COMUNE DI PISA

Disciplinare per l'utilizzo delle apparecchiature informatiche e relativi servizi applicativi e di rete.

Premessa

L'architettura di rete di comunicazione dati del Comune di Pisa (d'ora in poi indicato come Comune) è costituita dall'insieme di tutte le reti dei diversi palazzi comunali ubicate sul territorio comunale pisano ed interconnesse tra loro.
Tramite la rete è possibile accedere alle risorse condivise e a diversi ambienti applicativi residenti su appositi server di rete (anche situati in ambienti cloud), oltre a consentire l'uso di servizi di rete quali: l'accesso al sito di rete civica del Comune, ad internet, alla posta elettronica, alla intranet comunale, ai servizi della Rete Telematica Regionale Toscana, ad altri servizi della Pubblicazione Amministrazione su portali web specializzati.

L'utilizzo delle risorse informatiche messe a disposizione del personale deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti richiesti nello svolgimento di ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, in qualsiasi forma esso sia.
Questo è ancora più importante quando l'accesso a queste risorse e servizi presenti sulla rete implica il trattamento di dati personali.
La protezione dei dati e delle informazioni nel loro complesso è condizione necessaria per garantire il rispetto dei requisiti di sicurezza che la normativa vigente impone a tutti i soggetti che, a vario titolo, effettuano il trattamento di dati personali.
Il datore di lavoro, inoltre, deve assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori.

Scopo del documento

Questo documento ha lo scopo di individuare regole comuni per tutelare i reciproci diritti e doveri di lavoratori e datore di lavoro attraverso la definizione:

- delle norme di corretto uso delle postazioni e dei servizi di rete messi a disposizione dal Comune ai dipendenti comunali e di tutti gli altri soggetti che a vario titolo prestano servizi o attività per conto e nelle strutture del Comune
- del diritto dell'Amministrazione di verificare che non si attuino usi impropri;
- del diritto del lavoratore (e dei terzi) ad una sfera di riservatezza anche nelle relazioni lavorative.

Le prescrizioni contenute si aggiungono e integrano le norme già previste dal contratto collettivo nazionale di lavoro nonché dalla normativa in materia di protezione dei dati personali.

Contesto normativo[1]

I principi applicati nella stesura del disciplinare sono tratti dal quadro normativo nazionale che segue:

- Art. 15 Costituzione[2]
- Norme del codice civile: artt. 2087, 2104, 2105 e 2106[3]
- L. 20 maggio 1970, n. 300 (Statuto dei lavoratori) - artt. 4 e 8[4]
- Allegato XXXIV, par. 3, D.Lgs. 9-4-2008 n. 81 e succ. mod. in materia di tutela della salute e della sicurezza nei luoghi di lavoro[5]
- REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016
- Art. 49, D.Lgs. 7 marzo 2005 n. 82, Codice dell'amministrazione digitale, "Segretezza della corrispondenza trasmessa per via telematica"[6]

---

[1] Se i riferimenti sono "brevi" sono riportati in nota altrimenti si riporta il relativo file .pdf nell'area intranet PRIVACY

[2] Art.15 –

La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.
La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

[3] Art. 2087 - L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.

Art. 2104 - Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale.
Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.

Art. 2105 - Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio.

Art. 2106 - L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione

[4] Art. 4 - Impianti audiovisivi. –

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.
2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

Art. 8 Divieto di indagini sulle opinioni. –

È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

[5] Allegato XXXIV paragrafo 3. Interfaccia elaboratore/uomo –

All'atto dell'elaborazione, della scelta, dell'acquisto del software, o allorché questo venga modificato, come anche nel definire le mansioni che implicano l'utilizzazione di unità videoterminali, il datore di lavoro terrà conto dei seguenti fattori: a) il software deve essere adeguato alla mansione da svolgere; b) il software deve essere di facile uso adeguato al livello di conoscenza e di esperienza dell'utilizzatore. Inoltre nessun dispositivo di controllo quantitativo o qualitativo può essere utilizzato all'insaputa dei lavoratori; c) il software deve essere strutturato in modo tale da fornire ai lavoratori indicazioni comprensibili sul corretto svolgimento dell'attività; d) i sistemi devono fornire l'informazione di un formato e ad un ritmo adeguato agli operatori; e) i principi dell'ergonomia devono essere applicati in particolare all'elaborazione dell'informazione da parte dell'uomo.

[6] Art. 49. Segretezza della corrispondenza trasmessa per via telematica

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.
2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

• "Linee guida del Garante per posta elettronica e Internet", emanate con deliberazione 1 marzo 2007 n. 13
• Provvedimento del Garante per la protezione dei dati personali del 27.11.2008 "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" così come modificato con successivo provvedimento del 25.6.2009
• Direttiva n.2/09 del Ministro per la Pubblica Amministrazione e l'Innovazione riguardante "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro"
• CIRCOLARE 18 aprile 2017 , n. 2/2017 dell'Agenzia per l'Italia Digitale (AGID) Misure minime di sicurezza ICT per le pubbliche amministrazioni.

Vanno altresì considerati i seguenti atti del Comune di Pisa:
• Regolamento per l'accesso ai documenti e alle informazioni e per la tutela dei dati Personali del Comune di Pisa approvato con deliberazione C.C. 1/2006
• La circolare del Segretario generale n. 26738/2009 a seguito della Direttiva n.2/09 del Ministro per la Pubblica Amministrazione e l'Innovazione prima citata
• il Codice di comportamento dei dipendenti del Comune di Pisa approvato con deliberazione di Giunta Comunale n° 96 del 15.07.2014, ed in particolare l'art. 13, commi 1, 3 e 6[7]
• Delibera di G.C. n. 164 del 27.9.2016 con la quale è stato approvato il piano triennale per la razionalizzazione dell'utilizzo delle dotazioni strumentali informatiche e di telefonia mobile per gli uffici comunali,
• la determinazione n. 1039 del 23.8.2017 relativa all'aggiornamento delle attribuzioni delle funzioni di amministratore di sistema.

Definizioni

Amministratore di sistema
Come delineato dal Provvedimento del Garante per la protezione dei dati personali del 27.11.2008 "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" così come modificato con successivo provvedimento del 25.6.2009
"Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.
Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

[7] Art. 13 Gestione delle risorse
1. Ai fini del presente regolamento, per gestione delle risorse si intende la disponibilità, giuridica o materiale, di qualsiasi bene, strumento o utilità appartenente al Comune di Pisa.
3. Il dipendente utilizza il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione.
6. In ogni caso, non può essere autorizzato l'utilizzo, da parte di soggetti estranei all'organizzazione dell'ente, di denominazioni e intestazioni di uffici comunali nonché di indirizzi di posta elettronica e certificata propri dell'ente

Attività tecniche quali il salvataggio dei dati (backup/recovery), l´organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un´effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l´amministratore non consulti "in chiaro" le informazioni medesime."

Dati personali e trattamento di dati personali

Dal REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016:

«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

Uso degli apparati

Il Comune è proprietario degli strumenti e delle apparecchiature informatiche assegnati ai dipendenti o collaboratori. Tali strumenti sono affidati ai medesimi a condizione che vengano custoditi con cura, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone, per scopi non consentiti.

Dette risorse informatiche deve essere utilizzate unicamente per perseguire gli scopi lavorativi.

Le postazioni di lavoro sono preventivamente individuate ed assegnate personalmente a ciascun utente; il collegamento in rete da una postazione diversa da quella assegnata avviene solo in caso di esigenze di servizio preventivamente autorizzate dal dirigente/funzionario competente.

L'utente generico non può modificare alcuna impostazione di accesso alla rete della propria postazione di lavoro (modifica dell'indirizzo IP, del nome del computer, del gruppo di lavoro, ecc.); queste attività sono riservate all'utente "amministratore".

Per evitare accessi non desiderati alle postazioni, ogni utente deve impostare una password di accesso al dominio.

Il personal computer deve essere spento ogni sera prima di lasciare gli uffici se non richiesto diversamente dall'Amministratore di Sistema. In caso di assenza dall'ufficio l'elaboratore, se non viene spento, deve essere lasciato con attivo lo screen saver con password abilitata.

L'utente non può far lavorare sulla propria macchina un altro soggetto che non lavori per conto del Comune, eccetto i tecnici delle ditte addette alla manutenzione dell'hardware o del software.

Nel caso di personal computer assegnati a più di un utente (es. postazioni di front-office), ognuno degli utenti abilitati all'accesso userà per l'accesso al dominio la propria password (eccetto i casi dove una password generica sia autorizzato dall'Amministratore di Sistema).

E' responsabilità del funzionario/dirigente verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato, compreso l'utilizzo da parte di terzi di punti rete in luoghi non presidiati.

Non è consentito, neppure per necessità attinenti all'attività lavorativa e salvo autorizzazione dell'Amministratore del sistema, il collegamento ai personal computer affidati al lavoratore, alla rete comunale e più in generale al sistema informatico comunale di dispositivi (come ad esempio telefoni cellulari, palmari, modem, dispositivi di memorizzazione, lettori musicali, stampanti, ecc .), di apparati (come ad esempio modem, apparati di rete o wireless) o di personal computer che non siano di proprietà dell' Ente e che non siano quelli affidati al lavoratore stesso.

Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo.

Nel caso ci sia la necessità di far collegare ad internet un personal computer di una persona "ospite" degli uffici comunali, questi dovrà utilizzare la rete wifi dove presente. L'eventuale collegamento in rete locale dovrà essere concordato con l'Amministratore di Sistema.

Ambiente software di un personal computer

In ogni postazione client sono presenti un insieme minimo di applicativi, per i quali è garantito il supporto tecnico:
- il pacchetto Office (nelle sue numerose versioni);
- i browser per la navigazione nel Web;
- l'ambiente per la gestione della posta elettronica;
- l'antivirus Karpersky
- gli applicativi comunali client-server;
- gli applicativi specifici per ciascun settore;
- altri programmi di utilità di sistema.

L'antivirus Karpersky offre la protezione totale contro i virus. All'accensione del computer viene automaticamente aggiornata la definizione dei virus.
In modo automatico l'antivirus Karsperky eseguirà scansioni complete del sistema con cadenza settimanale.
E' assolutamente vietato installare sul proprio personal computer un antivirus diverso da quello scelto per tutti i computers dell'Ente (salvo quei casi autorizzati dall'Amministratore di Sistema per specifiche esigenze tecniche).

Non è consentito installare autonomamente programmi di qualunque tipo oltre quelli sopra indicati. Nel caso vi sia la richiesta da parte del Funzionario/Dirigente responsabile del settore cui è stato fornito il personal computer, il personale del Sistema Informativo, verificata la compatibilità dello stesso con gli altri programmi software in uso all'ente, provvederà ad installarlo o farlo installare dalla ditta che gestisce la manutenzione dei posti di lavoro.

Servizi di rete ed attività non ammesse

Tutti coloro i quali lavorano per il Comune e all'interno della struttura di rete comunale hanno diritto di accesso ai servizi di rete offerti dal Comune.
Per la condivisione sicura di documenti o di interi ambienti di lavoro sono messi a disposizione degli utenti:
-l'ambiente intranet comunale
-spazi condivisi situati su strutture centrali di server.

Gli utenti non possono accedere ai servizi di rete mascherando la propria identità.
Inoltre non possono impersonare altri individui o usare false identità.

Inoltre non devono assolutamente utilizzare applicativi per l'intercettazione del traffico di rete.

Non sono ammesse le seguenti attività sia all'interno della rete locale del Comune che tramite l'utilizzo dei servizi di rete, intranet, internet e posta elettronica:
- violare la privacy degli altri utenti o l'integrità di dati personali;
- utilizzare servizi o risorse in un modo che danneggi o molesti altre persone o che attenti alla dignità umana;
- visionare, creare o trasmettere qualunque immagine, dato o altro materiale offensivo, osceno o indecente;
- creare o trasmettere materiale finalizzato allo scopo di arrecare disturbi o produrre ingiustificate preoccupazioni;
- creare o trasmettere materiale diffamatorio;
- scaricare o trasmettere materiale che violi i diritti d'autore;
- usare le risorse informatiche per scopi diversi da quelli lavorativi;
- sprecare risorse di rete, dei calcolatori connessi o risorse del personale addetto al loro funzionamento;
- danneggiare, distruggere o cercare di accedere senza autorizzazione a dati di altri utenti;
- interferire nel lavoro di altri utenti;
- accedere alla rete comunale con apparecchiature o software che interferiscono con il corretto funzionamento della rete stessa o di altre reti ad essa collegate;
- svolgere sulla rete comunale ogni altra attività vietata dalla legge dello Stato, dalle normative vigenti nei Paesi ospitanti i servizi di rete ai quali si accede e dalla normativa Internazionale in materia;
- danneggiare i sistemi di rete comunale o di altre organizzazioni;
- fornire a soggetti non ammessi all'accesso alla rete del Comune di Pisa il servizio di connettività di rete o altri servizi che la includono, quali la fornitura di servizi di housing, di hosting e simili;
- permettere il transito di dati e/o informazioni sulla rete comunale tra due soggetti entrambi non ammessi all'accesso alla rete comunale (third party routing);

Sicurezza

Ogni utente deve contribuire alla sicurezza complessiva del sistema. In particolare:
- deve assicurare la protezione delle proprie login/password e dei propri files;
- non deve salvare su file "in chiaro" la/e password assegnata/e;
- deve segnalare agli amministratori di sistema ogni tentativo di violazione delle proprie login/password e le eventuali anomalie constatate;
- si impegna ad adoperare password non banali e a tenerle segrete; negli ambienti dove l'aggiornamento della password non sia effettuato in modo automatica, si impegna cambiarla periodicamente (anche su motivata richiesta degli amministratori di sistema);
- si impegna a non sfruttare eventuali buchi di sicurezza o le anomalie che riguardano il funzionamento delle risorse informatiche; tali vulnerabilità devono essere segnalate tempestivamente agli amministratori di sistema in forma riservata.

Utilizzo dei dati e del software

I dati e le informazioni sono beni comunali. I dati e le informazioni detenute su apparecchiature comunali o altri supporti sono utilizzati dal personale, anche fuori dagli uffici comunali, ai soli fini lavorativi. Nessun dato del Comune di Pisa o personale

può essere trattato o memorizzato su dispositivi di qualsiasi tipologia, non finalizzati all'attività lavorativa.
Per il salvataggio dei dati, l'uso delle unità di rete e dei supporti di memorizzazione, il lavoratore si deve attenere alle seguenti regole:
- le unità di rete sono aree di condivisione di informazioni strettamente lavorative 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;
- è in generale da evitare il salvataggio di dati personali riferiti all'attività lavorativa sui singoli personal computer o su altri strumenti informatici o elettronici; i dati personali devono essere salvati di norma sulle unità di rete predisposte dall'amministratore di sistema;
- qualora, per motivi di necessità, sia necessario conservare dati personali inerenti l attività lavorativa sui singoli personal computer o su altri strumenti informatici o elettronici, i lavoratori hanno l'obbligo di provvedere con cadenza almeno settimanale ad effettuare una copia di detti dati su supporti rimovibili;
-l'utilizzo e la conservazione di detti supporti rimovibili devono essere effettuati da parte dei lavoratori in modo da non permettere l'accesso agli stessi da parte di terzi;
-al termine del trattamento i supporti rimovibili contenenti dati personali dovranno essere cancellati ove possibile oppure distrutti o resi inutilizzabili al fine di rendere non intelligibili e tecnicamente non ricostruibili le informazioni in essi contenute.

Attività dell'amministratore di sistema

Per i soli fini di amministrazione, gestione e manutenzione del sistema informatico, l'amministratore di sistema ha la possibilità di utilizzare oppure di connettersi da remoto alle risorse disponibili su ciascun personal computer in dotazione ai lavoratori e più in generale a ciascun dispositivo connesso alla infrastruttura informatica.
In particolare per gli scopi suddetti sono utilizzati alcuni software che permettono all'amministratore di sistema di vedere in tempo reale le attività svolte dal lavoratore all'interno della propria sessione di lavoro ed eventualmente di intervenire attivamente. L'attivazione di tale funzionalità può essere richiesta solamente da parte degli amministratori di sistema e solo quando strettamente necessario per poter svolgere l'attività di assistenza tecnica informatica ed è sottoposta ad un preventivo e contestuale consenso da parte del lavoratore a cui vengono indicati anche il perdurare e il successivo termine dell'attività stessa.
In nessun caso è possibile l'ingresso in una sessione di lavoro da parte di un amministratore di sistema senza che prima il lavoratore ne abbia fornito il consenso.
L'amministratore di sistema provvede ad implementare, configurare e gestire uno o più software sui server di competenza e le relative postazioni di lavoro.
In previsione della possibilità che in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba accedere a dati accessibili solamente con le credenziali di autenticazione di un lavoratore, ciascun lavoratore può delegare un altro lavoratore a rendere disponibili al dirigente/funzionario responsabile i dati necessari per lo svolgimento dell'attività lavorativa. Questa delega può avvenire anche su richiesta del dirigente/funzionario responsabile.
Qualora tale delega non sia stata espressa, le predette operazioni sono effettuate dall' amministratore di sistema, sempre su richiesta del dirigente/funzionario responsabile.
A cura del dirigente/funzionario responsabile, di tale attività viene redatto apposito verbale e viene informato il lavoratore tramite posta elettronica oppure, qualora non possibile, mediante comunicazione scritta.

Per i soli fini di amministrazione, gestione e manutenzione del sistema informatico, l'amministratore di sistema ha la possibilità di accedere a tutti i dati presenti nel sistema informatico stesso compresi tutti i file conservati nei dischi di rete, nei dischi dei personal computer e negli altri dispositivi connessi.
L'amministratore di sistema ha la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente documento, dandone contestuale comunicazione al lavoratore interessato, ove ciò sia possibile.
All'amministratore di sistema e più in generale al personale del Sistema Informativo è consentito l'uso di supporti rimovibili per le operazioni di backup dei dati. Le modalità di realizzazione, utilizzo, conservazione e distruzione dei dati di backup sono specificate nelle lettere di incarico per gli amministratori di sistema.

Utilizzo della posta elettronica

Ogni utente e/o Unità Operativa e/o Direzione dispone di una propria casella di posta elettronica.
Nel caso di casella di posta elettronica assegnata ad Unità Operativa o a Direzione, il Funzionario/Dirigente identifica il dipendente responsabile della gestione della stessa.

Per facilitare la lettura della posta da parte del destinatario è opportuno definire una propria firma da apporre automaticamente ai messaggi (o signature file). Questa dovrebbe essere breve e significativa.

Il servizio fornito dal Comune all'utente è il seguente:
-attivazione di un servizio di posta elettronica con casella postale personale ad accesso riservato e controllato da password
-iscrizione alle mailing list presenti in Comune.

L'utente si impegna a conservare la password assegnata e a non consentire a terzi l'uso del servizio, nonché a notificare immediatamente al Sistema Informativo l'eventuale perdita di riservatezza della password.

In caso di assenza dal lavoro dell'utente per brevi periodi, è a disposizione un apposita funzionalità di sistema che consente di inviare automaticamente un messaggio di risposta che avvisa il mittente dell'assenza del destinatario, individuando eventualmente altre modalità di contatto con la struttura di appartenenza.

In caso di assenza non programmata o dove non sia stata attivata la procedura di cui sopra, l'utente può delegare un altro dipendente dell'ufficio a verificare il contenuto dei messaggi e ad inoltrare al funzionario/dirigente competente quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Al fine di un utilizzo efficiente della rete:
- è necessario consultare la posta elettronica almeno una volta al giorno per poter attingere alle eventuali comunicazioni del Comune e per liberare spazio all'interno della propria mailbox;
- è proibita la propagazione delle "chain letters" (ovvero le cosiddette "Catene di S.Antonio", messaggi di posta elettronica contenenti informazioni che richiedono la diffusione ad altri), in quanto congestionano la rete;
- è proibita la diffusione dei "virus hoaxes" (comunicazioni riguardanti la presenza di nuovi virus, in realtà inesistenti, con la richiesta di diffusione ad altri). In caso di ricezione di tali informazioni, è necessario rivolgersi al Sistema Informativo;

- è proibito lo "spamming" (messaggi pubblicitari o comunicazioni che non siano sollecitati in modo esplicito) e il "bombing" (invio ripetuto di messaggi verso un indirizzo di posta elettronica allo scopo di bloccarne l'accesso);
- è proibito inviare grosse moli di dati: indicare (ove possibile) la locazione dei dati nel messaggio, rendendoli disponibili per il prelievo o la consultazione sulla rete.

Il Comune, onde garantire un elevato livello di sicurezza del sistema informativo si è dotato, al solo scopo di filtraggio, di uno strumento che regolamenti l'utilizzo della posta elettronica.
In particolare il Comune utilizza filtri antivirus (ovvero finalizzati ad impedire la ricezione di allegati potenzialmente pericolosi) e filtri antispam (ossia, finalizzati a filtrare la posta elettronica non desiderata).
Con riferimento alla posta elettronica, il Comune utilizza filtri finalizzati a limitare i messaggi con le seguenti caratteristiche:
- dimensioni: sono bloccate le e-mail o i singoli allegati che superano la dimensione di 25 MB;
- estensione dei files allegati: sono bloccati gli allegati alle e-mail con estensione ritenuta "pericolosa" dal sistema (es. file eseguibili)

Mailing list

Nella rete locale sono presenti le seguenti mailing list:
-"Dipendenti" mailing-list "istituzionale" che raggruppa tutti i dipendenti comunali
-"Dirigenti" mailing-list "istituzionale" che raggruppa tutti i dirigenti comunali
-"Pos-Org" mailing-list "istituzionale" che raggruppa tutti le posizioni organizzative comunali
-altre mailing-list "non istituzionali" create per gruppi di dipendenti comunali diversi dai precedenti, su loro espressa richiesta, e comunque inerenti problematiche connesse al loro rapporto di lavoro all'interno del Comune di Pisa

Ogni mailing-list ha un moderatore che ha il compito di ricevere la singola mail indirizzata alla propria mailing-list e deciderne o meno la pubblicazione.

Nel caso delle mailing-list "istituzionali":
-il moderatore è un dipendente del Sistema Informativo
-in questo caso sono pubblicate tutte e sole le mail che riguardino avvisi, comunicazioni, circolari o documenti di interesse dei componenti del gruppo in quanto dipendenti, o dirigenti o posizioni organizzative.

Nel caso delle mailing-list "non istituzionali":
-il moderatore è un dipendente appartenente al gruppo designato dallo stesso
-in questo caso il criterio di pubblicazione deriva dalla regole che il gruppo stesso si darà.

Utilizzo di Internet

Ogni utente è abilitato alla navigazione in Internet in quanto quest'ultimo costituisce uno strumento necessario allo svolgimento della propria attività lavorativa.
E' proibita la navigazione in internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.

L'utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di accesso a internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

All’utente non è consentito servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione al diritto di autore od altri diritti tutelati dalla normativa vigente.

E' tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.
E' vietata la partecipazione a forum non professionali, l'utilizzo di chat lines (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames), se non attinenti l'attività lavorativa svolta.
Il Sistema Informativo si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.

Uso sistemi di monitoraggio

Il Comune di Pisa rispetta le leggi vigenti e i provvedimenti che vietano il trattamento effettuato mediante sistemi hardware e software preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire sistematicamente l'attività dei lavoratori.

Nel contesto lavorativo del Comune di Pisa non si effettuano ad esempio:
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- analisi occulta di computer affidati in uso.

L’attività di eventuale controllo, lecitamente svolta dal Comune di Pisa ai sensi del presente disciplinare, si attiene in ogni caso ai seguenti fondamentali principi:

- Principio di necessità, di pertinenza e di non eccedenza
I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite, osservando altresì il principio di pertinenza e non eccedenza. Il Comune raccoglie e tratta i dati nella misura meno invasiva possibile; le eventuali attività di controllo sono svolte solo da soggetti preposti e sono mirate sull'area individuata come di rischio.

-Principio di finalità e di correttezza
I trattamenti sono effettuati per finalità determinate, esplicite e legittime. Le finalità perseguite dal Comune di Pisa riguardano o possono riguardare, caso per caso:
- sicurezza sul lavoro
- sicurezza dei sistemi e relativa risoluzione di problemi tecnici
- esigenze di organizzazione
- esigenze di produzione
- rispetto di obblighi legali
- tutela del Comune.

I servizi di rete e i software applicativi sono monitorati tramite sistemi di Log che consentono la registrazione degli accessi e degli eventi (operazioni) nei limiti previsti dalla normativa.
Con i file di Log si possono registrare eventi ai vari livelli di astrazione del sistema informatico:
•log del sistema operativo atto ad identificare ingressi, anomalie ed errori;
•log del Data Base atti ad identificare ingressi, anomalie ed errori;
•log dei sistemi di rete (firewall e router) atti ad identificare ingressi, anomalie ed errori;

•log delle applicazioni software utilizzate atti ad identificare ingressi, principali attività svolte dagli utenti, sequenze del processo, accessi ai dati.
L'intero processo di creazione del file di log è svolto dal sistema informatico in forma totalmente automatica.
I file di log non sono modificabili o eliminabili da parte degli utenti che usano il sistema.
Gli Amministratori di sistema si riservano il diritto di accedere ai dati sugli ingressi ai sistemi:

- nel caso in cui sia necessario identificare o diagnosticare problemi o vulnerabilità presenti nel sistema al fine di preservarne l'integrità;
- su richiesta delle autorità giudiziarie;
- quando abbiano ragionevoli dubbi sull'avvenuta violazione delle presenti norme e ritengano che il monitoraggio dei dati possa essere d'aiuto nell'individuazione dei responsabili.

Procedure in caso di cessazione del rapporto lavorativo

In caso di cessazione del rapporto lavorativo, si applicano le seguenti procedure:

Documenti memorizzati sui sistemi comunali
I documenti informatici prodotti dal lavoratore nell'esercizio dell'attività professionale a favore del Comune di Pisa, inseriti nei sistemi informativi comunali restano nella piena ed esclusiva disponibilità del Comune. Salvo esplicita autorizzazione scritta da parte di Comune di Pisa il lavoratore non può formare o ottenere copia dei predetti documenti né farne alcun uso dopo la cessazione del rapporto di lavoro.

E-mail
Le e-mail relative all' account di posta elettronica comunale nominativa restano nella piena disponibilità del Comune. Trattandosi tuttavia di corrispondenza formatasi in relazione ad un account e-mail nominativo, il lavoratore può chiedere copia delle e-mail e conservarle a fini esclusivamente personali, con esclusione di ogni diverso utilizzo dopo la cessazione del rapporto di lavoro.

File di log
I log, ossia le tracce elettroniche relative all'utilizzo di strumenti elettronici da parte del lavoratore, tracciati dai sistemi comunali sono conservati per il tempo strettamente necessario alle finalità perseguite caso per caso.

Rispetto delle presenti norme
Ogni utente della rete locale del Comune di Pisa è tenuto a rispettare le norme sopra riportate.
Salvo che il fatto costituisca più grave reato, nel caso di violazione delle presenti norme da parte del personale dipendente si procederà ad avvertire il dirigente competente e la Direzione Personale per l'eventuale attivazione di un procedimento disciplinare secondo la normativa vigente in merito.