COMUNE DI CAPOTERRA

Città Metropolitana di Cagliari

DISCIPLINARE SUI SISTEMI INFORMATIVI, L'UTILIZZO DEGLI STRUMENTI INFORMATICI E ICT, DI INTERNET E DELLA POSTA ELETTRONICA DEL COMUNE DI CAPOTERRA

Approvato con Delibera G.C. 286 del 17/12/2025

Sommario

ART. 1 – FINALITÀ

Il presente Disciplinare definisce i principi generali e le procedure operative per l'accesso e l'utilizzo dei sistemi informativi, dei servizi internet e di posta elettronica, nonché degli strumenti ICT del Comune di Capoterra, al fine di garantire un uso appropriato e ottimale delle risorse, in conformità alle disposizioni e direttive nazionali.

ART. 2 – RIFERIMENTI NORMATIVI

Il presente Disciplinare regola l'utilizzo degli strumenti informatici e telematici del Comune nel rispetto della normativa europea e nazionale in materia di protezione dei dati personali, sicurezza ICT, digitalizzazione amministrativa e tutela dei lavoratori. Nello specifico:

- Regolamento (UE) 2016/679 – GDPR, con particolare riferimento agli artt. 5, 6, 24, 25, 28, 29, 32, 33–34, 35 e 88, relativi a principi del trattamento, basi giuridiche, responsabilità del titolare, misure di sicurezza, gestione dei Data Breach e trattamenti nel contesto lavorativo.

- Disposizioni del Codice Privacy (D.Lgs. 196/2003) come modificato dal D.Lgs. 101/2018, nonché le norme del Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) in materia di sicurezza, gestione documentale e servizi digitali.

- Art. 4 della L. 300/1970, che disciplina gli strumenti dai quali possa derivare un controllo dell'attività lavorativa, garantendo trasparenza, proporzionalità e corrette procedure autorizzative.

- Linee guida del Garante del 2007, che definiscono limiti dei controlli, corretto utilizzo e obblighi informativi per l'utilizzo della posta elettronica, navigazione Internet e servizi di comunicazione digitale.

- Disposizioni dei provvedimenti del Garante del 2008–2009, riguardanti nomina, tracciamento e verifiche periodiche dell'Amministratore di Sistema.

- Provvedimento del Garante n. 364/2024 relativo al trattamento dei dati connesso agli strumenti ICT e alle attività di monitoraggio, sulle misure tecniche e organizzative adeguate e, ove necessario, la DPIA.

- Opinion 2/2017 del Gruppo art. 29 / EDPB sul trattamento dei dati dei lavoratori nell'uso delle tecnologie digitali, con particolare attenzione a necessità, minimizzazione e proporzionalità.

  Piano Triennale per l'Informatica nella PA 2024–2026, in materia di sicurezza, interoperabilità, gestione dei servizi digitali e continuità operativa.

ART. 3 – AMBITO DI APPLICAZIONE

Il presente Disciplinare si applica a tutti i dipendenti dell'Ente e a tutti gli utenti interni.

Per dipendenti si intendono gli amministratori, i responsabili, il personale con rapporto di lavoro a tempo indeterminato o determinato, i collaboratori coordinati e continuativi, nonché il personale in servizio con altre forme contrattuali (collaboratori).

Per utenti interni si intendono tutti i soggetti autorizzati ad accedere alle dotazioni informatiche dell'Ente, come definite all'articolo 4, che non rientrano tra i dipendenti.

ART. 4 – DEFINIZIONI

1. **Sistema Informativo**: qualunque sistema di gestione delle informazioni che può includere uno o più sistemi informatici;

2. **Sistema Informatico**: una componente di un sistema informativo per la gestione automatizzata delle informazioni

e/o dei dati;

3. **Postazione di lavoro**: insieme di elementi che servono a una persona per svolgere la propria attività lavorativa. Include sia componenti informatiche come l'hardware (pc, monitor, tastiera, ecc.) e/o il software sia componenti non informatiche che vengono forniti ad un assegnatario per l'espletamento delle proprie mansioni;

4. **Dotazioni o apparecchiature informatiche**: singoli dispositivi o strumenti tecnologici utilizzati all'interno di una postazione di lavoro;

5. **Assegnatario**:

   a. **utente di casella di posta elettronica ordinaria (PEO) o certificata (PEC):** è il soggetto fisico, dipendente o meno dell'Ente, al quale è attribuita una casella di posta elettronica ordinaria o certificata.

      - Se la casella rappresenta un ufficio, una funzione istituzionale o un soggetto non fisico l'assegnatario è il soggetto individuato come responsabile del suo utilizzo al momento della richiesta di creazione.

      - In assenza di tale indicazione, l'assegnatario coincide con il richiedente. L'assegnatario può avere accesso esclusivo o autorizzare altri utenti (delegati). Per le caselle personali, l'accesso è esclusivamente riservato all'assegnatario.

   b. **di postazione di lavoro**: è il soggetto fisico cui è assegnata una specifica postazione di lavoro. Qualora la postazione sia attribuita a un settore o ufficio, l'assegnatario si identifica nel Responsabile del medesimo.

   c. **di risorsa condivisa (ad esempio: cartelle condivise, spazi cloud, sistemi di archiviazione o condivisione file):** è il soggetto fisico designato come responsabile dell'utilizzo della risorsa, il quale, d'intesa con il Titolare d'Incarico di Elevata Qualificazione o con il Responsabile del Settore competente, definisce gli utenti autorizzati all'accesso e i relativi livelli di permesso.

6. "**Servizi di piattaforma**" o "**servizi orizzontali**": sistemi, infrastrutture e servizi ICT dell'Ente non legati a un ambito applicativo specifico, ma indispensabili per il funzionamento e lo sviluppo dei servizi applicativi.

7. **"Servizi di applicazione"**, **"servizi verticali"** o **"applicazioni verticali"**: sistemi e servizi ICT dell'Ente specifici di una funzione, settore o ufficio, che utilizzano i servizi di piattaforma e richiedono competenze proprie dell'ambito di utilizzo.

8. **Servizio ICT**: l'ufficio dell'Ente competente per i servizi ICT (Information and Communication Technology) dell'ente;

9. **Intranet**: la connettività di rete e i servizi ad essa connessi nell'ambito della rete privata (interna) dell'amministrazione;

10. **Internet**: la connettività di rete ed i servizi ad essa connessi nell'ambito della rete pubblica;

11. **Posta elettronica**: quando non diversamente specificato per posta elettronica è inteso sia il servizio di posta elettronica ordinaria (PEO) che quello certificato (PEC);

12. **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;

13. **CAD**: il Codice dell'Amministrazione Digitale.

ART. 5 – PRINCIPI GENERALI

L'Amministrazione promuove l'impiego degli strumenti informatici, delle reti informatiche e telematiche, delle tecnologie digitali, di Internet e della posta elettronica come mezzi fondamentali per perseguire in modo efficace ed efficiente le proprie finalità istituzionali.

L'Amministrazione adotta tutte le misure organizzative e tecnologiche necessarie a prevenire l'uso improprio delle proprie dotazioni informatiche e telematiche.

Ogni utente è civilmente e penalmente responsabile del corretto utilizzo delle risorse, dei programmi e degli apparati informatici a cui ha accesso, nonché dei dati trattati per finalità istituzionali.

L'utente è inoltre responsabile del contenuto delle comunicazioni inviate e ricevute per motivi di servizio, anche con riferimento alla tutela della riservatezza dei dati, la cui diffusione non autorizzata può costituire violazione del segreto d'ufficio o della normativa in materia di protezione dei dati personali.

Saranno perseguiti i comportamenti che possano arrecare danno, anche d'immagine, all'Ente.

ART. 6 – SERVIZIO INFORMATICO

All'interno della macrostruttura dell'Ente è istituito un Ufficio per i servizi informatici, l'innovazione tecnologica e la digitalizzazione incardinato nel Settore 5 - Segreteria, Affari Generali, Organi Istituzionali, Urp, Informatizzazione, Archivio , Pubblica Istruzione.

L'Ufficio è composto da personale tecnicamente competente per i servizi di piattaforma e per i servizi di applicazione, come definiti all'articolo 4.

Al suo interno sono individuati i servizi ICT relativi ai diversi ambiti tecnologici. La loro responsabilità è affidata a personale con comprovata esperienza, competenza e adeguata formazione nelle discipline informatiche, delle telecomunicazioni e nella normativa sulla digitalizzazione e sull'e-government.

Per i sistemi informativi non gestiti direttamente dall'Ente (es. sistemi ANAC, piattaforme per la verifica della regolarità contributiva, ecc.), il settore o ufficio fornisce supporto tecnico-specialistico nei rapporti con i soggetti esterni competenti.

ART. 7 – REFERENTI TECNOLOGICI DEI SETTORI DELL'ENTE

La nomina dei Referenti Tecnologici avviene tra i dipendenti del Settore o Ufficio ritenuti maggiormente competenti nell'utilizzo degli strumenti tecnologici; non è richiesta una competenza formalmente certificata.

Il Referente Tecnologico svolge le seguenti funzioni:

- interfacciarsi con il personale del Servizio Informatico per la gestione delle richieste di assistenza provenienti dal proprio settore o ufficio, secondo le modalità definite dal Servizio Informatico, al fine di ottimizzare i tempi di risoluzione delle problematiche;
- partecipare a incontri, iniziative o attività formative sulle nuove tecnologie promosse dal Servizio Informatico;
- fungere da primo punto di riferimento per il personale del proprio ufficio in materia di tecnologie informatiche e digitali, promuovendone la conoscenza e l'utilizzo;
- svolgere eventuali ulteriori compiti assegnati in materia di digitalizzazione dei processi e dei procedimenti.

ART. 8 – ASSISTENZA TECNICA AGLI UTENTI

Assistenza tecnica ICT

L'assistenza tecnica su hardware e software del Servizio Informatico deve essere richiesta, di norma, tramite servizio Ticketing o via mail.

Nel caso della mail, la richiesta deve essere inoltrata all'indirizzo mail: help_desk@comune.capoterra.ca.it, indicando nell'oggetto:

- categoria;
- tipo di problema;
- informazioni utili alla diagnosi.

In casi urgenti non gestibili dal sistema automatizzato, l'assistenza può essere richiesta anche tramite contatto diretto.

Le richieste vengono prese in carico, con riscontro al richiedente, e gestite dall'addetto informatico, che può interagire anche con il Referente Tecnologico del settore o ufficio (art. 7).

Le richieste sono evase in ordine di ricezione, dando priorità ai problemi che coinvolgono più utenti o che rischiano di compromettere la continuità dei servizi.

Accesso ai dispositivi e teleassistenza

Gli Amministratori di Sistema possono accedere ai dispositivi comunali, direttamente o in remoto, per:

- risolvere problemi sistemistici o applicativi segnalati dagli utenti;
- verificare il corretto funzionamento dei dispositivi;
- effettuare aggiornamenti software e manutenzione preventiva.

Gli interventi che richiedono accesso ad aree personali richiedono il consenso dell'utente; negli altri casi non è necessario.

L'accesso in teleassistenza da parte di terzi (fornitori o altri) deve essere autorizzato dall'Amministratore di Sistema. Durante l'intervento, deve essere presente l'utente richiedente o il Referente Tecnologico (art. 7) per garantire conformità alle policy e alla normativa vigente.

ART. 9 – POSTAZIONI DI LAVORO (HARDWARE E SOFTWARE)

La postazione di lavoro è generalmente costituita da:

- un Computer (desktop o notebook);
- periferiche collegate (monitor, tastiera, mouse, lettore smart card, stampante, ecc);
- tutti i software e le risorse centralizzate;
- l'apparecchio telefonico.

Le postazioni di lavoro e tutte le dotazioni informatiche dell'Ente sono strumenti di lavoro e devono essere utilizzate esclusivamente per lo svolgimento delle attività professionali e istituzionali.

L'uso deve limitarsi alle finalità istituzionali e coerenti con le attività lavorative. In particolare, non è consentito salvare dati non pertinenti all'attività lavorativa.

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 e l'Ente non è responsabile per eventuali danni o deterioramenti derivanti da un utilizzo non conforme alle finalità professionali.

Computer portatili (notebook)

Nel caso di assegnazione di computer portatili (notebook), gli utenti:

- devono custodire gli stessi con diligenza.
- se vengono portati all'esterno dei locali dell'Ente devono custodire gli apparati in un luogo protetto e sicuro.

In caso di furti, mancanze o anomalie nelle dotazioni informatiche e telematiche assegnate, occorre darne immediata comunicazione al proprio Responsabile, per la denuncia alle Autorità competenti.

Assenza dalla postazione di lavoro

Ogni volta che si allontana dal locale dove è custodita la postazione di lavoro, il dipendente è tenuto a scollegarsi dal sistema o bloccare l'accesso.

In ogni caso, le postazioni informatiche sono state configurate per eseguire il blocco dopo 15 minuti di inattività. Per sbloccare la postazione sarà necessario reinserire le credenziali di accesso.

Archiviazione dei dati

I dati personali propri o di terzi, qualora l'archivio sia necessario per lo svolgimento delle attività lavorative, devono essere archiviati nei servizi di piattaforma o orizzontali, nei servizi di applicazione o verticali (art. 4) o in risorse condivise centralizzate (es. cartelle documentali o condivise), in modo da garantirne disponibilità, sicurezza e accessibilità per tutti gli utenti autorizzati.

Per motivi operativi è possibile conservare sul computer locale copie temporanee di dati già presenti nei sistemi centralizzati.

Modifiche hardware e software

All'utente non è consentito apportare autonomamente modifiche sia hardware che software alla postazione di lavoro.

Deve essere esplicitamente autorizzato dal Servizio Informatico:

- ogni collegamento delle postazioni di lavoro a reti diverse da quelle configurate dall'Amministratore di Sistema;
- qualunque installazione di software anche se libero, modem;
- qualunque alterazione delle funzionalità (es. indirizzi e protocolli di rete) del collegamento in rete della postazione di lavoro;
- ogni archiviazione/memorizzazione di dati, file e documenti digitali e informatici in forma crittografata.

Controlli sull'uso delle risorse assegnate

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. 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 o ufficio.

È compito di ogni Responsabile, 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.

Divieti sull'uso delle risorse assegnate

È vietato utilizzare gli strumenti informatici per scopi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica e adottare comportamenti che possano determinare danni economici e di immagine dell'Ente;

Inoltre, nell'ambito dell'utilizzo degli strumenti informatici e telematici non è consentito:

1. Accedere e modificare le impostazioni del BIOS o UEFI;
2. Accedere ad un personal computer o a qualunque sistema con credenziali diverse dalle proprie;
3. Installare software 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 a meno che sia stato precedentemente autorizzato;
4. Eseguire programmi che possano determinare un danneggiamento o un sovraccarico dei sistemi e/o della rete;
5. Archiviare/memorizzare dati, file e documenti digitali e informatici contrari alle vigenti norme di legge;
6. 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 a meno che sia stato precedentemente autorizzato;
7. 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;
8. 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 servizio ICT per comprovate esigenze di servizio;
9. 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.);
10. 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.);
11. 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;
12. Utilizzare risorse informatiche e telematiche private (es PC, notebook, tablet, smartphone, periferiche etc.) direttamente e fisicamente collegate alla rete indicata e configurata dall'amministrazione come rete di lavoro;
13. Trasferire documenti elettronici dai sistemi informativi e strumenti dell'Ente a device esterni (Hard disk, chiavette, CD, DVD e altri supporti);
14. Ogni altro utilizzo non inerente all'attività lavorativa.

ART. 10 – 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 servizio ICT.

ART. 11 – GESTIONE DELLE PASSWORD E DEGLI ACCOUNT

Account e credenziali

L'accesso a un insieme di funzionalità, strumenti e contenuti di un sistema ICT è consentito tramite credenziali. Esso è costituito da:

- un codice identificativo personale (username o user ID);
- una parola chiave (password);
- eventuali strumenti di autenticazione aggiuntiva, quali generatori di one-time password o dispositivi hardware (ad esempio, Carta Nazionale dei Servizi o simili).

Tali strumenti rimangono nella disponibilità esclusiva dell'utente e non possono essere ceduti a terzi. Ad ogni account è associato un profilo che definisce le operazioni consentite nel contesto operativo.

Gestione delle password

Le password sono personali, segrete e devono avere le seguenti caratteristiche:

- devono rispettare i requisiti minimi previsti dai sistemi (lunghezza minima: 14 caratteri, deve contenere: lettere, lettere maiuscole, lettere minuscole, numeri, caratteri speciali);
- non deve essere uguale alla login o contenere riferimenti facilmente riconducibili all'utente;
- non deve essere stata utilizzata le ultime 10 volte;
- deve essere modificata periodicamente, la cui durata massima delle password è configurabile dai sistemi ICT;
- al primo accesso, l'utente è tenuto a modificare la password, che non deve essere condivisa con altri.

L'utente è responsabile di abusi o incidenti di sicurezza derivanti da una gestione inadeguata delle proprie credenziali.

Nel caso in cui l'utente svolga mansioni che trattano i dati sensibili è obbligatorio il cambio di password ogni tre mesi.

Autenticazione a più fattori (MFA)

Per aumentare la sicurezza degli account e ridurre il rischio di accessi non autorizzati, l'Amministrazione può richiedere l'uso dell'autenticazione a più fattori (MFA) per l'accesso a sistemi critici o sensibili. L'autenticazione a due fattori consiste nell'utilizzo combinato di due elementi distinti per confermare l'identità dell'utente:

- Qualcosa che l'utente conosce, come la password personale;
- Qualcosa che l'utente possiede, come un dispositivo mobile con app di generazione di codici temporanei (OTP), un messaggio di conferma sul dispositivo registrato o una chiave di sicurezza hardware fornita

dall'Amministrazione.

Gli utenti devono evitare di condividere con terzi sia le proprie credenziali sia i dispositivi utilizzati per l'autenticazione a più fattori (MFA).

Policy BYOD (Bring Your Own Device)

L'utilizzo di dispositivi personali da parte del personale dipendente per accedere alle risorse informatiche dell'Ente è consentito esclusivamente previa autorizzazione formale del Servizio Informatico e nel rispetto delle presenti disposizioni.

I dispositivi personali autorizzati devono essere conformi ai requisiti minimi di sicurezza stabiliti dall'Ente, tra cui: aggiornamenti di sistema regolarmente installati, presenza di software antivirus attivo e aggiornato, crittografia del dispositivo, protezione tramite PIN, password o sistemi biometrici: tali attività sono a carico e sotto la responsabilità del dipendente utilizzatore.

È fatto divieto di utilizzare dispositivi personali non autorizzati per attività lavorative o per l'accesso a servizi, applicazioni o dati dell'Ente.

Il Servizio Informatico può revocare in qualsiasi momento l'autorizzazione al BYOD in caso di rischi per la sicurezza.

Il mancato rispetto delle presenti disposizioni costituisce violazione delle norme interne in materia di sicurezza informatica ed espone l'utente all'applicazione delle misure disciplinari previste.

Compromissione e sicurezza delle credenziali

In caso di sospetta perdita di riservatezza della password, l'utente provvede alla sua modifica personale o, se non possibile, con l'assistenza dell'Amministratore di Sistema.

È vietato utilizzare account o credenziali altrui, anche su richiesta del titolare.

Qualora l'utente venisse a conoscenza delle credenziali di un altro utente, deve informare immediatamente l'Amministratore di Sistema competente.

Blocco e inattività **degli account**

Dopo un numero prestabilito di tentativi di accesso errati, il profilo dell'utente può essere disabilitato; la riattivazione avviene tramite le procedure stabilite dal Servizio Informatico.

Le credenziali inattive da almeno sei mesi sono disattivate, salvo autorizzazioni speciali per scopi di gestione tecnica.

Compiti dei responsabili di settore

I Responsabili devono comunicare tempestivamente al Servizio Informatico eventuali cambi di mansione dei dipendenti che comportino modifiche o revoche delle autorizzazioni di accesso.

Devono assicurare che per ogni dipendente sia presente almeno un altro soggetto con profilo autorizzativo equivalente, a garanzia della continuità operativa.

Devono altresì garantire che ogni dipendente abbia almeno un sostituto con autorizzazioni equivalenti per assicurare la continuità operativa.

ART. 12 – INIZIO DEL RAPPORTO DI LAVORO

Nel momento in cui viene formalizzato l'avvio del rapporto di lavoro di un nuovo dipendente, il settore competente per la gestione del personale comunica tale evento al Servizio Informatico attraverso le modalità digitali previste, utilizzando

i meccanismi centralizzati predisposti da quest'ultimo (ad esempio, sistema automatizzato di assistenza tecnica via mail).

Il Servizio Informatico provvederà quindi alle seguenti attività:

- Assegnazione dell'account di dominio;
- Assegnazione di una casella di posta elettronica istituzionale (PEO);
- Consegna del Disciplinare sui sistemi informativi, l'utilizzo degli strumenti informatici e ICT, di internet e della posta elettronica del Comune di Capoterra.

Successivamente, il Responsabile di Settore o il Titolare d'Incarico di Elevata Qualificazione a cui l'utente è assegnato dovrà inoltrare, tramite i medesimi meccanismi centralizzati (es. sistema di gestione ticket o richiesta via e-mail), le richieste relative alle specifiche abilitazioni necessarie per lo svolgimento delle attività lavorative.

Tali richieste potranno riguardare:

- "Servizi di piattaforma" o "servizi orizzontali" (art. 4), come ad esempio la navigazione Internet o l'accesso a servizi cloud;
- "Servizi di applicazione" o "servizi verticali" (art. 4), quali il protocollo informatico, la gestione degli atti, la contabilità finanziaria o l'accesso a risorse condivise.

Credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alle risorse informatiche dei dipendenti o di eventuali collaboratori esterni vengono assegnate dall'Amministratore di Sistema previa formale richiesta del Responsabile di Settore. La richiesta di attivazione delle credenziali dovrà essere completa delle generalità dell'utente e dell'elenco dei sistemi e delle profilazioni per cui deve essere abilitato l'accesso.

ART. 13 – MODIFICA O CESSAZIONE DEL RAPPORTO DI LAVORO

Decadenza dell'assegnazione

In caso di cessazione del posto di lavoro, il Responsabile del Settore 10 - Amministrazione del Personale, Organizzazione e Relazioni Sindacali dovrà comunicare formalmente e preventivamente all'Amministratore di Sistema la data effettiva in cui le credenziali dovranno essere disabilitate. L'assegnatario è tenuto a restituire la strumentazione della postazione di lavoro. Prima della restituzione, l'assegnatario deve:

1. Comunicare al proprio responsabile tutte le informazioni relative all'ubicazione dei dati aziendali nei sistemi centralizzati, provvedendo alla cancellazione di eventuali copie locali;
2. Rimuovere eventuali dati personali propri o di terzi ancora presenti sulla postazione;

Gestione successiva alla cessazione

Trascorsi quindici giorni dalla data di modifica o cessazione del rapporto con l'Ente, l'Amministrazione potrà procedere alla formattazione e/o cancellazione delle aree di memorizzazione, sia locali che di rete.

Postazioni non assegnate

Qualora una postazione di lavoro non sia assegnata a un utente specifico, il Responsabile di Settore presso cui è fisicamente collocata ne assume temporaneamente la responsabilità.

Il Responsabile è tenuto a comunicare formalmente al Responsabile informatico la disponibilità della postazione per una nuova assegnazione a un dipendente di altro settore o ufficio.

Assegnazione di nuove postazioni

In caso di nuova assegnazione, il Servizio Informatico provvede, entro 10 giorni dalla richiesta, a fornire la necessaria dotazione informatica, previa verifica della disponibilità.

Comunicazioni interne

In tutti i casi di trasferimento interno o cessazione del rapporto di lavoro, il settore o ufficio competente per la gestione del personale deve comunicare formalmente l'evento al servizio ICT, attraverso i canali digitali previsti, come i sistemi automatizzati di gestione ticket.

Attività del Servizio informatico

A seguito della comunicazione, il Servizio Informatico procede come segue:

- In caso di trasferimento ad altro settore o ufficio: vengono disattivate tutte le abilitazioni dell'utente ai servizi di applicazione o servizi verticali (art. 4), comprese quelle relative ai portali e alle banche dati esterne gestite dal il Servizio Informatico. Restano attive le abilitazioni ai servizi di piattaforma o servizi orizzontali (es. utente di dominio, posta elettronica).

- In caso di cessazione del rapporto di lavoro: tutti gli account associati all'utente vengono disabilitati e/o eliminati.

Responsabilità sui dati condivisi

Il Responsabile della risorsa condivisa (art. 21) di ciascuna cartella di rete o risorsa accessibile all'utente è tenuto a richiedere la modifica o la revoca dei permessi di accesso in caso di trasferimento o cessazione del rapporto.

Nuove abilitazioni

In caso di trasferimento ad altro settore o ufficio, spetta al Titolare d'incarico di Elevata Qualificazione o al Responsabile di Settore inoltrare richiesta al il Servizio Informatico per l'attivazione delle specifiche abilitazioni necessarie allo svolgimento delle attività lavorative, relative sia ai servizi di piattaforma o orizzontali (es. navigazione Internet, cloud), sia ai servizi di applicazione o verticali (es. protocollo, gestione atti, contabilità, risorse condivise, ecc.).

ART. 14 – AMMINISTRAZIONE E GESTIONE DELLE RISORSE INFORMATICHE O ICT

Il Servizio Informatico è responsabile del monitoraggio e della verifica della corretta applicazione, da parte di tutti i soggetti coinvolti, delle disposizioni contenute nel presente Disciplinare e delle misure di sicurezza previste dalla normativa vigente in materia di protezione dei dati personali.

Gli Amministratori di Sistema sono i soggetti tecnici incaricati di sovrintendere alla gestione, manutenzione, sicurezza e al corretto funzionamento delle risorse informatiche, telematiche e ICT dell'Amministrazione e possono operare esclusivamente nell'ambito delle attività per le quali sono stati formalmente autorizzati.

Nomina formale

Gli Amministratori di Sistema sono nominati e revocati con atto formale dal Titolare del trattamento, su proposta del Responsabile dell'Area ICT.

La nomina deve indicare:

- l'identità dell'Amministratore di Sistema;

- le funzioni attribuite;

- le aree di sistema amministrate;

- le credenziali assegnate;
- i limiti e le responsabilità del ruolo.

ART. 15 – INTERNET

Uso consentito

L'utilizzo di internet deve essere finalizzato esclusivamente allo svolgimento delle attività lavorative e istituzionali.

Un uso personale è ammesso solo in via eccezionale e per un tempo limitato, al fine di consentire ai dipendenti di adempiere a necessità amministrative o burocratiche senza doversi allontanare dal luogo di lavoro, nel rispetto dei seguenti principi:

- assenza di aggravio diretto di spesa per l'amministrazione;
- assenza di interferenze con i tempi e le attività lavorative condivise con colleghi e collaboratori;
- rispetto del divieto di svolgere le attività non consentite indicate al successivo paragrafo.

In ogni caso, l'Ente non assume alcuna responsabilità per eventuali danni arrecati a terzi o allo stesso dipendente derivanti dall'utilizzo della rete Internet per finalità non istituzionali.

Attività non consentite

È vietato qualsiasi uso personale di internet che possa danneggiare o compromettere la sicurezza e l'efficienza dei sistemi informativi dell'amministrazione.

Controlli e misure di sicurezza

Per prevenire usi impropri o non autorizzati della rete Internet, come l'accesso a siti non attinenti all'attività lavorativa o l'utilizzo di servizi potenzialmente dannosi o illegali, l'amministrazione applica filtri di accesso (URL filtering).

I filtri limitano automaticamente la navigazione verso siti o servizi non consentiti.

L'Amministrazione può modificare in qualsiasi momento le categorie di siti bloccati o autorizzati e creare profili di navigazione personalizzati per specifici gruppi di utenti o settori, in base alle esigenze operative o su richiesta motivata.

Limitazioni tecniche

Per mantenere efficiente il funzionamento del sistema informatico e della rete, si raccomanda (salvo comprovate esigenze di servizio) di non accedere a siti o servizi che consumano molta banda, come piattaforme di streaming audio/video, web radio o portali multimediali di informazione.

ART. 16 – INTRANET

All'interno degli edifici dell'amministrazione è disponibile una rete Intranet (LAN), destinata esclusivamente agli utenti dell'Ente, come definito nell'articolo 4. La rete interna permette la connessione sicura ai sistemi e alle risorse dell'Amministrazione, garantendo l'accesso ai servizi digitali interni, alla posta elettronica istituzionale e agli applicativi necessari per l'attività lavorativa.

La gestione della rete interna, compresa l'autenticazione degli utenti, il monitoraggio della rete e la sicurezza dei dati, è effettuata dal personale tecnico interno dell'amministrazione, in conformità alle normative vigenti in materia di protezione dei dati e sicurezza informatica. I log delle connessioni e delle attività sulla rete vengono registrati esclusivamente per finalità di sicurezza e gestione del corretto funzionamento del sistema e sono accessibili solo al personale autorizzato.

L'accesso alla rete interna è regolamentato da politiche interne di sicurezza e gestione degli account, tra cui l'uso di credenziali personali e sistemi di autenticazione sicura (ad esempio, autenticazione a due fattori). Tutti i dati scambiati sulla rete interna sono protetti mediante misure di sicurezza avanzate, come firewall, segmentazione della rete e protocolli di crittografia, per prevenire accessi non autorizzati e garantire la riservatezza delle informazioni.

ART. 17 – RETE WI-FI

All'interno degli edifici dell'amministrazione potrà essere disponibile una rete Wi-Fi pubblica, pensata per i cittadini e/o gli ospiti dell'ente, per consentire loro di navigare su internet. Il servizio Wi-Fi è pensato per gli utenti che non sono registrati in anticipo (ad esempio, cittadini o turisti) e permette loro di registrarsi autonomamente e navigare seguendo le politiche stabilite, utilizzando, ad esempio, l'autenticazione tramite social login.

La gestione del servizio di autenticazione, monitoraggio e connessione a internet è affidata a un fornitore esterno, che opera nell'ambito del Servizio Pubblico di Connettività (SPC) che agisce come provider di servizi internet che offra connettività ad Internet, ufficialmente registrato presso AGCOM, in conformità con la legislazione vigente.

Inoltre, all'interno degli edifici, potrebbe esserci una rete Wi-Fi privata o di lavoro, destinata esclusivamente agli utenti dell'amministrazione (come definito nell'Articolo 4). A questa rete si applicano, principalmente, le stesse regole previste per la rete cablata dell' Amministrazione.

ART 18 – TRACCIAMENTO DELLE ATTIVITÀ SUGLI STRUMENTI INFORMATICI

Il sistema informatico comunale registra in forma automatica gli accessi e le attività rilevanti ai fini della sicurezza informatica e della tutela dei dati personali. Tali registrazioni (log) sono conservate in conformità alla normativa vigente, con misure tecniche che ne garantiscono integrità e inalterabilità. I log non sono accessibili agli utenti e sono consultabili esclusivamente dal personale autorizzato per finalità di sicurezza, controllo degli accessi e adempimenti previsti dal GDPR e dal Provvedimento del Garante sugli Amministratori di Sistema.

ART. 19 – ACCESSO REMOTO

L'accesso da remoto alle risorse informatiche aziendali è consentito esclusivamente tramite il protocollo di Desktop Remoto di Windows, configurato e gestito dal Servizio Informatico.

Per collegarsi al sistema comunale tramite Desktop Remoto, l'utente deve completare tre passaggi di autenticazione per garantire la sicurezza del collegamento:

- Primo passaggio – verifica l'identità del sistema del Comune di Capoterra;
- Secondo passaggio – permette di individuare il computer interno a cui collegarsi;
- Terzo passaggio – consente di accedere al proprio desktop e utilizzare le risorse e i servizi disponibili.

Ogni passaggio è obbligatorio e serve a proteggere i dati e la sicurezza del sistema.

Gli utenti sono tenuti a mantenere riservate le proprie credenziali e a rispettare tutte le procedure di sicurezza, incluse autenticazione a più fattori.

Durante l'utilizzo di risorse in modalità di lavoro da remoto, gli utenti sono tenuti a utilizzare i sistemi di MFA messi a disposizione dall'Amministrazione. Qualora un utente non desideri utilizzare il proprio dispositivo mobile, l'Amministrazione può fornire un'apposita chiave di sicurezza hardware come alternativa.

Il mancato utilizzo della MFA, se richiesto, può comportare limitazioni nell'accesso ai sistemi o azioni correttive secondo le procedure interne.

Registro degli accessi remoti

Il Servizio Informatico provvede alla registrazione e al monitoraggio degli accessi remoti, al fine di garantire la tracciabilità delle operazioni e la sicurezza dell'infrastruttura.

Rete Privata Virtuale (VPN)

Quando sarà attiva la rete privata virtuale (VPN), l'accesso alle risorse informatiche e ai servizi interni del comune avverrà tramite la VPN fornita dall'Ente.

L'utilizzo della VPN è riservato al personale autorizzato e deve essere effettuato solo per motivi di lavoro, nel rispetto delle politiche di sicurezza e delle disposizioni del presente Disciplinare.

Le credenziali di accesso alla VPN sono personali e non trasferibili: non possono essere comunicate, condivise o utilizzate da altri soggetti. L'accesso alla VPN richiede l'attivazione della doppia autenticazione, a garanzia della sicurezza del sistema.

ART. 20 – POSTA ELETTRONICA

La posta elettronica, sia ordinaria (PEO) che certificata (PEC), rappresenta, per il comune di Capoterra, il canale principale per tutte le comunicazioni istituzionali ed è uno strumento di lavoro e deve essere utilizzata esclusivamente per lo svolgimento delle attività connesse ai compiti istituzionali e professionali.

A riguardo l'Amministrazione mette a disposizione:

1. un servizio di posta elettronica (PEO), con indirizzi del tipo @comune.capoterra.it. Tali indirizzi possono corrispondere a caselle personali o a liste di distribuzione che inoltrano automaticamente i messaggi a più destinatari. Di tale servizio:
    - Il database della posta appartiene interamente all'ente;
    - Il personale del Servizio Informatico può accedere ai contenuti delle caselle per motivi tecnici o di sicurezza, ad esempio per prevenire o risolvere malfunzionamenti, nel pieno rispetto delle norme vigenti.
2. un servizio di posta elettronica certificata (PEC), con caselle aventi estensione @pec.comune.capoterra.it. Di tale servizio:
    - le caselle PEC destinate a singoli dipendenti devono essere richieste secondo le procedure definite dal Servizio Informatico, fornendo la documentazione necessaria (ad esempio codice fiscale e documento di identità) per garantirne l'associazione univoca alla persona;
    - per le caselle PEC riferite a uffici, servizi o settori istituzionali, la richiesta deve includere i dati utili a identificare il Responsabile di riferimento;
    - la posta elettronica istituzionale deve essere utilizzata esclusivamente per finalità connesse alle proprie mansioni. I messaggi inviati o ricevuti non devono avere carattere personale, ma riguardare esclusivamente l'attività lavorativa

Nell'utilizzo dei servizi di posta elettronica, ordinaria (PEO) e certificata (PEC), gli utenti devono rispettare le regole comportamentali stabilite dall'Ente riguardanti l'uso consentito:

- **Conoscenza degli strumenti:** gli utenti sono tenuti a consultare e seguire le guide utente e le istruzioni operative disponibili nei sistemi di posta elettronica per sfruttarne correttamente tutte le funzionalità;
- **Gestione dello spazio:** ogni casella di posta è soggetta a limiti di spazio. Il sistema avvisa automaticamente quando si raggiunge la quota massima; superato il limite, non sarà possibile inviare o ricevere messaggi fino al ripristino dello spazio disponibile;

- **Manutenzione periodica**: l'utente deve controllare regolarmente la propria casella, cancellare messaggi obsoleti o irrilevanti, eliminare lo spam e gestire lo spazio in modo da evitare il blocco della casella. I messaggi con rilevanza istituzionale devono essere conservati o protocollati secondo le regole di gestione documentale;

- **Dimensione dei messaggi**: si raccomanda di limitare la dimensione degli allegati, specialmente in caso di invii a più destinatari, per evitare problemi di recapito o eccessivo consumo di risorse;

- **Firma dei messaggi**: ogni messaggio deve riportare una firma che includa almeno nome, cognome, settore e ufficio di appartenenza.

- **Sicurezza**: occorre non aprire allegati sospetti o file eseguibili e non cliccare su collegamenti di provenienza incerta o non verificata;

- **Identità digitale**: è vietato inviare messaggi sotto falsa identità o impersonando altri utenti;

- **Riservatezza**: l'invio di documenti "strettamente riservati" all'esterno della rete comunale deve essere evitato o effettuato solo in caso di necessità, adottando tutte le cautele opportune;

- **Cessazione del servizio**: alla conclusione del rapporto di lavoro, la casella di posta elettronica viene disattivata e successivamente eliminata. Prima delle dimissioni, il dipendente deve salvare o inoltrare ai colleghi i messaggi necessari per la continuità operativa del servizio;

- **Tutela dei dati personali**: l'invio di dati, documenti e informazioni deve sempre rispettare le disposizioni del Regolamento (UE) 2016/679 (GDPR) e della normativa sulla protezione dei dati personali;

- **Mail con dati sensibili**: nel caso fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o sensibili, l'allegato viene criptato attraverso apposito software. La password dovrà essere comunicata al destinatario attraverso un canale diverso dalla mail (ad es. lettera o telefono);

- **Invio automatico**: In caso di assenza è raccomandabile utilizzare un messaggio "Out of Office" facendo menzione a chi all'interno dell'ente assumerà le mansioni durante l'assenza. È consigliabile inoltre, specificare che in caso di urgenze occorre trasmettere una mail al protocollo@comune.capoterra.ca.it;

- **Trasferimento dati**: in caso di disabilitazione della casella, l'utente deve — almeno 10 giorni prima — trasferire al proprio Responsabile i messaggi e i dati di interesse istituzionale, eliminare i dati personali e informare il Servizio Informatico dell'avvenuta operazione. L'amministrazione provvede comunque alla cancellazione definitiva della casella dopo 15 giorni. Per le caselle PEO o PEC associate a un ufficio o settore, l'assegnazione passa automaticamente al nuovo Responsabile individuato.

ART. 21 – RISORSE CONDIVISE

Per garantire la disponibilità dei dati e un'efficace gestione delle copie di sicurezza, gli utenti sono tenuti a salvare i propri file di lavoro esclusivamente nelle cartelle di rete o nelle risorse condivise (ad esempio la cartella documentale centralizzata o altre cartelle condivise centralizzate) ed evitare di conservare i file solo localmente nel computer in uso.

Le cartelle di rete e le risorse condivise devono essere utilizzate unicamente per finalità lavorative e non possono in alcun caso essere impiegate per scopi personali o diversi da quelli professionali.

Salvo diversa comunicazione, tali risorse sono soggette a regolari attività di amministrazione e backup.

Gli Amministratori di Sistema, nell'ambito delle funzioni loro assegnate dal Responsabile informatico, possono in qualsiasi momento procedere alla rimozione di file o applicazioni che ritengano potenzialmente pericolosi per la sicurezza, sia sui computer degli utenti sia sui server.

Per ogni cartella di rete o risorsa condivisa centralizzata viene designato, al momento della creazione, un Responsabile della risorsa condivisa, incaricato di collaborare alla corretta gestione della stessa. Egli dovrà:

- verificare che l'utilizzo della risorsa sia coerente con i trattamenti previsti dalla normativa vigente;
- controllare e, se necessario, modificare – con il supporto degli Amministratori di Sistema – i permessi di accesso, affinché risultino conformi alle mansioni e ai ruoli del personale autorizzato.

Le stesse attività e prerogative attribuite al responsabile della risorsa condivisa sono riconosciute anche ai Responsabili di Settore.

ART. 22 – GESTIONE DEGLI INCIDENTI ICT E VIOLAZIONI DI DATI PERSONALI

Flusso interno di segnalazione degli incidenti ICT

Ogni utente, dipendente o soggetto che rilevi anomalie, eventi sospetti o possibili incidenti ICT (malfunzionamenti, accessi non autorizzati, perdita di disponibilità o integrità dei dati, diffusione indebita, malware, phishing, ecc.) è tenuto a segnalarli immediatamente al Servizio Informatico tramite i canali interni dedicati (e-mail istituzionale o numero di telefono).

Le segnalazioni devono essere tempestive e comprendere tutte le informazioni utili per la valutazione dell'evento.

Ruolo del Responsabile informatico e del DPO

Il Responsabile informatico coordina la gestione operativa dell'incidente, attiva le misure tecniche di contenimento e analisi, valuta la gravità dell'evento e collabora con gli Amministratori di Sistema per il ripristino delle funzionalità compromesse.

Il Responsabile della Protezione dei Dati (RPD/DPO) supporta la valutazione sotto il profilo della protezione dei dati personali, verifica se l'incidente comporti una "violazione di dati personali" (data breach) ai sensi dell'art. 4, n. 12, GDPR e fornisce indicazioni sulla conformità delle azioni intraprese.

Il DPO è consultato per ogni incidente informatico che possa coinvolgere dati personali:

1. Valutazione preliminare (triage)
2. Alla ricezione della segnalazione, il Responsabile informatico effettua una valutazione preliminare (triage) per determinare:
   - la natura dell'incidente;
   - l'impatto tecnico e funzionale;
   - la possibile compromissione di dati personali;
   - il rischio per i diritti e le libertà degli interessati;
   - l'urgenza degli interventi correttivi.

In caso di sospetto Data Breach, il DPO è immediatamente coinvolto nella valutazione.

Documentazione dell'evento nel Registro degli Incidenti

Ogni incidente ICT, indipendentemente dalla gravità, deve essere documentato nel Registro interno degli incidenti ICT e dei Data Breach, contenente almeno:

- data e ora della segnalazione;

- soggetto segnalante;
- descrizione dell'evento;
- sistemi e dati coinvolti;
- interventi adottati per contenere e mitigare l'incidente;
- esito del triage e valutazione del rischio;
- decisioni circa l'obbligo di notifica o comunicazione;
- soggetti coinvolti (ICT, Amministratori di Sistema, DPO, Titolare).

Il registro è custodito dal Responsabile informatico e messo a disposizione del DPO e del Titolare.

Notifica al Garante per la protezione dei dati personali (art. 33 GDPR)

Qualora l'incidente ICT integri una violazione di dati personali suscettibile di presentare un rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, su proposta del Responsabile informatico e previo parere del DPO, provvede alla notifica al Garante entro 72 ore dalla conoscenza dell'evento.

La notifica deve contenere tutti gli elementi previsti dall'art. 33, par. 3, GDPR.

Comunicazione agli interessati (art. 34 GDPR)

Se la violazione di dati personali comporta un rischio elevato per i diritti e le libertà degli utenti, il Titolare, con il supporto del Responsabile informatico e del DPO, provvede alla comunicazione agli interessati, in forma chiara e semplice, nel più breve tempo possibile.

La comunicazione deve descrivere la natura della violazione, le conseguenze probabili e le misure adottate per porvi rimedio, nonché le misure suggerite agli interessati per proteggersi da effetti negativi.

Chiusura dell'incidente e misure preventive

Al termine della gestione dell'incidente, il Responsabile informatico redige una relazione di chiusura e valuta, con il DPO, eventuali misure tecniche e organizzative da adottare per prevenire incidenti analoghi.

Quando necessario, il Titolare aggiorna le politiche di sicurezza, le procedure interne o le misure di protezione dei dati.

ART. 23 – ACQUISTO DI DOTAZIONI INFORMATICHE O ICT

L'acquisto di beni e servizi in ambito ICT (come hardware, software, servizi telematici, ecc.) avviene seguendo le seguenti modalità:

1. **Piano annuale**: Ogni anno, entro il mese di settembre, i responsabili di tutti i settori devono comunicare al Responsabile del Servizio Informatico e al Responsabile per la Transizione Digitale le necessità per l'anno successivo. Questo per permettere la redazione del "Piano Generale di Acquisizione di beni e servizi ICT" e l'eventuale aggiornamento del "Piano Triennale per l'informatica" previsto dal CAD.

2. **Coinvolgimento del Servizio Informatico:** Per gestire al meglio le risorse umane, economiche e tecnologiche, è necessario coinvolgere il Servizio Informatico in tutte le azioni dell'ente che riguardano i sistemi informatici, la rete dati, i sistemi di fonia, videosorveglianza cittadina e qualsiasi altro sistema ICT. Questo permette di effettuare le necessarie analisi di fattibilità, valutare il carico di lavoro e pianificare correttamente le tempistiche.

   Alcune precisazioni:

- **Esigenze urgenti**: Se ci sono necessità impreviste e urgenti, il funzionario del settore o ufficio interessato deve inviare una richiesta formale al Responsabile del Servizio ICT. Quest'ultimo valuterà la congruità tecnica della richiesta e, se c'è copertura finanziaria disponibile, avvierà le procedure di acquisto.

- **Acquisizioni fuori budget**: Se il Servizio Informatico non ha abbastanza fondi disponibili nei propri capitoli di spesa, altri settori possono effettuare l'acquisto di beni e servizi ICT, previa valutazione e approvazione tecnica da parte del Responsabile informatico e del Responsabile della Transizione Digitale. In questo caso, il Servizio Informatico deve fornire un riscontro entro 3 giorni dalla richiesta.

ART. 24 – DISMISSIONE APPARECCHIATURE INFORMATICHE

I vari settori sono tenuti a procedere alla dismissione e smaltimento delle apparecchiature informatiche e tecnologiche (come PC, monitor, stampanti, ecc.) in loro possesso, per le quali è stata dichiarata l'inutilizzabilità o l'obsolescenza da parte del Servizio Informatico. Tale operazione dovrà avvenire nel rispetto delle normative vigenti, tra cui il GDPR e la legislazione sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE), nonché seguendo le procedure stabilite dal settore o ufficio competente per la gestione del patrimonio dell'ente.

Prima della dismissione e dello smaltimento, sarà necessario provvedere all'eliminazione di eventuali dati memorizzati nei dispositivi.

ART. 25 – PRINCIPI GENERALI PER I DATI PERSONALI RACCOLTI ED INFORMATIVA AGLI UTENTI

Il trattamento dei dati personali nell'ambito dei sistemi ICT dell'Ente avviene nel rispetto del Regolamento (UE) 2016/679 – GDPR, del Codice Privacy (D.Lgs. 196/2003 e D.Lgs. 101/2018), del Provvedimento 364/2024 del Garante, delle Linee guida del 2007 e della normativa in materia di controlli a distanza (art. 4 L. 300/1970).

I trattamenti ICT sono improntati ai principi di liceità, correttezza, trasparenza, minimizzazione, proporzionalità, integrità e riservatezza (artt. 5, 24 e 25 GDPR).

Le attività sono svolte esclusivamente per finalità istituzionali dell'Ente e nel rispetto delle misure tecniche e organizzative adeguate di cui all'art. 32 GDPR.

Titolari, responsabili e persone autorizzate al trattamento

Per i servizi applicativi di cui all'art. 4, ciascun Settore dell'Ente riveste il ruolo di Titolare del trattamento in relazione ai dati trattati nell'ambito delle proprie competenze, mentre i fornitori ICT sono designati Responsabili del trattamento ai sensi dell'art. 28 GDPR.

Il personale del Servizio Informatico e degli uffici competenti è formalmente autorizzato al trattamento ai sensi degli artt. 29 GDPR e 2-quaterdecies del Codice Privacy.

L'accesso ai dati è consentito esclusivamente sulla base di profili di autorizzazione adeguati e proporzionati alle funzioni e alle responsabilità assegnate.

Di seguito viene illustrato un elenco dei dati personali trattati tramite i servizi di piattaforma (art. 4) e i sistemi informativi dell'Ente:

- **Dati raccolti nei sistemi informativi dell'Ente:** vengono generalmente raccolti i seguenti dati: nome, cognome, codice fiscale, data e luogo di nascita, nonché data e ora dell'ultimo accesso di tutti gli utenti che, a qualsiasi titolo, dispongono di credenziali per accedere ai sistemi informatici o ICT dell'ente.

- **Dati relativi al traffico di rete (Intranet e Internet):** il traffico Internet generato da ciascun utente attraverso la rete dell'amministrazione viene registrato automaticamente in file di log, sia sui dispositivi di competenza dell'amministrazione che dal fornitore dei servizi di connettività Internet. Tra le informazioni salvate ci sono: l'indirizzo IP di origine, la porta utilizzata, i siti web visitati, l'inizio e la durata di ogni connessione, nonché la

quantità di dati trasferiti.

- **Dati raccolti dai sistemi di protezione degli Endpoint (antivirus, antimalware, ecc.) e di sicurezza perimetrale:** i sistemi di protezione degli Endpoint (ossia delle postazioni di lavoro) e di sicurezza perimetrale (che tutelano il perimetro interno ed esterno della rete), al fine di consentire la configurazione delle politiche di sicurezza dei sistemi, possono raccogliere dati relativi alle minacce informatiche individuate sui dispositivi e sulle postazioni di lavoro. Questi dati vengono inviati a sistemi centralizzati per l'analisi delle minacce informatiche.

- **Dati relativi alle comunicazioni mediante posta elettronica:** per i servizi di posta elettronica (PEO e PEC) gestiti direttamente dall'amministrazione o tramite fornitori esterni, i dati personali relativi alle comunicazioni inviate e ricevute tramite tali strumenti sono conservati dai rispettivi gestori, in conformità con il GDPR.

L'Ente adotta misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali e dei sistemi informativi.

Trattamento dei log tecnici e dei dati di sicurezza

Vengono generati i log tecnici necessari al corretto funzionamento dei sistemi ICT, alla sicurezza informatica e alla continuità operativa. Tali log trattano di informazioni registrate dai sistemi per garantire che tutto funzioni correttamente, per proteggere i dati e prevenire problemi o incidenti.

Questi dati sono conservati e gestiti da fornitori esterni che trattano i dati in qualità di Responsabili ai sensi dell'art. 28 GDPR.

Nei casi di controlli difensivi, l'accesso è ammesso solo in presenza di circostanze documentate, nel rispetto dell'art. 4 L. 300/1970 e con il coinvolgimento del DPO.

ART. 26 – AMMINISTRATORI DI SISTEMA

Gli Amministratori di Sistema devono essere individuati e nominati con atto formale nel rispetto di una serie di principi normativi e organizzativi derivanti dal GDPR, dal Codice Privacy e dai provvedimenti del Garante. Sono considerati Amministratori di Sistema i soggetti (interni o esterni) che, per funzione o contratto, dispongono di privilegi tecnici di accesso ai sistemi, alle reti, ai database o ai servizi cloud dell'Ente.

L'Ente mantiene un elenco aggiornato degli Amministratori di Sistema, contenente:

- nominativo;
- ruolo;
- sistemi e risorse amministrate;
- tipo di accesso con privilegi.

Gli Amministratori di Sistema operano sulla base del principio di minima autorizzazione (least privilege) e accedono ai dati personali solo quando strettamente necessario e sono tenuti al rispetto del segreto d'ufficio, del Codice Privacy, del GDPR e dei regolamenti interni dell'Ente.

Ogni abuso, accesso immotivato o attività priva di attinenza alle funzioni comporta responsabilità disciplinare e, se del caso, penale.

ART. 27 – CONTROLLI E RESPONSABILITÀ

L'Amministrazione, per ragioni organizzative, produttive, di sicurezza e di tutela del patrimonio informativo dell'Ente, può effettuare verifiche sull'uso degli strumenti informatici nel rispetto delle normative vigenti, con particolare

riferimento all'art. 4 della Legge 20 maggio 1970 n. 300 (Statuto dei lavoratori), al Regolamento (UE) 2016/679 e al d.lgs. 196/2003 come modificato dal d.lgs. 101/2018.

Ogni controllo deve rispettare i principi di necessità, proporzionalità, minimizzazione, finalità e non deve comportare un monitoraggio generalizzato o proattivo dell'attività degli utenti.

Le tipologie di controllo includono:

- **Controlli tecnici di sicurezza**: attività tecniche necessarie al corretto funzionamento e alla sicurezza dei sistemi (es. analisi automatica dei log di sistema, rilevazione di anomalie di rete, malware, tentativi di intrusione), purché non utilizzate per finalità disciplinari e non idonee, per impostazione e configurazione, a monitorare in modo sistematico e individuale l'attività degli utenti.

- **Controlli difensivi mirati:** consentiti esclusivamente:

    - dopo il verificarsi di un evento anomalo, illecito, dannoso o potenzialmente lesivo, e in presenza di indizi concreti;

    - per utilizzo anomalo persistente nonostante l'avviso generalizzato;

    - in caso di minacce all'integrità o alla sicurezza dei sistemi che richiedano la consultazione dei log per individuare e rimuovere la criticità;

    - in presenza di indizi concreti relativi a illeciti civili, penali o amministrativi (controllo difensivo);

    - per accesso ai log necessario per l'esercizio o la difesa di un diritto in sede giudiziaria;

    - in caso di richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Tali controlli non possono mai essere preventivi o proattivi, e devono essere limitati ai dati pertinenti ai fatti da accertare e devono essere proporzionati, limitati ai soli dati indispensabili e condotti da personale autorizzato.

È vietato ogni monitoraggio continuativo, massivo o generalizzato dell'attività degli utenti (es. lettura sistematica della posta elettronica, monitoraggio proattivo del traffico web, keylogging, sorveglianza occulta), in quanto lesivo della dignità e riservatezza dell'utente e contrario all'art. 4 dello Statuto dei lavoratori.

L'Amministrazione assicura che:

- gli utenti siano informati, tramite informativa ai sensi del GDPR, sulle tipologie di dati trattati e sulle modalità dei controlli tecnici;

- i controlli non comportino la lettura dei contenuti della corrispondenza elettronica, salvo le eccezioni di legge;

- siano garantiti riservatezza, sicurezza e tracciabilità delle operazioni;

- i controlli mirati siano effettuati soltanto da soggetti formalmente autorizzati al trattamento.

Gli accessi e le attività degli Amministratori di Sistema sono registrati e sottoposti a controlli periodici da personale autorizzato, nel rispetto del Provvedimento del Garante Privacy sugli Amministratori di Sistema.

La relativa documentazione e i registri dei controlli sono conservati secondo procedure interne riservate, a tutela della sicurezza dei sistemi e della riservatezza dei dati.

Il registro è custodito dal Responsabile della Protezione dei Dati (RPD/DPO) o da altro soggetto individuato dall'Ente.

ART. 28 – AGGIORNAMENTO DELLE DISPOSIZIONI E DELLE REGOLE TECNICHE

Le disposizioni del presente Disciplinare possono essere soggette a modifiche, integrazioni e/o aggiornamenti, in funzione dell'evoluzione tecnologica, dell'entrata in vigore di nuove normative o del mutamento delle esigenze dell'amministrazione. Il Servizio Informatico è responsabile dell'emanazione e dell'aggiornamento delle regole tecniche necessarie per l'attuazione delle disposizioni contenute nel Disciplinare.

Tutti i dipendenti/collaboratori possono proporre, qualora ritenuto necessario, integrazioni e modifiche al presente Disciplinare tramite comunicazione scritta al Responsabile di Settore e al Responsabile del Servizio Informatico.

ART. 29 – DIFFUSIONE DEL DISCIPLINARE

Il presente Disciplinare verrà trasmesso per posta elettronica istituzionale a tutti i dipendenti/collaboratori e verrà pubblicato sulla sezione Amministrazione Trasparente sotto la sezione "Atti Generali".

GLOSSARIO

Account	Insieme di credenziali (ad esempio, username e password) assegnato a un individuo per permettergli l'accesso a un servizio o sistema. Esempi comuni includono: L'account richiesto da un ISP per fornire accesso a Internet e servizi di posta elettronica. Un account creato da un Amministratore di Sistema per consentire a un utente di accedere a un computer o a risorse condivise in una rete aziendale.
AGID	L'agenzia istituzionale che supporta la Presidenza del Consiglio nell'attuazione dell'Agenda Digitale Italiana. La sua missione è favorire l'adozione delle tecnologie digitali in Italia, incentivando l'innovazione, la digitalizzazione dei servizi pubblici e la crescita economica attraverso la trasformazione digitale.
Amministratori di Sistema	Gli Amministratori di Sistema sono professionisti IT responsabili della gestione, manutenzione e sicurezza dei sistemi informatici. Possono avere accesso ai dati personali, ma tale accesso è consentito solo se strettamente necessario per l'esecuzione dei compiti legati al loro ruolo.
ANPR	Sistema centralizzato del Ministero dell'Interno che raccoglie e gestisce i dati anagrafici dei cittadini italiani residenti. È un registro nazionale che consente di centralizzare e aggiornare le informazioni relative alla popolazione residente nel territorio italiano.
Antivirus	Programma progettato per rilevare, isolare e rimuovere software dannoso, come virus, da un computer o dispositivo, prevenire danni ai sistemi e proteggere i dati memorizzati.
API	Interfaccia che definisce un insieme di funzioni e regole che permettono a diverse applicazioni o sistemi di comunicare tra loro. Le API facilitano l'integrazione e l'interoperabilità tra software, senza bisogno di conoscere i dettagli interni del sistema.
Apparati attivi	Gli apparati attivi sono dispositivi hardware che gestiscono e instradano il traffico di rete, come switch e altri componenti che abilitano la trasmissione dei dati attraverso una rete.
Application Server	Server dedicato all'esecuzione e gestione di applicazioni software. Fornisce le risorse necessarie (come il calcolo e l'archiviazione) per eseguire la logica applicativa e supporta i client nella fruizione dei servizi offerti dall'applicazione.
Archivio informatico	Sistema di conservazione elettronica di documenti, organizzati in modo strutturato per facilitare l'accesso e la gestione. Può includere una varietà di documenti digitali, come file, immagini e dati.

Aree condivise	Spazi di memorizzazione centralizzati a disposizione degli utenti, che consentono la condivisione e lo scambio di file tra diversi utenti e sistemi all'interno della rete.
ATM	Sportello Bancomat
Attachment	File allegato: può essere inviato insieme a un'email o essere associato a software per la gestione dei file. Può trattarsi di documenti, immagini, o altri tipi di file.
Backup	Procedura che prevede la creazione di una copia di riserva dei dati su un supporto diverso rispetto a quello originale. Questo processo serve a proteggere i dati in caso di guasti o perdita delle informazioni originali.
Replica	Creazione di copie identiche di dati, file o interi sistemi su più posizioni. Il suo scopo principale è garantire alta disponibilità, affidabilità e continuità operativa.
Banda	Quantità di dati che può essere trasmessa attraverso una connessione in un dato intervallo di tempo. Nella banda ampia, le velocità vanno da 64 Kbps a 1,544 Mbps, mentre nella banda larga la velocità di trasmissione è superiore a 1,544 Mbps.
Bootstrap del pc	Insieme di operazioni che il computer esegue durante la fase di avvio. Inizia con l'accensione e prosegue fino al caricamento completo del sistema operativo in memoria principale, a partire dalla memoria secondaria (come il disco rigido o SSD).
CAD	Normativa italiana che regolamenta l'informatizzazione della Pubblica Amministrazione, stabilendo le modalità di interazione digitale tra la PA, i cittadini e le imprese.
CBILL	Piattaforma utilizzata per il pagamento dei servizi bancari, disponibile anche per la Pubblica Amministrazione. Integra il sistema pagoPA ed è accessibile tramite home banking o sportelli ATM, permettendo agli utenti di effettuare pagamenti per servizi pubblici e privati.
CIE	Documento ufficiale di riconoscimento previsto dalla legge italiana, che sostituisce la vecchia carta d'identità cartacea, attesta l'identità del cittadino italiano e viene utilizzata per accedere a vari servizi online e pubblici.
Client	Componente (hardware o software) che accede ai servizi o alle risorse offerte da un altro sistema, chiamato server. Il client è il dispositivo o l'applicazione che richiede e riceve i dati dal server per eseguire specifici compiti o operazioni.
Cloud Computing	Modello di erogazione di servizi tramite internet, che consente a un fornitore di offrire risorse (come spazio di archiviazione, capacità di elaborazione o trasmissione di dati) a un cliente finale. Queste risorse sono accessibili a distanza attraverso una rete distribuita e configurabile, permettendo di fruire di servizi informatici senza la necessità di infrastrutture fisiche locali.
Comunicazioni Elettroniche	Scambio di informazioni tra due o più soggetti utilizzando dispositivi elettronici. Questo può includere diversi strumenti, come la posta elettronica, i sistemi di messaggistica istantanea, la telefonia VoIP o i cellulari.
CONSIP	Centrali acquisti della Pubblica Amministrazione italiana. Si tratta di una società per azioni sotto il controllo del Ministero dell'Economia e delle Finanze, con l'obiettivo di ottimizzare gli acquisti pubblici, favorire la razionalizzazione delle risorse e operare nell'interesse esclusivo dello Stato italiano.
Cookie	File salvato sul computer di un utente, che permette a un sito web di riconoscere il dispositivo quando si ricollega. I cookie sono utilizzati per memorizzare preferenze o altre informazioni, migliorando l'esperienza di navigazione.

CSP	Fornitore che offre servizi in cloud, come l'archiviazione dei dati, l'elaborazione o la gestione delle risorse IT. Questi servizi sono accessibili attraverso internet e vengono utilizzati da aziende o utenti per esternalizzare alcune funzioni tecnologiche.
Data breach	Violazione della sicurezza che comporta l'accesso, la divulgazione o la distruzione non autorizzata di dati personali, che può avvenire accidentalmente o in modo illecito, con rischi per la privacy e la sicurezza delle informazioni trattate.
Database	Archivio di dati strutturati, organizzati in modo tale da facilitare l'accesso, la gestione e l'analisi delle informazioni. Questi dati possono riguardare un singolo argomento o diversi ambiti correlati tra loro.
DNS (Domain Name System)	Il DNS è un sistema che traduce i nomi di dominio, come www.example.com, in indirizzi IP numerici (ad esempio, 192.168.1.1) utilizzati per identificare i dispositivi in rete. Grazie al DNS, gli utenti possono accedere a siti web e risorse tramite nomi facilmente leggibili, senza dover ricordare indirizzi IP complessi.
Documento elettronico	Qualsiasi tipo di contenuto conservato in formato digitale, che può includere testi, immagini, registrazioni sonore, video o qualsiasi altro tipo di informazione che può essere visualizzata o archiviata elettronicamente.
Documento informatico	Particolare forma di documento elettronico che contiene una rappresentazione digitale di atti o fatti giuridicamente rilevanti. Questi documenti sono utilizzati nel contesto legale e amministrativo e hanno validità giuridica.
Dominio (nome di dominio)	Stringa di caratteri separata da punti, utilizzata per identificare un dominio su internet o una rete privata (Intranet). Ogni nome di dominio è legato a un indirizzo IP specifico che può identificare un sito web, un server o un altro servizio online. I nomi di dominio sono gestiti dal sistema DNS e sono suddivisi in livelli (ad esempio example.com, dove ".com" è il dominio di primo livello).
Dominio Microsoft	Rete di computer gestita centralmente, in cui tutti i dispositivi condividono un database di risorse di rete. I computer all'interno di un dominio sono amministrati come un'unità unica, applicando regole e procedure comuni. In altre parole, si tratta di una struttura di rete (come LAN, MAN o WAN) che adotta un modello client-server, dove i client devono autenticarsi tramite servizi offerti da un server. Le regole di connessione, comprese quelle di sicurezza, stabiliscono chi può accedere a determinate risorse, e determinano l'appartenenza e il livello di accesso degli utenti al dominio. Questo tipo di organizzazione permette una gestione centralizzata delle risorse e dei permessi all'interno di un'azienda, ente pubblico, scuola o università.
Download	L'azione di prelevare un file da una rete (come un sito web o un server) e salvarlo sul proprio dispositivo, come un computer, un tablet o uno smartphone. Questa operazione è solitamente avviata dall'utente, che richiede di ricevere il file per salvarlo localmente. L'operazione opposta, ovvero caricare un file dal proprio dispositivo su una rete, viene definita upload.
E-mail	Servizio che consente agli utenti di inviare e ricevere messaggi tramite internet o una rete interna (Intranet). Gli utenti possono accedere a questo servizio tramite un computer o dispositivo mobile (come uno smartphone o un tablet) connesso alla rete, utilizzando un account di posta elettronica registrato.
EC	Entità che beneficia di un pagamento da parte dei contribuenti o da altri enti. In genere, si tratta di una Pubblica Amministrazione, ma può essere anche una società a partecipazione pubblica o un Gestore di Pubblici Servizi (come nel caso dei servizi di mobilità, gestione dei rifiuti, ecc.).

File	Insieme di dati, informazioni o comandi che vengono raccolti sotto un nome univoco e vengono registrati nella memoria di un computer, utilizzando un programma. Un file può contenere qualsiasi tipo di informazione, come testo, immagini, o comandi eseguibili.
File di log	File che tiene traccia di eventi o attività che si verificano su un sistema informatico. Ad esempio, gli accessi ai dispositivi, le operazioni svolte su server o altre attività di rete. Questi file sono utili per il monitoraggio e la diagnostica, poiché consentono di rilevare anomalie o problemi nei sistemi informatici.
File server	Computer o dispositivo di rete progettato per memorizzare, gestire e rendere accessibili i file su una rete. Consente agli utenti di una rete di salvare, leggere, modificare e condividere file e cartelle. Il file server può essere un computer tradizionale o un Network Attached Storage (NAS), un dispositivo appositamente creato per il salvataggio dei dati. Questo sistema centralizza la gestione dei file e offre accesso a questi in base a regole di autorizzazione stabilite dal Responsabile di Sistema.
Filesystem	Sistema che gestisce l'archiviazione e l'organizzazione dei file su un dispositivo di memoria, come un disco rigido o un'unità SSD. Utilizza una struttura gerarchica (di tipo albero) per assegnare nomi ai file, per memorizzarli e per organizzarli all'interno di un'area di archiviazione.
Firewall	Dispositivo di rete, che può essere sia hardware che software, progettato per monitorare e filtrare il traffico informatico in entrata e in uscita. Il suo scopo è proteggere la rete da accessi non autorizzati o da attacchi informatici.
Firma Digitale	Tipo di firma elettronica che utilizza un sistema di chiavi crittografiche (una pubblica e una privata) per garantire l'integrità e l'autenticità di un documento elettronico. Il titolare della firma usa la sua chiave privata per firmare il documento, mentre la chiave pubblica consente a un soggetto terzo di verificare la validità della firma. Questo processo garantisce che il documento non sia stato alterato e che provenga da una fonte autentica.
Firma Elettronica	Tecnologia che permette di associare in modo logico dati elettronici (come una firma o un simbolo) a un altro documento elettronico. Questo strumento viene utilizzato per autenticare il firmatario e dimostrare la validità di un atto digitale. Il regolamento europeo eIDAS (articolo 3) definisce la firma elettronica come dati elettronici che consentono al firmatario di esprimere il proprio consenso su un documento elettronico.
Firma Elettronica Qualificata	Firma elettronica avanzata che soddisfa i requisiti giuridici definiti dal regolamento eIDAS e dal Codice dell'Amministrazione Digitale (CAD). È un tipo di firma elettronica che deve essere creata utilizzando un dispositivo di creazione sicura della firma e un certificato qualificato, emesso da un fornitore di servizi di certificazione qualificati. La firma qualificata ha valore legale equivalente a una firma autografa su carta.
GDPR	Normativa dell'Unione Europea che regola la protezione dei dati personali. È entrato in vigore il 27 aprile 2016 e riguarda il trattamento dei dati personali delle persone fisiche all'interno dell'UE. Il GDPR mira a garantire la privacy e la protezione dei dati, a facilitare la libera circolazione dei dati personali e a rafforzare i diritti dei cittadini riguardo ai loro dati personali.
Hardware	Parte fisica e materiale di un sistema informatico. Comprende tutte le componenti elettroniche, elettriche, meccaniche, ottiche e magnetiche che costituiscono un computer o qualsiasi altra apparecchiatura elettronica. Il termine può includere anche componenti di rete come router, switch e dispositivi di memorizzazione. L'hardware è complementare al software, che rappresenta la parte logica e programmatica del sistema.
Help Desk	Servizio di assistenza tecnica e supporto informatico che fornisce aiuto e soluzioni per i problemi relativi all'uso di hardware, software o altre tecnologie. Questo servizio può

	rispondere a domande, risolvere malfunzionamenti e offrire supporto nell'utilizzo di dispositivi elettronici o programmi informatici. Spesso l'help desk è organizzato in modo da risolvere problemi tecnici tramite telefonate, chat o ticket system, e può essere interno all'organizzazione o esterno tramite un provider di supporto.
ICT	Acronimo di Information and Communications Technology, si riferisce all'insieme di tecnologie utilizzate per gestire, trasmettere, ricevere e elaborare informazioni. Queste includono tecnologie digitali come computer, software, reti, internet, sistemi di telecomunicazione e dispositivi mobili.
Indirizzamento	Processo mediante il quale vengono assegnati indirizzi logici (ad esempio, indirizzi IP) agli apparati di rete. L'indirizzamento consente ai dispositivi all'interno di una rete di comunicare tra loro, indirizzando correttamente il traffico dati verso i destinatari giusti. In un contesto di rete, questo processo è fondamentale per garantire la connessione tra dispositivi e per il corretto funzionamento della rete stessa.
Integrità	Protezione dei dati da modifiche non autorizzate, perdita o distruzione. Garantire l'integrità significa assicurarsi che i dati siano accurati, completi e non alterati da parti esterne non autorizzate. La protezione dell'integrità dei dati è un aspetto fondamentale della sicurezza informatica e della gestione delle informazioni.
Internet	Rete globale di comunicazione elettronica che consente di connettere dispositivi e terminali in tutto il mondo.
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi, consentendo lo scambio automatico di dati e la fruizione di servizi attraverso interfacce standardizzate e aperte.
Intranet	Rete locale (LAN) utilizzata all'interno di un'organizzazione, come una azienda o un ente pubblico, per facilitare la comunicazione interna e l'accesso a risorse condivise. È una rete privata, completamente isolata da Internet, sebbene possa comunicare con reti esterne (come Internet) tramite connessioni protette (ad esempio, tramite VPN o firewall). L'intranet può anche estendersi oltre i confini locali utilizzando tecnologie come le reti WAN (Wide Area Network).
IP	Identificatore numerico univoco assegnato a ciascun dispositivo connesso a una rete, come computer, server, router o switch. L'indirizzo IP si suddivide in due parti: una che identifica la rete a cui il dispositivo appartiene e una che individua il dispositivo stesso all'interno di quella rete. Gli indirizzi IP possono essere di due tipi principali: IPv4 e IPv6.
IPSEC	Insieme di protocolli di sicurezza progettati per proteggere le comunicazioni che viaggiano su una rete tramite il protocollo IP (sia nella versione 4 che nella versione 6). IPSEC fornisce crittografia, autenticazione e integrità dei dati trasmessi tra dispositivi di rete (come server, router o firewall), garantendo che i pacchetti di dati non possano essere intercettati, alterati o falsificati durante il loro percorso.
IUV	Codice univoco assegnato a ogni pagamento effettuato verso una Pubblica Amministrazione, che consente di tracciare e identificare in modo preciso ogni transazione. Viene utilizzato per la gestione e l'elaborazione dei pagamenti elettronici nelle operazioni finanziarie pubbliche, in modo da garantire una corretta registrazione e monitoraggio dei flussi di denaro.
LAN	Rete di computer e dispositivi interconnessi all'interno di una area geografica limitata, come un edificio o un campus, che consente la condivisione di risorse, come file, stampanti e connessioni internet, tra i dispositivi connessi. Le LAN sono generalmente ad alta velocità e supportano la comunicazione tra dispositivi tramite cavi (Ethernet) o wireless (Wi-Fi).
Linee guida o policy	Insieme di regole operative, tecniche e/o organizzative che forniscono orientamenti pratici per la gestione dei processi lavorativi, decisionali e operativi. Questi documenti definiscono

	come le attività debbano essere svolte, stabilendo gli standard da seguire per garantire l'efficienza, la sicurezza e il rispetto delle normative all'interno di un'organizzazione.
Logging	Attività di registrazione e archiviazione cronologica delle informazioni relative alle operazioni compiute su un sistema informatico, come l'accesso a dispositivi, l'esecuzione di processi, o le modifiche apportate ai dati.
Malware	Qualsiasi software progettato per danneggiare un sistema informatico, compromettere la sua funzionalità o rubare informazioni in modo nascosto. Può manifestarsi sotto forma di virus, trojan, worm, spyware, ransomware e altri tipi di codice dannoso. In italiano è spesso chiamato codice maligno e rappresenta una minaccia per la sicurezza informatica.
MAN	Rete di telecomunicazioni che copre un'area metropolitana o una città, con l'obiettivo di interconnettere più edifici o strutture, permettendo la comunicazione e la condivisione di risorse tra di esse. Le MAN sono più estese delle LAN (Local Area Networks) ma più piccole rispetto alle WAN (Wide Area Networks). Combinando più MAN è possibile creare una rete WAN.
Misure minime di sicurezza	Linee guida fornite dall'AgID (Agenzia per l'Italia Digitale) per garantire che le Pubbliche Amministrazioni adottino un livello adeguato di protezione contro le minacce informatiche. Queste misure sono orientate a contrastare le minacce più comuni e a garantire la protezione dei dati e delle risorse digitali.
Multicanalità	Possibilità di effettuare transazioni o pagamenti utilizzando vari strumenti (come carte di credito, bonifici bancari, bollettini postali, ecc.) e attraverso diversi canali, come smartphone, web, ATM o punti fisici sul territorio.
NAS	Dispositivo di memorizzazione collegato a una rete che fornisce ampi spazi di archiviazione per il salvataggio, la lettura e la condivisione di file tra vari dispositivi. È composto da uno o più dischi rigidi (HDD) o SSD, ed è progettato per garantire l'accesso ai dati a tutti i dispositivi della rete, come server, computer e altri dispositivi collegati.
OEM	Original Equipment Manufacturer: produttore che fabbrica prodotti o componenti destinati ad essere venduti da altre aziende come parte di un prodotto finale. Nel contesto software, una licenza OEM consente ai produttori di computer o server di preinstallare software (come sistemi operativi o applicazioni) sui dispositivi venduti, ma generalmente limita la trasferibilità della licenza e la possibilità di vendere il software separatamente dall'hardware.
Office automation	Uso di software e strumenti tecnologici per automatizzare e ottimizzare le attività d'ufficio. Questi applicativi comprendono programmi per la gestione di documenti, comunicazioni elettroniche (email), calendari, fogli di calcolo, presentazioni, e altre applicazioni utili nelle mansioni lavorative quotidiane.
Open data	Formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi
PagoPA	Sistema di pagamenti online creato per rendere più facile, sicuro e trasparente il pagamento di tasse e servizi verso la Pubblica Amministrazione.
Password	Parola segreta che, insieme all'identificativo dell'utente (user-id), permette l'accesso a reti, computer, sistemi informatici o siti web.
Path	Vedi la definizione di "Percorso".
Pathname	Combinazione del percorso di un file nel sistema e del nome stesso del file.

PEC	Sistema di invio di email con valore legale, simile alla raccomandata con ricevuta di ritorno, che garantisce la prova della consegna e dell'invio.
PEO	Posta elettronica tradizionale, come la conosciamo comunemente (email).
Percorso	Serie di informazioni che indicano la posizione di un file all'interno di un sistema, elencando i vari passaggi o cartelle che portano al file stesso.
Policy	Insieme di regole o configurazioni che determinano come devono essere usati e gestiti certi software o risorse da parte degli utenti.
Policy di riferimento	Documento che descrive le attuali politiche in uso, aggiornato periodicamente per riflettere cambiamenti tecnologici o organizzativi.
PSD	Direttiva europea che stabilisce le regole per i servizi di pagamento, e la normativa nazionale che li regolamenta.
PSD2	Versione aggiornata della direttiva PSD, recepita anche a livello nazionale, che include nuove regole per i pagamenti online.
PSP	Entità che offre il servizio di pagamento e gestisce i trasferimenti di denaro verso l'Ente Creditore, raccogliendo i pagamenti effettuati dai cittadini.
Quietanza di Pagamento	Documento rilasciato dall'ente che ha ricevuto il pagamento, che attesta il pagamento effettuato, equivalente a una ricevuta.
RDP	Protocollo di rete creato da Microsoft che consente di connettersi a un altro computer tramite internet e interagirvi in modalità grafica, come se si stesse utilizzando direttamente il dispositivo remoto.
Responsabile per la protezione dati – RPD o DPO	Professionista che, sia come figura interna che esterna all'organizzazione, deve possedere competenze legali, informatiche, di gestione del rischio e di analisi dei processi aziendali. La sua principale responsabilità è quella di monitorare, valutare e gestire il trattamento dei dati personali all'interno dell'azienda o dell'ente, pubblico o privato, garantendo che tali dati siano trattati in conformità con le normative europee e nazionali sulla privacy.
Responsabile per la Transizione al Digitale - RTD	incaricato di garantire la trasformazione digitale della Pubblica Amministrazione. Questo ruolo implica il coordinamento delle attività di sviluppo dei servizi pubblici digitali e l'adozione di modelli di comunicazione trasparenti e accessibili tra le amministrazioni e i cittadini. Secondo l'articolo 17 del Codice dell'Amministrazione Digitale, tutte le amministrazioni devono designare un ufficio per la transizione digitale, il cui responsabile è l'RTD. Le sue competenze riguardano le attività organizzative e i processi necessari per creare una pubblica amministrazione digitale che fornisca servizi di qualità, fruibili e utili.
Rete dati	Rete che comprende l'infrastruttura fisica (come cavi e prese) e gli apparati attivi (come switch, router, modem) necessari per connettere e intercomunicare diversi dispositivi informatici all'interno di una rete.
Router	Dispositivo di rete che funge da punto di collegamento tra reti diverse, sia omogenee che eterogenee. Lavorando a livello logico come nodo di rete, il router si occupa di instradare i pacchetti di dati tra le sottorete, permettendo l'interoperabilità tra di esse attraverso un corretto indirizzamento, facilitando così la comunicazione tra diversi sistemi.
RPT	Richiesta Pagamento Telematica ovvero l'insieme dei dati che riguardano il pagamento (es. importo, Ente Creditore, IUV, etc.).

RT	Ricevuta via messaggio che riporta all'ente creditore l'esito di un pagamento effettuato tramite modalità telematica. Questo documento conferma l'avvenuto pagamento e viene utilizzato come prova dell'operazione.
Sandbox	Ambiente sicuro in cui è possibile eseguire un processo di rete, come l'analisi di file o applicazioni, senza compromettere la sicurezza della rete principale. Questo processo permette di testare e ispezionare file sospetti in un contesto isolato, riducendo i rischi per l'infrastruttura.
SEPA	Area unica dei pagamenti in euro, che stabilisce norme e procedure per i pagamenti che possono essere utilizzati nei paesi dell'Unione Europea.
Server	Dispositivo o sistema che gestisce e processa il traffico di dati, offrendo servizi ad altri dispositivi (chiamati "client") attraverso una rete, che può essere sia online che locale.
SIOPE+	Sistema che facilita la comunicazione tra le amministrazioni pubbliche e le banche, con l'obiettivo di migliorare la qualità dei dati sulla spesa pubblica e monitorare i tempi di pagamento delle Pubbliche Amministrazioni nei confronti dei fornitori.
Software	Insieme di programmi o componenti immateriali di un sistema informatico, contrapposto all'hardware che rappresenta invece la parte fisica del sistema. Il termine "software" deriva da "soft" (morbido) e "ware" (merce), indicandone la natura intangibile.
Software web-based	Tipo di software che funziona tramite un'interfaccia accessibile online, cioè utilizzando un browser web, senza necessitare di installazioni particolari sui singoli dispositivi.
Spamming	Si riferisce all'invio di email non richieste, generalmente con finalità pubblicitarie. In un senso più ampio, comprende anche messaggi con scopi fraudolenti, come tentativi di truffa o furto di identità.
SPC	Il Sistema Pubblico di Connettività (SPC) è la rete che collega tutte le amministrazioni pubbliche italiane, permettendo loro di condividere dati e risorse. Stabilisce anche le modalità tecniche che i sistemi informatici delle pubbliche amministrazioni devono seguire per interagire tra di loro.
SPC2	Rappresenta la seconda fase del Sistema Pubblico di Connettività e cooperazione, un aggiornamento e potenziamento della rete e dei servizi offerti alle pubbliche amministrazioni.
SPCCloud	Versione "cloud" del Sistema Pubblico di Connettività, che permette la gestione dei servizi pubblici attraverso il cloud, per un'erogazione più efficiente dei servizi alla 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
SSID	"Service Set Identifier", ovvero il nome che identifica una rete Wi-Fi.
SSL	Secure Sockets Layer: protocollo crittografico utilizzato in ambito telecomunicazioni e informatico per garantire una comunicazione sicura da una sorgente al destinatario (end-to-end) su reti TCP/IP (come Internet). Fornisce autenticazione, integrità dei dati e riservatezza, operando sopra il livello di trasporto.
Storage	Si riferisce a dispositivi hardware, supporti di memorizzazione, infrastrutture e software utilizzati per archiviare grandi quantità di dati in formato elettronico e in modo permanente.

	Il mercato dello storage si occupa delle necessità di conservazione dei dati e si suddivide in diverse aree applicative, come: • File sharing: la condivisione di file tra server o tra server e PC; • Data backup: la creazione di copie di sicurezza dei dati per ripristinarli in caso di perdita o danneggiamento dell'originale.
SURCHARGE	Sovrapprezzo applicato dal beneficiario su un pagamento per coprire i costi legati all'incasso, differenziandosi dalla commissione che un fornitore di servizi di pagamento (PSP) addebita al pagatore per eseguire la transazione.
Switch	Dispositivo di rete che collega vari dispositivi tra loro. I cavi di rete vengono collegati a uno switch, che gestisce il flusso dei dati, inviando i pacchetti di dati solo ai dispositivi a cui sono destinati. Ogni dispositivo collegato alla rete ha un indirizzo MAC unico, che consente allo switch di indirizzare correttamente il traffico, ottimizzando la sicurezza e l'efficienza della rete.
Traffico	Si riferisce al flusso di dati che transitano su una rete informatica o telefonica.
Upload	Processo di invio di un file, o di un flusso di dati, da un client a un sistema remoto (server) attraverso una rete. L'azione opposta è chiamata download, cioè il trasferimento di dati dal server al client.
UPS	Gruppo di Continuità Elettrica: è un dispositivo che fornisce energia elettrica di riserva per prevenire problemi causati da interruzioni o anomalie nella rete elettrica, come cali di tensione o blackout. Alcuni UPS sono in grado di erogare un'onda sinusoidale perfetta e stabile, mantenendo una frequenza fissa senza variazioni accidentali.
URL filtering	Sistema che consente di monitorare e limitare la navigazione su Internet, impedendo l'accesso a determinati siti web. Viene utilizzato per ridurre il rischio di utilizzo improprio della rete e per evitare che gli utenti accedano a contenuti non pertinenti o incompatibili con le attività aziendali.
User Id	Identificativo di un utente, che può essere un nome utente (username) utilizzato insieme a una password o ad altri sistemi di sicurezza per autenticarsi e accedere ai sistemi informatici.
Utente (User)	Persona fisica autorizzata ad accedere ai servizi informatici dell'Ente.
Virtualizzazione	Operazione che consiste nel creare una versione "virtuale" di una risorsa che normalmente è fisica. Questa tecnologia consente di ottimizzare l'uso delle risorse e di rispondere alle esigenze specifiche in modo più flessibile, seguendo il modello on-demand.
Virus	Tipo di software maligno progettato per danneggiare i computer, corrompendo file di sistema, sfruttando risorse del dispositivo o distruggendo dati. La principale caratteristica che distingue i virus da altri tipi di malware è la loro capacità di auto-replicarsi, cioè di creare copie di sé stessi all'interno di altri file o computer senza il consenso dell'utente.
VOIP	Voice over IP: tecnologia che permette di effettuare comunicazioni vocali attraverso il protocollo IP della rete dati, invece delle tradizionali linee telefoniche.
VPN	Virtual Private Network: è una rete privata virtuale che consente a utenti e dispositivi di connettersi in modo sicuro a una rete condivisa, utilizzando un protocollo di trasmissione pubblico come Internet, ma proteggendo i dati tramite cifratura.
WAN	Wide Area Network (WAN): rete di telecomunicazioni che copre un'ampia area geografica, collegando diverse postazioni (aziende, scuole, enti pubblici) per scambiare dati tra utenti,

	clienti, fornitori e altre parti da località diverse nel mondo. Solitamente, le WAN utilizzano circuiti di telecomunicazione affittati e sono fondamentali per le comunicazioni su larga scala.
WISP	Wireless Internet service provider: si intende generalmente un fornitore di servizi internet che offra connettività ad Internet.
WF	Il termine Work Flow (tradotto letteralmente come "flusso di lavoro") si riferisce alla creazione e gestione digitale dei processi lavorativi, che comprendono l'insieme dei compiti da svolgere e le varie figure professionali coinvolte nell'esecuzione di un processo operativo. In italiano, si può tradurre come Gestione elettronica dei processi lavorativi.

ALLEGATO – MODELLO DI RICHIESTA ASSISTENZA HELPDESK

Modello Richiesta Assistenza.odt