SIA – Sistemi Informativi Associati

DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI E SERVIZI INFORMATICI PER GLI ENTI IN GESTIONE ASSOCIATA DEL NUOVO CIRCONDARIO IMOLESE

(approvato con delibera di Giunta n. 38 del 10/12/2014)

Premessa

Il presente disciplinare costituisce atto a validità in ambito territoriale per tutti gli strumenti informatici gestiti dal SIA – Sistemi Informativi Associati del Nuovo Circondario Imolese (delibera di assemblea del Nuovo Circondario Imolese n. 17 del 27/09/2012)
Il presente disciplinare costituisce a valenza organizzativa complementare al regolamento sull'ordinamento degli uffici e servizi adottato dagli enti e ha per oggetto i criteri e le modalità di utilizzo e controllo degli strumenti informatici[1], dei servizi di posta elettronica, intranet ed internet, da parte dei propri dipendenti, a tempo determinato o indeterminato, e di tutti i collaboratori (es. personale comandato/distaccato, stagisti, fornitori, tirocinanti), amministratori o comunque soggetti autorizzati che, a vario titolo, svolgono un'attività accedendo al sistema informatico, nel rispetto dei regolamenti comunali per il trattamento dei dati personali e di quanto previsto dal Codice in materia di protezione dei dati personali (approvato con D.lgs. 30/06/2003 n. 196 e successive modificazioni ed integrazioni)

Punto 1 - Principi generali

Gli strumenti informatici forniti al personale dipendente sono utilizzati esclusivamente per lo svolgimento del lavoro assegnato, con modalità e comportamenti adeguati ai compiti ed alle responsabilità dei dipendenti pubblici, rispettando i comuni principi etici e di correttezza e i doveri stabiliti nel Codice di comportamento dei dipendenti della pubblica amministrazione nonché la privacy e la segretezza dei dati trattati secondo le normative vigenti (in special modo al D.Lgs. 196 /2003 e ss.mm.ii., al regolamento sui procedimenti disciplinari del personale e altri regolamenti afferenti all'argomento in oggetto adottati dagli enti del Nuovo Circondario Imolese).
Ciascun dipendente è direttamente responsabile in caso di utilizzo da parte di terzi degli strumenti informatici a lui affidati; deve custodire le proprie credenziali di autenticazione e la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile di servizio, che provvederà ad informare il SIA.

Punto 2 - Modalità di accesso alla rete

Per accedere ai servizi informatici da una postazione di lavoro l'utente deve utilizzare un codice identificativo (id utente) e una parola chiave segreta (password).
Le postazioni di lavoro devono sempre essere consegnate, installate e gestite dal SIA – Sistemi Informativi Associati, siano esse fisse, portatili, in rete o stand alone; è compito dei responsabili e dirigenti dei servizi degli enti circondariali segnalare eventuali irregolarità e trasgressioni al SIA, il quale provvederà alla regolarizzazione delle difformità segnalate. Le postazioni di lavoro vengono assegnate ai vari enti e servizi comunali, i cui responsabili ne attribuiscono l'utilizzo e la custodia al singolo dipendente del servizio stesso; è comunque possibile utilizzare una postazione diversa da quella assegnata utilizzando per l'accesso la coppia 'id utente – password personale'.
Le postazioni al pubblico o di utilizzo generico sono affidate al dirigente del servizio assegnatario o a persona designata dal dirigente stesso.
L'utente deve essere consapevole del fatto che permettere l'accesso col proprio identificativo a terzi (anche colleghi) non autorizzati alla rete comunale consente agli stessi l'utilizzo dei relativi servizi in nome dell'utente titolare nonché l'accesso ai dati cui il medesimo utente è abilitato, anche con

[1] Per strumenti informatici si intendono: personal computer fissi o portatili, videoterminali, stampanti locali o di rete, i prodotti software regolarmente licenziati, palmari, cellulari o altri dispositivi di telecomunicazione le relative periferiche nonché tutta l'infrastruttura logica e fisica che permette l'interconnessione delle postazioni di lavoro al fine di agevolare la trasmissione di dati.

possibilità di gestione degli stessi (ad es. visualizzazione di informazioni riservate, distruzione o modifica dei dati, lettura della propria posta elettronica, uso indebito di servizi ecc..).
Preso atto di tale conseguenza, l'utente deve:

a) custodire con cura la parola chiave personale e, in nessun caso, comunicarla a terzi;
b) non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione; nel caso l'utente abbia necessità di allontanarsi è tenuto a chiudere la sessione o a bloccare la propria stazione di lavoro utilizzando la sequenza di tasti "ctrl-alt-canc" e il tasto "Blocca Computer", o salvaschermo con password, o estrazione dell'hardware USB di autenticazione. E' evidente che lasciare un elaboratore incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
c) non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione ad altra persona se non per motivi tecnici autorizzati dal servizio SIA;
d) mantenere riservata la password. L'utente è personalmente soggetto a responsabilità civili e penali, in caso di abusi o incidenti di sicurezza, nel caso divulghi la password, ovvero renda disponibile ad altri l'accesso.

I dati, documenti o files gestiti dagli incaricati in relazione alle mansioni attribuite, nella loro forma definitiva, devono essere ricoverati sui server di sistema: solo in modo transitorio possono essere copiati sul disco fisso della postazione di lavoro ma devono a fine trattamento essere trasferiti sui server mediante le procedure, il sistema documentale o le cartelle condivise presenti nel sistema informativo circondariale. Si possono effettuare copie di dati su supporti rimovibili (es. dischetti CD, DVD, chiavi usb), o su sistemi di memorizzazione remoti (es. cloud, backup remoti), solo se autorizzati da parte del SIA, del proprio dirigente o responsabile di servizio. Qualora, secondo principio di necessità, sulle copie venissero trasferiti dati personali, il trattamento dovrà avvenire con le modalità previste dalla legge in materia di riservatezza e protezione dei dati personali; al termine del trattamento sarà cura del dipendente distruggere o rendere inutilizzabili i supporti rimovibili o comunque rendere le informazioni non intelligibili e in alcun modo ricostruibili.
Lo spazio di memoria nei server di sistema, a cura dello stesso personale che ne usufruisce, deve essere utilizzato per il salvataggio di file e dati in forma non ridondante ed esclusivamente per motivi di lavoro: nel rispetto dei principi di razionalizzazione degli strumenti informatici, il personale del servizio SIA potrà effettuare controlli e segnalare l'eventuale presenza di tipologie di file non pertinenti, chiedendone o, in caso di necessità, eseguendone la rimozione.
Tranne nei casi segnalati dal SIA per i lavori di manutenzione al sistema, al termine del servizio ciascun operatore deve spegnere il PC: lo spegnimento è importante al fine di evitare sprechi energetici ed inutile usura del PC

In caso di assenza del dipendente, e contingente necessità indispensabile e indifferibile di intervenire per esclusive necessità d'ufficio o di sicurezza del sistema, il dirigente o il responsabile del servizio potranno richiedere la disponibilità dei dati (protetti dalle credenziali del dipendente) e degli strumenti informatici al dirigente o al responsabile del servizio SIA. Il prima possibile, o comunque al suo ritorno, il dipendente verrà informato tempestivamente, dallo stesso richiedente, sull'intervento effettuato.

Punto 3 - Norme di comportamento

Il personale deve custodire la propria strumentazione in modo appropriato e diligente, segnalando tempestivamente ogni danneggiamento, furto o smarrimento al proprio responsabile di servizio e al Servizio SIA.
Le attività di gestione e manutenzione dei Personal Computer dell'Ente fanno capo al Servizio SIA e non è permesso agli utenti di intervenire personalmente, se non espressamente autorizzati dal medesimo Servizio, sulle apparecchiature informatiche.

In particolare:

1. è tassativamente proibito installare programmi software non autorizzati, anche se legali, (es: programmi salvaschermo, software peer-to-peer o altri software freeware o scaricati da internet) e/o modificare la configurazione hardware e software delle propria postazione di lavoro se non autorizzati dal personale del Servizio SIA. Qualora venissero trovati programmi non autorizzati sulle stazioni di lavoro questi potranno essere disinstallati dal personale tecnico addetto alla manutenzione dei Personal Computer (anche senza preavviso se ritenuti pericolosi per la sicurezza del sistema o dei dati);
2. le unità di rete definite nel sistema informativo comunale (lettera seguita da due punti, es. 'G:') e le cartelle di rete condivise sono aree di condivisione di informazioni relative all'attività lavorativa e non possono essere utilizzate per il salvataggio di file non pertinenti alla specifica attività o non istituzionali. Su queste unità vengono svolte attività di amministrazione e backup da parte dell'amministratore di sistema che potrà procedere alla rimozione senza preavviso di file o applicazioni ritenute pericolose per la sicurezza del sistema o non inerenti all'attività lavorativa;
3. sulle unità di memorizzazione della postazione (es. 'C:') non vengono svolte attività di backup; tutti i dati relativi alla propria attività lavorativa di cui si voglia salvaguardare la sicurezza vanno memorizzati nelle unità di rete predisposte dal servizio SIA;
4. sono proibite le violazioni della privacy così come sancito dal D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" e ss.mm.ii. contenente standard e regole che disciplinano il trattamento di dati personali, sensibili o giudiziari;
5. gli utenti devono rispettare diritti d'autore, copyright e licenze d'uso di software, materiali audiovisivi, documenti ed ogni altra informazione digitale protetta a norma di legge;
6. .gli utenti sono tenuti ad osservare le disposizioni di cui al presente ed eventuali direttive del servizio SIA volte a garantire il corretto funzionamento delle procedure di sicurezza e conservazione dei dati;
7. gli utenti sono obbligati a segnalare immediatamente al SIA ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza;
8. gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive del SIA divulgate tramite intranet ed e-mail.

Non è inoltre consentito:

I. usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente disciplinare e dalle istruzioni del Dirigente/Responsabile del Servizio;
II. utilizzare la rete per scopi incompatibili con l'attività istituzionale;
III. utilizzare una password a cui non si è autorizzati e violare la riservatezza di altri utenti o di terzi. Qualsiasi accesso alla posta elettronica di altri soggetti senza autorizzazione od al di fuori di una specifica attività di controllo, anche da parte di superiori gerarchici o di addetti al SIA costituisce"Accesso abusivo a un sistema informatico o telematico" e come tale è punito dal codice penale art.615-ter e costituisce comportamento rilevante dal punto di vista disciplinare;
IV. divulgare informazioni tecniche relative alla struttura informatica comunale che possano pregiudicare la sicurezza della stessa;
V. utilizzare gli strumenti informatici comunali al fine di custodire, far circolare o promuovere materiale pubblicitario personale o codice maligno (spam, virus, trojan horses, programmi pirata o altre porzioni di codice maligno e/o altro materiale non autorizzato);
VI. utilizzare la strumentazione informatica, per la realizzazione, redazione, memorizzazione e spedizione di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione, appartenenza sindacale e politica;

VII. installare o connettere alla rete dei dispositivi o delle periferiche proprie e di persone esterne senza autorizzazione del servizio SIA;
VIII. scaricare da internet o da supporto magnetico proveniente dall'esterno file di dubbia provenienza e sicurezza senza farli sottoporre a opportuno controllo;
IX. l'utilizzo degli strumenti informatici al di fuori dell'orario di servizio senza preventiva autorizzazione del proprio responsabile o del servizio SIA.

Il personale del servizio SIA può, nel rispetto delle normative previste dal D.Lgs. 196/03 e dell'articolo 615-ter c.p., per fini di sicurezza, diagnostici e tecnici, verificare il corretto utilizzo della postazione di lavoro dell'utente e l'osservanza delle regole qui descritte. Tali verifiche potranno essere effettuate anche attraverso sistemi di connessione remota previo avviso all'utente, eccezion fatta per i casi in cui l'utente non presidi da postazione in cui sussista una minaccia alla sicurezza del sistema informativo e dei dati in esso contenuti.
Su indicazione del dirigente competente, potranno essere effettuati controlli di conformità alla legge, anche saltuari o occasionali, precisando le ragioni legittime, specifiche e non generiche della richiesta. Analoghi controlli potranno essere consentiti all'autorità giudiziaria o per l'esercizio di un diritto in sede giudiziaria.

3.1 -Postazioni ed apparati informatici "mobili"
Le regole di utilizzo dei PC portatili sono le stesse dei PC collegati alla rete locale anche se i servizi disponibili e la loro modalità di erogazione potrebbe differenziarsi dalle postazioni "fisse". I portatili che rimangono sconnessi a lungo dalla rete non ricevono gli aggiornamenti automatici e possono avere quindi un livello di protezione non allineato con gli standard dell'Ente. E' quindi a carico dell'utilizzatore garantire la funzionalità e l'aggiornamento del sistema collegandolo periodicamente (almeno ogni mese) al sistema informativo comunale per gli opportuni aggiornamenti di sicurezza. La configurazione e la gestione delle apparecchiature è a carico dell'utente utilizzatore. L'utente è responsabile del PC portatile eventualmente assegnatoli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. I PC portatili devono comunque essere custoditi in un luogo protetto.

Per quanto riguarda le smart card, business key e altri dispositivi per il riconoscimento che contengono certificati di firma dei titolari, utilizzabili ad esempio nei procedimenti amministrativi dell'Ente, i destinatari sono responsabili del corretto utilizzo e devono custodire adeguatamente i dispositivi, il relativo PIN e altro materiale a corredo.

L'utilizzo di memorie (chiavette) USB per la memorizzazione ed il trasferimento dei dati deve essere circoscritto, per motivi di sicurezza, ai soli casi di effettiva necessità. Per trasmettere i dati tra le postazioni dell'Ente si raccomanda l'utilizzo delle aree condivise che sono messe a disposizione, mentre per le trasmissioni di dati da e per l'esterno si raccomanda l'utilizzo della posta elettronica o altri strumenti di trasferimento dati sicuri (es. portali istituzionali ad accesso autenticato ecc.) ; tali modalità sono infatti soggette a controlli antivirus sistematici, mentre, viceversa, le chiavi USB possono entrare in contatto con ambienti che possono portare pericolose infezioni all'interno dell'Ente. Qualora tali comportamenti venissero disattesi, il Servizio SIA si riserva di disabilitare sui PC dell'Ente il riconoscimento automatico di chiavette USB.

3.2 - Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti magnetici, supporti digitali, ecc.) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

Punto 4 - Regole per la navigazione su internet e intranet

La rete Internet è una risorsa messa a disposizione del personale come fonte di informazione per finalità di documentazione, ricerca e studio utili per lo svolgimento del proprio lavoro.
Per ragioni di sicurezza e per garantire l'integrità dei sistemi informatici, l'accesso ad Internet effettuato tramite elaboratori connessi alla rete comunale è scrupolosamente protetto da appositi dispositivi di sicurezza informatica (firewall, antivirus, etc.).
Per ridurre il rischio di uso improprio della navigazione sono state individuate categorie di siti non correlate con la prestazione lavorativa (il sistema è dotato di una 'black list' aggiornata, cioè di una lista di siti ad accesso bloccato) e configurati sistemi o filtri che prevengono accessi e operazioni reputati non attinenti all'attività d'ufficio.
Alcuni dati relativi agli accessi ai siti internet, quali l'utente, il sito visitato e l'orario di accesso, sono conservati in appositi file di log il cui accesso è consentito al solo personale tecnico preposto, nelle modalità previste dal D.lgs. 30/06/2003 n. 196 e successive modificazioni ed integrazioni, e dalla normativa vigente in materia. Su indicazione del dirigente competente, potranno essere effettuati su tali file controlli di conformità alla legge, anche saltuari o occasionali, precisando le ragioni legittime, specifiche e non generiche della richiesta. Analoghi controlli potranno essere effettuati per ragioni legate alla funzionalità e sicurezza del sistema. L'accesso a tali dati potrà essere consentito all'autorità giudiziaria o per l'esercizio di un diritto in sede giudiziaria.
Tutto il personale può connettersi alla intranet comunale ed ai servizi da essa accessibili in base alle proprie credenziali di accesso; sono generalmente accessibili alcuni siti istituzionali o di pubblica utilità visualizzabili tramite link presente nella home page della intranet comunale.

Il personale autorizzato può connettersi alla rete Internet tramite gli strumenti a disposizione, tuttavia non è consentito:

- lo scarico (upload e/o download) di files e/o programmi software, se non previsto per motivi di lavoro o esplicitamente autorizzati;
- l'effettuazione di ogni genere di transazione finanziaria, acquisti on-line e simili salvo i casi direttamente autorizzati con il rispetto delle normali procedure per gli acquisti;
- la partecipazione a Forum non autorizzati, l'utilizzo di chat line, social network, bacheche elettroniche e la registrazione a mailing list o guestbooks anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di questi servizi Internet se non connessi all'attività lavorativa;
- l'utilizzo del collegamento ad Internet per attività in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- l'utilizzo di sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting o similari, così come connettersi a siti che trasmettono programmi in streaming (come radio o TV via WEB) senza espressa autorizzazione.
- prelevare da Internet e/o archiviare sul proprio elaboratore, ovvero sulle risorse di rete condivise, documenti informatici (testo, audio, immagini, filmati, etc.) di natura oltraggiosa, discriminatoria per sesso, religione, origine etnica appartenenza sindacale o politica o che comunque possano risultare offensivi della dignità umana
- diffondere attraverso Internet materiale commerciale o pubblicitario non richiesto
- trasmettere via Internet virus o altro codice maligno, per arrecare danni e malfunzionamenti a sistemi informatici.
- prelevare da Internet, ovvero inviare tramite Internet, dati o altre risorse informatiche per scopi non consentiti dalle norme vigenti.
- fornire a soggetti non autorizzati l'accesso alla connessione Internet comunale;

- utilizzare la connessione Internet al fine di arrecare danno o disturbo a terzi
- lo svolgimento di qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno o pubblico, incluso il possesso o l'uso di strumenti o software intesi ad eludere schemi di protezione da copia abusiva del software, rivelare password, identificare eventuali vulnerabilità della sicurezza dei vari sistemi, decrittare illecitamente file crittografati o compromettere la sicurezza della rete e internet in qualsiasi modo.

Il personale del servizio SIA può in ogni momento, nel rispetto delle normative vigenti e di quanto previsto dal D.Lgs. 196/03, per fini meramente diagnostici e tecnici, verificare il corretto utilizzo delle connessioni e degli accessi ad internet. Le violazioni riscontrate al presente punto, in relazione alla loro gravità sarà oggetto di segnalazione all'Ufficio procedimenti disciplinari.

4.1 Punti di accesso WiFi pubblico ad internet

Presso spazi pubblici o sale ad accesso pubblico, è possibile la realizzazione di impianti WiFi per l'accesso ad internet tramite connettività a rete pubblica o privata (es. la rete regionale Lepida); l'attivazione di punti d'accesso pubblico ad internet sarà comunque concordato col SIA e, se non diversamente richiesto ed autorizzato, separato dalla rete MAN circondariale istituzionale. Tutte le modalità di accesso ed autenticazione al WiFi sono regolamentate da atti specifici e autorizzati dal responsabile degli accessi ad internet del Comune appaltante, nel rispetto delle normative vigenti.

Punto 5 – Utilizzo della Posta Elettronica

Il servizio di posta elettronica è disponibile, su richiesta del dirigente o del responsabile del servizio, per ogni dipendente tramite un sistema gestito in forma centralizzata.
Oltre all'indirizzo di posta elettronica personale sono messi a disposizione degli uffici indirizzi di posta elettronica non nominali, condivisi fra più utenti o più enti (es. i servizi gestiti in forma associata), che possono essere richiesti dal dirigente o dal responsabile competente. Per questi indirizzi deve essere indicato un referente responsabile al quale verrà delegata la funzione di stabilire i diritti di accesso alla casella; se non espressamente indicato, la responsabilità è in carico al dirigente medesimo.

Nell'utilizzo della posta devono essere adottate le seguenti misure:
- l'uso della posta istituzionale è consentito unicamente per ragioni di servizio;
- le caselle nominali sono da ritenersi personali e accessibili esclusivamente da parte dell'utente proprietario attraverso l'inserimento di una password personale; la password deve essere mantenuta riservata e non deve essere comunicata. L'utente, utilizzando le apposite funzioni di delega fornite dal sistema di posta o richiedendo l'attivazione da parte del personale del servizio SIA, può eccezionalmente in caso di necessità e per ragioni di servizio, concedere l'accesso alla propria casella ad altri: in tal caso è necessario che i messaggi di posta elettronica contengano avvertimenti ai destinatari che le risposte potranno essere conosciute da altri soggetti.
- è a disposizione di ciascun utente di posta, e ne è consigliabile l'utilizzo, una apposita funzionalità di sistema che consente di inviare automaticamente, in caso di assenze programmate, messaggi di risposta personalizzabili segnalando eventualmente l'indirizzo della persona da contattare;
- a seguito dell'assenza di un dipendente, su richiesta del dirigente di servizio competente o di un suo delegato espressamente nominato, esclusivamente per ragioni di servizio e in caso di necessità improrogabile, è consentito l'accesso alla casella di posta elettronica individuale

di un dipendente da parte del dirigente stesso o, preferibilmente, l'inoltro in copia al dirigente dei messaggi di posta in arrivo alla casella nominale. Il prima possibile, o comunque al suo ritorno, il dipendente verrà informato tempestivamente, dallo stesso richiedente, sull'intervento effettuato.

- se autorizzato dal dirigente ai dipendenti, esclusivamente per motivi riguardanti l'attività lavorativa, può essere consentito l'accesso alla propria casella di posta elettronica anche all'esterno del sistema informativo comunale attraverso internet e il servizio di web mail; resta comunque l'obbligo dell' uso della posta unicamente per ragioni di servizio;
- l'invio di e-mail con allegati a mittenti multipli deve essere limitata onde evitare sovraccarico sul server centrale e sulle linee esterne. La dimensione massima degli allegati accettati dal sistema di posta è di circa 20 Megabytes;
- è vietata l'apertura di allegati a messaggi di posta elettronica senza il previo accertamento dell'identità del mittente e la sua identificazione come utente sicuro e pertinente all'attività istituzionale;
- le caselle di posta elettronica devono essere mantenute in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti e/o effettuando l'archiviazione dei documenti allegati, in base alle informazioni specifiche indicate dal servizio SIA

In ogni caso non è consentito:

- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione esterne o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare "catene di S. Antonio", appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi, barzellette, o comunque materiale non pertinente alla propria attività lavorativa;
- utilizzare la casella personale per la partecipazioni a dibattiti, forum o mailing-list se non inerenti alla propria attività lavorativa;
- utilizzare il servizio di posta elettronica per trasmettere pubblicità personale o commerciale.
- l'invio di posta a destinatari non espressamente indicati (la cosiddetta 'copia conoscenza nascosta' o 'Ccn') se non per cause evidentemente dovute al rispetto della privacy o per inoltro di comunicazioni di carattere generico (es. comunicazioni al personale senza indicare l'elenco puntuale dei destinatari) che rendono necessario evitare la conoscenza di tutti gli indirizzi dei destinatari;
- utilizzare la posta come 'strumento di archiviazione' di dati, soprattutto se si tratta di dati sensibili o giudiziari, in quanto strumento non idoneo per la sicurezza, economicità e segretezza dei dati.

Conclusioni

Il presente disciplinare viene consegnato a ciascun dipendente degli enti del Nuovo Circondario Imolese, che firma per ricevuta, all'atto dell'assunzione unitamente a copia del regolamento di organizzazione.
Il dipendente deve attenersi, nell'utilizzo e nella gestione delle risorse strumentali informatiche comunali, alle norme e ai principi del presente disciplinare e ai doveri stabiliti nel "Codice di comportamento dei dipendenti delle pubbliche amministrazioni".

La violazione da parte dei lavoratori o degli addetti ai sistemi di manutenzione informatica dei principi e delle norme contenute nel presente disciplinare costituisce violazione degli obblighi e dei doveri del dipendente pubblico e, pertanto, in relazione alla gravità dell'infrazione, i rispettivi dirigenti, previo espletamento di procedimento disciplinare, possono procedere all'applicazione delle sanzioni previste dalle disposizioni contrattuali vigenti in materia ed in particolare delle sanzioni penali relative all'accesso abusivo a sistemi informatici o telematici.