C O M U N E D I P R I Z Z I

Città Metropolitana di Palermo

Corso Umberto I° TEL. 0918344611 FAX 0918344630

www.comune.prizzi.pa.it

PEC: comunediprizzi.protocollo@certificata.com

REGOLAMENTO COMUNALE PER LA SICUREZZA DELLE INFORMAZIONI

Approvato con Deliberazione della
Giunta Comunale N.150 del 19/12/2023

Indice

Articolo 1 – Oggetto e Scopo

1) Il presente Regolamento:

   - definisce le regole (compiti e responsabilità di tutto il personale) previste per mitigare i rischi per la sicurezza delle informazioni nonché per assicurare un corretto utilizzo degli strumenti informatici messi a disposizione da parte del Comune;

   - definisce le modalità per il corretto utilizzo degli strumenti ICT resi disponibili dal comune.

2) Nel documento vengono definite le modalità per il corretto trattamento delle informazioni contenute su supporto cartaceo ovvero gestite con strumenti elettronici, in particolare il PC e i cellulari. Tali informazioni devono essere sempre trattate in modo da garantirne la riservatezza, l'integrità e la disponibilità, e quando esse riguardano dati personali, i trattamenti devono tener conto della normativa in materia di protezione dei dati personali.

3) Questo regolamento deve essere osservato da tutti i dipendenti e amministratori, senza distinzione di ruolo e/o livello, nonché da tutti i collaboratori del comune, a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratore a progetto, in stage, ecc.).

4) Il mancato rispetto o la violazione delle norme contenute nella presente istruzione potrebbe comportare dei provvedimenti disciplinari e/o azioni giudiziarie previste dalle leggi vigenti.

5) Si precisa che la presente istruzione è integrativa di quanto previsto da:

   - informative in materia di trattamento dei dati personali rilasciate ai dipendenti ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali;

   - lettere di incarico e designazioni destinate a responsabili e incaricati e le relative istruzioni ivi contenute, così come qualsiasi altra prescrizione in materia di privacy.

Articolo 2 - Riferimenti normativi

1. L'attività si realizza in conformità alle seguenti disposizioni normative:

• Decreto Presidente della Repubblica 13 giugno 2023, n. 81, Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165»

• Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (aggiornata 25.06.2009)

• Direttiva del Ministero per la pubblica amministrazione e l'innovazione 26 novembre 2009, n. 8; – Decreto legislativo 7 marzo 2005, n. 82, "Codice dell'amministrazione digitale" (e successive modificazioni e integrazioni);

• Legge 7 giugno 2000, n. 150, recante "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni".

• Linee guida per i siti web della PA, pubblicate dal Dipartimento per la digitalizzazione

della pubblica amministrazione e l'innovazione tecnologica (ed. 2011 e smi)

- Decreto legislativo 18 agosto 2000, n. 267 Testo unico delle leggi sull'ordinamento degli enti locali a norma dell'articolo 31 della legge 3 agosto 1999, n. 265

- Legge 7 agosto 1990, n. 241 Nuove norme sul procedimento amministrativo.

Articolo 3 – Gli archivi cartacei – "scrivania pulita"

1. Le informazioni riservate e contenute su supporto cartaceo devono essere custodite e trattate, mediante l'adozione di idonee e preventive misure di sicurezza, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta. Al termine del lavoro o durante lunghe pause, sulle scrivanie non deve essere lasciata alcuna documentazione riservata (nel senso che contiene dati personali sensibili, ecc.) cartacea o su supporti rimovibili.

2. A tal fine si devono utilizzare contenitori (armadi, schedari eccetera) oppure le stesse stanze ove la documentazione è riposta (da interpretarsi estensivamente quali "contenitori"), purché muniti di serratura tale da consentire un'effettiva selezione degli accessi a favore dei soli soggetti incaricati.

3. Non lasciare accessibile la postazione di lavoro durante la propria assenza: bloccarla, prevedendo lo sblocco con password e attivare comunque uno screen-saver automatico protetto da password che pulisca la videata entro alcuni minuti in caso di inutilizzo.

4. Sullo schermo della postazione, anche durante lo svolgimento della propria attività non devono essere facilmente visibili o accessibili informazioni riservate inutili per la corrente sessione di lavoro (ad esempio: lasciare aperto inutilmente un documento contenente informazioni sensibili, che possono essere inopportunamente lette da terzi durante o alla ripresa della sessione).

Articolo 4 - Utilizzo delle credenziali informatiche

1. Le credenziali di autenticazione per l'accesso ai sistemi e alla rete informatica sono costituite da un codice identificativo personale (username o user id) e da una parola chiave segreta (password) che dovrà essere custodita dall'utente con la massima diligenza e non divulgata, e che dovrà essere cambiata dall'utente al primo utilizzo, e successivamente almeno ogni sei mesi, oppure ogni tre mesi in caso di trattamento di dati sensibili e di dati giudiziari. La password deve essere costituita da almeno otto caratteri costituiti da lettere (maiuscole e/o minuscole), numeri e caratteri speciali, evitando parole di senso compiuto facilmente individuabili.

2. Le username o userid non hanno scadenza, se non alla cessazione del rapporto di lavoro. In caso di furto delle credenziali l'utente è tenuto a segnalarlo tempestivamente al Data Protection Officer, al proprio responsabile e al RTD; la rigenerazione delle credenziali è a cura del RTD. Al momento della cessazione del rapporto di lavoro, l'ufficio personale del comune segnala, via e-mail, al RTD la necessità di revocare le credenziali.

3. Si distinguono credenziali di accesso alla rete e di accesso ai programmi autorizzati, ciascuna con una specifica password, in particolare:
   - password di rete, per l'avvio e l'utilizzo del sistema operativo e di tutte le risorse di rete;
   - password per l'accesso a particolari programmi e applicativi.

4. L'utente, in caso di prolungata e improvvisa assenza, può delegare un altro utente (c.d. fiduciario) all'accesso ai dati ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

Dell'avvenuto conferimento della delega, l'utente delegante deve informare tempestivamente il Segretario comunale e il proprio responsabile d'ufficio. Di ciascun accesso dovrà essere redatto apposito verbale e informato l'utente delegante alla prima occasione utile. Nel caso in cui il dipendente non abbia delegato un suo fiduciario, il Segretario/Responsabile dell'ufficio di appartenenza a cui il dipendente è assegnato può richiedere al RTD di disporre l'accesso alla postazione e/o alla casella di posta elettronica del dipendente assente da parte dell'Amministratore di sistema, in modo che si possa prendere visione delle informazioni e dei documenti per inderogabili necessità di svolgimento dell'attività lavorativa. Contestualmente, il RTD deve informare il dipendente dell'avvenuto accesso appena possibile fornendo adeguata spiegazione e redigendo apposito verbale.

5. In relazione alla necessità di limitarne gli accessi al solo personale specificamente autorizzato e di evitare l'uso improprio della rete informatica, il Segretario//Responsabile dell'ufficio di competenza ha il dovere di segnalare al RTD la necessità di disattivare le credenziali di accesso ai sistemi o alla rete o alla casella di posta elettronica, precedentemente attribuite ad utenti su richiesta del medesimo Segretario//Responsabile, qualora le motivazioni poste a base della richiesta venissero meno.

6. La sospensione delle credenziali avverrà d'ufficio qualora le stesse non vengano utilizzate per un periodo di sessanta giorni consecutivi.

7. L'accesso alle risorse della rete interna dall'esterno è consentito esclusivamente tramite un collegamento che necessita di autenticazione VPN (Virtual Private Network) ovvero solo gli utenti autorizzati vi possono accedere. L'abilitazione e le credenziali di accesso vengono forniti dal RTD, previa autorizzazione del Segretario//Responsabile competente e con assunzione di responsabilità da parte del dipendente, ed unicamente tramite PC o laptop configurati ed installati secondo i profili definiti dal Comune e verificati dal RTD.

8. È assolutamente vietato fare accesso a qualsiasi sistema informatico con credenziali diverse da quelle assegnate.

9. Ogni utente è responsabile della corretta gestione della propria password, dei dispositivi di riconoscimento, delle informazioni per l'accesso ai sistemi e ai dati. Le credenziali sono personali e non cedibili, devono essere riconducibili al proprietario e devono essere assegnate in base alla necessità di accedere ai dati o ai sistemi comunali sulla base del principio del "minimo privilegio".

10. Le password devono soddisfare i seguenti requisiti minimi:
    - Non devono contenere il nome dell'account dell'utente o parti del nome completo dell'utente che superino due caratteri consecutivi
    - Devono avere almeno 8 caratteri di lunghezza
    - Devono contenere almeno tre delle seguenti quattro categorie:
        - Caratteri maiuscoli inglesi (dalla A alla Z)
        - Caratteri minuscoli inglesi (dalla a alla z)
        - Numeri (da 0 a 9)
        - Caratteri non alfabetici (ad esempio, !, $, #, %)
    - Devono essere cambiate almeno ogni 180 giorni
    - Le vecchie password non possono essere riutilizzate prima di sei modifiche

11. Quando l'autenticazione a più fattori non è supportata, le utenze con ruolo amministratore devono utilizzare credenziali di elevata robustezza (e.g. almeno 14 caratteri). Le stesse utenze devono inoltre sostituire le password con cadenza trimestrale.

12. Per un livello di sicurezza maggiore, è consigliabile per tutti gli utenti utilizzare un "pass

phrase" anziché una password. Per "pass phrase" si intende una frase di senso compiuto, compreso spazi e segni ortografici. Tali frasi possono essere significative per l'utente e quindi facilmente ricordabili, ma risultano molto difficili da indovinare per i sistemi automatici. A puro titolo di esempio: "Il-mio-gatto-è-Silvestro"; "Mia-figlia-è-nata-il 21.05.2007"

Articolo 5 - Utilizzo del personal computer

1. Il Personal Computer, sia fisso che portatile, affidato al dipendente è uno strumento di lavoro; pertanto vi devono essere archiviati solo dati relativi all'attività svolta e non dati propri.
2. Le impostazioni dei PC e dei relativi programmi sono predisposte dal RTD sulla base di criteri e profili decisi dal comune in funzione della qualifica del dipendente e delle mansioni a cui questo è adibito. Il dipendente non può modificarle autonomamente; eventuali variazioni necessarie possono essere effettuate solo dal RTD.
3. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal RTD. Non è altresì consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
4. Solo il personale incaricato dal RTD è autorizzato a compiere interventi nel sistema informatico comunale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento, installazione di programmi, manutenzione hardware etc.).
5. Non è consentita all'utente l'attivazione della password all'accensione del PC (BIOS), senza preventiva autorizzazione da parte del RTD.
6. I PC portatili devono essere collegati alla rete almeno ogni 15 giorni. In questo modo si garantisce che ricevano dai sistemi centrali gli aggiornamenti predisposti per tutte le postazioni client.

Articolo 6 - Utilizzo di strumenti privati

1. L'utilizzo di computer di proprietà di dipendenti, dirigenti, assessori, collaboratori, è consentito solo se questi siano dotati da software antivirus, approvato dal RTD, e regolarmente aggiornato.
2. L'utilizzo dei personal computer portatili deve seguire le stesse regole previste per i personal computer connessi in rete.
3. Ove possibile, i dischi dei PC portatili devono essere cifrati.
4. L'eventuale furto o smarrimento del pc portatile deve essere tempestivamente denunciato all'autorità competente con indicazione della marca, modello, numero seriale. Successivamente dovrà essere presentata copia della denuncia al RTD ed informato il Responsabile per la protezione dei dati personali ed il proprio Responsabile.
5. È vietato l'utilizzo di smartphone e tablet per connettersi dall'esterno alle applicazioni e dati del S.I comunale. Tali strumenti possono essere utilizzati per connettersi al sistema di posta elettronica.

Articolo 7 - Salvataggio dei dati, utilizzo supporti rimovibili

1. Nel rispetto dell'obbligo, previsto dall'art. 35 del D.L. 76/2020, di migrare i propri CED verso ambienti cloud, il Comune ha migrato il software che compone il proprio Sistema Informativo in tale modalità. Eventuali applicativi legacy operanti in modalità diversa devono essere segnalati al RTD che procederà a individuare la modalità per il successivo passaggio al cloud o gestione del server.
2. La sicurezza e il salvataggio dei dati, nonché il regolare aggiornamento del software in Cloud è assicurato dai contratti stipulati con i vari fornitori.
3. I dischi e le altre unità di memorizzazione locali (es. disco C: del PC, pen drive) non sono soggetti al salvataggio automatico.
4. I supporti magnetici rimovibili (CD, DVD, pen drive, dischi fissi esterni, etc.) contenenti dati personali e/o informazioni di proprietà del Comune e/o di terzi, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato, perso, distrutto o, successivamente alla normale cancellazione, recuperato da terzi. In ogni caso, i supporti magnetici devono essere custoditi sotto chiave o, comunque, in luoghi non accessibili a terzi. È preferibile che i dati contenuti in questi dispositivi siano criptati.

Articolo 8 - Utilizzo di altri dispositivi, stampanti e materiali di consumo

1. L'utilizzo delle stampanti e dei materiali di consumo (carta, inchiostro, toner, supporti magnetici, supporti digitali) è riservato esclusivamente ai compiti di natura strettamente istituzionale.
2. Ciascun utente avrà cura di evitare sprechi o utilizzi inappropriati dei suddetti materiali. In particolare, per quanto riguarda le operazioni di stampa, verificherà previamente le impostazioni della stampante e il numero delle pagine da stampare, onde evitare stampe errate o superflue e prediligerà la stampa fronte-retro.
3. Il dipendente è tenuto ad osservare le medesime precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti i dispositivi elettronici comunali di cui fa uso, tra cui ad esempio fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari, pen drive e supporti di memoria. In generale tutti i dispositivi elettronici comunali sono forniti al dipendente per lo svolgimento della sua attività lavorativa. L'uso per fini personali è da considerare pertanto eccezionale e limitato ad utilizzo occasionale e di breve durata.

Articolo 9 - Protezione antivirus e anti-malware

1. All'atto del collegamento in rete, il software antivirus sui singoli PC viene controllato ed eventualmente aggiornato da un server centrale gestito dal RTD; il software su tale server è aggiornato costantemente.
2. Il sistema informatico del Comune è protetto da apposito software anti-malware, aggiornato con la massima frequenza rispetto alle ultime tipologie di attacco scoperte, gestito tramite una console centralizzata che assicura la massima efficacia dell'azione di contrasto. Il SII configura ed attiva, nei personal computer assegnati al personale per la propria postazione di lavoro, i firewall locali; le relative regole di protezione sono definite, controllate e distribuite dal sistema centrale di gestione.
3. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico comunale mediante virus o mediante ogni altro software dannoso. Nel caso in cui il

software antivirus rilevi la presenza di un virus, l'utente deve immediatamente sospendere ogni elaborazione in corso nonché segnalare prontamente l'accaduto al RTD.

4. Ogni dispositivo magnetico di provenienza esterna al comune deve essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso sia rilevato un virus, deve essere prontamente catalogato come “fuori uso” e bonificato.

Articolo 10 – Posta elettronica

1. La posta elettronica è uno strumento fornito dal comune esclusivamente quale supporto all’attività lavorativa, ivi comprese le attività che siano strumentali e connesse alla stessa.
2. Poiché le caselle di posta sono di proprietà del Comune, che ne concede l’uso ai dipendenti secondo le norme indicate nella presente istruzione, i dipendenti assegnatari sono responsabili del corretto utilizzo delle stesse.
3. L’utilizzo di account istituzionali è consentito per i soli fini connessi all’attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione dell’amministrazione. L’utilizzo di caselle di posta elettronica personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all’account istituzionale.
4. Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall’amministrazione. Ciascun messaggio in uscita deve consentire l’identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.
5. È vietato l’invio di messaggi di posta elettronica, all’interno o all’esterno dell’amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell’amministrazione.
6. Le comunicazioni via posta elettronica devono avere un contenuto professionale, corretto e rispettoso a tutela della dignità delle persone e dell’immagine e reputazione del Comune. Le comunicazioni in uscita devono essere firmate inserendo sempre il proprio nome e cognome, servizio di appartenenza, “Comune” e recapito telefonico.
7. A ciascun utente, al momento dell’assunzione e/o attivazione del contratto, è assegnata una casella di posta elettronica. L'attivazione di una ulteriore casella di posta elettronica a supporto della funzione, per esempio di gruppo o di progetto, deve essere richiesta tramite il responsabile della struttura organizzativa.
8. In caso di assenza preventivata (ad es., per ferie o attività di lavoro fuori sede) gli utenti dovranno impostare il proprio sistema di Posta Elettronica in modo che possa inviare automaticamente, messaggi di risposta contenenti i riferimenti di un altro soggetto o altre utili modalità di contatto della struttura.
9. In caso di eventuali assenze non programmate (ad es. per malattia), qualora il lavoratore non possa attivare la procedura sopra descritta (anche avvalendosi di servizi webmail), il Titolare del trattamento, perdurando l’assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l’amministratore di sistema) l’attivazione di un analogo accorgimento, avvertendo gli interessati.
10. In previsione che in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all’attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, il lavoratore dovrà delegare, anche preventivamente, un utente (c.d. fiduciario) a verificare il contenuto di messaggi e ad inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo

svolgimento dell'attività lavorativa. Il Fiduciario provvederà a verbalizzare tale attività e ad informare il lavoratore interessato alla prima occasione utile.

11. I messaggi di posta elettronica devono contenere un avvertimento ai destinatari nel quale sia dichiarata la natura non personale dei messaggi stessi, precisando: *"Messaggio riservato attinente all'attività del Comune e contenente informazioni di natura professionale. Le eventuali risposte potranno essere conosciute da altri soggetti nell'ambito dell'organizzazione del mittente. Se ricevuto per errore, o non delegati dal destinatario, Vi preghiamo di comunicarcelo e di eliminarlo definitivamente".*
12. Il personale è tenuto a non aprire allegati di posta contenuti in e-mail aventi mittente e/o oggetto sospetti; ciò al fine di prevenire danni causati da software nocivi (per es. virus, worm, spyware, ecc.) che potrebbero essere contenuti negli allegati delle e-mail stesse.
13. Al fine di prevenire spamming e phishing, si raccomanda di:
    - non rispondere mai a messaggi di presunto spamming, neppure se al momento della cancellazione della mail viene richiesta conferma di lettura dal mittente, poiché ciò consente al mittente di verificare l'effettiva esistenza dell'indirizzo di posta dell'utente;
    - non rispondere o inoltrare e-mail di c.d. "Catene di S. Antonio", ovvero messaggi dal contenuto ambiguo che esortano ad inoltrare urgentemente delle copie ad altre persone;
    - non spedire un'e-mail a tutti i dipendenti del Comune; se proprio necessario, si deve utilizzare ":bcc" sia per rispettare la privacy sia per evitare che le eventuali risposte vadano anch'esse a tutti i dipendenti;
    - prestare massima attenzione alle e-mail che richiedono di fornire dati riservati quali password o numeri di carta di credito, attraverso la compilazione di moduli web (per es. da parte di una banca, di un operatore telefonico, di studi legali o di fornitori di servizi, ecc.).
14. È vietato l'utilizzo dell'indirizzo e-mail comunale per l'iscrizione a qualsiasi servizio on line (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale etc.) che non sia strettamente correlato alla propria attività istituzionale.
15. La posta elettronica comunale può essere utilizzata da dispositivi personali (es. Tablet, cellulare, etc) solo tramite il servizio Webmail.

Articolo 11 - Navigazione Internet

1. L'accesso alla rete Internet è stato fornito al personale a beneficio della produttività dando la possibilità di usufruire delle risorse informative presenti nella rete. Il personale ha la responsabilità di utilizzare la rete Internet per finalità legittime e strettamente necessarie allo svolgimento delle mansioni lavorative.
2. Non è consentito ai dipendenti l'utilizzo di modem personali (es. hotspot o altri sistemi), o di qualunque altro dispositivo di navigazione del tipo "internet-Key" con account personali;
3. È espressamente vietato:
    - lo scarico di software gratuiti e shareware prelevati da siti internet, salvo casi espressamente autorizzati;
    - ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
    - la partecipazione, per motivi non professionali a Forum, l'utilizzo di Chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (nickname);

- la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinione e appartenenza sindacale e/o politica;
- scaricare/scambiare materiale coperto da diritto d'autore (es. film, musica, ebook, etc.);
- scaricare/scambiare materiale a contenuto pornografico o pedopornografico;
- eseguire o favorire pratiche di Spamming.

4. È ammesso l'utilizzo di Internet per assolvere a proprie incombenze amministrative e burocratiche (ivi comprese le operazioni di remote Banking, acquisti on line e simili) senza allontanarsi dal luogo di lavoro. Tale modalità di utilizzo di Internet deve essere contenuta nei tempi strettamente necessari allo svolgimento delle transazioni e privilegiando, quando possibile, l'utilizzo delle pause di lavoro. Il fine è quello di contribuire a ridurre gli spostamenti delle persone e gli oneri logistici e di personale a carico dell'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi (par. 3 "Utilizzo della rete Internet" della Direttiva n. 2/2009 della Presidenza del Consiglio dei ministri, Dipartimento della funzione pubblica).

Articolo 12 - Controlli e monitoraggio

1. Il Comune si riserva di effettuare controlli sul corretto utilizzo degli strumenti informatici e telematici nel rispetto delle normative vigenti e della presente istruzione.
2. Per esigenze organizzative, produttive e di sicurezza il Comune può avvalersi di strumenti che consentono un controllo a distanza di tipo generalizzato e indiretto, relativo ad aree, settori o gruppi di utenti. Qualora – durante un controllo generalizzato – vengano rilevate anomalie nell'utilizzo degli strumenti informatici, il Comune procede preliminarmente all'invio di un avviso generalizzato relativo all'uso improprio riscontrato, con l'invito ad attenersi scrupolosamente alla presente istruzione, e riservandosi la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo.
3. In nessun caso il Comune perseguirà finalità di controllo a distanza diretto, sistematico e/o intenzionale dell'attività dei lavoratori. In particolare, in linea con quanto previsto dalla Deliberazione n. 13/2007 del Garante per la protezione dei dati personali, non si procederà:
    - alla lettura e alla registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per lo svolgimento del servizio;
    - alla riproduzione e alla eventuale memorizzazione sistematica delle pagine web visualizzate;
    - alla lettura e alla registrazione dei caratteri inseriti tramite tastiera o analogo dispositivo;
    - all'analisi occulta di computer affidati in uso.
4. I sistemi informativi sono verificati sia periodicamente sia su segnalazione di incidenti di sicurezza, allo scopo di garantirne l'efficienza, la disponibilità ed il rispetto di leggi e regolamenti interni, ed in particolare dei requisiti minimi di sicurezza previsti dalla normativa vigente in materia di protezione dei dati personali.
5. Le attività degli utenti possono essere registrate in files di LOG come di seguito indicato:
    - log del firewall: tale raccolta viene attivata solo in caso di necessità per effettuare verifiche sul funzionamento della rete e poter identificare incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;

- log del server di posta: tali log vengono raccolti e conservati per poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log del software applicativo del Sistema Informativo: tali log vengono raccolti e conservati per poter effettuare verifiche di sicurezza e poter identificare anche a posteriori incidenti di sicurezza, violazione delle policy o attività fraudolente e procedere alla raccolta delle evidenze;
- log degli accessi degli amministratori di sistema ai sistemi amministrati: la raccolta e conservazione di tali log è motivata dalla necessità di ottemperare al Provvedimento del Garante per la Protezione dei dati personali relativo agli amministratori di sistema.

6. L'accesso ai log ed ai contenuti dei sistemi di posta elettronica è permesso solo ed esclusivamente nei seguenti casi:
   - Richiesta Autorità Giudiziaria;
   - Richiesta Pubblica Sicurezza;
   - Attività ispettive preventive e/o difensive (Organi di vigilanza);
   - Soluzione di incidenti informatici o telematici;
   - Esigenze di continuità operativa (recupero dati, assenze prolungate, etc.).
7. I tempi di conservazione previsti per le tipologie di log sopra elencate è fissato per un periodo semestrale. Ciò è motivato dalla necessità di utilizzare tali log per la verifica delle attività degli amministratori di sistema prevista dal provvedimento del Garante per la Protezione dei dati personali relativi agli amministratori di sistema e di avere una policy di retention dei log adeguata a tutte le tipologie, in modo da semplificare ed economizzare la gestione del sistema dei log e delle politiche di backup.
8. In caso di controlli preventivi (di effettivo rispetto di regole comunali) e per accesso dovuti ad esigenze di continuità, il lavoratore interessato dovrà essere preavvisato al fine di garantire la correttezza e la trasparenza verso il lavoratore per mezzo della preventiva informazione.
9. Per i controlli difensivi o richiesti da Pubbliche Autorità (PS, ecc.), ovvero in casi di incidenti che necessitino interventi immediati e urgenti, la preventiva informazione può essere omessa, in quanto può compromettere la difesa o l'accertamento di diritti o di responsabilità in giudizio o l'attività istituzionale dell'ente. Nel caso di incidenti di tal natura, l'informazione potrà/dovrà essere data a posteriori.
10. Nell'espletare controlli e verifiche, le funzioni preposte devono garantire la massima riservatezza dei dati conosciuti, anche incidentalmente, pena l'applicazione di sanzioni disciplinari in base alla gravità dell'accaduto. I dati potranno essere comunicati solo ed esclusivamente a soggetti interni o esterni del comune per cui la comunicazione sia dovuta in relazione alle finalità perseguite con l'accesso (per esempio, nei casi indicati al comma 3, alle Forze dell'Ordine, ad incaricati di funzioni comunali preposte alle azioni legali o alla soluzione dei problemi.

Articolo 13 - Controllo accessi fisici

1. Le indicazioni contenute nel presente capitolo mirano alla riduzione dei rischi derivanti dall'accesso di soggetti non autorizzati alla sede del Comune e ai locali tecnici.
2. I vani tecnici delle sedi sono deputati a rappresentare le aree sicure finalizzate a prevenire l'accesso fisico non autorizzato, danni e disturbi alle informazioni del Comune ed alle infrastrutture di elaborazione delle informazioni.

3. L’accesso ai suddetti vani è consentito unicamente al RTD o un suo delegato.

Articolo 14 – L’Amministratore di Sistema

1. L’amministratore di sistema è individuato con atto del Legale Rappresentante dell’Ente, sentito il Responsabile per la Transizione al Digitale (RTD).
2. L’accesso ai sistemi con privilegi amministrativi è consentito solo all'Amministratore di sistema e al Responsabile per la Transizione Digitale (o un loro delegato che abbia le competenze ed effettive necessità di modificare la configurazione dei sistemi).
3. Tutte le funzioni, di cui al presente regolamento, affidate al Responsabile per la Transizione Digitale, possono essere delegate dallo stesso all’Amministratore di Sistema.
4. L’atto di incarico dell'Amministratore di sistema deve indicare almeno le seguenti attività allo scopo di soddisfare quanto previsto dalle Misure Minime di Sicurezza dell’AGID:
   a. Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato
   b. Scrivere un documento, approvato dal RTD, che indichi la configurazione standard e le policy di dominio con la quale tutte le postazioni PC vengono create e gestite utilizzando un’immagine standard. L’immagine standard è creata con l’obiettivo di limitare le azioni degli utenti che possano compromettere la propria postazione o la rete dell’ente. L’utente non può installare software, modificare configurazioni (es. impostazioni dei browser installati, associazione delle estensioni), creare/modificare utenti e gruppi locali, modificare i permessi su file system ecc.
   c. Predisporre e mantenere aggiornata la configurazione base da installare sui PC
   d. Effettuare, con cadenza mensile, la procedura di monitoraggio e di vulnerability assessment, nonché l'aggiornamento del antivirus ogni volta venga rilasciata un aggiornamento del codice o della base dati
   e. Verificare che le vulnerabilità emerse dalle scansioni dei software siano effettivamente sanate dopo l’installazione di patch o di azioni correttive che ne limitano il possibile rischio
   f. Predisponga un documento in cui elencare quali apparati sono esposti a maggior rischio rispetto ad altri (es. per tipologia di servizio o per i tipi di dati trattati, ecc.) indicando precisamente il livello di rischio corrispondente (Alto, Medio e Basso). Per rischio si intende il tipo di criticità, che al verificarsi dell’evento malevolo, potrebbe influire gravemente sul funzionamento della struttura o di una sua parte.

Art. 15 – Dismissione apparecchiature informatiche

1. 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 RTD/Servizio Patrimonio/Servizio ICT, secondo quanto previsto dalla normativa (GDPR, Rifiuti di apparecchiature elettriche ed elettroniche (Raae), ecc) e secondo le procedure previste dal servizio 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. 16 – Aggiornamento delle disposizioni e delle regole tecniche

1. 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 Responsabile per la Transizione al Digitale (RTD) 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
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
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.
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
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.XXX.it , 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.XXXXX.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
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 specificamente 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'Informazione 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
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.

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

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.
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
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
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
Sandbox	È 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
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.

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 fase 2
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"
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 ad un'impresa di svolgere efficacemente la propria funzione quotidiana indipendentemente dalla posizione.