



Città di Arese

PROVINCIA DI MILANO

*REGOLAMENTO PER L'UTILIZZO
DEGLI STRUMENTI INFORMATICI E TELEMATICI*

Approvato con deliberazione della Giunta comunale n. 11 in data 11.07.2013

OGGETTO

Premessa.....	3
Scopo e campo di applicazione.....	3
Definizioni	4
Funzionamento delle risorse informatiche.....	5
Dati trattati attraverso le risorse informatiche concesse in dotazione.....	5
Utilizzo delle Postazioni di lavoro	6
Utilizzo dei supporti mobili e PC portatili	7
Utilizzo della rete LAN e delle risorse condivise	8
Acquisizione e installazione software.....	9
Servizi con impatto sui sistemi informatici.....	9
Gestione delle password e degli accessi	10
Attività di backup.....	11
Attività e strumenti di assistenza remota	11
Posta elettronica	12
Internet	13
Social Networks	14
Sicurezza generale e perimetrale.....	15
Telefonia mobile e dispositivi che consentono la navigazione internet.....	15
Attività dell'Amministratore di Sistema	16
Osservanza delle regole sulla privacy.....	16
Osservanza del presente disciplinare	16
Entrata in vigore.....	17

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete tramite i personal computer, espone il Comune a rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

L'utilizzo delle risorse informatiche e telematiche dell'Ente deve sempre ispirarsi al principio di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro.

Il personal computer, i relativi programmi e/o applicazioni e/o dati ed archivi affidati in uso ai dipendenti sono strumenti di lavoro di proprietà comunale. Tutto quanto messo a disposizione, ricevuto, rilasciato e comunque memorizzato sul posto di lavoro e sui mezzi di comunicazione è e rimane di proprietà dell'Ente.

Il Garante della Privacy è intervenuto sul tema dell'utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet con il provvedimento n. 13 del 1° marzo 2007, indicando ai datori di lavoro le linee guida da adottare a garanzia degli interessi del personale dipendente, garantendo l'adozione delle misure di sicurezza idonee ad assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati.

Inoltre lo Statuto dei Lavoratori (L.300/70) all'art. 4 prevede che

“Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna.”

Scopo e campo di applicazione

Alla luce di quanto premesso, il Comune di Arese adotta il presente disciplinare interno al fine di

- evitare comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati;
- informare il personale dipendente di quali sono le misure di tipo organizzativo e tecnologico adottate dall'Ente per la sicurezza dei dati;
- informare il personale dipendente su come vengono trattati i dati relativi all'uso dei mezzi informatici per la tutela dei lavoratori.

Questo documento non si riferisce solamente all'utilizzo di internet o della rete locale, ma si riferisce a tutto l'insieme delle risorse informatiche, di calcolo, di comunicazione, elettroniche e a qualsiasi altra tipologia di risorsa presente nell'Ente.

Nel caso di soggetto esterno nominato dal Comune responsabile del trattamento, questi deve impegnarsi a far rispettare il presente documento a tutti i propri dipendenti e ad eventuali altri soggetti nei trattamenti di dati effettuati per conto dell'Ente.

Definizioni

TITOLARE del trattamento dei dati: è la figura individuata dall'art. 28 del Decreto Legislativo 30 giugno 2003, n. 196. Vigila sulla puntuale osservanza di tutte le disposizioni in materia di trattamento dei dati. Coordina la designazione di tutte le altre figure coinvolte nel trattamento informatico dei dati.

RESPONSABILE del trattamento: è la figura prevista dall'art. 29 del Decreto Legislativo 30 giugno 2003, n. 196 ed è nominata dal Titolare. Garantisce il pieno rispetto delle vigenti disposizioni in materia di trattamento (anche informatico) dei dati; i compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare al momento della nomina.

RESPONSABILE dei sistemi informativi: è la figura che gestisce e coordina le attività di configurazione/aggiornamento dei sistemi e degli archivi informatici. Il ruolo del Responsabile è solo quello di coordinatore dell'applicazione della normativa sulla riservatezza, ferme restando le responsabilità dei singoli Responsabili e del Titolare in merito all'adozione degli atti (nomina incaricati, rilevazione banche dati, istruzione agli incaricati, ecc). Il ruolo di Responsabile dei Sistemi Informativi è svolto dal Responsabile dell'Area a cui fanno capo i Sistemi Informativi dell'Ente.

RESPONSABILE dei sistemi informativi per trattamenti in outsourcing: eventuali società che interagiscano con i sistemi informativi dell'Ente (hardware o software) con mansioni di amministratore di sistema.

AMMINISTRATORI DI SISTEMA: sono i soggetti (fisici o giuridici) designati dal Titolare che provvedono operativamente alla gestione e manutenzione del sistema informatico comunale.

INCARICATO del trattamento: è la figura prevista dall'art. 30 del Decreto Legislativo 30 giugno 2003, n. 196 ed è nominata dal Responsabile o dal Titolare del trattamento; tratta i dati sia in forma cartacea sia attraverso strumenti informatici; opera sotto la diretta autorità del Responsabile del trattamento, attenendosi alle istruzioni impartite.

CUSTODE DELLE PASSWORD: ove i sistemi informatici o le banche dati non consentano una gestione automatizzata delle credenziali di accesso e comunque in tutti i casi in cui sia necessario tenere traccia delle credenziali per iscritto, viene nominato un custode delle password che provvede a conservare tali credenziali.

SISTEMI INFORMATIVI: è l'ufficio preposto alla gestione dei sistemi informatici in generale; può essere altrimenti denominato CED.

TRACCIAMENTO: memorizzazione di eventi e operazioni effettuata automaticamente da un qualsivoglia dispositivo informatico, per finalità manutentive e di funzionamento dello stesso.

RILEVAZIONE: complesso di operazioni di analisi e verifica dei tracciamenti effettuati dai dispositivi effettuate a fronte di comprovate necessità definite nei capitoli seguenti del presente disciplinare.

Funzionamento delle risorse informatiche

I dispositivi elettronici tracciano una serie di eventi di sistema per attività amministrative, manutentive e/o di sicurezza, che variano a seconda della tipologia dei dispositivi stessi.

Il tracciamento di tali eventi non è generalmente oggetto di rilevazione da parte del servizio informatico. Qualora, per necessità manutentive o di gestione della sicurezza si renda necessario rilevare e/o registrare gli eventi tracciati di una risorsa specifica, tali trattamenti verranno preventivamente segnalati al personale comunale nelle modalità indicate nei successivi paragrafi.

Dati trattati attraverso le risorse informatiche concesse in dotazione

Le risorse informatiche sono messe a disposizione dall'Ente ai propri appartenenti per finalità legate alle attività istituzionali dell'Ente stesso, pertanto l'utilizzo degli strumenti in dotazione e il trattamento è di prevalente carattere professionale.

E' consentito l'utilizzo per finalità personali della postazione di lavoro a condizione che:

- venga effettuato al di fuori dell'orario di lavoro;
- non sia contrario alle regole di condotta indicate nei paragrafi successivi e non possa in alcun modo ledere l'immagine dell'Ente;
- non danneggi in alcun modo, diretto o indiretto, le proprietà dell'Ente;
- sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente.

E' importante precisare che è consentito l'utilizzo personale esclusivamente della postazione di lavoro, compresa la navigazione internet in siti legali; non è in alcun modo consentito trattare dati di cui l'Ente è Titolare del Trattamento se non per attività di carattere professionale.

E' ammessa la custodia di dati personali sulla postazione di lavoro a condizione che:

- siano riposti in cartelle di cui sia esplicitamente indicata la privatezza del dato (es. cartelle con dicitura "personale");
- vengano rimossi prima del rilascio della postazione di lavoro.

Alla riconsegna delle attrezzature da parte degli utenti all'Ente, questo potrà liberamente disporre di eventuali informazioni ivi presenti. Eventuali dati personali ancora residenti al momento della riconsegna della postazione verranno rimossi indiscriminatamente.

Utilizzo delle Postazioni di lavoro

La postazione di lavoro affidata al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente l'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Non è consentito installare programmi provenienti dall'esterno salvo preventiva autorizzazione del Responsabile dei Sistemi Informativi, onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli messi a disposizione dall'Ente stesso, in quanto l'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Ente a gravi responsabilità civili e penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (Legge 633 del 22 aprile 1941 sulla tutela della proprietà intellettuale, D.Lgs. 518 del 29 dicembre 1992 sulla tutela giuridica del software e aggiornamenti successivi) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Il PC viene consegnato all'utente con una configurazione coerente con le misure organizzative e di sicurezza impostate dall'Ente stesso: non è consentito all'utente di modificare le caratteristiche impostate sul PC.

Il PC deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio, salvo specifica disposizione dell'Amministratore di Sistema e/o a seguito di pianificazione dello spegnimento automatico. In ogni caso, poiché 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'uso indebito, l'utente che si allontana dalla postazione deve bloccare l'uso tramite la combinazione dei tasti CTRL + ALT + CANC e successivo INVIO. Lo screen saver deve essere attivato con la richiesta di password per lo sblocco e deve partire automaticamente dopo 15 minuti di non utilizzo.

Ogni utente deve prestare la massima cautela nell'utilizzo dei supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevate minacce dal sistema antivirus.

Non è consentito l'utilizzo di giochi o altre applicazioni di tipo ludico anche se comprese nel sistema operativo installato.

Non sono permesse, a meno di specifiche e documentate autorizzazioni le seguenti attività:

- caricare, memorizzare, pubblicare, diffondere, distribuire, tramite risorse dell'Ente documenti, informazioni, immagini, filmati ecc. in generale, ed in particolare:
 - a carattere violento, pornografico o contrario alla pubblica decenza, o suscettibile di mancare di rispetto agli esseri umani o alla loro dignità, con contenuto discriminatorio razziale ed etnico, contrario al buon costume, oltraggioso nei confronti dei minori, contrario all'ordine pubblico, diffamatorio o che contenga contenuti illeciti penalmente o civilmente riconducibili a categorie qui non espressamente indicate;
 - pregiudizievoli per le risorse dell'Ente e per l'integrità e la conservazione dei dati dell'Ente stesso;
 - pregiudizievoli per l'immagine e il buon nome dell'Ente presso terzi;

- accedere a server web trattanti materie o soggetti ricadenti nelle categorie sopra elencate;
- tenere comportamenti che possano indurre taluno ad effettuare invii di materiale rientrante nelle tipologie sopra elencate; laddove l'utente si trovi a ricevere anche contro il suo volere tali materiali, è tenuto a informare il CED ed attenersi alle sue istruzioni circa il trattamento di tali materiali;
- utilizzare le risorse dell'Ente con fini di molestia, minaccia o comunque violando le norme di legge in vigore;
- caricare, memorizzare, trasmettere o utilizzare programmi, software, procedure o altri strumenti e/o contenuti che siano protetti dalle leggi sulla proprietà intellettuale, salvo che il Comune di Arese ne detenga regolare licenza e/o autorizzazione del produttore;
- utilizzare strumentazioni, programmi, software, procedure, ecc. messi a disposizione dall'Ente in violazione delle Leggi sulla proprietà intellettuale, delle regole di buona tecnica applicabili e delle prescrizioni emanate dall'Ente;
- caricare o trasmettere, consapevolmente, archivi o programmi contenenti virus o dati alterati;
- manomettere sistemi o archivi in maniera tale da inficiare la riservatezza, la disponibilità e/o l'integrità dei dati;
- inviare messaggi in massa ("spam") o favorire il propagarsi di notizie riconducibili a ciò che abitualmente viene definito "catena di S. Antonio";
- utilizzare le risorse dell'Ente in modo da consentire a soggetti non abilitati l'accesso ai dati e ad alle informazioni riservate, se non nei casi espressamente previsti dalla Legge e dai Regolamenti.

Poiché alcune attività sopra elencate possono avere conseguenze di natura penale, esse originano in capo al trasgressore tutte le responsabilità previste dalla Legge.

Nonostante la presenza di programmi antivirus, è ritenuto statisticamente probabile che l'utilizzo di applicazioni di comunicazione (internet, posta elettronica, ecc.) e di supporti magnetici rimovibili (chiavette USB, hard disk esterni, DVD/CD, ecc.) comporti la trasmissione di virus informatici o di programmi in grado di alterare, distruggere o monitorare l'attività e i contenuti dei personal computer.

In caso di anomalie dell'hardware e del software affidatogli l'utente deve immediatamente bloccarne l'operatività, fermare le eventuali elaborazioni in corso ed informare immediatamente il CED per le incombenze di competenza.

Utilizzo dei supporti mobili e PC portatili

Tutti i supporti magnetici riutilizzabili (chiavette USB, hard disk esterni, DVD/CD, ecc.) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato da soggetti non autorizzati all'accesso a tali dati.

I supporti magnetici contenenti dati sensibili e giudiziari non possono generalmente essere portati all'esterno della sede comunale, all'interno della quale devono comunque essere

custoditi con cautela. Qualora si renda necessario portare all'esterno dati sensibili e giudiziari si dovranno valutare con il CED opportune misure atte a garantire la sicurezza dei dati.

L'utente è responsabile delle attrezzature informatiche portatili assegnategli dai Sistemi Informativi e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai portatili si applicano le regole di utilizzo previste per i PC connessi alla rete, con particolare attenzione alla rimozione di eventuali file elaborati sugli stessi prima della riconsegna.

Gli utenti di PC portatili si impegnano, dovunque dovessero trovarsi, a mettere in sicurezza la strumentazione utilizzata e i dati nella stessa contenuta.

Danni arrecati alle attrezzature o la loro perdita dovuta ad incauta custodia saranno a carico dell'utente utilizzatore.

Non è consentito l'utilizzo sul PC di nessun dispositivo di memorizzazione, comunicazione o altro (ad es. masterizzatori, modem ...) se non concordato preventivamente con il CED.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna. Prima dell'apertura del supporto deve provvedere alla sua scansione tramite il software antivirus. L'utente deve avvertire immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevate minacce.

Utilizzo della rete LAN e delle risorse condivise

Al fine di garantire la disponibilità dei dati e un'efficace politica di backup, gli utenti devono salvare su cartelle di rete tutti i file di lavoro ed astenersi dal salvarli sul disco locale della postazione di lavoro (si specifica che la cartella "desktop" si trova sulla postazione in locale, pertanto è inadatta al salvataggio dei file perché non sottoposta a procedure di backup).

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

Su tali cartelle/unità di rete vengono svolte regolari attività di amministrazione e backup.

Le credenziali di accesso alla rete ed ai programmi sono personali: è assolutamente vietato entrare nella rete e nei programmi con profili di altri utenti.

L'Amministratore di Sistema, nell'espletamento delle mansioni attribuitegli dal Responsabile dei Sistemi Informativi, può in qualunque momento procedere alla rimozione di ogni file o applicazione che ritenga pericolosi per la sicurezza, sia sui PC degli incaricati sia sui server.

I Responsabili del Trattamento dovranno partecipare alla corretta gestione degli archivi informatici:

- verificando la coerenza delle cartelle con i trattamenti individuati a norma di legge;
- verificando ed eventualmente variando, avvalendosi dell'Amministratore di Sistema, le "permissions" di accesso a tali risorse affinché siano coerenti con le nomine di incarico del trattamento dati ed eventuali disposizioni sulla fascicolazione.

Per la trasmissione di files all'interno dell'Ente è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare la cartella "SCAMBIO" creata a tale scopo. Tale cartella deve essere tenuta in ordine dagli stessi utenti, eliminando i file non più necessari anche al fine di non consentire il trattamento dei dati a soggetti non espressamente incaricati. Il CED, nello svolgimento delle proprie attività di manutenzione dei sistemi informatici, si riserva di cancellare indiscriminatamente files depositati per troppo tempo senza validi motivi nella cartella "SCAMBIO".

La gestione delle cartelle di lavoro degli utenti salvate su server è di competenza del CED, dietro indicazioni del Responsabile dei Sistemi Informativi. Per qualsiasi necessità legata all'utilizzo e alla configurazione delle cartelle i Responsabili del Trattamento possono rivolgersi al Responsabile dei Sistemi Informativi che incaricherà il CED degli eventuali adempimenti operativi.

Gli utenti dovranno effettuare la stampa dei dati solo se strettamente necessaria e dovranno ritirarla prontamente dai vassoi delle stampanti comuni. Su richiesta dell'utente, potrà essere attivato il sistema di stampa differito per le stampe di dati soggetti alle norme che tutelano la privacy, previa digitazione di un codice personale. (Sistema supportato dalle attuali stampanti dipartimentali installate presso l'Ente).

Il collegamento alla rete comunale di personal computer portatili o di attrezzature informatiche non di proprietà del Comune di Arese è generalmente non consentito. Il CED potrà consentire deroghe a quanto previsto solo dopo attenta valutazione.

Acquisizione e installazione software

Sulle postazioni è consentita l'installazione esclusiva delle seguenti categorie di software:

- software commerciale dotato di licenza d'uso (es. pacchetti di Office Automation);
- software gestionale realizzato specificatamente per l'Amministrazione comunale dalle ditte specializzate nel settore della P.A. (es. applicativi in uso ai vari servizi);
- software realizzato specificatamente dagli organi centrali della Pubblica Amministrazione o Enti nazionali (es. INPS, Ministeri...);
- software gratuito (freeware) e shareware prelevato dai siti internet, solo se espressamente autorizzato da un Amministratore di Sistema;
- qualsiasi altro software si renda necessario per l'esercizio delle attività lavorative e istituzionali.

L'acquisto e la conseguente installazione di software devono essere sempre preventivamente valutati, autorizzati ed effettuati in collaborazione con i Sistemi Informativi, al fine di garantire la stabilità dei sistemi e la compatibilità del software con gli stessi.

Servizi con impatto sui sistemi informatici

L'acquisizione di materiale hardware o di qualsiasi dispositivo che interagisca con la rete e/o la strumentazione informatica comunale o possa avere un impatto con essi, qualora non venga eseguita direttamente dal CED, deve essere concordata preventivamente con questo, onde evitare malfunzionamenti, cadute prestazionali o altri problemi alla sicurezza e all'immagine dell'Ente stesso.

Qualora nell'esercizio di una funzione amministrativa sia prevista la fornitura di software accessorio alla gestione/erogazione di un servizio (es. gestione rette mensa, gestione smart card ...), l'ufficio competente provvede a consultare i Sistemi Informativi nelle fasi preliminari del processo di acquisizione per la corretta definizione delle caratteristiche del software, affinché esso risulti:

- compatibile con il sistema informatico comunale;
- conforme alle misure di sicurezza adottate dall'Ente con particolare riguardo alla sicurezza degli accessi;
- certificato per l'installazione sulle macchine in dotazione al Comune (server e pc);
- installato correttamente.

In caso di mancata consultazione preventiva dei Sistemi Informativi non verrà effettuata alcuna installazione.

Qualora venga affidata all'esterno la gestione di dati comunali per l'erogazione di servizi, l'ufficio competente deve concordare preventivamente con il servizio informatico le modalità e i formati con cui questi dati devono essere scambiati sia in ingresso che in uscita e le condizioni di consegna dei dati al termine del rapporto di collaborazione.

Gestione delle password e degli accessi

L'utente deve utilizzare sempre una password quando viene richiesto dalla procedura, avendo cura che nessuno ne venga a conoscenza.

Le password di ingresso al dominio e dello screensaver sono previste e vengono attribuite dall'Amministratore di Sistema all'utente per il primo accesso. Dopo il primo accesso il sistema chiederà all'utente di modificare la password, la quale sarà conosciuta solo dall'utente stesso. Qualora si renda necessario (per manutenzione, aggiornamenti, assenza prolungata imprevista che renda indisponibili risorse gestite dall'utente) che l'Amministratore debba entrare nel sistema con il profilo dell'utente, verrà modificata la password di accesso dell'utente stesso. Al successivo accesso da parte dell'utente l'Amministratore rilascerà una password di cortesia che verrà immediatamente modificata dall'utente.

L'accesso agli applicativi può a sua volta essere regolato da un'ulteriore password: le modalità di gestione e di scadenza della password sono specifiche per ogni programma. All'utente sarà fornito un profilo personale e verranno attivate procedure per garantire all'utente stesso la conoscenza esclusiva della propria password. Nel caso il sistema non lo consenta o sia necessario l'intervento dell'Amministratore di Sistema per garantire la disponibilità dei dati, verranno concordate procedure specifiche per la gestione degli accessi fra il Responsabile dei Sistemi Informativi e il Responsabile del Trattamento.

La combinazione dell'accesso al dominio e agli applicativi garantirà il rispetto delle regole minime di sicurezza indicate nel Codice della Privacy.

Le password del dominio e degli applicativi, salvo impossibilità dovute all'obsolescenza del software, devono essere modificate ogni 3 mesi, devono essere formate da almeno un carattere numerico, almeno un carattere non alfabetico (\$,* ,% ecc); devono essere composte da otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'incaricato.

Nel caso in cui si sospetti che una password abbia perso la sua riservatezza, l'utente provvederà ove possibile a modificarla personalmente, altrimenti provvederà a modificarla con il supporto dell'Amministratore di Sistema.

Non è consentito utilizzare il profilo personale di altri soggetti per connettersi al dominio o agli applicativi. Qualora l'utente venisse a conoscenza delle password di un altro utente, è tenuto a darne immediata notizia all'Amministratore di Sistema competente.

Nel caso di inserimento di password errata, dopo un numero di tentativi dipendenti dal contesto informatico di utilizzo, il profilo dell'utente potrebbe venire disabilitato; in questo caso sarà possibile richiederne la riattivazione all'Amministratore di Sistema competente.

Come indicato al punto 7 dell'Allegato B del Codice della Privacy *“Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica”*.

Attività di backup

Sono oggetto di attività di salvataggio centralizzato su supporti magnetici o ottici:

- i file salvati sulle cartelle/unità di rete messe a disposizione dai Sistemi Informativi;
- le banche dati di applicativi ed i relativi file di sistema;
- il contenuto delle caselle di posta elettronica gestite dall'apposito server;
- tutti i dati e le informazioni di sistema ritenuti necessari e rilevanti al fine di assicurare la continuità dei servizi.

Gli elementi sopra indicati vengono salvati sistematicamente di notte con una politica di storicizzazione impostata dai Servizi Informativi. Le modalità di salvataggio dei dati comportano la registrazione dei dati su supporti ottici o magnetici per un massimo di 12 mesi.

I dati che risiedono sulle postazioni PC non sono soggetti a operazioni di backup centralizzato.

Per quanto riguarda gli archivi residenti sulle postazioni di lavoro per inevitabili necessità di servizio, l'attività di backup dovrà essere organizzata dagli incaricati in collaborazione con i Servizi Informativi.

Attività e strumenti di assistenza remota

Per finalità di carattere manutentivo sono attivi presso l'Ente strumenti di assistenza remota che consentono agli Amministratori di Sistema di connettersi alle postazioni degli utenti per fornire supporto in tempo reale e assistere gli utenti nella risoluzione di problematiche di carattere informatico (tale connessione è chiaramente visibile da parte degli utenti sulla postazione).

L'utente dovrà consentire l'intervento remoto da parte dell'amministratore di sistema tramite autorizzazione esplicita.

Per quanto riguarda gli interventi di assistenza remota sulle postazioni da parte di Amministratori esterni, detti interventi dovranno comunque essere preventivamente concordati con il CED o comunque comunicati al servizio stesso.

Posta elettronica

La casella di posta elettronica, assegnata dall'Ente all'utente, è uno strumento di lavoro.

Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Qualsiasi attività istituzionale realizzata tramite utilizzo di posta elettronica deve essere svolta con l'esclusivo utilizzo di caselle registrate sotto il dominio di posta istituzionale dell'Ente o tramite caselle di posta elettronica certificata registrate dall'Ente stesso.

E' fatto divieto di utilizzare le caselle di posta elettronica comunale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione da parte del Responsabile dei Sistemi Informativi per esigenze di lavoro.

E' inoltre da evitare ove possibile l'invio di messaggi con allegati di grandi dimensioni al fine di evitare eventuali sovraccarichi al sistema informativo e nuocere all'efficacia della comunicazione.

La casella di posta deve essere tenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Per la trasmissione di file all'interno dell'Ente è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, oppure è possibile utilizzare la cartella "SCAMBIO" creata a tale scopo.

E' vietato inviare mail con allegati contenenti file eseguibili (estensione .exe, .bat, ecc.).

E' vietato inviare catene telematiche (o di S. Antonio). Se si dovessero ricevere messaggi di tale tipo, si dovrà cancellare il messaggio ricevuto senza divulgarlo in alcun modo. Non si dovranno in alcun caso attivare gli allegati di tali messaggi.

Qualora si ricevessero messaggi sospetti di richiesta di password o altre informazioni oppure di invito a svolgere operazioni sulla propria postazione di lavoro (es. apertura o cancellazione di file, installazione aggiornamenti, ecc) di cui non è certa la provenienza, l'utente è tenuto a segnalarli immediatamente all'Amministratore di Sistema competente prima di effettuare qualsiasi azione.

Al fine di garantire la continuità di servizio, sono previste 3 differenti modalità per la gestione delle assenze, programmate o non, degli operatori preposti alla lettura dei messaggi di una specifica casella di posta:

- 1) in caso di assenza programmata, attivazione di un risponditore automatico che notifichi al mittente la temporanea indisponibilità del destinatario;
- 2) attivazione da parte dell'Amministratore di Sistema, su richiesta del Responsabile del Trattamento, dell'inoltro automatico dei messaggi pervenuti alla casella dell'utente assente;
- 3) abilitazione da parte dell'Amministratore di Sistema dell'accesso alla casella dell'utente da parte di un soggetto incaricato dal Responsabile del trattamento.

Nei casi 2) e 3) l'Amministratore di Sistema redigerà un rapporto dell'intervento effettuato, indicando il nominativo del Responsabile che ha autorizzato l'operazione. Il rapporto di intervento verrà inviato all'utente assente, al suo Responsabile e al Responsabile dei Sistemi Informativi.

E' vietato utilizzare client di posta elettronica differenti da quelli installati e configurati dall'Amministratore di Sistema.

Gli indirizzi di posta elettronica in uso presso l'Ente sono di 2 tipologie:

- 1) caselle nominative, assegnate con la convenzione <nome.cognome>@comune.aresse.mi.it. Tali caselle sono intestate personalmente agli utenti: è importante sottolineare che, nonostante le caselle siano intestate ad un individuo, sono da considerarsi uno strumento di lavoro e non corrispondenza privata; pertanto, l'utilizzo verso destinatari esterni dovrà essere consono con le funzioni istituzionali svolte dall'Ente. La divulgazione dell'indirizzo di posta nominativo deve essere limitata ai soli casi in cui non possa essere divulgato l'indirizzo di posta relativo all'ufficio di appartenenza;
- 2) caselle di posta assegnate ad un ufficio o ad una funzione sul dominio comune.aresse.mi.it. In caso di gruppi di distribuzione assegnati a più persone, la continuità nella gestione della corrispondenza e delle attività ad essa correlate dovrà essere assicurata dal competente Responsabile del Trattamento dei dati attraverso opportune scelte organizzative.

L'Amministratore di Sistema competente, nell'espletamento delle sue funzioni, potrà accedere alle caselle di posta assegnate per finalità manutentive solo in presenza dell'assegnatario (o su sua esplicita autorizzazione) della casella o su richiesta del Responsabile del Trattamento secondo le modalità illustrate precedentemente.

In ogni caso l'Ente si impegna a rispettare la confidenzialità dei messaggi elettronici di provenienza o a destinazione di eventuali recapiti sindacali (contenuto, autori e destinatari), delle mailing list elaborate e scambiate in rete da organismi sindacali, ecc.

Internet

Il collegamento ad Internet è uno strumento messo a disposizione per finalità di carattere lavorativo: è consentita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa a condizione che

- venga effettuata al di fuori dell'orario di lavoro;
- non sia contraria alle regole di condotta indicate nel presente disciplinare e non possa in alcun modo ledere l'immagine dell'Ente;
- non danneggi in alcun modo, diretto o indiretto, le proprietà dell'Ente;
- sia esplicito verso terzi che la responsabilità di qualsiasi operazione svolta per finalità personali sia imputabile esclusivamente all'utente.

Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione. Pertanto, per garantire quanto previsto dalla Legge e secondo le direttive emanate dal Garante per la tutela e protezione dei dati, al fine di evitare abusi, viene attivato un filtro che blocca l'accesso ai siti ritenuti palesemente non pertinenti con le attività istituzionali. Il filtro adottato utilizza sistemi euristici di scarto di siti facenti parte di categorie appositamente selezionate. Qualora, per lo svolgimento della attività istituzionali, un utente necessitasse di accedere a un sito scartato dai sistemi di filtraggio, potrà richiederne lo sblocco per tramite del Responsabile del Trattamento (che ne assume la responsabilità) al Responsabile dei Sistemi Informativi.

E' fatto assoluto divieto all'utente di scaricare software gratuito (freeware) e shareware prelevato dai siti internet, se non espressamente autorizzato dall'Amministratore di Sistema competente.

E' tassativamente vietato qualsiasi genere di transazione privata in campo finanziario ivi comprese le operazioni di remote banking, acquisti on line e simili, salvo che non sia espressamente consentito per ragioni di servizio.

E' tassativamente vietata ogni forma di registrazione e connessione a siti i cui contenuti non siano legati all'attività lavorativa, se non nelle eccezioni indicate precedentemente.

E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line, di blog, di bacheche elettroniche e in generale di strumenti di social network anche utilizzando pseudonimi (o nicknames), esclusi gli strumenti autorizzati per esigenze di lavoro.

A fini statistici, di qualità del servizio e di sicurezza, l'occupazione di banda generata dal traffico internet e dallo scambio di posta elettronica potrà essere soggetta a controlli da parte dell'Ente sotto forma di dati aggregati ed anonimi, in osservanza dei limiti posti dalla legge in materia di riservatezza.

Qualora i sistemi di sicurezza segnalino delle potenziali criticità che possano minare l'integrità dei dati e la stabilità del sistema stesso, potrebbero essere effettuati dei controlli sulla navigazione internet. Tali controlli saranno preventivamente segnalati al personale e si opereranno secondo stadi successivi:

- 1) controlli generici sulle pagine visitate, senza che vengano tracciati gli utenti che le visitano;
- 2) controlli aggregati sulle pagine visitate con suddivisione del traffico effettuato per aree;
- 3) controlli specifici sulle pagine visitate, con tracciamento dell'indirizzo IP da cui si effettua la visita o dell'utente che la effettua.

Il tracciamento specifico verrà effettuato solo qualora il trattamento generico e quello aggregato non abbiano consentito di risolvere le criticità riscontrate e verrà comunque nuovamente segnalato in forma preventiva agli utenti.

Tutti i dati di traffico internet sono comunque sottoposti a tracciamento da parte di sistemi automatici implementati presso l'Ente e custoditi per limitati periodi di tempo. La consultazione di tali dati, al di fuori dei casi indicati precedentemente, è consentita solo alle forze dell'ordine per attività di carattere ispettivo consentite dalla normativa sulla privacy.

Social Networks

Non è consentito l'utilizzo di social networks durante l'orario di lavoro, a meno che tali piattaforme non vengano espressamente impiegate in maniera strumentale per lo svolgimento delle proprie attività lavorative.

E' assolutamente vietato esprimere opinioni su informazioni acquisite durante lo svolgimento delle proprie attività istituzionali o condividere informazioni e riferimenti di carattere professionale che in qualche modo possano ledere l'immagine dell'Ente. Tale divieto è da intendersi anche al di fuori dell'orario di lavoro ed eventualmente oltre la cessazione della collaborazione professionale con il Comune.

Per qualsiasi danno che potesse derivare all'immagine dell'Ente imputabile a comportamenti non conformi alle indicazioni sopra riportate e comunque contrari alle norme sulla pubblica amministrazione, il Comune potrà applicare al trasgressore un provvedimento disciplinare ed eventuali sanzioni previste dalla legge.

Sicurezza generale e perimetrale

Presso l'Ente è attivato un sistema di sicurezza perimetrale a difesa dei sistemi e dei dati comunali, che traccia eventi che possono essere indizio di minacce informatiche. Il sistema è soggetto a procedure di aggiornamento automatico per quanto riguarda la lista e le caratteristiche delle minacce.

E' gestito dal CED, il quale effettua attività di verifica delle segnalazioni attivate dal sistema stesso, con lo scopo di comprendere e prevenire eventuali minacce esterne.

Qualora il sistema attivato rilevi delle minacce a specifici indirizzi IP interni delle postazioni di lavoro, il CED verificherà le cause delle minacce rilevate insieme all'utente/utenti che abitualmente utilizza/utilizzano la postazione, con l'obiettivo di comprendere la natura dell'intrusione e prevenire eventuali danni.

Una volta individuate le cause dell'evento rilevato verranno adottati provvedimenti correttivi, con segnalazione al Titolare dei trattamenti di eventuali violazioni alle regole indicate nel presente disciplinare.

Telefonia mobile e dispositivi che consentono la navigazione internet

Tutti i dispositivi di telefonia mobile e/o che consentono la navigazione internet attraverso un piano tariffario a carico dell'Ente costituiscono uno strumento di lavoro e/o attività istituzionale, pertanto gli eventuali affidatari devono prestare adeguate cautele durante il loro utilizzo.

I dati contabili relativi al traffico telefonico ed internet potranno essere analizzati dall'Ente al fine di consentire un adeguato controllo e contenimento dei costi. I numeri telefonici presenti nei dati di traffico saranno oscurati nelle ultime tre cifre, per cui non sarà possibile risalire ai numeri contattati.

A causa della sempre maggiore interazione tra i dispositivi telefonici e informatici, l'abuso di tali strumenti può costituire una potenziale fonte di minaccia ai sistemi dell'Ente. Pertanto è vietato:

- utilizzare i dispositivi per navigare in Internet presso siti che esulino dalle attività istituzionali;
- installare applicazioni sui dispositivi cellulari senza prima aver concordato l'operazione con i Sistemi informativi;
- installare sulle postazioni di lavoro in ufficio programmi di sincronizzazione/backup dei dati contenuti sui dispositivi cellulari senza la preventiva autorizzazione dei Sistemi informativi;
- apportare interventi sulle configurazioni del dispositivo o sulle condizioni di servizio che possano incidere in maniera rilevante sui consumi senza averlo concordato con i Sistemi Informativi.

Al momento della restituzione dei dispositivi, il personale assegnatario dovrà cancellare i dati contenuti sul cellulare (es. Rubrica telefonica, SMS, contenuti multimediali, ecc). Qualora il dispositivo restituito contenga dati personali, questi verranno cancellati.

Per quanto riguarda gli aspetti concernenti i consumi telefonici e il traffico internet generati sui dispositivi si rimanda alle norme comunicate in fase di assegnazione del bene.

Attività dell'Amministratore di Sistema

S'intende per Amministratore di Sistema qualsiasi soggetto le cui funzioni di gestione ed amministrazione di sistemi informatizzati rendano tecnicamente possibile l'accesso, anche fortuito, a dati personali. In questa definizione rientrano pertanto le funzioni tecnicamente definite di amministratore di sistema (*system administrator*), amministratore di base di dati (*database administrator*) o amministratore di rete (*network administrator*).

La designazione quale Amministratore di Sistema deve essere conforme alle normative sulla protezione dei dati personali e ai provvedimenti relativi emanati dal Garante della Privacy sull'argomento.

La designazione deve inoltre recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Fra le funzioni dell'Amministratore di sistema, sia esso interno all'Ente che esterno, vi possono essere:

- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare e/o coordinare interventi di manutenzione hardware per i dispositivi di competenza;
- effettuare interventi di manutenzione software su sistemi operativi e applicativi di competenza;
- coordinare e sovrintendere l'operato di eventuali tecnici esterni all'Amministrazione (nel caso di Amministratore interno);
- coordinare a livello operativo la gestione e la distribuzione dei profili di accesso e delle password degli utenti del sistema e/o dei sottosistemi di competenza nel rispetto delle normative relative alla protezione dei dati personali;
- gestire le password di amministrazione di sistema o dei sottosistemi di competenza;
- collaborare con i responsabili del trattamento dei dati personali per l'organizzazione delle politiche di sicurezza;
- informare il responsabile dei Sistemi Informativi e/o il Titolare sulle non corrispondenze con le norme di sicurezza e su eventi di sicurezza rilevanti.

Osservanza delle regole sulla privacy

Oltre a quanto indicato nel presente documento, è obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza ai sensi dell'allegato tecnico B al Decreto Legislativo 196/2003 e normative successive.

Osservanza del presente disciplinare

La finalità del presente documento è quella di regolamentare l'utilizzo delle risorse informatiche comunali, al fine di garantire l'adeguata riservatezza, integrità e disponibilità dei dati gestiti dall'Ente.

A tali scopi, in caso si riscontrino delle criticità che possano ledere la sicurezza del sistema informativo, l'Ente potrà verificare che l'utilizzo delle risorse informatiche concesse in dotazione agli utenti sia conforme alle indicazioni riportate nel presente disciplinare. Qualora l'utilizzo delle risorse informatiche possa in qualche maniera rivelare dati personali relativi agli utilizzatori, la rilevazione verrà effettuata secondo i principi di pertinenza e non eccedenza del trattamento dei dati rispetto alle finalità di sicurezza per cui tali dati sono trattati. L'ufficio CED si riserva di rimuovere tutti i dati presenti sulle postazioni di lavoro riconsegnate.

Il mancato rispetto delle regole e delle misure di sicurezza elencate nel presente documento implica la responsabilità personale dell'utente.

I fatti negativi e/o pregiudizievoli espongono il trasgressore oltre che all'apertura di specifico procedimento disciplinare, alle sanzioni previste dalla legge.

Entrata in vigore

Il presente documento entrerà in vigore decorsi 15 giorni dalla data di pubblicazione all'albo pretorio online della relativa deliberazione di adozione.

Gli uffici competenti provvederanno a consegnare al momento dell'assunzione ad ogni utente copia del presente disciplinare.