CITTA' DI FERMO

Disciplinare sull'Utilizzo degli Strumenti Informatici

(Approvato con deliberazione G.C. n.225 del 04/05/2010)

DISCIPLINARE SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI CON RIGUARDO ALLA TUTELA DEI DATI PERSONALI PER IL

COMUNE DI FERMO

Capo I

DISPOSIZIONI GENERALI

Art. 1 - Oggetto del disciplinare

1. Il presente disciplinare regola le modalità di accesso e l'utilizzo degli strumenti informatici e il conseguente trattamento di dati personali nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 e dal provvedimento del Garante per la protezione dei dati personali del 1 marzo 2007.

2. L'Amministrazione promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni e delle banche dati di proprietà del Comune di Fermo.

Art. 2 - Applicabilità

1. Le disposizioni del presente disciplinare sono applicabili a tutti gli incaricati del Comune di Fermo , a prescindere dal rapporto contrattuale che li lega all'Ente.

Art. 3 - Definizioni

1. Per quanto attiene alle definizioni presenti nel presente disciplinare, si fa riferimento a quanto disposto dall'Art. 4 del Decreto Legislativo 30 giugno 2003, n. 196, di seguito denominato "codice della privacy".

Art. 4 - Principi Generali

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

2. Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi e programmi cui ha accesso e dei dati trattati a fini istituzionali. E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali.

3. Sono vietati comportamenti che possono creare un danno, anche d'immagine, all'Ente.

Art. 5 - Incaricati

1. Sono nominati incaricati del trattamento tutti i dipendenti a tempo indeterminato, a tempo determinato, i collaboratori ed ogni altra persona fisica che a qualunque titolo tratta dati personali per conto del Comune di Fermo.

2. Gli incaricati possono trattare solo i dati necessari allo svolgimento della funzione alla quale sono stati assegnati dal proprio dirigente di riferimento.

3. Nel trattare i dati di cui al comma 2, gli incaricati devono attenersi, oltre a quanto disposto dalla legislazione vigente, anche alle disposizioni del seguente disciplinare e a quelle ulteriori eventualmente impartite dal proprio dirigente di riferimento.

4. Gli incaricati devono vigilare, per quanto di loro competenza, sulla corretta applicazione e funzionamento delle misure di sicurezza a tutela della riservatezza dei dati trattati, ed informare immediatamente il dirigente o il responsabile del trattamento di riferimento in caso di malfunzionamento delle misure stesse.

5. Quanto disposto nel presente disciplinare si intende esteso, fatto salvo il principio di separatezza delle funzioni di cui all'Art. 107 del TUEL, agli amministratori, nonché ai componenti delle commissioni che trattano dati personali per lo svolgimento delle loro funzioni istituzionali.

Capo II

RAPPORTI CON IL PUBBLICO

Art. 6 - Rapporti di front office

1. Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello (cd. front office) deve essere prestata attenzione al rispetto dello spazio di cortesia e, ove possibile, invitare gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza.

2. Identificazione dell'interessato:ove sia necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere, l'operatore è autorizzato a richiedere ed ottenere un documento di identità o di riconoscimento .

3. Obbligo di riservatezza e segretezza: l'incaricato deve mantenere l'assoluta riservatezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione non autorizzata delle informazioni stesse. L'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy.

Art. 7- Cautele da seguire per la corretta comunicazione dei dati a soggetti terzi

1. Verifica dell'esattezza dei dati comunicati: nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione all'esattezza del dato che viene comunicato.

Art. 8 - Presenza di ospiti o di personale di servizio

1. L'incaricato deve fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.

2. Nel caso in cui l'incaricato debba allontanarsi dalla scrivania in presenza di ospiti, egli deve riporre i documenti e attivare uno dei sistemi di protezione previsti dal successivo Art. 13.

3. L'incaricato non deve rivelare le proprie password al personale di assistenza tecnica ne consentirne la digitazione da parte dello stesso.

4. L'incaricato non deve rivelare le password in alcun modo, in quanto nessuno è autorizzato a chiederle.

5. L'incaricato deve segnalare qualsiasi anomalia al proprio responsabile.

Capo III

ISTRUZIONI PER L'USO DEGLI STRUMENTI

Art. 9 - Istruzioni per l'uso degli strumenti informatici

1. Computer: l'utilizzo dei computer di proprietà del Comune di Fermo è consentito solo se connesso e finalizzato allo svolgimento delle attività istituzionali dell'ente.
Non è consentito quindi:
a) modificare le configurazioni relative all'accesso alla rete
b) attivare l'accesso alle postazioni dall'esterno
c) installare modem;
d) connettere dispositivi esterni personali
e) copiare su dispositivi esterni personali dati la cui titolarità è del Comune di Fermo;
f) installare software;

2. Telefono: nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
a) chiedere l'identità del chiamante e la motivazione della richiesta;
b) richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
c) verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante (ad esempio caserma dei carabinieri, servizi pubblici e di PS, ...);
d) procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò

accertandosi dell'identità dichiarata in precedenza.

3. Fax: nell'utilizzare questo strumento occorre prestare attenzione a:

a) digitare correttamente il numero di telefono, cui inviare la comunicazione;
b) controllare l'esattezza del numero digitato prima di inviare il documento;
c) verificare che non vi siano inceppamenti della carta ovvero che non siano presi più fogli contemporaneamente;
d) attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
e) qualora siano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
f) in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax.

4. Scanner: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile.

5. Distruzione delle copie cartacee: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto. Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in mancanza, devono essere sminuzzati in modo da non essere più ricomponibili.

6. Distruzione dei supporti fissi di memorizzazione dei dati (hard disk**):** Qualora sia necessario dismettere il supporto, si dovrà procedere a rendere inintelligibile il contenuto.

7. Riutilizzo dei supporti di memorizzazione**:** I supporti fissi possono essere riutilizzati da parte di terzi solo se i dati precedentemente memorizzati non siano più visionabili o ricostruibili. I supporti rimovibili (floppydisk, cd, dvd, chiavi USB, hard disk esterni, ecc.) possono essere riutilizzati solo se i dati precedentemente memorizzati non siano più visionabili da parte di terzi che procedano al riutilizzo del supporto medesimo.

8. Utilizzo delle stampanti e dei materiali di consumo: l'utilizzo delle stampanti e dei materiali di consumo (carta, inchiostro, toner, CD, DVD, chiavi USB, ecc.) è riservato esclusivamente alla preparazione di materiale inerente l'attività istituzionale dell'Ente. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

Art. 10 - Credenziali di autenticazione

1. L'accesso alle procedure informatiche dell'Ente è consentito agli incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione e di autorizzazione.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (userid o username) associato ad una parola chiave riservata (password). Possono essere utilizzati, allo scopo, strumenti con livelli di sicurezza superiori, quali dispositivi di autenticazione (es. smart card) o biometrici.

3. Gli incaricati sono responsabili della custodia e dell'utilizzo delle proprie credenziali di autenticazione e devono utilizzarle e gestirle attenendosi alle seguenti istruzioni:
a) la parola chiave, assegnata a ciascun incaricato, è composta da un minimo di otto caratteri o comunque dal numero massimo di caratteri consentito dal sistema;
b) la parola chiave assegnata dal Responsabile del Sistema Informatico deve essere prontamente sostituita dall'incaricato al primo utilizzo e, laddove non prevista la forma di sostituzione automatica governata dal server di rete, deve essere modificata da parte dell'incaricato con cadenza almeno trimestrale;
c) la password non deve contenere riferimenti agevolmente riconducibili all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
d) l'incaricato, nello scegliere la propria password, deve utilizzare anche caratteri speciali, numeri, lettere maiuscole e minuscole. L'incaricato non deve scegliere come password parole presenti in un dizionario, sia della lingua italiana che di lingue straniere, ne utilizzare parole ottenute come combinazione di tasti vicini sulla tastiera o sequenze di caratteri (ad esempio qwerty, asdfgh, 123321, aabbcc, ecc.);
e) la parola chiave deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
f) la parola chiave non deve essere scritta su nessun tipo di supporto (cartaceo, elettronico, ecc.);
g) l'incaricato è responsabile di ogni utilizzo indebito o non consentito delle credenziali di autenticazione di cui sia titolare;
h) nel caso in cui altri utenti debbano poter accedere ai dati protetti dalle credenziali di un utente assente o impedito, è necessario richiedere l'autorizzazione al Dirigente Responsabile di competenza; dietro richiesta scritta motivata il Responsabile dei Sistemi Informatici provvederà a resettare la parola chiave dell'utente assente o impedito il quale, al suo ritorno, dovrà procedere nuovamente al cambio della stessa
i) le credenziali di autenticazione individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se incaricati del trattamento). Qualora un utente dovesse avere la necessità di trattare dati o usare le procedure, il dirigente o il responsabile del servizio di riferimento potrà richiedere formalmente al Responsabile dei Sistemi Informatici, le relative credenziali di autenticazione, dotate dei privilegi necessari all'accesso ai dati o ai servizi richiesti;
l) se l'incaricato ha il sospetto di una violazione delle proprie credenziali (ad es. perché crede che queste siano conosciute da altri) è tenuto immediatamente a darne notizia al Responsabile dei Sistemi Informatici e contestualmente procedere al cambio della parola chiave.
m) nel caso l'incaricato dimentichi la propria password, dovrà chiedere formalmente al Responsabile dei Sistemi Informatici l'assegnazione di una nuova parola chiave da gestire come indicato al precedente Punto 3 lettera b).

Art. 11- Backup

1. Salvo che non sia previsto un sistema di salvataggio di dati automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione dell'incaricato e consegnare i supporti contenenti le copie di salvataggio al soggetto nominato e incaricato della conservazione, ovvero riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati.

2. Viene ribadito quanto prescritto dall'Allegato B al D.Lgs. n. 196/2003 (Disciplinare tecnico in

materia di misure minime di sicurezza).

3. Il Responsabile dei Sistemi Informatici, e per estensione eventuali suoi collaboratori facenti parte del servizio, non è responsabile del backup delle banche dati di cui non è a conoscenza e che non sono memorizzati nei server sottoposti a politiche di backup. Le banche dati non censite, non regolarmente depositate presso i server, ovvero in generale create dai singoli utenti, devono essere sottoposte a procedure di backup dagli utenti stessi, secondo le modalità previste dalla normativa vigente che li individua come diretti responsabili, e secondo quanto disposto ai precedenti punti 1 e 2.

Art. 12 - Antivirus

1. Il Comune di Fermo è dotato di un sistema centralizzato e automatizzato di protezione antivirus. E' fatto divieto sospendere, cancellare o alterare in alcun modo il sistema antivirus; ogni danno conseguente alla manomissione del sistema antivirus sarà addebitato al manomissore.

2. E' compito degli incaricati verificare il corretto funzionamento ed aggiornamento del software antivirus, avvisando il Responsabile dei Sistemi Informatici qualora riscontrassero anomalie.

3. Laddove non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da virus, gli incaricati devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando sia segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza di virus sull'elaboratore in dotazione.

Art. 13 - Protezione degli strumenti di lavoro

1. In caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito è necessario adottare un sistema di oscuramento (cd. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando, ovvero, in alternativa, occorrerà porre la macchina in posizione di standby o spegnere l'elaboratore che si sta utilizzando.

Art. 14 - Software installati

1. Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa. Sono vietati i software scaricati da Internet o acquisiti autonomamente se non preventivamente autorizzati dal Dirigente della struttura di appartenenza e dal Responsabile dei Sistemi Informatici. I software installati senza autorizzazione verranno rimossi senza alcun preavviso. Il fatto sarà formalmente segnalato al dirigente competente per i procedimenti disciplinari.

2. Sui PC devono essere installati, appena sono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.

Capo IV

POSTA ELETTRONICA

Art. 15 - Indirizzo di posta elettronica

1. Ogni incaricato è dotato di un indirizzo di posta elettronica. La casella di posta, assegnata all'incaricato, è uno strumento di lavoro ed il suo utilizzo è consentito solo per finalità connesse allo svolgimento della propria attività lavorativa, Non sono, pertanto, ammessi utilizzi diversi o privati dell'indirizzo. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2. E' fatto divieto di utilizzare la casella di posta elettronica per: trasmissione di dati sensibili, salvo i casi espressamente richiesti dalla normativa vigente in materia; trasmissione di dati confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali; Partecipazione a dibattiti, forum o mailing list non attinenti la propria attività o funzione svolta per l'Ente, salvo diversa ed esplicita autorizzazione.

3. Le strutture che lo richiedano possono disporre di una casella di posta elettronica istituzionale "di struttura". La casella di posta elettronica di ogni singola struttura può essere utilizzata secondo quanto stabilito dal responsabile della struttura stessa e comunque nel rispetto del presente disciplinare.

Art.16 - Indirizzo istituzionale

1. L'indirizzo di posta assegnato dal Comune di Fermo è un indirizzo istituzionale e deve essere utilizzato solo ed esclusivamente per esigenze connesse all'attività lavorativa. Non sono, pertanto, ammessi utilizzi diversi o privati dell'indirizzo.

Art. 17 - Sistema di protezione

1. Il sistema di posta elettronica del Comune di Fermo è filtrato e, per motivi di sicurezza, non consente l'invio e la ricezione in allegato di alcuni tipi di file potenzialmente pericolosi. Se il messaggio di posta elettronica inviato contiene uno di questi tipi di file,l'allegato verrà rimosso e il destinatario sarà avvisato con un messaggio di notifica dal sistema.

Art.18 - Invio a "tutti gli utenti"

1. Fermo restando l'uso esclusivamente istituzionale della posta elettronica è possibile inviare un messaggio a "tutti gli utenti" della rete informatica del Comune di Fermo, tale messaggio non deve contenere allegati di eccessiva grandezza

Art. 19 - Lettura degli allegati

1. E' fatto divieto di aprire messaggi, sia manualmente, sia in forma automatica, con allegati di cui

non si conosce l'origine. Essi possono contenere virus

2. E' fatto divieto di aprire filmati e presentazioni non attinenti l'attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul PC.

Capo V

INTERNET

Art. 20 - Autorizzazione all'uso di internet

1. L'accesso ad Internet è consentito a tutti gli incaricati del Comune di Fermo per lo svolgimento delle proprie attività istituzionali, mediante le attrezzature informatiche messe loro a disposizione.

2. L'utilizzo di internet deve essere limitato a scopi inerenti l'attività lavorativa.

Art. 21 - Meccanismi di controllo automatizzati

1. Il Comune di Fermo si avvale di sistemi che consentono di filtrare il traffico effettuato da e verso la rete internet.

2. Gli strumenti utilizzati, nel rispetto dello Statuto dei lavoratori (Legge 20 maggio 1970 n. 300) e del Codice della Privacy, attuano un controllo preventivo sui tipi attività compiute durante la navigazione e impediscono in maniera automatizzata la maggior parte degli usi impropri della rete Internet. I filtri automatici, impedendo all'origine tutta una serie di attività ritenute dannose, evitano che sia effettuato un controllo sistematico della navigazione del singolo utente, a vantaggio della privacy.

3. Per esigenze di sicurezza delle informazioni dell'ente e per le attività di tutela che gli sono proprie, qualora si ravvisi un traffico anomalo o accessi a siti non connessi ad attività istituzionali o in grado di generare eventi dannosi o situazioni di pericolo o di disfunzioni operative per il Comune di Fermo, il dirigente competente può autorizzare il funzionario Responsabile dei Sistemi Informatici ad individuarne le cause e l'origine.

Art. 22 - Modalità di controllo

1. E' presente un controllo sulla navigazione internet che restituisce un report con i siti visitati. Tale statistica è anonima e contiene solo dati aggregati dell'intero ente.

2. Nel caso vengano riscontrate anomalie sulla navigazione internet verranno aggiornati i meccanismi di filtraggio. Qualora il fenomeno persista si procederà ad effettuare controlli più approfonditi sull'uso degli strumenti elettronici. L'Ente eviterà in ogni modo ogni forma di ingerenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori.

3. In ogni caso, i controlli saranno sempre limitati al tempo strettamente necessario alla individuazione della causa ed origine, nel rispetto delle disposizioni di legge ed effettuati con

preavviso agli incaricati.

4. Le registrazioni del traffico effettuato saranno conservate per un periodo non inferiore a ventiquattro mesi, elevabile fino ad ulteriori ventiquattro mesi e in ogni caso, in conformità con la normativa vigente ai fini di permettere un'indagine a posteriori di eventuali anomalie e problemi di sicurezza; in ogni caso i dati sul traffico non saranno consultabili se non dalle forze dell'ordine o, previa richiesta motivata, dal dirigente di competenza.

Art. 23 - Comportamenti non tollerati

1. E' fatto divieto di utilizzare la navigazione in Internet per usi non istituzionali. In particolare non sono permesse le seguenti attività:
a) scaricamento (download) di qualunque genere di file o programmi salvo non sia indispensabile per svolgere l'attività lavorativa a cui il dipendente è preposto;
b) caricamento (upload) di file di qualunque genere presso siti esterni alla rete del Comune di Fermo;
c) la partecipazione a social network, chat o blog esterni alla rete del Comune di Fermo;
d) l'utilizzo di protocolli di streaming che consentono ad esempio di ascoltare radio o vedere materiali video da siti diversi da quelli istituzionali;
e) l'utilizzo di programmi peer to peer;

2. L'elenco sopra riportato non si intende come esaustivo e verrà pertanto impedito ogni altro tipo di utilizzo ritenuto dannoso per l'Ente.

3. Non è consentito collegare alla rete dell'ente, anche tramite collegamento WiFi, qualsiasi tipo di apparato di rete o PC, se non previa autorizzazione del dirigente del servizio presso il quale l'attrezzatura va collegata e dal Responsabile del SIC. In ogni caso il loro utilizzo dovrà avvenire in conformità al presente disciplinare.

Art. 24 - Installazione di software scaricato

1. Nel caso previsto dall'Art. 23 Punto 1 lettera a), l'installazione di software necessari all'attività lavorativa va richiesta al Responsabile dei Sistemi Informatici o suo delegato.

Capo VI

ALTRI SERVIZI

Art. 25 - Misure adottate in caso di assenza del lavoratore

1. Le credenziali di cui all' Artt. 10 hanno la funzione di impedire l'accesso indiscriminato alla postazione. E' vietato comunicare le proprie credenziali ad altri, in quanto tale comportamento espone al rischio, tra l'altro, di permettere l'accesso ai propri dati in caso di assenza.

2. Nel caso in cui si renda necessario accedere ai dati presenti esclusivamente nel PC dell'incaricato e questi risulti assente, si seguirà la seguente procedura
a) il dirigente del settore a cui appartiene l'incaricato avanza richiesta scritta e motivata in cui è dettagliatamente indicato il file o la cartella alla quale si intende accedere. La richiesta va indirizzata al Responsabile dei Sistemi Informatici;

b) il Responsabile dei Sistemi Informatici, o tecnico autorizzato, modifica la password dell'incaricato assente in modo da permettere l'accesso alla sua postazione, non essendo tecnicamente possibile, per il Responsabile dei Sistemi Informatici, conoscere le password degli utenti
c) il dirigente del settore a cui appartiene l'incaricato riceve dal funzionario Responsabile dei Sistemi Informatici la nuova password così come modificata ovvero comunicazione dell'annullamento della password, ed effettua, o fa effettuare ad altri utenti appositamente delegati per iscritto, l'accesso alla postazione dell'incaricato assente. Il dirigente o suo delegato provvede alla modifica immediata della password. Ogni altro accesso costituisce un trattamento illecito dei dati con ogni conseguenza penale, civile e amministrativa;
d) al rientro in servizio dell'incaricato, il dirigente del settore di appartenenza provvede ad avvisare prontamente lo stesso circa l'avvenuto accesso alla sua postazione, invitandolo a modificare immediatamente la password;
e) l'incaricato modificherà la password immediatamente al suo rientro, impedendo così successivi accessi alla sua postazione.

Art. 26 - Deroghe

1. Il personale del Servizio Informatico, ai fini esclusivi dell'espletamento delle sue funzioni, per esigenze organizzative e di sicurezza, può operare in deroga al presente disciplinare, mantenendo sempre elevati livelli di sicurezza ed in conformità alle norme previste dal Garante Privacy in materia di Amministratori di Sistema

Art. 27 - Conseguenze per utilizzi indebiti

1. Nel caso di indebito utilizzo, oltre ai provvedimenti disciplinari previsti dal CCNL, il Comune di Fermo si riserva ogni azione a sua tutela.

2. I costi di beni, servizi e di personale necessari per il ripristino della situazione "quo ante" derivante da un uso improprio delle strumentazioni in uso o in violazione del presente disciplinare da parte del personale saranno addebitati ai trasgressori.

Art. 28 - Sanzioni per inosservanza delle norme

1. L'inosservanza delle norme del presente disciplinare, da parte dell'incaricato, può comportare sanzioni anche di natura penale ai sensi delle disposizioni di cui alla parte III, titolo III, capi I e II del D.Lgs. n. 196/2003.