Regolamento sui sistemi informativi, l'utilizzo degli strumenti informatici e ICT, di internet e della posta elettronica del Comune di Sassari

Indice generale

Art. 1 – Finalità

Il presente Regolamento definisce i principi generali sull'utilizzo dei sistemi informativi e i criteri e le modalità operative di accesso ed utilizzo del servizio internet, di posta elettronica e degli strumenti informatici e telematici (ICT) del Comune di Sassari, al fine di assicurare la corretta fruizione degli strumenti stessi da parte degli utenti e un uso delle risorse razionale, efficiente e nei limiti dettati dalle norme e dalle direttive nazionali.

Art. 2 – Ambito di applicazione

Il presente regolamento si applica a tutti i dipendenti dell'Ente e a tutti gli utenti interni. Per dipendenti si intendono gli amministratori, i dirigenti, i dipendenti a tempo indeterminato e determinato, i collaboratori coordinati e continuativi e il personale con altre forme di rapporto di lavoro. Per utenti interni si intendono tutti quei soggetti che accedono, previa autorizzazione, alle dotazioni informatiche dell'Ente, come definite all'articolo 3, che non siano anche dipendenti dello stesso.

Art. 3 – Definizioni

(a) Comune, Amministrazione o Ente: il Comune di Sassari;
(b) Sistema Informativo: qualunque sistema di gestione delle informazioni che può includere uno o più sistemi informatici;
(c) Sistema Informatico: una componente di un sistema informativo per la gestione automatizzata delle informazioni e/o dei dati;
(d) Postazione di lavoro: l'hardware (personal computer, monitor, tastiera, ecc.) e/o il software forniti ad un assegnatario per l'espletamento delle proprie mansioni;
(e) Dotazioni o apparecchiature informatiche: l'hardware, il software ed i servizi informatici necessari per l'espletamento delle funzioni istituzionali dell'Ente;
(f) Assegnatario (o utente) di casella di posta elettronica ordinaria (PEO) o certificata (PEC): il soggetto fisico dipendente o meno dell'ente al quale è assegnata una casella di posta elettronica tradizionale o certificata. In caso di casella atta a rappresentare un ufficio, un soggetto giuridico, una carica istituzionale o comunque un soggetto non fisico si intende per "assegnatario" il soggetto fisico individuato come responsabile dell'uso di quella casella all'atto della richiesta della creazione della stessa. In caso non sia specificato l'assegnatario della casella nella richiesta di creazione o non possa evincersi dalla stessa è da intendersi per assegnatario il soggetto fisico richiedente. Un assegnatario può avere accesso esclusivo ad una casella oppure può individuare altri soggetti che abbiano accesso alla casella (delegati). In caso di casella assegnata ad una persona fisica l'assegnatario può avere accesso solamente esclusivo;
(g) Assegnatario (o utente) di una postazione di lavoro: il soggetto fisico cui è assegnata una postazione di lavoro. In caso di postazione di lavoro assegnata ad un Settore l'assegnatario è il dirigente dello stesso;
(h) Assegnatario (o utente) di una risorsa condivisa (es. cartella condivisa, cloud per la condivisione dei file, ecc.): il soggetto fisico individuato come responsabile dell'uso della risorsa che stabilisce, oltre alle posizioni organizzative o al dirigente del settore, quali altri utenti possono accedervi e con quali livello di accesso;

(i) Assegnatario (o utente): con tale termine in dipendenza del contesto si intende l’assegnatario di una casella di posta elettronica o posta elettronica certificata, di una postazione di lavoro o di una risorsa condivisa;
(j) “servizi di piattaforma o servizi orizzontali”: tutti i sistemi informatici, gli hardware, i software ed i servizi informatici e di telecomunicazioni all’interno dell’Ente non specifici di un particolare campo di applicazione ma il cui approvvigionamento, manutenzione ed evoluzione risulta obbligatorio per i servizi di applicazione;
(k) “servizi di applicazione o servizi verticali o applicazioni verticali”: tutti i sistemi informatici, gli hardware, i software ed i servizi informatici e di telecomunicazioni all’interno dell’Ente che, pur necessitando per il loro funzionamento dei servizi di piattaforma, sono peculiari di una particolare funzione dell’Ente e che richiedono per il loro uso la competenza e la conoscenza di quella funzione;
(l) Settore ICT: il Settore dell’Ente competente per i servizi ICT (Information and Comunication Tecnology) dell’ente;
(m) intranet: la connettività di rete e i servizi ad essa connessi nell’ambito della rete privata (interna) dell’amministrazione;
(n) internet: la connettività di rete ed i servizi ad essa connessi nell’ambito della rete pubblica internet;
(o) Posta elettronica: quando non diversamente specificato per posta elettronica è inteso sia il servizio di posta elettronica ordinaria (PEO) che quello certificato (PEC);
(p) GDPR: il Regolamento (UE) 2016/679 del Parlamento europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
(q) CAD: il Codice dell'Amministrazione Digitale.

Art. 4 – Principi Generali

L’Amministrazione promuove l’utilizzo degli strumenti informatici, della rete informatica e telematica, delle tecnologie digitali, di Internet e della posta elettronica, quali strumenti utili a perseguire con efficacia ed efficienza le proprie finalità istituzionali, rendere l'azione amministrativa più snella, efficiente e trasparente, migliorare la qualità dei servizi offerti in accordo con le linee guida e i principi delineati dalla normativa vigente e agevolare il lavoro degli utenti/dipendenti dell’amministrazione.
L’Amministrazione adotta ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri delle strumentazioni informatiche e telematiche di sua proprietà.
Gli strumenti informatici e telematici assegnati agli utenti sono strumenti di lavoro e come tali non devono essere usati per fini diversi dalla normale attività lavorativa. Ogni utente risponde, civilmente e penalmente, del corretto uso delle risorse informatiche, dei servizi/programmi/apparati informatici a cui ha accesso e dei dati trattati a fini istituzionali. E' altresì responsabile del contenuto delle comunicazioni effettuate e ricevute a fini istituzionali anche per quanto attiene la riservatezza dei dati ivi contenuti, la cui diffusione impropria potrebbe configurare violazione del segreto d'ufficio o della normativa per la tutela dei dati personali. Sono perseguiti i comportamenti che possono creare un danno, anche di immagine, all'Ente.

Art. 5 – Settore ICT (Information and Communications Technology) o TIC (Tecnologie dell'Informazione e della Comunicazione)

All’interno delle macrostruttura dell’Ente è individuato un Settore per i servizi ICT (information and communications technology), l’innovazione tecnologica e la digitalizzazione. Tale Settore è competente, dal punto di vista tecnico, sia per i servizi di piattaforma che per i servizi di applicazione come definiti all’Art.3.
In tale Settore vanno individuati i servizi ICT afferenti a differenti ambiti tecnologici. La responsabilità di tali servizi è attribuita a funzionari in possesso di comprovata competenza, esperienza e titoli di studio nell’ambito delle materie informatiche e di telecomunicazioni e della normativa vigente in ambito di digitalizzazione dei processi e di E-Gov per le pubbliche amministrazioni.

Per i sistemi informativi che non siano di competenza dell’Ente (es. sistemi dell’Autorità Nazionale Anticorruzione, sistemi telematici per la verifica della regolarità contributiva delle aziende ecc.) il Settore garantisce comunque supporto nell’interlocuzione con i soggetti esterni in presenza di problematiche di natura tecnico – specialistica.

Art. 6 – Referenti tecnologici dei Settori dell’Ente

Ciascun dirigente nomina, all’interno del proprio Settore, uno o più referenti tecnologici allo scopo di semplificare la gestione dei servizi ICT e favorire la diffusione delle nuove tecnologie.
L'individuazione dei referenti dovrà essere operata tra i dipendenti del Settore che vengano ritenuti dal dirigente maggiormente competenti all'uso delle tecnologie. Non è richiesta una competenza certificata.
Il referente tecnologico è chiamato a svolgere le seguenti attività:

(a) Interloquire con il personale del Settore ICT per le richieste di assistenza inoltrate dai dipendenti del proprio Settore, secondo le modalità stabilite dal Settore ICT, in modo da ottimizzare i tempi di risoluzione delle problematiche;
(b) Partecipare ad incontri o iniziative formative nell'ambito delle nuove tecnologie promosse dal Settore ICT;
(c) Fungere da primo riferimento per il personale del proprio Settore per le problematiche relative alle nuove tecnologie facendosi anche promotore, nel lavoro quotidiano, della diffusione della conoscenza delle stesse verso i colleghi;
(d) Svolgere altri compiti conferiti dal dirigente riguardanti la digitalizzazione dei processi e procedimenti;

Art. 7 – Assistenza tecnica agli utenti

L’assistenza tecnica sulla strumentazione software e hardware di competenza del Settore ICT è richiesta dagli utenti, di norma, mediante meccanismi centralizzati predisposti dal Settore ICT (es. sistema di gestione ticket automatizzato) che permettano il tracciamento delle richieste e il bilanciamento dei carichi di lavoro, scegliendo opportunamente la categoria, indicando chiaramente il tipo di inconveniente riscontrato ed ogni tipo di informazione utile a diagnosticare il problema.
Eccezionalmente, nei casi di urgenza non compatibili con il sistema automatizzato, l’assistenza tecnica può essere richiesta anche in via informale a mezzo mail o comunicazione diretta.

La richiesta di assistenza viene presa in carico nell'immediatezza dando riscontro al richiedente e viene evasa dall'addetto del Settore ICT che può contattare tanto il richiedente quanto il referente tecnologico del Settore come definito nell'articolo 6.

Le richieste di assistenza vengono evase in ordine di ricezione e nel più breve tempo possibile, compatibilmente con il tipo di problema segnalato, dando priorità agli interventi che coinvolgono più utenti o che mettono a rischio la continuità dei servizi erogati ai cittadini.

Gli Amministratori di Sistema possono accedere ai dispositivi informatici del Comune sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'Utente;
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
- richiesta di aggiornamento software e manutenzione preventiva hardware e software.

Gli interventi possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento in loco o in remoto non necessiti di accedere mediante credenziali utente, gli Amministratori di sistema sono autorizzati ad effettuare gli interventi senza il consenso dell'utente a cui la risorsa è assegnata. L'accesso in teleassistenza ai computer della rete del Comune richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento. Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o il "Referente tecnologico del settore" definito nell'Art.6. deve presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento o alle disposizioni di legge.

Art. 8 – Utilizzo delle postazioni di lavoro (hardware e software)

1. La postazione di lavoro è generalmente costituita da un Computer (desktop o notebook), dalle periferiche ad esso collegate (monitor, tastiera, mouse, lettore smart card, stampante, ecc), dal software installato nel computer, da tutti i software e le risorse centralizzate per il quale l'utente è autorizzato all'utilizzo (per estensione) e dall'apparecchio telefonico.

2. L'assegnatario è responsabile della cura della propria postazione di lavoro ed è tenuto a porre in essere ogni azione in suo potere per impedire deterioramenti o danneggiamenti della stessa.

3. Nel caso di assegnazione di computer portatili (notebook) gli utenti devono custodire gli stessi con diligenza, sia durante gli spostamenti che durante l'utilizzo nel luogo di lavoro. Quando vengono portati all'esterno dei locali dell'Ente questi devono essere custoditi in un luogo protetto e sicuro. Nel caso in cui gli utenti dovessero riscontrare furti, mancanze o anomalie nelle dotazioni informatiche e telematiche assegnate, devono darne immediata comunicazione al proprio responsabile, per la denuncia alle Autorità competenti.

4. La postazione ed ogni dotazione informatica dell'Ente sono strumenti di lavoro e il loro utilizzo deve essere finalizzato esclusivamente allo svolgimento delle attività professionali e istituzionali dell'Amministrazione. Qualsiasi utilizzo per fini diversi non è consentito. In particolare non è consentito conservare dati non pertinenti l'attività lavorativa sulle postazioni di lavoro (come definite

dal presente articolo) e l'Ente non assume responsabilità alcuna per il deterioramento o danneggiamento di tali dati.

5. L'utente non può conservare su una postazione di lavoro dati personali propri o di terzi a meno che ciò non sia indispensabile per lo svolgimento dell'attività lavorativa. In tal caso i dati, file o documenti digitali dovranno essere conservati tramite l'utilizzo dei "servizi di piattaforma o servizi orizzontali" e/o dei "servizi di applicazione o servizi verticali o applicazioni verticali" come definiti all'Art.3 o tramite l'utilizzo di risorse condivise centralizzate (es. cartella documentale centralizzata, cartelle condivise). In nessuno caso è consentita l'archiviazione di dati, file e documenti digitali in modo esclusivo nel computer assegnato. È consentita solo l'archiviazione locale di copie già presenti nei sistemi centralizzati al fine di proteggere opportunamente il patrimonio informativo dell'Ente.

6. All'utente non è consentito apportare autonomamente modifiche sia hardware che software alla postazione di lavoro. Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica. È vietato, inoltre, installare modem o altri dispositivi che consentano il collegamento a reti diverse da quella indicata e configurata dall'amministrazione come rete di lavoro e in nessun caso è comunque consentito configurare e collegare la postazioni di lavoro a reti non esplicitamente autorizzate.

7. L'utente, con cadenza periodica esegue la pulizia degli archivi digitali di propria competenza, con la cancellazione dei file inutili o obsoleti al fine di evitare la ridondanza e la duplicazione dei dati.

8. Nel caso di interventi di manutenzione sulle postazioni di lavoro da parte dei tecnici incaricati, va sempre garantita la presenza dell'assegnatario o del referente tecnologico o, in loro assenza, di altro dipendente del settore.

9. È responsabilità di ogni dirigente, nell'ambito dei propri settori, verificare il coerente utilizzo delle risorse assegnate ed evitarne l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato.

10. Durante l'utilizzo della postazione di lavoro (strumenti informatici e telematici) inoltre non è consentito:
    - adottare comportamenti che possano determinare danni economici e di immagine dell'Ente;
    - accedere e modificare le impostazioni del BIOS o UEFI;
    - accedere ad un personal computer o a qualunque sistema con credenziali diverse dalle proprie;
    - installare e/o duplicare qualunque software, anche se libero, non fornito o autorizzato dal Settore ICT;
    - installare software non autorizzato finalizzato ad alterare la funzionalità del collegamento in rete della stazione di lavoro o ad eludere o ingannare i sistemi di controllo di accesso e/o di sicurezza di qualsiasi sistema informatico o informativo interno o pubblico;
    - installare o eseguire programmi che possano determinare un danneggiamento o un sovraccarico dei sistemi e/o della rete;
    - alterare le funzionalità (es. indirizzi e protocolli di rete) del collegamento in rete della postazione di lavoro;

- apportare modifiche hardware alla postazione di lavoro in dotazione;
- archiviare/memorizzare dati, file e documenti digitali e informatici contrari alle vigenti norme di legge;
- archiviare/memorizzare dati, file e documenti digitali e informatici in forma crittografata senza preventiva autorizzazione del Settore ICT;
- inibire o sospendere, anche temporaneamente, il funzionamento del software antivirus e di qualunque altro software o sistema di sicurezza e protezione attivato nella postazione di lavoro;
- utilizzare sistemi di scambio file (es. google document, MS onedrive, wetransfer, ecc.), diversi da quelli messi a disposizione dall'amministrazione (es. posta elettronica, cloud, ecc), per inoltrare dati, file e documenti digitali e informatici verso l'esterno;
- utilizzare dispositivi di memorizzazione rimovibili (es. dischetti, dischi esterni, memorie USB ecc.) per inoltrare o ricevere dati, file e documenti digitali e informatici all'esterno se non espressamente autorizzati dal settore ICT per comprovate esigenze di servizio;
- connettere alla rete dell'amministrazione apparati e dispositivi atti ad effettuare connessioni con reti esterne (es.: router, bridge, modem, access point wireless, telefoni cellulari, smartphone, etc.);
- configurare autonomamente i servizi essenziali già resi in modo centralizzato (es.:DNS, WINS, DHCP, NTP, FTP, HTTP/HTTPS, posta elettronica, accesso remoto, proxy server, etc.);
- intraprendere comportamenti che possano influenzare negativamente la regolare operatività della rete e ne l'imitino l'utilizzabilità e/o le prestazioni per gli altri utenti;
- ogni altro utilizzo non inerente l'attività lavorativa.

12. È vietato utilizzare risorse informatiche e telematiche private (es PC, notebok, tablet, smartphone, periferiche etc.) direttamente e fisicamente collegate alla rete indicata e configurata dall'amministrazione come rete di lavoro.

Art. 9 – Utilizzo dei dispositivi di telefonia mobile e smartphone

L'assegnatario dei dispositivi di telefonia mobile o smartphone e relativa SIM è responsabile di tenere con cura il dispositivo e di intraprendere ogni azione in suo potere per impedire deterioramenti o danneggiamenti dello stesso. Tutte le attività non espressamente previste nei relativi contratti di fornitura di beni e servizi (es. aggiornamento software, backup, ripresa dati, configurazioni varie ecc.) sono a carico e sotto la responsabilità dell'assegnatario.
L'assegnazione, la consegna iniziale e la restituzione, in caso di modifica o cessazione del rapporto con l'amministrazione, dei dispositivi avverrà secondo le modalità stabilita del Settore ICT.

Art. 10 – Gestione delle password e degli account

L'account, ovvero le credenziali con le quali viene consentito l'accesso all'insieme di funzionalità, strumenti e contenuti di uno specifico sistema o contesto operativo, è costituito da un codice identificativo personale (username o user id), da una parola chiave (password) ed eventualmente uno strumento di seconda autenticazione (generatore di one time password o altri) o uno strumento hardware da agganciare alla postazione (es. carta nazionale dei servizi o simili). Tali strumenti rimangono nella disponibilità dell'utente e non possono essere ceduti a terzi. Ad ogni account è

associato sempre un profilo che identifica le operazioni che è possibile eseguire all'interno dello specifico contesto operativo.
Per la corretta gestione delle credenziali di autenticazione è necessario osservare le seguenti regole:

- Le password sono personali e segrete e devono rispettare i criteri minimi previsti dai sistemi (es. lunghezza minima, presenza di caratteri speciali, ecc.), devono essere modificate periodicamente e possibilmente devono essere costituite da almeno un carattere numerico, almeno un carattere non alfabetico (caratteri speciali es. $,* ,% ecc), con lunghezza pari ad almeno otto caratteri e non devono contenere riferimenti agevolmente riconducibili all'utente. Le password hanno, di norma, una durata massima configurabile da sistema.
- L'utente, dopo il primo accesso ai sistemi, provvederà a modificare la password che quindi non potrà essere nota a nessun altro e dovrà aver cura che nessuno possa anche accidentalmente venirne a conoscenza. L'utente è responsabile di abusi o incidenti di sicurezza nel caso in cui non custodisca adeguatamente le proprie credenziali.
- Nel caso in cui si sospetti che una password abbia perso la sua riservatezza, l'utente provvederà ove possibile a modificarla personalmente, altrimenti provvederà a modificarla con il supporto dell'Amministratore di Sistema.
- E' esplicitamente vietato, anche su richiesta o indicazione del titolare, utilizzare l'account e in generale le credenziali di accesso e quindi il profilo personale di altri soggetti per utilizzare qualunque sistema informativo, informatico o in ambito ICT.
- Nel caso l'utente venisse a conoscenza delle credenziali di accesso (account e password o altro sistema adottato) di un altro utente, è tenuto a darne immediata notizia all'Amministratore di Sistema competente.

Nel caso di inserimento di password errata, dopo un numero di tentativi dipendenti dal contesto informatico di utilizzo, il profilo dell'utente potrebbe venire disabilitato e in questo caso sarà possibile richiederne le riattivazione all'Amministratore di Sistema competente tramite le procedure previste dal Settore ICT. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
É compito dei dirigenti comunicare tempestivamente al Settore ICT eventuali cambi di mansione dei dipendenti assegnati che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche o in generale ai sistemi ICT. Provvedono inoltre a richiedere, per ogni dipendente del proprio settore, che ci sia almeno un altro dipendente con profilo autorizzativo equivalente allo scopo di permettere la continuità operativa in assenza del primo.

Art. 11 – Inizio del rapporto di lavoro

Nel momento in cui viene formalizzato l'inizio del rapporto di lavoro di un soggetto, il settore competente per la gestione del personale, lo comunica formalmente al Settore ICT secondo le modalità digitali stabilite e quindi mediante i meccanismi centralizzati predisposti dal Settore ICT (es. sistema di gestione ticket automatizzato) che procederà con le seguenti attività:

i. assegnazione dell'account di dominio
ii. assegnazione di una casella di posta elettronica (PEO)

Il responsabile di servizio, una P.O. o il Dirigente del settore a cui viene assegnato l'utente dovrà procedere alla richiesta, mediante i meccanismi centralizzati predisposti dal Settore ICT (es. sistema di

gestione ticket automatizzato), delle specifiche abilitazioni necessarie per lo svolgimento dell'attività lavorativa ovvero per gli ulteriori "servizi di piattaforma o servizi orizzontali" (Art.3) (es. navigazione internet, cloud, ecc.), i necessari "servizi di applicazione o servizi verticali o applicazioni verticali" (Art.3) (es. protocollo, gestione atti, finanziaria, risorse condivise ecc.).

Art. 12 – Modifica o cessazione del rapporto di lavoro

Di norma l'assegnazione della strumentazione che costituisce la postazione di lavoro (come definita all'Art.8 e quindi comprensiva anche dell'apparecchio telefonico) decade in caso di spostamento ad altro settore dell'Ente, fatti salvi accordi diversi tra i dirigenti dei settori coinvolti e il dirigente del Settore ICT opportunamente formalizzati.

L'assegnatario in caso di:

(a) trasferimento ad altro Settore all'interno dell'Ente;
(b) cambio di assegnazione della strumentazione della postazione di lavoro ad altro assegnatario;
(c) cessazione del rapporto di lavoro con l'Ente o pensionamento.

Prima della restituzione della strumentazione della postazione di lavoro, è tenuto a:

i. comunicare tutte le informazioni relative all'ubicazione nei sistemi centralizzati di tutti i dati concernenti l'attività lavorativa al proprio responsabile o al soggetto che, in accordo alla normativa, è deputato a trattarli, cancellando le eventuali copie presenti nella postazione stessa;
ii. cancellare eventuali altri dati personali propri o di terzi e non personali che dovessero risultare ancora presenti;
iii. ottenere, su specifica richiesta e nel caso di cessazione dal rapporto di lavoro, copia delle e mail associate al proprio profilo.

Trascorsi quindici giorni dalla data di modifica o cessazione del rapporto con l'Ente, l'Amministrazione può provvedere alla formattazione/cancellazione delle aree di memorizzazione sia in locale che di rete.

In caso di postazione di lavoro non assegnata a nessun utente specifico, l'assegnatario temporaneo sarà il dirigente del settore in cui è fisicamente ubicata la postazione. Trascorsi quindici giorni senza che la postazione sia assegnata ad un nuovo utente, il dirigente deve comunicare formalmente al Settore ICT la disponibilità della postazione di lavoro per l'assegnazione ad un utente appartenente ad altro settore dell'Ente.
Nel caso di assegnazione di una nuova unità, il Settore ICT provvede a fornire la necessaria dotazione informatica, previa verifica della disponibilità, entro 10 giorni dalla richiesta.

In tutti i casi in cui si verifichi un trasferimento interno alla struttura o cessazione del rapporto con l'ente, il settore competente per la gestione del personale, lo comunica formalmente al Settore ICT secondo le modalità digitali stabilite e quindi mediante i meccanismi centralizzati predisposti dal Settore ICT (es. sistema di gestione ticket automatizzato).

Il Settore ICT procede, quindi, secondo le seguenti modalità:

(a) Nel caso di assegnazione ad altro settore verranno disattivate tutte le abilitazioni dell'utente relative ai "servizi di applicazione o servizi verticali o applicazioni verticali" definite all'Art.3 comprese quelle relative ai portali e alle banche dati esterne le cui credenziali di accesso sono gestite dal Settore ICT. Resteranno valide le abilitazioni ai "servizi di piattaforma o servizi orizzontali" (es. utente di dominio e posta elettronica)
(b) Nel caso di cessazione del rapporto tutti gli account relativi all'utente verranno disabilitati e/o eliminati

Resta in capo al "Responsabile della risorsa condivisa" (Art.16) di ogni cartella di rete o risorsa condivisa, a cui l'utente per il quale è sopraggiunta la modifica o la cessazione del rapporto è abilitato, richiedere la modifica o eliminazione dei permessi di accesso.

Nel caso di assegnazione ad altro settore sarà competenza e responsabilità del Dirigente, di una P.O. o del responsabile di servizio procedere alla richiesta delle specifiche abilitazioni necessarie per lo svolgimento dell'attività lavorativa ovvero per gli ulteriori "servizi di piattaforma o servizi orizzontali" (Art.3) (es. navigazione internet, cloud, ecc.) e i necessari "servizi di applicazione o servizi verticali o applicazioni verticali" (Art.3) (es. protocollo, gestione atti, finanziaria, risorse condivise ecc.).

Art. 13 – Amministrazione e gestione delle risorse informatiche o ICT

Il Settore ICT è incaricato di monitorare la corretta attuazione, da parte di tutti i soggetti coinvolti, delle disposizioni contenute nel presente Regolamento.
Gli Amministratori di Sistema sono i soggetti a cui è conferito il compito di sovrintendere alle risorse informatiche, telematiche e ICT dell'Amministrazione. Il Dirigente del Settore ICT nomina e revoca gli Amministratori di Sistema.
Nessun utente, ad eccezione degli Amministratori di Sistema, può disporre della password di amministrazione dei PC messa a propria disposizione o di qualunque altro sistema informatico, di rete o in ambito ICT.

Art. 14 – Utilizzo della rete internet

1. L'utilizzo di Internet deve essere destinato esclusivamente a scopi inerenti l'attività lavorativa. Un utilizzo personale è consentito, solo eccezionalmente e per un tempo limitato, anche al fine di consentire ai dipendenti di assolvere incombenze amministrative e burocratiche senza allontanarsi dai luoghi di lavoro, in conformità ai seguenti principi:
    - Assenza di aggravio diretto di spesa per l'amministrazione;
    - Assenza di interferenza con i tempi di lavoro condivisi con colleghi e collaboratori;
    - Assenza delle attività non consentite di cui al successivo punto 2.

   In tali casi, comunque, l'Ente, non è responsabile in alcun modo di danni causati a terzi o al soggetto che ha utilizzato Internet per scopi non istituzionali.
2. Nell'ambito dell'uso personale di Internet non sono comunque consentite le attività che interferiscono con l'efficienza e le funzionalità dei sistemi informativi.

3. L'Amministrazione, al fine di ridurre il rischio di usi impropri e/o non consentiti della navigazione in Internet che possono consistere in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti o l'uso di servizi potenzialmente dannosi e che potrebbero essere illegali e puniti dalla legge penale, oltre che essere causa di danno patrimoniale per l'amministrazione, applica in maniera preventiva politiche di filtraggio all'accesso (URL filtering).
   L'Amministrazione si riserva di modificare le categorie e i siti da bloccare/autorizzare e la creazione di profili di navigazione personalizzati per gruppi di utenti o per settori, a seconda dell'attività professionale svolta o sulla base di richieste specifiche.
4. Per motivi tecnici e di buon funzionamento del sistema informatico e della rete telematica è opportuno, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante la banda di trasmissione (filmati tratti da youtube, siti di informazione, siti di streaming o web radio).

Art. 15 – Utilizzo della Posta Elettronica

La posta elettronica, sia ordinaria (PEO) che certificata (PEC), è assunta, per il Comune di Sassari, quale strumento ordinario per tutte le comunicazioni.
Il Comune di Sassari fornisce un servizio di posta elettronica (PEO), mettendo a disposizione indirizzi con estensione @comune.sassari.it; gli indirizzi possono corrispondere a caselle di posta elettronica individuali o a liste di distribuzione che inoltrano i messaggi ricevuti a più caselle di posta elettronica personali. Il servizio di posta elettronica è uno strumento di lavoro e deve essere utilizzato per lo svolgimento di attività connesse agli incarichi lavorativi e/o istituzionali. Il database di posta è di esclusiva proprietà dell'Ente. Il personale del Settore ICT per motivi tecnici e di sicurezza, in particolare per prevenire o correggere malfunzionamenti, può accedere al suo contenuto nel rispetto della normativa vigente.
L'amministrazione rende disponibile un servizio di posta elettronica certificata (PEC), mettendo a disposizione caselle i cui indirizzi hanno estensione @pec.comune.sassari.it. Le caselle PEC assegnate a singoli individui devono essere richieste secondo le procedure previste dal Settore ICT fornendo la necessaria documentazione (es. codice fiscale, copia del documento d'identità) per associarla univocamente ad una persona fisica. Nel caso di PEC associate a servizi, settori o istituzionali la richiesta dovrà essere corredata della documentazione necessaria ad identificare il responsabile.

Nell'utilizzo del servizio di posta elettronica, sia PEO che PEC, si richiede l'osservanza delle seguenti norme comportamentali:

- L'uso della posta elettronica aziendale è consentito esclusivamente per motivi attinenti allo svolgimento delle funzioni assegnate L'utente è consapevole che i contenuti della posta elettronica dell'Ente non devono avere carattere privato o personale, ma devono riguardare esclusivamente questioni connesse all'attività lavorativa;
- Allo scopo di utilizzare totalmente e al meglio le funzionalità dei sistemi di posta elettronica (PEO e PEC) resi disponibili dall'amministrazione, gli utenti sono tenuti a leggere le istruzioni d'uso (guida in linea, guida utente, ecc.) disponibili all'interno degli stessi sistemi;
- Al fine di un impiego razionale dello spazio disponibile per la memorizzazione, ogni utente è soggetto a limiti di utilizzazione. Il sistema avvisa l'utente all'approssimarsi del raggiungimento della quota limite impostata. Quando la quota viene superata non è più possibile inviare o ricevere messaggi fino a quando non viene liberato spazio sufficiente;

- L’utente è tenuto a controllare periodicamente la propria casella elettronica; verificare l'arrivo di nuovi messaggio; cancellare i messaggi obsoleti o inutili; verificare lo spazio occupato; prestare attenzione ai messaggi di quota raggiunta; ripulire la casella di posta prima del raggiungimento della quota massima consentita ovvero sono tenuti ad eseguire tutte le azioni necessari per minimizzare lo spazio di occupazione delle caselle e impedire la perdita di messaggi istituzionali che debbano essere conservati finché gli stessi hanno rilevanza istituzionale. In particolare l’utente provvede a cancellare i messaggi di spam o di non rilevanza istituzionale al fine di minimizzare l’occupazione di spazio sul server e a valutare i messaggi ricevuti o spediti secondo le norme sulla gestione documentale al fine di inviarli alla protocollazione.
- Limitare la dimensione dei messaggi inviati, soprattutto nel caso di destinatari multipli. Un allegato di grandi dimensioni potrebbe impedire il corretto smistamento del messaggio o richiedere un uso eccessivo delle risorse;
- È richiesto, nei messaggi inviati, di riportare in calce la firma del soggetto mittente contenente, al minimo: nome e cognome, Settore e Servizio di appartenenza;
- È necessario porre particolare attenzione ad aprire allegati contenenti programmi “eseguibili” o comunque potenzialmente pericolosi e ad utilizzare collegamenti presenti come allegati o nel corpo dei messaggi;
- È illecito scambiare messaggi sotto falsa identità, ovvero impersonando un altro mittente;
- Poiché la posta elettronica diretta all’esterno della rete informatica comunale può essere intercettata da estranei, l’invio tramite tale mezzo di documenti di lavoro "strettamente riservati" è sconsigliato e comunque va valutato con particolare attenzione;
- Alla cessazione dell’attività lavorativa presso il Comune, la casella di posta elettronica del dipendente sarà disattivata e successivamente eliminata, è pertanto opportuno salvare o inoltrare ad altri i messaggi che fossero necessari per le successive esigenze lavorative del servizio prima delle dimissioni;
- In caso di cessazione del rapporto di lavoro con l’Ente, pensionamento o disabilitazione di una casella di posta elettronica tradizionale o certificata l’assegnatario, almeno dieci giorni prima di uno degli eventi sopra elencati è tenuto a trasferire i dati di interesse istituzionale al proprio responsabile o al soggetto che, in accordo alla normativa, è deputato a trattarli e a cancellare eventuali altri dati personali propri o di terzi e non personali ancora presenti. L’assegnatario informa tramite il sistema informativo interno il Settore ICT dei suddetti trasferimenti e cancellazioni di dati attestando che è possibile procedere alla cancellazione della casella. In ogni caso l’Amministrazione provvede alla cancellazione della casella di posta trascorsi 15 giorni. In caso di casella di posta elettronica tradizionale (PEO) o certificata (PEC) atta a rappresentare un ufficio, servizio o Settore dell’Ente, al presentarsi di uno degli eventi sopra elencati, è individuato come assegnatario della casella di posta il nuovo responsabile dell’ufficio, servizio o Settore;
- L’utilizzo della casella di posta elettronica per l’invio di dati, documenti e informazioni deve essere sempre compatibile con quanto previsto nel GDPR.

Art. 16 – Utilizzo della risorse condivise

Al fine di garantire la disponibilità dei dati e un’efficace politica di backup, gli utenti devono salvare nelle cartelle di rete o risorse condivise (es. Cartella Documentale Centralizzata, cartelle condivise centralizzate) tutti i file di lavoro ed astenersi dal salvarli esclusivamente sul disco locale della

postazione di lavoro non sottoposto a procedure centralizzate di backup. Le cartelle di rete o risorse condivise sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.
Per tali risorse, salva diversa indicazione, vengono svolte regolari attività di amministrazione e backup.
Gli Amministratori di Sistema, nell'espletamento delle mansioni attribuitegli dal dirigente del Settore ICT (Responsabile dei Sistemi Informativi), possono in qualunque momento procedere alla rimozione di ogni file o applicazione che ritengano pericolosi per la sicurezza, sia sui PC sia sui server.
Per ogni cartella di rete o risorsa condivisa centralizzata viene identificato, all'atto della creazione, il "Responsabile della risorsa condivisa" che dovrà partecipare alla corretta gestione delle risorse stesse:

- verificandone la coerenza con i trattamenti individuati a norma di legge;
- verificando ed eventualmente variando, avvalendosi degli Amministratori di Sistema, i permessi di accesso a tali risorse affinché siano coerenti con le mansioni del personale autorizzato.

Le attività consentite al "Responsabile della risorsa condivisa" sono altresì consentite alle P.O. e al dirigente del settore di appartenenza.

Art. 17 – Utilizzo della rete Wi-Fi

All'interno degli stabili dell'amministrazione può essere presente una rete Wi-Fi pubblica destinata ai cittadini e/o agli "ospiti" dell'ente per consentire la navigazione internet. Il servizio reso disponibile dall'Ente prevede un servizio di connettività WiFi per ospiti non pre-censiti (ad es. cittadini/turisti) che saranno in grado di auto-registrarsi al servizio e navigare secondo le policy impostate utilizzando ad esempio l'autenticazione tramite "Social Login".
Il servizio di autenticazione, tracciamento e connessione verso internet è affidato ad un fornitore di servizio nell'ambito del Servizio Pubblico di Connettività (SPC). La conservazione dei log delle sessioni degli utenti autenticati (nel pieno rispetto delle normative legate alla privacy), nonché il tracciamento dei log, verrà effettuata dalla società che agisce in qualità di WISP ufficialmente registrato presso AGCOM ai sensi della normativa vigente in materia. Le informazioni verranno conservate esclusivamente per scopi di sicurezza e di tutela in merito all'erogazione del servizio. Il fornitore di servizio si impegna a rispettare le normative italiane in termini di trattamento dei dati, di rafforzare tutti i processi e i meccanismi di gestione dei dati in maniera da garantire il massimo livello di sicurezza e protezione dei dati degli utilizzatori del servizio.

All'interno degli stabili dell'amministrazione può essere presente una rete Wi-Fi privata ovvero di "lavoro" destinata agli utenti dell'amministrazione (come definiti all'Art.3) a cui si applicano, in prima istanza, tutte le regole stabilite per la rete cablata dell'amministrazione.

Art. 18 – Acquisto di dotazioni informatiche o ICT

L'acquisizione di beni e servizi in ambito ICT (prodotti informatici sia hardware che software, telematici, ecc.) prevede le seguenti modalità operative:

(a) Ogni anno, entro il mese di settembre, i dirigenti di tutti i settori comunicano al dirigente del Settore ICT e al dirigente nominato "Responsabile per la transizione al digitale" le proprie necessità per l'anno successivo, al fine di permettere la redazione di un "Piano Generale di Acquisizione di beni e servizi ICT" e l'eventuale aggiornamento e armonizzazione con il "Piano Triennale per l'informatica" previsto dal CAD;

(b) In caso di impreviste e urgenti esigenze, il dirigente del settore interessato formalizza la richiesta al dirigente del Settore ICT che valuterà dal punto di vista tecnico la congruità della richiesta pervenuta e verificata l'adeguata copertura finanziaria avvierà le adeguate procedure di acquisto.
(c) Per ragioni di sicurezza, efficienza, efficacia, omogeneità del sistema informatico e telematico e per garantire la compatibilità funzionale, tecnica ed il mantenimento dell'efficienza operativa dei sistemi e delle reti è necessario che, nei casi in cui il Settore ICT non abbia sui propri capitoli di spesa sufficiente copertura finanziaria, le acquisizione di beni e servizi anche in ambito ICT vengano svolte da altri settori previa valutazione e formale approvazione tecnica del Settore ICT e del dirigente nominato "Responsabile per la transizione al digitale". In tale caso il Settore ICT garantisce un riscontro entro 3 giorni dal ricevimento della richiesta.
(d) Al fine di consentire la gestione ottimale delle risorse umane, economiche e tecnologiche è necessario coinvolgere il Settore ICT nella ideazione, pianificazione, progettazione e realizzazione di tutte la azione dell'Ente che coinvolgono il sistema informatico, la rete dati, il sistema di fonia, il sistema di videosorveglianza cittadino e/o qualunque sistema ICT dell'amministrazione in modo che possano essere effettuate tutte le analisi e le valutazioni in merito alla fattibilità, al carico di lavoro e alla tempistica.

Art. 19 – Dismissione apparecchiature informatiche

I settori dovranno procedere alla dismissione/smaltimento, delle apparecchiature informatiche e tecnologiche (PC, monitor, stampanti, ecc.) nella loro disponibilità per le quali sia intervenuta una dichiarazione di fuori uso o di obsolescenza da parte del Settore ICT, secondo quanto previsto dalla normativa (GDPR, Rifiuti di apparecchiature elettriche ed elettroniche (Raae), ecc) e secondo le procedure previste dal settore competente per la gestione del patrimonio dell'ente.
La dismissione e lo smaltimento dei dispositivi deve essere preceduta dall'eliminazione dei dati eventualmente memorizzati negli stessi.

Art. 20 – Principi generali per i dati personali raccolti dai sistemi informativi dell'Ente ed informativa agli utenti

Di seguito vengono descritti i principi applicabili al trattamento dei dati personali per i servizi di piattaforma (Art.3) dei sistemi informativi dell'Ente ed i relativi controlli. Per i servizi di applicazione (Art.3), ad esempio sistemi informatici di gestione del personale, possono essere raccolti e trattati altri dati personali e anche dati particolari sensibili e giudiziari di cui all'art. 9 e 10 del GDPR. L'adempimento degli obblighi normativi per tali trattamenti sono a carico dei settori competenti che ottemperano con atti propri.
L'informativa per gli utenti di cui agli art. 13 e 14 del GDPR viene fornita in allegato al presente regolamento e si intende nota agli utenti stessi con la pubblicazione del medesimo sul sito intranet dell'Ente.
Tutti i dipendenti incardinati nel Settore ICT sono autorizzati a trattare dati personali anche sensibili e giudiziari ai sensi del GDPR per lo svolgimento delle proprie funzioni.

Art. 21 – Dati personali raccolti nei sistemi informativi dell'Ente

Per tutti gli utenti che a qualsiasi titolo abbiano delle credenziali per accedere ai sistemi informatici o ICT dell'Ente sono raccolti, di norma, i seguenti dati: nome, cognome, codice fiscale, data e luogo di nascita, data ed ora dell'ultimo accesso.
Per i sistemi informatici facenti parte dei servizi di piattaforma e dei servizi di applicazione sono raccolti, per tutti gli utenti, dati personali e dati particolari sensibili e giudiziari di cui all'art. 9 e 10 del GDPR. I dati sono protetti con le seguenti misure minime:

(a) creazione di profili autorizzativi che permette solo ai soggetti autorizzati di accedere ai dati per compiti istituzionali
(b) salvataggio periodico ovvero backup dei dati.

I fornitori di servizi informatici sono individuati come responsabili del trattamento dei dati ai sensi dell'articolo 28 del GDPR.

Art. 22 – Dati relativi al traffico di rete (Intranet e Internet)

Il traffico Internet effettuato da ciascun utente attraverso la rete dell'amministrazione viene registrato automaticamente in file di log nei dispositivi di competenza dell'amministrazione e dal fornitore dei servizi di connettività internet. In particolare, tra le informazioni che vengono salvate vi sono: indirizzo IP sorgente, porta, siti web visitati, inizio e durata di ogni connessione, byte trasferiti.
Nel filtraggio del traffico internet (URL filtering) possono essere raccolti, tra gli altri, i file di log e l'elenco dei siti bloccati.
I file di log sono conservati, di norma, per un periodo di un anno tenendo conto anche delle soluzioni tecniche adottate.

Art. 23 – Dati raccolti dai sistemi di protezione degli Endpoint (antivirus, antimalware, ecc.) e di sicurezza perimetrale

I sistemi di protezione degli Endpoint (ovvero delle postazioni di lavoro) e di sicurezza perimetrale (protezione del perimetro interno/esterno della rete), allo scopo di permettere la configurazione delle politiche di sicurezza dei sistemi, possono raccogliere dati relativi alle minacce informatiche rilevate sui sistemi e sulle postazioni di lavoro inviando gli stessi a sistemi centralizzati per l'analisi delle minacce informatiche.

Art. 24 – Dati relativi alle comunicazioni mediante posta elettronica

Per i servizi di posta elettronica (PEO e PEC) gestiti direttamente dall'amministrazione o tramite fornitore di servizi, i dati personali inerenti le comunicazioni effettuate con tali strumenti, sono detenuti dai rispettivi gestori nel rispetto della normativa in materia di protezione dei dati personali (GDPR).

Art. 25 – Controlli e responsabilità

L'Amministrazione, per esigenze organizzative, produttive, di sicurezza e di tutela del patrimonio dell'Ente, si riserva di effettuare controlli sul corretto utilizzo di internet, della posta elettronica, delle

apparecchiature informatiche e di tutti i sistemi ICT nel rispetto delle normative vigenti e del presente regolamento.
Qualora durante tali controlli vengano rilevate anomalie nell'utilizzo degli strumenti informatici (strumenti ICT), l'Amministrazione procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente al presente regolamento, e riservandosi la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.
Controlli specifici e mirati, anche su base individuale, potranno essere effettuati nei seguenti casi:

(a) persistente utilizzo anomalo da parte degli utenti di una specifica struttura/area rilevabile attraverso il controllo anonimo e generalizzato nonostante sia stato notificato l'avviso a cessare tale comportamento;
(b) minacce all'integrità e/o alla sicurezza dei sistemi informativi per cui sia indispensabile la consultazione dei file di log al fine di individuare e eliminare l'anomalia;
(c) per la prevenzione e l'accertamento, in presenza di indizi, di illeciti civili, penali e amministrativi;
(d) indispensabilità dei dati di log rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
(e) obbligo di rispondere ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Art. 26 – Aggiornamento delle disposizioni e delle regole tecniche

Le disposizioni generali contenute nel presente Regolamento possono essere soggette ad aggiornamenti, integrazioni e/o correzioni, in relazione all’evolversi della tecnologia, all’entrata in vigore di sopravvenute disposizioni di legge o all’evolversi delle esigenze dell’Amministrazione.
Il Settore ICT è incaricato di emanare ed aggiornare le regole tecniche necessarie per l’ attuazione delle disposizioni di carattere generale contenute nel presente Regolamento.

Glossario

Access Point	L'access point (AP) è un dispositivo di rete che, collegato ad una rete LAN (Local Area Network) tramite uno switch, un router o una presa di rete, costituisce il punto di unione tra una rete cablata e i dispositivi dotati di schede di rete senza fili o Wi-Fi Più AP possono collegarsi direttamente tra loro in “mesh” per costituire una rete Wi-Fi più estesa. I nodi di una rete mesh sono tutti accomunati dallo stesso SSID, un acronimo di “service set identifier”, cioè il nome che identifica la nostra rete WiFi
Account	Creare o acquistare un account vuol dire fare una richiesta affinché vengano dati ad una persona le credenziali (es. user ID e password) con i quali l'utente può accedere ad un servizio. Gli esempi più noti sono: • l'account che si chiede ad un ISP per accedere ad Internet e alla posta elettronica • l'account che un amministratore di rete crea per fare in modo che un utente acceda al PC e ai servizi di rete
AGID	E’ l’agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell’Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica
Amministratori di sistema	Soggetti deputati a intervenire per garantire l’efficienza e la funzionalità di un determinato sistema informatico, aventi la possibilità di accedere a dati personali qualora l’accesso sia assolutamente necessario per raggiungere le finalità proprie del ruolo ricoperto
ANPR	Anagrafe nazionale della popolazione residente, è il registro anagrafico centrale del Ministero dell'interno della Repubblica Italiana
Antivirus	Programma in grado di riconoscere un virus presente in un file e di eliminarlo o di renderlo inoffensivo
API	Un insieme di procedure (in genere raggruppate per strumenti specifici) atte all'espletamento di un dato compito
Apparati attivi	Apparecchiature hardware collegate alla rete che ne permettono il funzionamento (es. router, switch)
Application Server	Server dedicato all’esecuzione di applicazioni alle quali fornisce servizi di tipo infrastrutturale. Nelle architetture software è il server in cui è localizzata la logica applicativa.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.

Aree condivise	Spazi di memorizzazione messi a disposizione degli utenti sui sistemi centralizzati per la condivisione e lo scambio di files
ATM	Sportello Bancomat
Attachment	File allegato: può essere un allegato alla posta elettronica o a qualsiasi software di gestione dei file
Backbone	Una dorsale di rete o backbone, in ambito ICT, è un collegamento ad alta velocità di trasmissione e capacità tra due server o router di smistamento informazioni e appartenente normalmente alla rete di trasporto di una rete di telecomunicazioni. Una dorsale è una linea logica che può essere fisicamente singola o multipla con la quale vengono interconnessi ad un livello superiore (facendoli confluire) parti di rete con velocità e capacità inferiore grazie a meccanismi di multiplazione.
Backup	Procedura per la duplicazione dei dati su un supporto distinto da quello sul quale sono memorizzati, in modo da garantirne una copia di riserva
Banda	Quantità di dati per unità di tempo che può viaggiare su una connessione. Nella “banda ampia” la velocità varia da 64 Kbps a 1,544 Mbps. Nella “banda larga” la comunicazione avviene a velocità superiori a 1,544 Mbps
Bootstrap del pc	Indica, in generale, l'insieme dei processi che vengono eseguiti da un computer durante la fase di avvio, in particolare dall'accensione fino al completo caricamento in memoria primaria del kernel (nucleo) del sistema operativo a partire dalla memoria secondaria
CAD	Il Codice dell'Amministrazione Digitale è il testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Istituito con il decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato.
CBILL	Identifica la piattaforma di incasso delle banche disponibile anche alla Pubblica Amministrazione. CBILL è fruibile da Home Banking o ATM ed è integrato a pagoPA.
CIE	La carta d'identità elettronica italiana è un documento di riconoscimento previsto in Italia dalla legge. Ha sostituito la carta d'identità in formato cartaceo nella Repubblica Italiana. La carta di identità elettronica attesta l'identità del
Client	In informatica, con client (in italiano detto anche cliente) si indica una componente che accede ai servizi o alle risorse di un'altra componente, detta server. In questo contesto si può quindi parlare di client riferendosi all'hardware o al

Cloud Computing	Il cloud computing (in italiano nuvola informatica) indica, in informatica, un paradigma di erogazione di servizi offerti su richiesta da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita. Indica un paradigma di erogazione di servizi offerti on demand da un fornitore ad un cliente finale attraverso la rete Internet. Il cloud è un modello che consente di disporre, tramite internet, di un insieme di risorse di calcolo (ad es. reti, server, storage, applicazioni e servizi) che possono essere erogate come un servizio
Comunicazioni Elettroniche	Scambio di informazioni tra due o più interlocutori che avvenga utilizzando mezzi di comunicazione basati su dispositivi elettronici quali ad esempio posta elettronica, sistemi di comunicazione istantanea, telefonia VoIP o cellulare
CONSIP	E’ la centrale acquisti della pubblica amministrazione italiana; è una società per azioni il cui unico azionista è il Ministero dell'economia e delle finanze del governo italiano ed opera nell’esclusivo interesse dello Stato
Cookie	Tradotto letteralmente significa biscotto. E’ un file memorizzato sul proprio computer che identifica il computer quando è collegato ad alcuni siti Internet
CSP	Cloud Service Provider–Fornitori di servizi in cloud
Data breach	Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati
Database	In informatica, il termine database, tradotto in italiano con banca dati, base di dati (soprattutto in testi accademici) o anche base dati, indica un archivio di dati, riguardanti uno stesso argomento o più argomenti correlati tra loro,
DNS (Domain Name System)	Sistema che gestisce gli indirizzi dei domini Internet e Intranet traducendo una richiesta human-friendly – un nome di dominio come www.comune.sassari.it , www.intranet.comuness.it o PC_Utente1 – e lo traduce in un indirizzo IP , come 212.210.147.8
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Dominio (nome di dominio)	Un nome di dominio, in informatica, è costituito da una serie di

	stringhe separate da punti, che identifica il dominio dell'autonomia amministrativa, dell'autorità o del controllo all'interno di internet. I nomi di dominio sono formati dalle regole e dalle procedure del Domain Name System (DNS). Qualsiasi nome registrato nel DNS (ad esempio *comune.sassari.it*) è un nome di dominio. Essi vengono utilizzati in diversi contesti di rete e in ambito specifico per la denominazione o l'indirizzamento. In generale, un nome di dominio rappresenta una risorsa Internet Protocol (IP), ad esempio un computer utilizzato per accedere a Internet (host), un server che ospita un sito web o il sito web stesso, oppure qualsiasi altro servizio comunicato tramite Internet. A differenza degli indirizzi IP, dove la parte più importante del numero è la prima partendo da sinistra, in un nome DNS la parte più importante è la prima partendo da destra: questa è detta dominio di primo livello (o TLD, Top Level Domain), per esempio ".it" o ".com".
Dominio Microsoft	Definizione di Microsoft: "un insieme di computer che condividono un database di risorse di rete e che vengono amministrati come un'unità con regole e procedure comuni" In termini molto semplici, un dominio è una rete di computer, LAN, MAN o WAN di un'organizzazione (ad esempio un'azienda o un ente pubblico o una scuola/università), ove la logica client-server è supportata, oltre che da connessioni fisiche e relativi protocolli (ad esempio il comune indirizzo IP), anche da regole (policy) di connessione logica di tipo autorizzativo (regole di sicurezza). In questo contesto, un client deve sottostare a procedure di autenticazione specifiche, definite da servizi che risiedono su un server. Queste procedure, che solitamente sottendono una gerarchia di profili (in termini di permessi e accessi alle risorse o ai sistemi), determinano l'appartenenza o meno al dominio, struttura di distribuzione e condivisione centralizzata.
Download	Il download, anche noto come “scaricamento”, indica in informatica l'azione di ricevere o prelevare da una rete telematica (ad esempio da un sito web) un file, trasferendolo sul disco rigido del computer o su altra periferica dell'utente. Nella maggior parte dei casi, il download di un file è la conseguenza di una richiesta più o meno trasparente da parte di un utente del sistema; l'azione inversa è invece detta upload.
E-mail	La posta elettronica, in inglese e-mail (abbreviazione di electronic mail), è un servizio Intranet/Internet grazie al quale ogni utente abilitato può inviare e ricevere dei messaggi utilizzando un computer o altro dispositivo elettronico (come palmare, smartphone, tablet) connesso in rete attraverso un proprio account di posta registrato

	presso un fornitore del servizio
EC	Ente Creditore, ovvero l'Ente beneficiario del pagamento, che di solito è una Pubblica Amministrazione, ma potrebbe anche essere, ad esempio, una società a controllo pubblico o un Gestore di Pubblico Servizio (es. mobilità, rifiuti, etc.).
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
File di log	File che registra attività di base, quali l'accesso ai dispositivi, e che è presente sui PC, server e dispositivi di rete
File server	In informatica, il termine file server si riferisce generalmente ad una macchina progettata per mettere a disposizione degli utilizzatori di una rete di computer dello spazio su un disco (disco singolo o composto da più dischi) nel quale sia possibile salvare, leggere, modificare, creare file e cartelle centralizzate, condivise da tutti oppure accessibili secondo regole o autorizzazioni generalmente assegnate dal gestore di rete organizza e gestisce. Tale macchina può essere un computer o un Network Attached Storage (NAS), cioè un apparecchio specificatamente studiato e costruito allo scopo. Per estensione il termine si riferisce anche al programma di tale macchina che si occupa di rendere disponibili i dati
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage
Firewall	Apparato di rete hardware o software che filtra tutto il traffico informatico in entrata e in uscita e che di fatto evidenzia un perimetro all'interno della rete informatica e contribuisce alla sicurezza della rete stessa. Apparato di protezione perimetrale della rete
Firma Digitale	Firma Digitale: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Firma Elettronica	«firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare - articolo 3 del Regolamento eIDAS (Regolamento Europeo) vedi CAD (decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni)

Firma Elettronica Avanzata	Vedi articoli 3 e 26 del Regolamento eIDAS (Regolamento Europeo) e CAD (decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni)
Firma Elettronica Qualificata	Vedi articoli 3 del Regolamento eIDAS (Regolamento Europeo) e CAD (decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni)
GDPR	Il Regolamento (UE) 2016/679 del Parlamento europeo del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
Hardware	L'hardware, traducibile in italiano come componente fisico, materiale informatico o supporto fisico (sigla HW, dall'inglese hard «duro, pesante» e ware «merci, prodotti», su imitazione del termine software), è la parte materiale di un computer, ovvero tutte quelle parti elettroniche, elettriche, meccaniche, magnetiche, ottiche che ne consentono il funzionamento; più in generale il termine si riferisce a qualsiasi componente fisico di una periferica o di una apparecchiatura elettronica, ivi comprese le strutture di rete; l'insieme di tali componenti è anche detto componentistica
Help Desk	In informatica e organizzazione aziendale l'help desk (termine mutuato dalla lingua inglese che letteralmente significa scrivania di aiuto ovvero supporto tecnico) è un servizio professionale aziendale, in buona parte orientato al problem solving, volto a fornire assistenza/supporto tecnico e/o informativo, all'utente/cliente, relativamente all'acquisto e/o utilizzo di prodotti elettronici o servizi informatici, con lo scopo dunque di fornire indicazioni o risolvere problemi su prodotti hardware come computer, apparecchiature elettroniche o software
ICT	Acronimo di “Information and Communications Technology”, in italiano “Tecnologie dell’Iinformazione e della Comunicazione” (in acronimo TIC), sono l'insieme dei metodi e delle tecniche utilizzate nella trasmissione, ricezione ed elaborazione di dati e informazioni (tecnologie digitali comprese).
Indirizzamento	Attività di assegnazione di indirizzi logici (es. indirizzo IP) ad apparati attivi
Integrità	La protezione contro la perdita, la modifica, la creazione o la replica non autorizzata delle informazioni ovvero la conferma che i dati trattati siano completi
Internet	Internet è una rete di telecomunicazioni ad accesso pubblico che connette vari dispositivi o terminali in tutto il mondo, rappresentando

	dalla sua nascita uno dei maggiori mezzi di comunicazione di massa (assieme a radio e televisione), grazie all'offerta all'utente di una vasta serie di contenuti potenzialmente informativi e di servizi. Si tratta di un'interconnessione globale tra reti di telecomunicazioni e informatiche di natura e di estensione diversa, resa possibile da una suite di protocolli di rete comune chiamata "TCP/IP" dal nome dei due protocolli principali, il TCP e l'IP, che costituiscono la "lingua" comune con cui i computer connessi a Internet (gli host) sono interconnessi e comunicano tra loro a un livello superiore indipendentemente dalla loro sottostante architettura hardware e software, garantendo così l'interoperabilità tra sistemi e sottoreti fisiche diverse
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi
Intranet	La Intranet è una rete locale (Local Area Network), o un raggruppamento di reti locali, usata all'interno di una organizzazione per facilitare la comunicazione e l’accesso alle informazioni. E’ una rete aziendale privata completamente isolata dalla rete esterna (Internet) a livello di servizi offerti (es. tramite LAN), rimanendo dunque a solo uso interno, comunicando eventualmente con la rete esterna e altre reti attraverso opportuni sistemi di comunicazione (protocollo TCP/IP, estendendosi anche con collegamenti WAN e VPN) e relativa protezione (es. firewall).
IP	Indirizzo che permette di identificare in modo univoco un dispositivo (es. computer. Server, switch, router ecc) collegato in rete. Si suddivide in due parti, la prima individua la rete dove si trova il dispositivo, la seconda individua il dispositivo all’interno di quella rete
IPSEC	E’ una collezione (insieme) di protocolli implementati che fornisce un metodo per garantire la sicurezza del protocollo IP, sia esso versione 4 sia 6, e dei protocolli di livello superiore (come ad esempio UDP e TCP), proteggendo i pacchetti che viaggiano tra due sistemi host (es. server), tra due security gateway (ad esempio router o firewall) oppure tra un sistema host e una security gateway
IUV	Identificativo Univoco Versamento ovvero il codice che identifica univocamente il pagamento all’interno di una Pubblica Amministrazione.
LAN	Local Area Network (LAN) (in italiano rete in area locale, o rete locale), in informatica e telecomunicazioni, indica una rete informatica di collegamento tra più computer, estendibile anche a

	dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.
Linee guida o policy	Regole operative tecniche e/o organizzative atte a guidare i processi lavorativi, decisionali e attuativi
Logging	Attività di acquisizione cronologica di informazioni attinenti all'attività effettuata sui sistemi siano essi semplici apparati o servizi informatici
Malware	Malware (abbreviazione dell'inglese malicious software, lett. "software malevole"), in informatica, indica un qualsiasi programma informatico usato per provocare un malfunzionamento più o meno grave dei sistemi e/o rubare di nascosto informazioni di vario tipo . In italiano viene anche comunemente chiamato codice maligno
MAN	In ambito ICT, la Metropolitan Area Network (MAN, in italiano: rete in area metropolitana o più semplicemente rete metropolitana) è un tipo di rete di telecomunicazioni con un'estensione limitata a un perimetro metropolitano. L'interconnessione di più MAN dà vita a reti WAN.
Misure minime di sicurezza	Le misure minime di sicurezza ICT emanate dall'AgID, sono un riferimento pratico per attuare il livello di sicurezza informatica delle pubbliche amministrazioni, al fine di contrastare le minacce informatiche più frequenti
Multicanalità	Possibilità di pagare attraverso diversi strumenti (carta di credito, conto corrente, bollettino postale, etc.) e canali (smartphone, web, ATM, punto fisico sul territorio, etc.).
NAS	Network Attached Storage è un dispositivo collegato alla rete la cui funzione è quella di rendere disponibili grandi spazi di memorizzazione di massa, è costituito da molteplici hardware di memorizzazione di svariate tipologie (es. dischi rigidi, SSD ecc.), all'interno della propria rete
OEM	Original Equipment Manufacturer (produttore di apparecchiature originali). Nella vendita del software applicativo e di sistema trova posto nell'ambito della politica delle licenze d'uso la cessione dei diritti di preinstallazione ai produttori e agli assemblatori di personal computer e sistemi server proprietari. La cosiddetta licenza OEM è rilasciata da importanti produttori di sistemi operativi, di programmi per la grafica, di antivirus. Tale accordo di licenza generalmente prevede la non trasferibilità dei diritti di licenza e altre limitazioni circa la non vendibilità del software separatamente dall'hardware.
Office automation	Software di produttività, si intendono gli applicativi a corredo delle mansione lavorativa ovvero l'Insieme del software necessario al

	lavoro d'ufficio. Prevede almeno un programma di videoscrittura, un foglio di calcolo, un software di presentazione ovvero software di produttività personale
Open data	Formato aperto: un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi
PagoPA	E' un sistema di pagamenti elettronici realizzato per rendere più semplice, sicuro e trasparente qualsiasi pagamento verso la Pubblica Amministrazione
Password	Parola Chiave che, congiuntamente allo user-id, consente l'accesso di un utente ad una rete, ad un PC, ad un sistema informatico, o ad un sito Internet
Path	Vedi "Percorso"
Pathname	Concatenazione ordinata del percorso di un file e del suo nome
PEC	La Posta Elettronica Certificata (PEC) è il sistema che consente di inviare e-mail con valore legale equiparato ad una raccomandata con ricevuta di ritorno, come stabilito dalla normativa
PEO	La Posta Elettronica Ordinaria, vedi definizione di e-mail
Percorso	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
Policy	Modello di configurazione e adattamenti da riferirsi a gruppi di utenti o a uso del software
Policy di riferimento	Documento tecnico che descrive lo stato attuale delle policy in uso, aggiornato periodicamente in funzione dell'evoluzione tecnologica/organizzativa
PSD	Payment Services Directive ovvero la direttiva europea e la relativa normativa nazionale di recepimento, alle quali devono sottostare i sistemi di pagamento.
PSD2	La nuova versione della PSD, già recepita a livello nazionale.
PSP	Prestatore Servizi di Pagamento ovvero il soggetto che eroga il servizio di pagamento e effettua verso l'Ente Creditore il versamento delle somme incassate dal cittadino.
Quietanza di Pagamento	Documento che l'Ente Creditore mette a disposizione del cittadino in seguito alla ricevuta telematica fornitagli da pagoPA.
RDP	RDP (Remote Desktop Protocol) è un protocollo di rete sviluppato da Microsoft, che permette la connessione remota da un computer a un altro in maniera grafica. I client RDP esistono per la maggior parte

	delle versioni di Microsoft Windows, Linux, Unix, macOS, Android, iOS e altri. I server RDP ufficiali esistono per i sistemi operativi Windows nonostante ne esistano anche per i sistemi Unix-Like. L'applicazione (che usa il protocollo in oggetto) compresa in Windows si chiama Connessione Desktop remoto.
Responsabile per la protezione dati – RPD o DPO	Il Data Protection Officer (di seguito DPO) è una figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679 | GDPR, pubblicato sulla Gazzetta Ufficiale europea L. 119 il 4 maggio ’16. Il DPO è un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all’interno di un’azienda/ente (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.
Responsabile per la Transizione al Digitale - RTD	Il Responsabile per la Transizione al Digitale (RTD) ha tra le principali funzioni quella di garantire operativamente la trasformazione digitale della Pubblica Amministrazione, coordinandola nello sviluppo dei servizi pubblici digitali e nell’adozione di modelli di relazione trasparenti e aperti con i cittadini. L' articolo 17 del Codice dell’Amministrazione Digitale obbliga tutte le amministrazioni a individuare un ufficio per la transizione alla modalità digitale - il cui responsabile è il RTD - a cui competono le attività e i processi organizzativi ad essa collegati e necessari alla realizzazione di un’amministrazione digitale e all’erogazione di servizi fruibili, utili e di qualità.
Rete dati	Insieme dell’infrastruttura passiva (cavi, prese, ecc.) e degli apparati attivi (switch, router, modem ecc.) necessari alla interconnessione di apparati informatici
Router	Un router (letteralmente "instradatore"), in ambito ICT e nell'ambito di una rete informatica a commutazione di pacchetto, è un dispositivo di rete usato come interfacciamento tra sottoreti diverse, eterogenee e non, che lavorando a livello logico come nodo interno di rete deputato alla commutazione, si occupa di instradare i pacchetti dati fra tali sottoreti permettendone l'interoperabilità (internetworking) a livello di indirizzamento
RPT	Richiesta Pagamento Telematica ovvero l’insieme dei dati che riguardano il pagamento (es. importo, Ente Creditore, IUV, etc.).
RT	Ricevuta Telematica ovvero il messaggio che riporta all’Ente Creditore l’esito del pagamento.
Sandbox	E’ un processo di rete che consente di inviare i file a un dispositivo separato, da ispezionare senza rischiare la sicurezza della rete. Ciò

	consente il rilevamento di minacce che potrebbero aggirare altre misure di sicurezza, comprese le minacce zero-day
SEPA	Single Euro Payments Area - Area unica dei pagamenti in euro ovvero norme e processi per i pagamenti validi per i paesi dell'Unione Europea.
Server	In informatica e telecomunicazioni è un componente o sottosistema informatico di elaborazione e gestione del traffico di informazioni che fornisce, a livello logico e fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate clients, cioè clienti) che ne fanno richiesta attraverso una rete di computer, all'interno di un sistema informatico o anche direttamente in locale su un computer.
SIOPE+	E' l'infrastruttura che intermedia il colloquio tra pubbliche amministrazioni e banche tesoriere con l'obiettivo di migliorare la qualità dei dati per il monitoraggio della spesa pubblica e per rilevare i tempi di pagamento delle Pubbliche Amministrazioni nei confronti delle imprese fornitrici.
Software	Il software (sigla SW, dall'inglese soft «morbido, leggero» e ware «merci, prodotti», su imitazione del termine hardware), traducibile come componente logico, programma informatico o supporto logico, in informatica ed elettronica è l'insieme delle componenti immateriali (strato logico/intangibile) di un sistema elettronico di elaborazione; è contrapposto all'hardware, cioè la parte materiale (strato fisico/tangibile) dello stesso sistema
Software web-based	Il software che utilizza una interfaccia web per poter essere utilizzato
Spamming	Invio di comunicazioni (prevalentemente di posta elettronica) non sollecitate che contengano materiale pubblicitario; in modo improprio in questa categoria vengono anche catalogate le mail con intenti malevoli (es. truffe, tentativi di furto d'identità, etc.)
SPC	Il Sistema Pubblico di Connettività (SPC) è la rete che collega tra loro tutte le pubbliche amministrazioni italiane, consentendo loro di condividere e scambiare dati e risorse informative. Inoltre è una cornice nazionale di interoperabilità: definisce, cioè, le modalità preferenziali che i sistemi informativi delle pubbliche amministrazioni devono adottare per essere tra loro interoperabili
SPC2	Sistema Pubblico di Connettività e cooperazione fase2
SPCCloud	Sistema Pubblico di Connettività e cooperazione in cloud per l'erogazione di servizi a favore della Pubblica amministrazione
SPID	Sistema Pubblico di Identità Digitale, è la soluzione che permette a tutti i cittadini di accedere ai servizi on-line della Pubblica Amministrazione e dei soggetti privati aderenti con un'unica Identità

	Digitale utilizzabile da computer, tablet e smartphone.
SSID	Acronimo di “service set identifier”, cioè il nome che identifica una rete WiFi
SSL	Secure Sockets Layer: protocollo crittografico usato nel campo delle telecomunicazioni e dell'informatica che permette una comunicazione sicura dalla sorgente al destinatario (end-to-end) su reti TCP/IP(come ad esempio Internet) fornendo autenticazione, integrità dei dati e confidenzialità operando al di sopra del livello di trasporto.
Storage	In ambito informatico con il termine storage si identificano i dispositivi hardware, i supporti per la memorizzazione, le infrastrutture ed i software dedicati alla memorizzazione non volatile di grandi quantità di informazioni in formato elettronico. Il mercato dello storage è quel settore di mercato ICT che si occupa delle esigenze di memorizzazione di grandi quantità di dati. Esso si può dividere nei seguenti ambiti applicativi: • file sharing, ossia tutte le esigenze di condivisione di informazioni tra diversi server e tra i server e i personal computer; • data backup, ossia tutte le esigenze di creazione di copie delle informazioni da riutilizzare nel caso la versione originale venga danneggiata o persa. In italiano un termine che potrebbe sostituire quello inglese è “sistema di archiviazione dati”
SURCHARGE	Sovrapprezzo applicato dal beneficiario sull’importo da pagare che ha lo scopo di coprire i costi di incasso e che si distingue dalla commissione che il PSP chiede al pagatore per eseguire l’operazione.
Switch	Uno switch (letteralmente “commutatore”) è un dispositivo in una rete di computer che collega insieme altri dispositivi. Più cavi di rete sono collegati a uno switch per abilitare la comunicazione tra diversi dispositivi. Gli switch gestiscono il flusso di dati attraverso una rete trasmettendo un pacchetto di rete ricevuto solo a uno o più dispositivi per i quali il pacchetto è destinato. Ogni dispositivo collegato in rete a uno switch può essere identificato dal suo indirizzo MAC, consentendo allo switch di dirigere il flusso del traffico massimizzando la sicurezza e l'efficienza della rete
Traffico	Transito dei dati sulla rete informatica o telefonica
Upload	L'upload, anche noto come “caricamento”, in informatica è il processo di invio o trasmissione di un file (o più genericamente di un flusso finito di dati o informazioni) da un client ad un sistema remoto (denominato server) attraverso una rete informatica; l'azione inversa è chiamata download.

UPS	Dalla dicitura in lingua inglese Uninterruptible Power Supply ovvero gruppo di continuità elettrica. E' un'apparecchiatura elettrica utilizzata per ovviare a repentine anomalie nella fornitura di energia elettrica normalmente utilizzata (come cali di tensione e blackout), finanche per erogare costantemente una forma d'onda perfettamente sinusoidale alla frequenza di oscillazione prefissata, priva di variazioni accidentali.
URL filtering	E' il sistema che permette di monitorare e filtrare la navigazione in Internet, bloccando l'accesso a particolari categorie di siti, al fine di limitare il rischio di utilizzo improprio della rete e la navigazione in siti non pertinenti o non compatibili con l'attività aziendale
User Id	Identificativo utente, username o nome utente congiuntamente alla password o altri sistemi di sicurezza costituisce le credenziali di accesso ai sistemi
Utente (User)	Persona fisica autorizzata ad accedere ai servizi informatici dell'Ente.
Virtualizzazione	Per virtualizzazione si intende la creazione di una versione virtuale di una risorsa normalmente fornita fisicamente. La virtualizzazione permette l'ottimizzazione delle risorse e la capacità di far fronte a esigenze specifiche secondo il più classico paradigma dell'on demand.
Virus	Per virus informatico si intende un programma o del codice realizzato per danneggiare i computer corrompendone i file di sistema, sprecandone le risorse, distruggendone i dati o malfunzionamenti di altro genere. I virus si contraddistinguono da altre forme di malware in quanto sono auto-replicanti, ovvero sono in grado di creare delle copie di se stessi all'interno di altri file o computer senza il consenso o l'intervento di un utente
VOIP	(Voice over IP) tecnologia che rende possibile effettuare una comunicazione telefonica sfruttando il protocollo IP della rete dati
VPN	Virtual Private Network, è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano, come tecnologia di trasporto, un protocollo di trasmissione pubblico, condiviso e sicuro attraverso la rete internet
WAN	Una Wide Area Network (WAN) è una rete di telecomunicazioni che si estende su una grande distanza geografica per lo scopo principale della rete di computer. Le reti geografiche sono spesso stabilite con circuiti di telecomunicazione in affitto. Le imprese, l'istruzione e le entità governative utilizzano reti di area vasta per trasmettere dati a personale, studenti, clienti, acquirenti e fornitori da varie località in tutto il mondo. In sostanza, questa modalità di telecomunicazione consente a un'impresa di svolgere efficacemente la propria funzione

	quotidiana indipendentemente dalla posizione. Internet può essere considerato una WAN.
WF	Work Flow (flussi di lavoro). Viene detta "WorkFlow" (tradotto letteralmente "flusso di lavoro") la creazione di modelli e la gestione informatica dell'insieme dei compiti e i diversi attori coinvolti nella realizzazione di un processo lavorativo (detto anche processo operativo). Il termine di Workflow potrà quindi essere tradotto in italiano come Gestione elettronica dei processi lavorativi