

# Comune di Gambolò

Provincia di Pavia

---

<p><b>REGOLAMENTO PER L'ACCESSO ED UTILIZZO DEI SISTEMI INFORMATIVI E DELLE RISORSE INFORMATICHE, TELEMATICHE E TELEFONICHE</b></p>
---

---

Il testo del presente Regolamento è stato approvato con  
Deliberazione di Giunta Comunale n. 117 del 30/10/2008

## PRESENTAZIONE

Negli ultimi anni le Risorse Informatiche, di Rete Telematica, di Rete Telefonica fissa e mobile che l'Amministrazione ha messo a disposizione dell'utenza per lo svolgimento della normale attività lavorativa, sono cresciute in misura considerevole in virtù di diversi fattori concomitanti, quali ad esempio:

- l'introduzione di nuovi software applicativi
- la capillare diffusione della posta elettronica per le comunicazioni interne ed esterne
- l'utilizzo crescente di Internet quale abituale strumento di lavoro per la ricerca di informazioni e l'accesso a banche dati "on-line"
- l'ampio utilizzo della telefonia mobile per le comunicazioni di servizio.

La diffusione dei citati strumenti e tecnologie ICT (Information & Communication Technology) ha incrementato di fatto la complessità gestionale dei Sistemi Informativi dell'Amministrazione, portando in primo piano numerosi problemi di carattere operativo aventi però importanti ripercussioni dal punto di vista delle responsabilità in capo al singolo utente finale e all'Ente.

Tra i problemi ricorrenti che attengono all'accesso ed all'utilizzo di sistemi e tecnologie ICT vi sono quelli legati alla sicurezza fisica e logica dei Sistemi Informativi automatizzati, quelli legati al trattamento delle informazioni da parte degli utenti, le problematiche legate alla proprietà intellettuale e diritto d'autore di banche dati e programmi informatici ed i temi specificatamente legati ai cosiddetti "computer crimes" (ovvero: crimini informatici).

I fattori legati all'alta diffusione delle stazioni di lavoro informatizzate ad uso individuale oppure al sempre più esteso utilizzo della rete Internet hanno comportato, per i gestori dei sistemi e tecnologie ICT, la necessità di tenere alto il livello di attenzione nei confronti dei possibili comportamenti che il singolo addetto potrebbe attuare nel momento dell'accesso e dell'utilizzo delle risorse assegnategli per lo svolgimento del lavoro d'ufficio.

Molti dei problemi sopra accennati, possono essere affrontati e risolti dalle Amministrazioni sensibilizzando e formando opportunamente l'utenza sui temi afferenti il campo della cosiddetta "Informatica Giuridica", laddove si specificano le norme di legge che devono essere rispettate al fine di un corretto utilizzo delle Risorse Informatiche, Telematiche e Telefoniche costituenti i Sistemi Informativi di un Ente o Azienda.

Ai fini del presente Regolamento, si è voluto però dare un'accezione più ampia al termine "corretto" non limitandolo solo al concetto di utilizzo conforme alla normativa vigente, ma estendendolo alla necessità di perseguire, tramite adeguati comportamenti, un utilizzo efficiente ed efficace degli strumenti che l'Amministrazione mette a disposizione dell'utenza, con il fine ultimo di raggiungere una gestione ottimale dei sistemi informativi automatizzati.

Il personale incaricato 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 dei programmi, manutenzione hardware ecc.). Detti interventi 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.

Per esplicitare in maniera chiara i comportamenti corretti e funzionali, è stato predisposto il presente testo di Regolamento interno che disciplina le modalità di accesso e di utilizzo alle diverse risorse individuate nel seguito, richiamando i testi normativi vigenti, responsabilizzando l'utenza nei confronti di possibili comportamenti difformi dagli stessi ma anche richiamando alcuni esempi pratici di errato utilizzo delle risorse a disposizione.

Il Regolamento è strutturato in capitoli distinti a seconda della tipologia di risorsa in esame, al fine di facilitare la lettura all'utente e consentire un rapido accesso all'argomento desiderato.

## **A) PARTE GENERALE**

---

### **1. Definizioni**

*Amministrazione* (denominata anche: *Ente*): il Comune di Gambolò, con sede in Piazza Cavour n. 3, 27025 -Gambolò.

*Amministratori di sistema*: il personale che gestisce l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

*Custodi delle password*: coloro che, ai sensi del D.Lgs. 196/2003 e s.m.i., detengono, su base fiduciaria dell'Utente, la password di accesso alla stazione di lavoro, da utilizzarsi in caso di necessità e di assenza dell'Utente preposto all'utilizzo, di norma, della stessa.

*Administrator*: l'Utente di un PC che ha tutti i diritti di gestione nell'accesso al sistema ed ai dati.

*Poweruser*: l'Utente che è abilitato ad avere maggiori funzioni nell'accesso al sistema ed ai dati e alle modalità di trattamento degli stessi, in funzione delle particolari esigenze della struttura in cui si colloca.

*Servizio Informatico Comunale (SIC)*: la funzione organizzativa che è preposta all'acquisizione, alla gestione operativa e allo sviluppo delle tecnologie informatiche, telematiche e telefoniche (telefonia fissa) dell'Amministrazione ed alla quale è riconosciuto il ruolo di amministratore delle stesse.

*Fornitore sicurezza informatica ed assistenza sistemistica*: la ditta che è responsabile della sicurezza perimetrale informatica e che fornisce supporto sistemistico.

*Fornitore del servizio di sviluppo e manutenzione sw*: la ditta che è responsabile dello sviluppo di nuovi applicativi web e della manutenzione di applicativi esistenti in collaborazione con il personale del SIC

*Fornitori di specifici applicativi e relativa assistenza*: le ditte che hanno fornito sistemi informativi in uso all'Ente sui quali forniscono assistenza.

*Sistemi Informativi*: tutte le banche dati ed i programmi informatici che costituiscono l'insieme delle risorse software acquisite su licenza da fornitori esterni o di proprietà dell'Amministrazione oppure disponibili tramite collegamenti interni o esterni all'Ente, installati su un qualunque sistema elaborativo server, client o di rete trasmissione dati di cui si ha responsabilità di acquisizione, gestione operativa e sviluppo.

*Risorse Informatiche, Telematiche e Telefoniche*: le attrezzature ed i dispositivi fisici come ad esempio:

- le stazioni di lavoro (personal computers), le workstations, le stampanti ad uso individuale e per gruppi di lavoro

- le postazioni telefoniche fisse, gli apparati radiomobili cellulari, i centralini telefonici
- gli apparati di rete trasmissione dati e le altre attrezzature facenti parte della rete trasmissione dati comunale, della rete telefonica fissa e di quella mobile
- i collegamenti dati e telefonici acquisiti tramite noleggio da fornitori esterni oppure di proprietà dell'Amministrazione.

*Servizi di Rete Informatica, Telematica e Telefonica:* i servizi disponibili tramite l'accesso alle Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione.

Sono esempi di servizi di Rete Informatica quelli relativi all'autenticazione degli Utenti per l'utilizzo di stampanti di gruppo oppure per l'accesso e l'utilizzo del sistema di Posta Elettronica o di Internet. Esempi di servizi di Rete Telematica sono invece quelli che permettono il collegamento delle stazioni di lavoro ai sistemi dipartimentali server anche da locazioni remote. Infine sono servizi di Rete Telefonica ad esempio quelli disponibili dai centralini telefonici (trasferimento di chiamata, deviazione ad altro numero, ecc) oppure dalla rete del gestore di rete telefonica mobile (segreteria telefonica, "dual-billing", ecc.).

*Utente:* la persona fisica, di norma identificabile nell'incaricato del trattamento dei dati ai sensi dell'Art. 4, comma 1, lettera h, del D.Lgs. 30 giugno 2003, n.196, che, previa espressa autorizzazione, ha accesso ed utilizza i Sistemi Informativi e le Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione.

Sono Utenti di norma:

- i dipendenti dell'Amministrazione
- gli Amministratori dell'Ente
- il personale esterno con incarichi professionali assegnati dall'Amministrazione
- gli stagisti, i tirocinanti e gli addetti di società terze che prestano servizio o lavorano per conto dell'Amministrazione
- i tecnici informatici dipendenti di società fornitrici dell'Amministrazione
- tutti gli altri soggetti che, per periodi di tempo limitati o continuativi, hanno accesso e utilizzano a qualche titolo i Sistemi Informativi e le Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione.

*Supporti rimovibili:* si intendono i supporti di memoria esterni al PC (es. floppy disk, CD-R, CD-RW, DVD-R, DVD-RW, chiavette USB, dischi esterni USB ecc.)

## **2. Oggetto e adeguamento del Regolamento**

Con il presente Regolamento vengono definite le modalità di accesso e di utilizzo dei Sistemi Informativi, delle Risorse Informatiche, Telematiche e Telefoniche dell'Amministrazione.

Il presente Regolamento sarà sottoposto ad adeguamento, secondo necessità, in dipendenza dei futuri cambiamenti della normativa di riferimento oppure di quelli dettati dall'evoluzione tecnologica ed organizzativa che interesserà i sistemi e le tecnologie ICT.

Per quanto non espressamente specificato, il presente Regolamento deve essere interpretato secondo correttezza e buona fede.

## **3. Finalità del Regolamento**

L'adozione del presente Regolamento è finalizzata a garantire prioritariamente:

- il rispetto delle leggi in materia di trattamento delle informazioni e dei dati trattati dagli utenti dei sistemi informativi, anche tenuto conto delle esigenze di tutela della privacy e della sicurezza del trattamento degli archivi informatici;
- il rispetto delle leggi in materia di tutela giuridica dei programmi per elaboratore e delle banche dati;
- il rispetto delle leggi in materia di crimini informatici.

Inoltre il presente Regolamento mira ad assicurare:

- la riservatezza delle informazioni trattate con i Sistemi Informativi dell'Amministrazione e la sicurezza nello scambio di informazioni da parte degli Utenti;
- un responsabile utilizzo delle dotazioni tecnologiche da parte degli Utenti;
- il corretto utilizzo delle Risorse Informatiche, Telematiche e Telefoniche da parte degli Utenti per lo svolgimento del lavoro d'ufficio al fine di garantire la massima efficienza nell'utilizzo delle Risorse stesse;
- la massima disponibilità e continuità di servizio dei Sistemi Informativi dell'Amministrazione, nell'interesse degli Utenti e della collettività.

#### **4. Funzioni del Responsabile del Servizio Informatico Comunale**

Il Servizio Informatico Comunale (SIC) ha la funzione, in collaborazione con il *Fornitore sicurezza informatica ed assistenza sistemistica* e di ditte terze, di:

- adottare tutti i dispositivi di sicurezza necessari per proteggere l'integrità fisica e logica dei sistemi ed apparecchiature informatiche, telematiche e telefoniche che ha in gestione;
- implementare opportuni meccanismi di controllo e monitoraggio, anche a livello preventivo, atti ad evitare possibili intrusioni ai Sistemi Informativi ed alle apparecchiature informatiche, telematiche e telefoniche ovvero abusi nell'utilizzo delle stesse;

Per raggiungere gli obiettivi sopra descritti il SIC, mediante il *Fornitore sicurezza informatica ed assistenza sistemistica*, provvede, previa autorizzazione scritta, effettuando i necessari test di vulnerabilità dei sistemi (Vulnerability Assessment e Penetration Test) alla redazione ed al periodico aggiornamento dell'analisi dei rischi prevista dal D.Lgs. 30 giugno 2003, n.196 per la messa in sicurezza informatica dell'Amministrazione, adottando le più recenti tecnologie disponibili sul mercato ICT al fine di implementare misure idonee a salvaguardia delle Risorse Informatiche e Telematiche dell'Ente.

In particolare il SIC e il *Fornitore sicurezza informatica ed assistenza sistemistica* si riservano la facoltà di accedere in un qualunque momento alle Risorse Informatiche e Telematiche ai soli fini dell'espletamento di compiti di monitoraggio sulle Risorse stesse nonché ai fini della salvaguardia della sicurezza dei Sistemi Informativi dell'Amministrazione, nel rispetto della riservatezza dei dati personali di cui al D.Lgs. 30 giugno 2003, n.196.

In particolare vengono conservati, ai termini di legge (D.Lgs. 196/2003 art.123 - 132), i log delle seguenti attività:

- traffico e-mail dell'Ente in ingresso ed in uscita (data/ora, mittente, destinatario)
- traffico web - navigazione verso Internet dell'Ente (data/ora, gruppo di lavoro, sito visitato); non viene mantenuto, nei log, il nome dell'Utente, ma come prescritto dalle circolari del Garante per la Privacy, è possibile, previo preavviso degli Utenti e fornendo adeguate motivazioni, attivare il log nominativo;

- accessi ai siti web da Internet e dalla rete locale:
  - o dell'Ente (data/ora, indirizzo IP del client, pagine visitate)
  - o degli enti convenzionati (data/ora, indirizzo IP del client, pagine visitate)

La conservazione dei log sopra indicati avviene:

- per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
- per adempiere alla normativa antiterrorismo vigente, mettendo i log a disposizione dell'autorità giudiziaria.

I log del traffico telefonico fisso e mobile vengono memorizzati a cura del gestore del servizio telefonico.

Non vengono conservati i log del traffico Internet delle connessioni ADSL acquisite dall'Amministrazione e date in uso a scuole ed a enti pubblici o di interesse pubblico.

Il SIC sviluppa e mantiene, in collaborazione con il *Fornitore del servizio di sviluppo e manutenzione sw*, diversi applicativi web sviluppati con tecnologie Open Source, i cui codici vengono versionati in un repository centralizzato. I codici degli applicativi sviluppati internamente, non sono distribuibili, trattabili o modificabili senza autorizzazione da parte del SIC.

## **B) RISORSE INFORMATICHE**

---

### **5. Generalità delle risorse informatiche**

Le Risorse Informatiche che vengono assegnate agli Utenti costituiscono uno strumento di lavoro.

L'insieme delle Risorse Informatiche a disposizione degli Utenti è suddiviso di norma in due categorie:

- Risorse assegnabili individualmente, cioè per via nominativa, al singolo Utente
- Risorse non assegnabili individualmente al singolo Utente, in quanto condivise nell'accesso e nell'utilizzo tra più Utenti.

Per Risorsa Informatica **assegnabile nominalmente** all'Utente, si intende ad esempio:

- la stazione di lavoro (denominata anche: personal computer o PC), costituita di solito dall'unità base elaborativa dotata di supporti di memoria fissi e rimovibili, video, tastiera e mouse
- la stampante eventualmente collegata alla stazione di lavoro di cui sopra
- gli eventuali altri dispositivi accessori direttamente collegati alla stazione di lavoro (es. scanner, tavoletta grafica, lettore di smart-card ecc).

Per Risorsa Informatica **non assegnabile nominalmente** all'Utente ma a disposizione di gruppi di Utenti definiti dal SIC, si intende ad esempio:

- una stampante di gruppo collegata alla rete trasmissione dati comunale utilizzata da più Utenti (o fotocopiatrice di rete)
- uno spazio di memorizzazione su un sistema elaborativo dipartimentale (server) utilizzato da più Utenti che accedono e condividono le informazioni ivi contenute.
- postazioni condivise utilizzate part-time da più utenti (aule corsi, postazioni pubbliche ecc.)

L'Utente è reso edotto che qualunque utilizzo delle Risorse Informatiche o comportamento da parte dell'Utente non strettamente inerente l'attività lavorativa può dare luogo a malfunzionamenti o disservizi sia nei confronti dell'utenza interna sia di soggetti e persone esterne, causando maggiori costi per l'Amministrazione e diseconomie nella gestione dei sistemi e delle attrezzature informatiche. Taluni utilizzi impropri delle Risorse Informatiche possono inoltre mettere a rischio la sicurezza informatica dei Sistemi Informativi dell'Amministrazione.

Gli utilizzi di cui sopra sono pertanto vietati e fonte di responsabilità civile, penale e disciplinare.

### **6. Accesso alle risorse informatiche**

L'accesso alle Risorse Informatiche è riservato ai soli Utenti previa assegnazione delle stesse da parte del SIC.

L'assegnazione di Risorse Informatiche ad un Utente avviene di norma dietro presentazione al SIC di una richiesta motivata da parte del Dirigente/Responsabile di Servizio o suo delegato da cui l'Utente dipende, oppure su iniziativa del SIC nel caso di Risorse che rientrano in piani di sostituzione tecnologica di sistemi ed apparecchiature informatiche ormai obsolete.

Ogni Risorsa Informatica viene assegnata nominalmente a un Utente o, qualora si tratti di risorsa condivisa non assegnabile individualmente bensì ad un gruppo di Utenti, al Dirigente/Responsabile di Servizio o suo delegato dal quale l'Utente dipende.

Il SIC, ricevuta la richiesta di assegnazione della Risorsa, provvede all'assegnazione fisica della stessa sul posto di lavoro dell'Utente individuato, comunicando la relativa accoglibilità, previa verifica di congruità tecnica ed organizzativa, tenendo conto di fattori quali:

- disponibilità di Risorse Informatiche a magazzino
- piani periodici di acquisizione di nuove attrezzature informatiche
- carichi di lavoro connessi alle attività tecnico-amministrative degli uffici del SIC.

La comunicazione succitata indica altresì, in caso di riscontrata accoglibilità, i tempi previsti di evasione della richiesta medesima.

Tutte le richieste di assegnazione di Risorse Informatiche pervenute al SIC vengono evase nel più breve tempo possibile, di norma nel rispetto dell'ordine di arrivo delle stesse e tenendo in debito conto le situazioni organizzative e le esigenze debitamente segnalate che impongono particolare urgenza.

Ciascun Utente assegnatario di una Risorsa Informatica sottoscrive, firmando il Rapporto di intervento, la dichiarazione di presa in carico della risorsa stessa.

## **7. Utilizzo delle risorse informatiche**

Non è consentita all'Utente la modifica delle caratteristiche fisiche impostate sulla Risorsa Informatica assegnata ad uso individuale né sulla Risorsa condivisa con altri Utenti.

In particolare, nel caso di stazione di lavoro, non è consentito all'Utente di provvedere:

- all'installazione o alla rimozione di qualunque dispositivo interno o esterno all'unità base elaborativa o ad altre unità ad essa collegate al fine di modificare le caratteristiche tecniche o di funzionamento della stessa;
- alla modifica di qualsiasi parametro di configurazione o di funzionamento relativo a caratteristiche tecniche dell'unità base elaborativa.

E' espressamente vietato all'Utente provvedere in via autonoma allo spostamento fisico di una Risorsa Informatica, ovvero di parti e componenti della stessa, nell'ambito dello stesso ufficio, tra diversi uffici o tra le sedi dell'Amministrazione, senza l'autorizzazione del SIC e conseguente intervento da parte del personale per lo spostamento fisico e del personale tecnico incaricato dal SIC per la riconfigurazione logica e di rete.

E' altresì severamente vietato all'Utente, in particolar modo se dipendente di società esterne, il collegamento, anche temporaneo, alla rete di trasmissione dati comunale, di sistemi ed apparecchiature informatiche di proprietà personale o aziendale, salvo la preventiva autorizzazione e supervisione da parte del SIC.

E' responsabilità dell'Utente provvedere affinché la stazione di lavoro assegnata ad uso individuale venga spenta ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

L'Utente è consapevole 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. Per questo motivo viene richiesto all'Utente di attivare sulla stazione di lavoro ad uso individuale uno dei programmi salva schermo ("screen saver") forniti con il software installato dal SIC, dotato della relativa password di sblocco, scelta nel rispetto di quanto indicato all'articolo Codici di accesso ("password") del presente Regolamento.

Non è consentita l'attivazione della password di accensione (altresì denominata "password di

BIOS o di SETUP”) o di altre password e/o di altro blocco fisico o logico su una Risorsa Informatica, senza la preventiva autorizzazione da parte del SIC, salvo dove espressamente previsto dalle norme vigenti o dal presente Regolamento.

Ogni Utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il SIC nel caso in cui vengano rilevati dall’apposito software antivirus virus informatici sulla stazione di lavoro assegnata o nei casi di dubbia provenienza dei supporti.

I supporti rimovibili utilizzati per il trattamento delle informazioni possono essere reimpiegati solamente quando le informazioni precedentemente contenute siano state cancellate in maniera definitiva; in caso contrario è responsabilità dell’Utente provvedere affinché gli stessi supporti vengano distrutti.

L’Utente è responsabilizzato sul fatto che:

- è **fatto divieto di memorizzare dati sensibili** ai sensi del DLGS 196/2003 sul disco locale (di solito C:) e su supporti rimovibili;
- è **fatto divieto di memorizzare dati personali non sensibili** ai sensi del DLGS 196/2003 su supporti rimovibili;
- è sconsigliato memorizzare dati personali non sensibili ai sensi del DLGS 196/2003 sul disco locale (di solito C:);
- è sconsigliato, onde evitare perdite di dati in caso di guasto della stazione di lavoro, memorizzare dati sul disco locale (di solito C:);

L’Utente è responsabilizzato sul fatto che, nel caso di restituzione in via definitiva di una stazione di lavoro, è suo preciso compito avvertire preventivamente il SIC della eventuale presenza di archivi informatici contenenti dati memorizzati nella stessa, onde evitare la perdita di dati a fronte del ricondizionamento della stazione di lavoro.

## **8. Assistenza Tecnica (Help-desk)**

Tutti gli interventi di assistenza tecnica (Help-desk) prestati dal SIC o da parte di soggetti terzi debitamente autorizzati dal SIC, attuati per la risoluzione di malfunzionamenti su Risorse Informatiche, possono essere eseguiti solamente con il consenso esplicito dell’Utente o con l’assenso del Dirigente/Responsabili di Servizio o suo delegato da cui egli dipende. Qualora ciò non fosse possibile, il SIC non si assume alcuna responsabilità per la mancata effettuazione dell’intervento stesso ed in particolare per ogni ritardo nelle attività lavorative dell’Utente derivato dal mancato intervento.

L’apertura di chiamata all’Help-desk ha valore autorizzativo in tal senso, salvo che per interventi tecnici di carattere generale decisi dal SIC (es: aggiornamenti e riconfigurazioni), che non necessitano di autorizzazione preventiva.

In particolare il tecnico informatico potrà accedere alle Risorse Informatiche assegnate all’Utente per fornire ausilio nella soluzione dei problemi tecnici segnalati, anche remotamente mediante tecniche di teleassistenza e telediagnosi (ad esempio visualizzando il contenuto dello schermo video della stazione di lavoro o il contenuto degli archivi), solamente se autorizzato come sopra precisato. Di norma, sarà cura del personale del SIC o dell’Help-desk telefonare all’utente per avvisarlo.

## 9. Stazioni di lavoro portatili

L'Utente, qualora risulti assegnatario di una stazione di lavoro portatile (PC portatile o Notebook), è responsabile della custodia della stessa sia durante gli spostamenti che durante l'utilizzo nel luogo di lavoro. I Notebook devono essere assicurati al posto di lavoro, in modo da impedirne il furto in caso di assenza temporanea dell'Utente, oppure ritirati in luogo sicuro in assenza dell'Utente.

I Notebook utilizzati anche per attività esterne all'Amministrazione (es. convegni, missioni, visite fuori sede), in caso di allontanamento dell'Utente assegnatario, devono essere custoditi in un luogo protetto a sua cura e sotto la sua responsabilità.

Alle stazioni di lavoro portatili si applicano le stesse regole di utilizzo previste per le stazioni di lavoro connesse di norma alla rete di trasmissione dati comunale.

L'Utente deve evitare di conservare dati personali e/o sensibili sui Notebook. Nel caso sia necessario, deve obbligatoriamente provvedere a criptografare tali dati, al fine di garantirne la non leggibilità a terzi.

## 10. Protezione Antivirus

Tutte le stazioni di lavoro assegnate agli Utenti devono essere protette contro il rischio di attacco al sistema informatico a opera di virus o altro software aggressivo di cui all'art. 615 quinquies del codice penale; la protezione si estende di norma anche ai sistemi dipartimentali (server) che ospitano informazioni e programmi utilizzati dagli Utenti ed al sistema di Posta Elettronica in uso presso l'Amministrazione.

La protezione avviene mediante l'utilizzo di idonei programmi installati sui sistemi la cui efficacia e aggiornamento sono verificati, conformemente a quanto disposto dall'Allegato B del D.Lgs. 30 giugno 2003 n.196 dal SIC e dal *Fornitore sicurezza informatica ed assistenza sistemistica* (in particolar modo per i server perimetrali quali Mail-relay e Server di posta); ciononostante l'Utente è tenuto ad assumere comportamenti tali da ridurre al minimo tale rischio. Non è consentito l'utilizzo di supporti rimovibili di provenienza dubbia o ignota, oppure di proprietà dell'Utente. In ogni caso qualunque dispositivo di memorizzazione di provenienza esterna all'Ente dovrà essere prudenzialmente verificato da parte dell'Utente mediante il programma antivirus installato prima del suo utilizzo.

E' assolutamente vietata la rimozione dell'antivirus.

Nel caso vi sia il sospetto della presenza di un virus informatico su un supporto di memorizzazione, quest'ultimo dovrà essere consegnato tempestivamente al SIC per la successiva analisi e conseguente trattamento.

Nel caso in cui venga effettivamente rilevata dall'Utente la presenza di un virus su una stazione di lavoro dal programma software antivirus ivi installato, questi dovrà immediatamente:

- sospendere ogni elaborazione in corso, senza spegnere la stazione di lavoro
- staccare dalla rete dati la stazione di lavoro.
- segnalare tempestivamente l'accaduto al servizio di Help Desk del SIC

Le **stazioni di lavoro stand-alone** (non collegate alla rete) devono avere:

- una password all'accensione a conoscenza dell'Utente e del Custode delle password
- un antivirus installato in locale, da aggiornarsi a mano con la massima frequenza possibile, comunque di minima nei termini di legge (ogni 6 mesi).

## **11. Utente Administrator**

Per motivi di sicurezza, stante il previsto trend di crescita di software malevolo, anche attraverso il rilascio di tool per la produzione automatica di malware, è opportuno che, al di fuori dei tecnici del SIC, nessun utente abbia, su un PC, i diritti equivalenti all'Utente Administrator.

Gli attuali utenti ai quali sono stati rilasciati diritti equivalenti ad Administrator vanno convertiti in Poweruser, in modo da ridurre il rischio potenziale, e per le eventuali funzioni necessarie e non più disponibili devono rivolgersi all'Help-desk.

## C) SISTEMI INFORMATIVI

---

### 11. Generalità dei sistemi informativi

I Sistemi Informativi utilizzati dagli Utenti costituiscono uno strumento di lavoro.

L'utilizzo dei Sistemi Informativi da parte degli Utenti è preceduto, di norma, dalla nomina ad Incaricati del trattamento da parte dei Dirigenti/Responsabili di Servizio, ai sensi del D.Lgs.196/2003 e da esplicita richiesta (anche via e-mail) del Responsabile di struttura, con conseguente abilitazione, da parte del SIC, per l'accesso alle risorse informative (o banche dati) che compongono quel determinato sistema, e per l'utilizzo dei programmi informatici che permettono il trattamento delle informazioni e dei dati ivi contenuti.

Costituiscono esempi di risorse informative:

- le banche dati accessibili tramite collegamenti ai sistemi gestionali dell'Amministrazione, di norma memorizzate in elaboratori dipartimentali (server) gestiti dal SIC, come ad esempio:
  - o il sistema di contabilità, del personale, dell'anagrafe comunale, di gestione degli atti formali, di protocollo, ecc.;
- le banche dati memorizzate nella stazione di lavoro dell'Utente finale o su spazi di memorizzazione su server dipartimentali, anche condivisi, gestite da programmi informatici regolarmente autorizzati dal SIC;
- le banche dati accessibili tramite collegamenti dedicati ai servizi di rete informatica gestiti da soggetti esterni (es. ANCI, Ministero dell'Economia, Motorizzazione Civile, INPS ecc), anche via Internet;

Costituiscono invece esempi di programmi informatici che permettono il trattamento delle informazioni contenute nelle banche dati sopra descritte:

- programmi emulatori di terminali video come Netterm, ecc
- programmi di produttività individuale come OpenOffice, MSOffice (Word, Excel, Access, Powerpoint ecc.)
- client di posta elettronica quali Lotus Notes, Outlook ecc
- altri programmi client specializzati o sviluppati ad hoc dai fornitori per usi particolari come AutoCAD/AutoCAD Map, Acrobat Writer ecc.
- browsers quali Internet Explorer, Mozilla Firefox ecc. per l'accesso ad Internet e/o ad applicazioni web.

L'Utente che accede ai Sistemi Informativi è responsabilizzato sul fatto che tutti i dati personali oggetto di trattamento contenuti negli archivi informatici degli stessi devono essere protetti ai sensi del DLgs. 30 giugno 2003, n. 196.

L'Utente inoltre è consapevole che le banche dati sono tutelate dalla normativa sul diritto d'autore di cui alla L. 22 aprile 1943, n. 633 e successive modificazioni, e pertanto si impegna a non divulgarne i contenuti informativi al di fuori di motivi di servizio.

Sono altresì vietate ai sensi del D.Lgs. 6 maggio 1999 n.169 e s.m. la riproduzione, la distribuzione, la comunicazione, totale o parziale, con qualsiasi mezzo e in qualsiasi forma delle banche dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

L'Utente è altresì responsabilizzato sul fatto che taluni comportamenti impropri attuati nell'accesso e nell'utilizzo dei Sistemi Informativi possono violare le norme in tema di criminalità informatica di cui alla L. 23 dicembre 1993, n. 547 e s.m..

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

## **12. Accesso ai sistemi informativi**

L'accesso ai Sistemi Informativi è riservato ai soli Utenti previo rilascio di opportuna abilitazione all'uso da parte del SIC.

La concessione dell'abilitazione all'accesso di una specifica risorsa informativa o di utilizzo di programma informatico da parte di un Utente avviene di norma dietro presentazione, a chi è deputato a fornire le credenziali di accesso, di una richiesta motivata da parte del Dirigente/Responsabile di Servizio o suo delegato da cui l'Utente finale dipende.

Nella richiesta viene specificata la risorsa informativa ovvero il programma informatico per il quale viene chiesto l'accesso e l'utilizzo da parte dell'Utente.

Chi è deputato a fornire le credenziali di accesso, ricevuta la richiesta di accesso alla risorsa informativa, provvede di norma alle operazioni tecniche che permettono l'abilitazione all'uso della stessa, comunicando la relativa accoglibilità previa verifica di congruità tecnica ed organizzativa ed evadendo le richieste nel più breve tempo possibile, di norma nel rispetto dell'ordine di arrivo delle stesse e tenendo in debito conto le situazioni organizzative e le esigenze debitamente segnalate che impongono particolare urgenza.

Le operazioni tecniche di cui sopra possono consistere nella semplice abilitazione dell'Utente all'accesso ed utilizzo di una risorsa informativa effettuata dal personale deputato a fornire le credenziali di accesso, nel rilascio di un "account" personale ad uso esclusivo dell'Utente finale, nell'installazione sulla stazione di lavoro dell'Utente dell'opportuno programma informatico che permette l'utilizzo della risorsa informativa individuata, oppure in una combinazione di più azioni tra quelle sopra descritte.

Gli Utenti (interni o esterni) assegnatari di un'abilitazione all'accesso sottoscrivono, per poter ricevere le credenziali di accesso, la dichiarazione di presa visione delle norme contenute nel presente Regolamento.

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

## **13. Single-sign-on**

Al fine di permettere, secondo le condizioni tecniche disponibili, ad ogni Utente interno di arrivare all'accesso alle banche dati per le quali è autorizzato con un'unica autenticazione (Single-sign-on) è necessario prima ricondurre la gestione completa delle credenziali di accesso in capo al SIC. I soggetti che in virtù di disposizioni precedenti o dell'assetto organizzativo, hanno in gestione aree specifiche, sulle quali rilasciano credenziali di accesso ad Utenti interni, devono progressivamente e tassativamente passare tale gestione al SIC.

## 14. Utilizzo dei sistemi informativi

L'Utente si impegna ad utilizzare i Sistemi Informativi ai quali ha accesso unicamente per scopi attinenti la propria attività lavorativa e ne risponde civilmente, penalmente e dal punto di vista disciplinare, in caso di abuso.

Le cartelle e gli 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.

Il personale del SIC può, in qualunque momento, procedere alla rimozione di ogni file che ritiene essere pericoloso per la sicurezza, sia sui PC degli incaricati sia sulle unità di rete.

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

E' assolutamente vietato all'Utente, e sotto la sua personale responsabilità, divulgare ad altri Utenti informazioni relative ad un account personale ricevuto dal SIC per l'accesso ed utilizzo delle risorse informative assegnategli.

E' espressamente vietato all'Utente accedere in maniera non autorizzata a banche dati accessibili tramite collegamento ai servizi di rete informatica interna o esterna, compresa Internet, nonché di effettuare, o far effettuare da terzi, l'installazione di programmi informatici su qualunque tipo di elaboratore, in particolare sulle stazioni di lavoro assegnate agli Utenti.

Le predette attività di installazione dovranno essere oggetto di esplicita richiesta e saranno eseguite, di norma, dal personale tecnico del SIC (Help Desk), salvo diversa occasionale ed esplicita autorizzazione da parte del SIC stesso.

E' inoltre fatto divieto all'Utente di effettuare, o far effettuare da terzi, qualunque operazione di installazione o re-installazione di un qualunque prodotto software, anche facente parte della dotazione installata dal SIC sulla stazione di lavoro oppure aggiuntivo rispetto ad essa. Sono altresì vietate tutte le modifiche tecniche che alterino in maniera sostanziale le funzionalità o le caratteristiche di funzionamento di programmi informatici, di archivi informatici o di banche dati accessibili tramite collegamento ai servizi di rete trasmissione dati interna o esterna, compresa Internet.

Tutte le succitate attività di modifica della configurazione definita dovranno essere oggetto di richiesta e saranno eseguite di norma dal personale tecnico del SIC, salvo diversa occasionale ed esplicita autorizzazione da parte del SIC stesso.

E' inoltre espressamente vietato:

- distribuire, via rete e/o via Posta Elettronica, o duplicare qualunque software o file (audio e/o video ecc.) soggetto a *copyright* non rispettando i termini contrattuali contenuti nella relativa licenza d'uso;
- distribuire, via rete e/o via Posta Elettronica, o duplicare qualunque software prodotto da terzi per conto dall'Amministrazione;
- distribuire, via rete e/o via Posta Elettronica, qualsiasi tipo di software o file (audio e/o video ecc.) che possa danneggiare o limitare le funzionalità dei Sistemi Informativi o delle Risorse Informatiche dell'Amministrazione, in particolare software virale.

L'Utente è consapevole 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. Per questo motivo viene fatto obbligo all'Utente, prima dello spegnimento fisico della stazione di lavoro utilizzata per l'attività lavorativa oppure in caso di assenze prolungate dall'ufficio, di procedere

preventivamente allo scollegamento (logoff o logout) o al blocco dalla Risorsa Informativa che egli stava utilizzando. L'utente è quindi, in tal senso, sempre responsabile dell'uso improprio della propria stazione di lavoro.

Il SIC o personale da esso delegato è autorizzato a rimuovere d'ufficio ed eliminare qualsiasi software e/o file (audio e/o video ecc.) soggetto a *copyright* individuato in rete e/o su strumenti informatici dell'Amministrazione, del quale l'Utente non sappia giustificare il titolo.

### **15. Codici di Accesso (password)**

L'accesso alle informazioni contenute negli archivi di un qualunque elaboratore deve essere protetto da codice d'accesso (altrimenti denominato password), custodito secondo quanto previsto dall'Allegato B del D.Lgs. 30 giugno 2003 n.196.

**L'Utente ha la responsabilità di custodire la password, comunicata nella fase di sua abilitazione all'utilizzo della singola risorsa informativa, con la massima diligenza possibile e di non comunicarla o diffonderla a terzi, salvo, ove previsto dal presente Regolamento, al Custode delle password preposto.**

Tutte le password di accesso ed abilitazione all'utilizzo delle risorse informative e dei programmi informatici componenti i Sistemi Informativi vengono rilasciate dal SIC individualmente all'Utente utilizzatore, dietro presentazione di richiesta da parte del Dirigente/Responsabile di Servizio o suo delegato da cui l'Utente dipende.

Ogni Utente, a meno che la procedura non lo permetta, è tenuto a cambiare sollecitamente la password rilasciata inizialmente dal SIC per l'accesso alla risorsa informativa, al primo utilizzo della risorsa stessa e, successivamente, almeno ogni sei (6) mesi (in caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre (3) mesi) pena la perdita di validità e la disattivazione della stessa; è obbligo e responsabilità dell'Utente chiedere altresì la sostituzione della password di accesso, nell'eventualità in cui egli sospetti che essa abbia perso la necessaria segretezza.

Qualora un Utente venisse a conoscenza, anche in maniera fortuita, di password assegnate ad altro Utente, è tenuto a darne immediata notizia al SIC ai fini della sollecita sostituzione.

Il SIC indica come criterio generale di scelta delle password che le stesse vengano formate da almeno 8 caratteri, siano composte da lettere maiuscole/minuscole e cifre numeriche, non utilizzino i caratteri speciali (& ^ % \$ #), evitando parole riconducibili a termini di uso comune tratti dal dizionario, nomi propri o geografici e riferimenti agevolmente riconducibili all'Utente stesso (es. nome del coniuge o di familiari, luogo e data di nascita, ecc).

Il Dirigente o suo delegato da cui l'Utente dipende è tenuto a segnalare tempestivamente al SIC ogni variazione nei diritti di accesso ad applicativi e/o banche dati dell'Utente stesso (es: trasferimento d'ufficio, pensionamento ecc.).

#### *Casi particolari:*

Le **stazioni di lavoro in rete locale**, collegate ai server, devono avere:

- un Utente e relativa password iniziale, che l'Utente deve cambiare al primo accesso, per il collegamento al dominio;
- non è necessaria la consegna, in busta chiusa, al Custode delle password preposto, della password di volta in volta cambiata dall'Utente, in quanto il SIC, tramite i soggetti

Amministratori di sistema, è in grado, se necessario, di accedere, attraverso l'Utente Administrator, alla stazione di lavoro ed ai dischi condivisi sul server.

**Le stazioni di lavoro stand-alone** (non collegate alla rete) devono avere:

- la "password di BIOS o di SETUP", che deve essere consegnata, in busta chiusa, al Custode delle password preposto, segnalandone il nominativo al Dirigente o suo delegato..

**Le postazioni pubbliche di accesso ad Internet** devono avere:

- un'utenza locale di Windows limitata, senza password e senza connessione al dominio, con il browser abilitato alla navigazione Internet
- i gestori della postazione devono identificare gli utilizzatori temporanei e registrarne il tempo di utilizzo (dall'ora/minuto di inizio all'ora/minuto di fine), come previsto dalla normativa antiterrorismo vigente, conservando per il tempo previsto tali informazioni, in modo riservato.

**Le postazioni delle aule corsi che hanno accesso ad Internet** devono avere:

- un'utenza locale di Windows limitata, senza password e senza connessione al dominio, con il browser abilitato alla navigazione Internet
- i gestori dell'aula devono identificare gli utilizzatori temporanei e registrarne il tempo di utilizzo (dall'ora/minuto di inizio all'ora/minuto di fine), come previsto dalla normativa antiterrorismo vigente, conservando per il tempo previsto tali informazioni, in modo riservato.
- I gestori dell'aula devono altresì sottoscrivere apposita manleva nei confronti del Comune, per danni che possano derivare da uso improprio da parte degli utilizzatori

**Le postazioni non in dominio che hanno accesso ad Internet** devono avere:

- un'utenza locale di Windows limitata, senza password e senza connessione al dominio, con il browser abilitato alla navigazione Internet
- il responsabile della struttura interessata è responsabile di identificare gli utilizzatori temporanei e registrarne il tempo di utilizzo (dall'ora/minuto di inizio all'ora/minuto di fine), come previsto dalla normativa antiterrorismo vigente, conservando per il tempo previsto tali informazioni, in modo riservato.
- il responsabile della struttura interessata deve altresì sottoscrivere apposita manleva nei confronti del Comune, per danni che possano derivare da uso improprio da parte degli utilizzatori

## **D) SERVIZIO DI POSTA ELETTRONICA**

---

### **16. Generalità del servizio di posta elettronica**

La Posta Elettronica è un servizio di rete telematica disponibile per gli Utenti e costituisce uno strumento di lavoro che l'Amministrazione mette a disposizione degli stessi per migliorare la comunicazione interna ed esterna all'Ente.

Il servizio di Posta Elettronica dell'Amministrazione e degli enti convenzionati permette la spedizione, la ricezione e l'inoltro di messaggi di testo o composti tra i diversi Utenti dei Sistemi Informativi, ma può essere anche utilizzato per le comunicazioni da e verso l'esterno dell'Amministrazione tramite l'utilizzo della rete Internet.

All'Utente viene di norma assegnata una casella di posta elettronica individuale così composta:

[inizialecognome@comune.nomecomune.pv.it](mailto:inizialecognome@comune.nomecomune.pv.it)

esempio: Mario Bianchi del Comune di Gambolò → [m.bianchi@comune.gambolo.pv.it](mailto:m.bianchi@comune.gambolo.pv.it)

### **17. Accesso al servizio di posta elettronica**

L'accesso al servizio di Posta Elettronica è riservato ai soli Utenti, previa abilitazione da parte del SIC.

L'abilitazione per l'accesso al servizio di Posta Elettronica ed il rilascio della relativa casella di posta elettronica, avviene di norma dietro presentazione al SIC di una richiesta da parte del Dirigente o suo delegato da cui l'Utente dipende.

Con le modalità sopra descritte, il Dirigente/Responsabile di Servizio o suo delegato può anche richiedere al SIC l'attivazione di caselle di Posta Elettronica non nominative:

- in **sola ricezione**, chiamate "Liste di distribuzione" cioè non destinate ad uso di singoli Utenti bensì di carattere istituzionale (es. Sindaco@, Assessore@, Servizio-X@, Ufficio-Y@, biblioteca@ ecc), specificando la lista degli Utenti abilitati al ricevimento automatico di quanto ricevuto dalla Lista di distribuzione (di solito membri dello staff, del servizio o ufficio interessato ecc.).
- In **ricezione e spedizione** come "Alias" cioè indirizzo alternativo di un'e-mail individuale già assegnata ad un Utente

Il SIC, ricevuta la richiesta di attivazione del servizio di Posta Elettronica per un Utente, provvede al rilascio di un account personale (ID utente) provvisto della relativa password di accesso ed alla creazione della casella di Posta Elettronica nominativa. Similmente, nel caso in cui la richiesta riguardi l'attivazione di una casella di Posta Elettronica non nominativa, il SIC provvede alla creazione della stessa ed alle abilitazioni conseguenti.

L'Utente è responsabilizzato sul fatto che l'ID utente rilasciato dal SIC per l'accesso ed utilizzo del sistema di Posta Elettronica è a tutti gli effetti assimilabile ad un account dotato di codice di accesso (password) e come tale soggetto alle prescrizioni del medesimo articolo del presente Regolamento.

In caso di assenza prolungata dell'utente e qualora subentrino urgenti motivi d'ufficio, su richiesta del responsabile di struttura, gli amministratori di sistema del SIC possono forzare la password di accesso, al fine di garantire l'accesso per i motivi d'ufficio espressamente individuati.

Si consiglia altresì di attivare il “messaggio di assenza” per informare il mittente e fornirgli le coordinate di altri lavoratori cui rivolgersi.

## 18. Utilizzo del servizio di posta elettronica

L'Utente si impegna ad utilizzare la casella di Posta Elettronica unicamente per scopi attinenti la propria attività lavorativa e ne risponde civilmente, penalmente e dal punto di vista disciplinare, in caso di abuso ai sensi delle vigenti e relative norme, compreso il “Codice di comportamento dei dipendenti pubblici”.

Sono pertanto possibili memorizzazioni ed accessi per finalità istituzionali e/o di sicurezza informatica a cura esclusiva del competente Servizio Informatico Comunale.

La dimensione massima di un singolo messaggio di Posta Elettronica in spedizione o in ricezione (compresi eventuali documenti allegati) è fissata dal SIC, in funzione delle caratteristiche tecniche dei sistemi. La dimensione massima dello spazio di memorizzazione per tutti i messaggi di Posta Elettronica dell'Utente, contenuti cioè nelle cartelle dei messaggi arrivati, spediti, in bozza, ecc, è anch'essa fissata dal SIC.

Il SIC si riserva di valutare dal punto di vista tecnico-organizzativo le eventuali richieste da parte degli Utenti di aumento delle dimensioni della casella di Posta Elettronica.

E' precisa responsabilità dell'Utente:

- non allegare ai messaggi di Posta Elettronica documenti troppo voluminosi, utilizzare per tale scopo o gli spazi di rete condivisi oppure pubblicare in Intranet, limitandosi ad inviare via e-mail la comunicazione relativa;
- tenere in ordine la casella di Posta Elettronica, curando periodicamente la dimensione della stessa (sia documenti arrivati che spediti), cancellando o archiviando localmente i documenti inutili oppure obsoleti, soprattutto se dotati di allegati voluminosi. A tale scopo l'Help-desk del SIC è in grado di fornire strumenti e supporto tecnico, affinché l'Utente diventi autonomo in tal senso.

E' responsabilità dell'Utente controllare, in particolar modo prima della spedizione, che eventuali documenti allegati ad un messaggio di Posta Elettronica non siano affetti da virus informatici.

È espressamente vietato utilizzare il servizio di Posta Elettronica per:

- inviare o memorizzare **messaggi** interni o esterni **di natura oltraggiosa, discriminatoria** per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o partitica
- partecipare a dibattiti, forum o mailing-list non aventi attinenza con l'attività lavorativa
- partecipare alle cosiddette “catene telematiche” (altresì denominate “catene di S. Antonio”)
- inviare a gruppi di utenti, interni e/o esterni, messaggi non richiesti (Spamming).

Per quanto riguarda messaggi di carattere personale si suggerisce agli Utenti di non utilizzare le caselle individuali assegnate dall'Ente bensì, come suggerito dal Garante della privacy anche a livello europeo, di utilizzare account accessibili via webmail costituiti presso provider affidabili esterni all'Ente (es: gmail, aol, libero, tiscali, alice, aruba, mc-link ecc.). L'Ente si impegna a non impedire l'accesso a webmail esterne. In caso di problemi di accesso rivolgersi all'Help Desk.

Il SIC ed il *Fornitore sicurezza informatica ed assistenza sistemistica* assicurano la riservatezza dei contenuti delle caselle definite sul sistema di Posta Elettronica adottando opportune misure a garanzia della sicurezza informatica dei sistemi; resta però responsabilità dell'Utente curare la

riservatezza della visione di comunicazioni contenute nella propria casella di Posta Elettronica, proteggendo opportunamente l'accesso indebito da parte di terzi alla stazione di lavoro.

È possibile per l'Utente utilizzare la conferma dell'avvenuta lettura del messaggio spedito ad un destinatario interno del servizio di Posta Elettronica (altresì chiamata: ricevuta di ritorno); in dipendenza però delle diverse caratteristiche dei sistemi di Posta Elettronica utilizzati dai possibili corrispondenti esterni dell'Amministrazione, non potrà sempre essere assicurata all'Utente interno la conferma di ricezione di un messaggio spedito all'esterno dell'Amministrazione.

In caso di invio di messaggi di posta all'esterno dell'ente, l'utente dovrà inserire in calce all'e-mail il link al "disclaimer" che può assumere la forma:

**Disclaimer:**

---

Questo messaggio è destinato solamente alle entità in indirizzo.

Esso può contenere informazioni confidenziali e/o riservate.

Esso non è un messaggio di natura personale, le risposte ad esso potranno essere conosciute nell'organizzazione di appartenenza del mittente.

Se non sei tra i destinatari sappi che la copia, la distribuzione o ogni uso improprio di questo messaggio è proibita e fuorilegge.

Se hai ricevuto questa comunicazione per errore, per cortesia, rispondi a questa e-mail segnalandocelo e poi cancella questo messaggio dal tuo sistema.

Il mittente non è responsabile della corretta e completa trasmissione delle informazioni contenute in questo messaggio né di ogni ritardo nella sua ricezione.

---

This message is intended only for the use of the individual or entity to whom it is addressed.

It may contain confidential or legally privileged information.

It is not a message of personal nature, the answers to it could be known in the organization of belongings of the sender.

If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us by responding to this email and please delete it from your system.

The sender is neither liable for the proper and complete transmission of the information contained in this communication nor for any delay in its receipt.

---

## **19. Posta Elettronica Certificata (PEC)**

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.

"Certificare" l'invio e la ricezione - i due momenti fondamentali nella trasmissione dei documenti informatici - significa fornire al mittente, a cura del proprio gestore di posta, una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione. Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale. Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte, conservata per legge per un periodo di 30 mesi, consente la riproduzione, con lo stesso valore giuridico, delle ricevute stesse.

Il Comune di Gambolò è di una **casella di PEC istituzionale**: [comune.gambolo@legalmail.it](mailto:comune.gambolo@legalmail.it)

## **E) SERVIZIO DI RETE INTERNET**

---

### **20. Generalità del servizio di rete Internet**

La rete Internet è una risorsa informativa esterna che l'Amministrazione mette a disposizione degli Utenti per la ricerca di informazioni sul web e per migliorare la qualità del lavoro svolto negli uffici comunali.

L'accesso e l'utilizzo del servizio di rete Internet è prevalentemente riservato a scopi attinenti l'attività lavorativa degli Utenti.

L'Utente è reso edotto che qualunque utilizzo delle Risorse Informatiche o comportamento da parte sua non strettamente inerente l'attività lavorativa può dare luogo a malfunzionamenti o disservizi sia nei confronti dell'utenza interna sia di soggetti e persone esterne, causando maggiori costi per l'Amministrazione e diseconomie nella gestione dei sistemi e delle attrezzature informatiche. Gli utilizzi di cui sopra sono pertanto vietati e fonte di responsabilità civile, penale e disciplinare.

L'Utente è responsabilizzato sul fatto che taluni utilizzi impropri della rete Internet possono mettere a rischio la sicurezza informatica dei Sistemi Informativi.

### **21. Accesso al servizio di rete Internet**

L'accesso al servizio di rete Internet è attualmente a disposizione di tutti gli Utenti collegati in rete. L'Amministrazione si riserva, in caso di ripetuti abusi, di applicare limitazioni o blocchi dell'accesso.

### **22. Utilizzo del servizio di rete Internet**

E' vietata la consultazione e la navigazione sui siti della rete Internet per motivi diversi da quelli prevalentemente legati all'attività lavorativa svolta dall'Utente.

La consultazione e la navigazione sui siti della rete Internet per motivi personali è ammessa con moderazione durante le pause, purché svolta

- in modo rispettoso delle norme vigenti e del presente regolamento
- senza causare sensibili rallentamenti alla linea, ad esempio scaricando files di grosse dimensioni

L'Ente non assume alcuna responsabilità in merito ad eventuali problemi durante l'effettuazione di ogni genere di transazione finanziaria ad uso personale, ivi comprese le operazioni di *remote-banking*, acquisti on-line e simili.

E' assolutamente vietato scaricare dalla rete Internet sulla stazione di lavoro assegnata all'Utente o su qualsiasi tipo di supporto di memorizzazione (es. hard disk, floppy disk, chiavette USB ecc. della stazione di lavoro) qualunque tipo di materiale o file (audio e/o video ecc.) soggetto a *copyright*, ad eccezione di quello avente attinenza con l'attività lavorativa dell'Utente.

Per materiale non scaricabile da Internet si intendono:

- archivi o banche dati contenenti informazioni testuali, immagini, musica, video soggetti a *copyright*

- immagini e/o video a contenuto pedo-pornografico (Legge 6/2/2006 n.38 "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedo-pornografia anche a mezzo Internet").
- programmi informatici, in particolare quelli eseguibili sulla stazione di lavoro assegnata all'Utente, come, ad esempio, salva schermo o prodotti software anche su licenza, salvo esplicita autorizzazione da parte del SIC.

L'Utente è responsabilizzato sul fatto che la registrazione, ove non strettamente necessario, dei propri dati personali (ivi compreso l'indirizzo della casella di Posta Elettronica rilasciato dal SIC), su siti Internet non sicuri non è raccomandabile per motivi di sicurezza informatica.

Sono vietati inoltre:

- la partecipazione a *forum* non professionali
- l'utilizzo di *chat-line* anche via browser per lo scambio di files
- l'uso di radio via web
- le registrazioni in "*guest-books*" (anche utilizzando pseudonimi)
- l'utilizzo di software peer-to-peer (frequente fonte di *malware* e *spyware*)
- 

Al fine di evitare la navigazione al di fuori dei casi consentiti, il Comune può decidere l'adozione di un sistema che consenta, tramite alcune applicazioni software, determinati blocchi o filtri automatici che prevenano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list o la consultazione di video streaming, ecc.

Gli eventuali controlli, compiuti dal personale incaricato del SIC possono avvenire, mediante un controllo dei contenuti o mediante "file di log" della navigazione svolta. Il controllo sui file non è continuativo e sistematico, ma viene effettuato, soltanto su richiesta motivata e non generica del Dirigente del Settore del lavoratore da controllare, nel rispetto della normativa vigente, ed i file stessi sono conservati solo per il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'Ente.

## **F) SERVIZI DI TELEFONIA FISSA E MOBILE**

---

### **23. Generalità dei servizi di telefonia fissa e mobile**

I Servizi facenti parte della Rete Telefonica dell'Amministrazione assegnabili agli Utenti vengono di norma erogati da Risorse strumentali appartenenti alla Rete Telefonica Fissa (tipicamente le postazioni telefoniche da tavolo) ed apparati di Rete Telefonica Mobile (apparati radiomobili cellulari).

Le Risorse di cui sopra vengono assegnate all'Utente in ragione dello svolgimento dell'attività lavorativa e delle funzioni a essa strettamente inerenti, in modo da rispondere all'interesse e alle esigenze dell'Amministrazione ed al miglioramento della qualità del lavoro e della produttività individuale.

In questo contesto, qualunque impiego di Risorse di Rete Telefonica Fissa o Mobile deve essere considerato ai soli scopi lavorativi e comunque in un quadro di corretto controllo della spesa corrente e miglioramento dell'efficienza interna dell'Amministrazione.

L'Amministrazione si conforma, per l'accesso ed utilizzo dei sistemi e delle apparecchiature di telefonia fissa e mobile, alle direttive approvate con D.P.C.M 11 aprile 1997 e ss.mm. e Dir.Min. 30 ottobre 2001.

### **24. Accesso alle Risorse di Rete Telefonica Fissa**

L'accesso alle Risorse di Rete Telefonica Fissa è riservato ai soli Utenti, previa assegnazione delle stesse da parte del SIC.

L'assegnazione della Risorsa ad un Utente avviene di norma dietro presentazione di una richiesta motivata da parte del Dirigente o suo delegato da cui l'Utente dipende, che evidenzia anche le caratteristiche dell'apparecchio richiesto in considerazione del ruolo e delle funzioni svolte da parte dell'Utente.

Di norma ogni apparato di rete telefonica fissa viene assegnato nominalmente a un Utente oppure, qualora si tratti di Risorsa condivisa da più Utenti non assegnabile individualmente, al Responsabile dell'ufficio ovvero al Dirigente/Responsabile di Servizio o suo delegato dal quale egli dipende.

Il SIC, ricevuta la richiesta di assegnazione della Risorsa, effettua la verifica di fattibilità comunicando entro 7 giorni lavorativi dalla richiesta la relativa accogliibilità, provvedendo di norma all'acquisizione ed assegnazione fisica della stessa sul posto di lavoro dell'Utente ed all'attivazione di una nuova utenza telefonica (numero interno), se disponibile.

Il SIC provvede all'evasione delle richieste nel più breve tempo possibile di norma nel rispetto dell'ordine di arrivo delle stesse e tenendo in debito conto le situazioni organizzative e le esigenze debitamente segnalate che impongono particolare urgenza, riservandosi la facoltà di considerare l'effettiva esigenza della richiesta in relazione alle possibili alternative ed alla disponibilità di numeri interni.

### **25. Utilizzo delle Risorse di Rete Telefonica Fissa**

L'Utente è reso edotto che qualunque utilizzo delle risorse telefoniche o comportamento da parte dell'Utente non strettamente inerente l'attività lavorativa può dare luogo a malfunzionamenti o

disservizi sia nei confronti dell'utenza interna sia di soggetti e persone esterne, causando maggiori costi per l'Amministrazione e diseconomie nella gestione dei sistemi e delle attrezzature telefoniche. Taluni utilizzi impropri delle risorse telefoniche possono inoltre mettere a rischio la sicurezza dell'Amministrazione.

Gli utilizzi di cui sopra sono pertanto vietati e fonte di responsabilità civile, penale e disciplinare.

## **26. Accesso alle Risorse di Rete Telefonica Mobile**

L'accesso alle Risorse di Rete Telefonica Mobile è riservato esclusivamente agli Utenti per i quali ricorrano i seguenti criteri di base:

- a) esigenze di reperibilità e servizi fuori sede
- b) interventi, anche di prevenzione, per calamità naturali
- c) pubblica sicurezza
- d) particolari esigenze tecniche di comunicazione di altra natura che non possono essere altrimenti soddisfatte con impianti di telefonia fissa e/o altri strumenti di comunicazione da postazione permanente.

L'assegnazione della Risorsa ad un Utente avviene di norma dietro presentazione di una richiesta motivata da parte del Dirigente o suo delegato da cui l'Utente dipende.

Tuttavia, in virtù dei criteri base sopra esposti, l'assegnazione di un apparato radiomobile può anche non essere effettuata per via nominativa ma avvenire nei confronti di un gruppo di Utenti finali, qualora nella richiesta sia stata specificato l'utilizzo della Risorsa per motivi di reperibilità del personale che utilizza a rotazione l'apparato stesso.

In questo ultimo caso, l'Utente assegnatario della Risorsa è colui che viene individuato quale responsabile per il gruppo degli Utenti finali dal Dirigente/Responsabile di Servizio o suo delegato richiedente l'apparecchio.

L'Utente è inoltre tenuto ad usare la massima diligenza nella custodia e nella conservazione dell'apparecchio stesso ed a segnalare al SIC eventuali malfunzionamenti dello stesso.

E' precisa responsabilità dell'Utente assegnatario avvisare tempestivamente il SIC fornendo copia del verbale di denuncia per furto o smarrimento dell'apparato radiomobile cellulare .

## **27. Utilizzo delle Risorse di Rete Telefonica Mobile**

L'apparato telefonico cellulare assegnato nominalmente ad un Utente o gruppi di Utenti deve essere utilizzato (sia in modalità voce che relativamente a SMS e MMS) ai soli fini dell'attività lavorativa.

L'Utente che utilizza l'apparato radiomobile cellulare è responsabile del suo corretto utilizzo dal momento dell'assegnazione fino alla revoca ovvero alla restituzione dello stesso; qualora l'Utente assegnatario non coincida con l'Utente utilizzatore, come nel caso di assegnazioni di apparati ad uso di reperibilità del personale, è preciso compito del primo sensibilizzare opportunamente il responsabile affinché impartisca al gruppo degli utilizzatori finali le indicazioni per il corretto utilizzo dello strumento di lavoro.

L'utilizzo ai fini privati di un'utenza di Rete Telefonica Mobile assegnata nominalmente ad un Utente potrà avvenire esclusivamente mediante sottoscrizione di apposito contratto di dual-billing (letteralmente: doppia fatturazione) con il gestore del servizio; tale sottoscrizione avviene dietro presentazione al SIC di apposita richiesta di attivazione della modalità sopra esposta.

La modalità "dual-billing" permette di addebitare i soli costi relativi al traffico telefonico effettuato ad uso privato direttamente all'Utente finale assegnatario dell'utenza, separandoli dai costi addebitati all'Amministrazione causati dal traffico generato per l'utilizzo dell'apparato

radiomobile per motivi di servizio. Per questo motivo l'attivazione della modalità fatturazione separata è riservata ai singoli Utenti cui è stato assegnato un apparato radiomobile e non a gruppi di Utenti.

E' in ogni caso espressamente vietato l'utilizzo ai fini privati di un apparato radiomobile cellulare assegnato ad altro Utente.

A tutela dell'Amministrazione, il SIC si riserva la facoltà di verificare dagli appositi tabulati telefonici forniti dal gestore dei servizi di Rete Telefonica Mobile il flusso di traffico generato da un'utenza assegnata ad un Utente, anche dietro presentazione di richiesta motivata da parte del Dirigente/Responsabile di Servizio o suo delegato da cui l'Utente, o il gruppo di Utenti, dipende, assolvendo in tal modo alla funzione di controllo mirato rispetto all'utilizzo dell'apparecchio.

Il SIC si riserva inoltre di effettuare d'ufficio tutti i controlli del caso qualora dall'esame del traffico telefonico relativo alle utenze attive venga rilevato uno scostamento significativo dalla media rilevata in precedenza.

## **G) DISPOSIZIONI FINALI**

---

### **28. Responsabilità degli Utenti**

Ciascun Utente dei Sistemi Informativi ha la responsabilità di segnalare immediatamente al SIC ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza riguardante le Risorse Informatiche, Telematiche e Telefoniche ad egli assegnate o comunque utilizzate.

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento costituisce illecito perseguibile disciplinarmente, fatte sempre salve le responsabilità civili e penali.

### **29. Entrata in vigore**

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

**A- Allegato**

**Presenza visione del Regolamento comunale per l'accesso ed utilizzo dei Sistemi Informativi, delle Risorse Informatiche, Telematiche e Telefoniche 2008**

Il/la sottoscritto/a

---

appartenente al Servizio/Società

---

con la funzione di

---

nella sua qualità di Utente dei sistemi e delle risorse stesse, con la presente

**DICHIARA**

di averne inteso il significato e di impegnarsi ad accettare e rispettare le regole ivi contenute, sotto la propria responsabilità penale, civile e disciplinare.

A tal fine chiede di essere autorizzato ad accedere ai seguenti sistemi/risorse:

---

---

---

---

---

Gambolò, \_\_\_\_\_

Firma \_\_\_\_\_