedure previste in materia di relazioni sindacali.