



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

## **REGOLAMENTO INTERNO PER L'UTILIZZO DEI SISTEMI INFORMATICI/ TELEFONICI**

(approvato con delibera della G.M. n. 123 del 25/09/2008)



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

## Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, espone il Comune e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine del Comune stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, il Comune ha adottato un regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del decreto legislativo 30 giugno 2003 n. 196 e del disciplinare tecnico (Allegato B al citato decreto legislativo) contenente le misure minime di sicurezza, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Considerato inoltre che il Comune, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo messo a disposizione dei propri collaboratori che ne necessitano per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

## Art. 1

### *Campo di applicazione del regolamento*

1. Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori del Comune a prescindere dal rapporto contrattuale con lo stesso intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.), ai quali è consegnata la strumentazione d'ufficio disponibile (informatica, telefonica, etc).

2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura può anche venir indicata quale "incaricato del trattamento".

## Art. 2

### *Utilizzo del personal computer*

1. Il personal computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

2. Il personal computer dato in affidamento all'utente permette l'accesso alla rete LAN dell'ente solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo articolo 3.

3. Il Comune rende noto che il personale *incaricato* dell'amministrazione del sistema e della manutenzione dello stesso è autorizzato a compiere interventi nel sistema informatico comunale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi articoli 7, comma 2 e 8, comma 1, possono anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Comune, si applica anche in caso di assenza prolungata od impedimento dell'utente.

4. Il personale di cui al precedente punto ( 3 ) ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento è effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, è data comunicazione della necessità dell'intervento stesso.

5. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale di cui al precedente punto .3 per conto del Comune né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Comune a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, sono sanzionate anche penalmente.

6. Salvo preventiva espressa autorizzazione del personale incaricato, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.).

7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale incaricato nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo articolo 9 relativo alle procedure di protezione antivirus.

8. Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

## Art. 3

### *Gestione ed assegnazione delle credenziali di autenticazione*

1. Le credenziali di autenticazione per l'accesso alla rete sono assegnate dal personale incaricato, previa formale richiesta del Responsabile del settore nell'ambito del quale è inserito e va ad operare il nuovo utente

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal personale incaricato, associato ad una parola chiave (password) riservata che deve venir custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione.

3. Le password devono essere lunghe almeno 8 caratteri, (salvo impedimenti tecnici delle applicazioni, o aggiornamenti normativi più stringenti), formate da lettere (maiuscole e/o minuscole), numeri e caratteri speciali quali &, %, ^, #, \$, ricordando che lettere maiuscole e minuscole hanno significati diversi per i sistemi, evitando ovviamente contenuti di senso logico immediato che sono facilmente individuabili (per es. nomi/date di nascita e simili).

4. È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

5. Qualora la parola chiave deve venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, il personale incaricato procede alla disattivazione temporanea dell'account e alla reimpostazione della password. Nel periodo di tempo che intercorre fra la reimpostazione e la comunicazione all'utente, il personale incaricato del Servizio Sistema Informativo Comunale ( SIC ) è preposto alla custodia delle credenziali di autenticazione.

## Art. 4

### *Utilizzo della rete del Comune*

1. Per l'accesso alla rete del Comune ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

3. Le cartelle utenti presenti nell'area di storage del Comune sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del personale addetto. Tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato ( di cui al punto 3 dell'art. 2 ). La responsabilità del salvataggio dei dati ivi contenuti è a carico del singolo utente, pertanto gli utenti devono utilizzare le cartelle personali create nell'area di storage centralizzata il cui accesso in scrittura e lettura è concesso solo all'utente e agli operatori di



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

backup. Per garantire maggiore flessibilità vengono create su richiesta del dirigente del settore cartelle di lavoro condivise a seconda del gruppo di lavoro o del progetto.

4. Il personale incaricato può in qualunque momento procedere alla rimozione di ogni file o applicazione che ritiene essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

5. Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Nel caso di cessazione del servizio e/o trasferimento per mobilità, il Responsabile del Settore è tenuto ad impartire idonee istruzioni al fine di garantire la continuità del servizio e il rispetto della privacy, pertanto, i documenti di interesse per l'interno dell'ufficio devono essere trasferiti in opportune aree accessibili dai colleghi.

7. Rimane assolutamente vietato e sottoposto a sanzione, la pulizia del proprio computer in caso di cessazione del servizio e/o trasferimento per mobilità, costituendo i file archiviati documentazione amministrativa di proprietà del Comune.

## Art. 5

### *Utilizzo e conservazione dei supporti rimovibili*

1. Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti patrimonio informativo del Comune, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato o diffuso impropriamente e/o distrutto o, successivamente alla cancellazione, recuperato.

2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente deve contattare il personale incaricato e seguire le istruzioni da questo impartite.

3. In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

4. E' vietato l'utilizzo di supporti rimovibili personali.

5. L'utente è responsabile della custodia dei supporti e dei dati del Comune in essi contenuti.

## Art. 6

### *Utilizzo di PC portatili*

1. L'utente è responsabile del PC portatile eventualmente assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

2. Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

3. I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

4. Eventuali configurazioni di tipo accesso remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate esclusivamente dal dirigente del Settore e configurate a cura del Responsabile del SIC e del suo staff tecnico. E' vietato utilizzare le suddette connessioni all'interno delle sedi comunali se contemporaneamente connessi alla rete LAN.

## Art. 7

### *Uso della posta elettronica*

1. La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

2. È fatto divieto di utilizzare le caselle di posta elettronica personali per motivi diversi da quelli strettamente legati all'attività lavorativa. Tali caselle sono in genere codificate secondo il seguente schema iniziale nomeufficio@comune.xxxxxxx.it (esempio: sic@comune.xxxxxxx.it). Inoltre si precisa che la stessa regola si applica agli indirizzi condivisi (nome servizio@comune.xxxxxxx.it; esempio servizi.demografici@comune.xxxxxxx.it). In questo senso, a titolo puramente esemplificativo, l'utente non può utilizzare la posta elettronica per:

a) l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.: mp3) non legati all'attività lavorativa;

b) l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;

c) la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale incaricato. Non si deve in alcun caso procedere all'apertura degli allegati a tali messaggi.

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

4. Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analogo dicitura, deve essere visionata od autorizzata dal Responsabile del Settore.

5. È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

6. È obbligatorio porre la massima attenzione nell'aprire i file attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

7. Al fine di garantire la funzionalità del servizio di posta elettronica del Comune e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate e/o in caso di prolungata assenza (ad es. per ferie o malattie o attività di lavoro fuori sede dell'assegnatario della casella) deve essere configurato da un incaricato del SIC su richiesta del Responsabile del Settore in maniera tale da deviare i messaggi di posta elettronica del soggetto assente sulla casella mail di un suo collega puntualmente individuato e/o sulla casella di posta del Responsabile del Settore. Inoltre sempre con le stesse modalità è possibile richiedere la consultazione dell'archivio di posta elettronica dell'operatore assente.

8. E' comunque consentito al superiore gerarchico dell'utente o, comunque, sentito



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

l'utente, a persona individuata dal Comune, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui all'articolo 7, comma 7).

9. Il personale incaricato del SIC, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, può accedere alla casella di posta elettronica per le sole finalità di tipo tecnico o manutentive indicate all'articolo 2, comma 3.

10 Al fine di ribadire agli interlocutori la natura esclusivamente legata all'attività istituzionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato del Comune può accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella policy del Comune.

## Art. 8

### *Navigazione in internet*

1. Il PC assegnato al singolo utente ed abilitato alla navigazione in internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

2. In questo senso, a titolo puramente esemplificativo, l'utente non può utilizzare internet per:

a) l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, deve venir a tal fine contattato il personale incaricato del SIC);

b) l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Comune e comunque nel rispetto delle normali procedure di acquisto appositamente regolamentate;

c) ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;

d) la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile del Settore di appartenenza;

e) l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, il Comune rende peraltro nota l'adozione di una sistema definito proxy che consente tramite alcune applicazioni software determinati blocchi o filtri automatici che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list o la consultazione di video in streaming ecc.

4. Gli eventuali controlli, compiuti dal personale incaricato del SIC ai sensi del precedente articolo 2, comma 3, possono avvenire mediante un sistema di controllo dei contenuti (proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

file di log non è continuativo e sistematico, ma viene effettuato soltanto dietro richiesta opportunamente motivata e non generica del dirigente del Settore del lavoratore controllato ed i file stessi vengono conservati non oltre 7 giorni naturali, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

5. Qualora il file di log venga utilizzato come prova in caso di provvedimenti disciplinare, è compito del personale incaricato del SIC, dietro autorizzazione del Responsabile del Settore competente estrarre copia, memorizzarla su un supporto non riscrivibile e consegnarla al Segretario Comunale che provvede alla conservazione del supporto.

## Art. 9

### *Protezione antivirus*

1. Il sistema informatico del Comune è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico comunale mediante virus o mediante ogni altro software aggressivo.

2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente deve immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale incaricato.

3. Ogni dispositivo magnetico di provenienza esterna al Comune deve essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, non può essere utilizzato fin tanto che il virus non è rimosso.

## Art. 10

### *Utilizzo dei software gestionali*

1. Il sistema informatico del Comune è dotato di software gestionali per agevolare ed ottimizzare le attività svolte da ogni dipendente. Tutto il software è regolarmente licenziato e supportato dalla ditta fornitrice.

2. A fronte dell'esigenza di mantenere banche dati aggiornate, coerenti e consistenti, durante le operazioni quotidiane di gestione viene eseguita una tracciatura delle sole operazioni che comportino una modifica ai dati. I log sono conservati per un tempo adeguato in relazione alle finalità specifiche e alle tecnologie impiegate.

3. Al fine di verificare la correttezza, la diligenza ed eventualmente l'accertamento di abusi collegati all'utilizzo dei sistemi informatici, possono essere attivati sistemi di tracciatura delle operazioni di consultazione delle informazioni (se il sistema software è tecnicamente in grado di fornirlo). La richiesta deve essere eseguita ed adeguatamente motivata dal Responsabile del trattamento dati, in ogni caso prima dell'attivazione è data opportuna comunicazione da parte del Responsabile del trattamento a tutti i dipendenti incaricati.



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

## Art. 11

### *Utilizzo dei telefoni, fax e fotocopiatrici del Comune*

1. Il telefono e il fax del Comune sono affidati all'utente e sono uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate e/o fax personali è consentito solo nel caso di comprovata necessità ed urgenza.

2. Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo rimane responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale del SIC semprechè sia tecnicamente possibile la distinzione dei costi restanti a carico dell'utente.

3. È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali.

## Art. 12

### *Osservanza delle disposizioni in materia di privacy*

1. È obbligatorio attenersi alle disposizioni in materia di privacy e di misure minime di sicurezza, come indicato dai Responsabili di Settore in materia di trattamento dei dati ai sensi del disciplinare tecnico allegato al decreto legislativo 30 giugno 2003, n.196.

## Art. 13

### *Sistemi di controlli gradualati*

1. In caso di anomalie dei sistemi rilevate dal personale incaricato del SIC, sono effettuati controlli anonimi che si concludono con avvisi generalizzati, diretti ai dipendenti del settore in cui è stata rilevata l'anomalia, nei quali si evidenzia l'utilizzo irregolare degli strumenti aziendali e si invitano gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale possono essere autorizzati dal Responsabile del Settore competente dietro richiesta motivata e non generica, in ogni caso solo dopo ripetute anomalie, delle quali deve essere tempestivamente data informazione al Responsabile della struttura competente nonché al Segretario Comunale.

2. In nessun caso sono compiuti controlli prolungati, costanti o indiscriminati.

## Art. 14

### *Sanzioni*

1. È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e



# COMUNE DI OLIVETO CITRA

Provincia di Salerno

risarcitori previsti dal vigente Contratto collettivo nazionale di lavoro, nonché con tutte le azioni civili e penali consentite.

## Art. 15

### *Aggiornamento e revisione*

1. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente regolamento. Le proposte sono esaminate congiuntamente dall'incaricato dell'Amministrazione del sistema e dal Segretario Comunale.

2. Il presente regolamento è soggetto a revisione con frequenza annuale.

## Art. 16

### *Entrata in vigore del regolamento e pubblicità*

1. Il regolamento entra in vigore a seguito dell'approvazione da parte della Giunta. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

2. Copia del regolamento è trasmessa a ciascun Responsabile di Settore che ne curerà la divulgazione e l'osservanza.

\*\*\*\*\*

## **Indice**

### Premessa

- Art. 1 Campo di applicazione del regolamento
- Art. 2 Utilizzo del Personal Computer
- Art. 3 Gestione ed assegnazione delle credenziali di autenticazione
- Art. 4 Utilizzo della rete del Comune
- Art. 5 Utilizzo e conservazione dei supporti rimovibili
- Art. 6 Utilizzo di PC portatili
- Art. 7 Uso della posta elettronica
- Art. 8 Navigazione in Internet
- Art. 9 Protezione antivirus
- Art. 10 Utilizzo dei software gestionali
- Art. 11 Utilizzo dei telefoni, fax e fotocopiatrici aziendali
- Art. 12 Osservanza delle disposizioni in materia di Privacy
- Art. 13 Sistemi di controlli graduali
- Art. 14 Sanzioni
- Art. 15 Aggiornamento e revisione
- Art. 16 Entrata in vigore del regolamento e pubblicità