Comune di Padova

REGOLAMENTO SULL'UTILIZZO E ACQUISIZIONE DELLE RISORSE INFORMATICHE E TELEMATICHE DEL COMUNE DI PADOVA

°°°

Approvato con deliberazione G.C. n. 45 del 04/02/2025
In vigore dal 05/03/2025

INDICE

CAPO I: FINALITÀ - AMBITO DI APPLICAZIONE - PRINCIPI GENERALI....3
Art. 1 – Finalità....3
Art. 2 – Principi generali....3
Art. 3 – Ambito di applicazione....3
Art. 4 – Definizioni....4
Art. 5 – Accesso alle risorse informatiche e telematiche....5
Art. 6 – Tracciatura (Log) dei sistemi....5
Art. 7 – Disposizioni generali per l'utilizzo delle risorse informatiche e telematiche....6
Art. 8 – Disposizioni relative alle risorse di elaborazione centrali, storage e di rete....6
Art. 9 – Compiti degli/delle amministratori/amministratrici di sistema....7
CAPO II: REGOLE SPECIFICHE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE....8
Art. 10 – Assegnazione postazioni di lavoro....8
Art. 11 – Assegnazione telefono/tablet di servizio e/o SIM card aziendale....9
Art. 12 – Rilascio di certificati e dispositivi di firma digitale....9
Art. 13 – Assegnazione di servizi applicativi....10
Art. 14 – Utilizzo delle postazioni di lavoro....10
Art. 15 – Utilizzo degli strumenti stampa....12
Art. 16 – Utilizzo delle credenziali....12
Art. 17 – Utilizzo delle cartelle condivise e delle copie di salvataggio....12
Art. 18 – Utilizzo della navigazione su Internet....13
Art. 19 – Utilizzo delle Virtual Private Network (VPN)....13
Art. 20 – Utilizzo di caselle di posta elettronica....14
Art. 21 – Acquisizione nuove risorse informatiche e telematiche....16
Art. 22 – Controlli di cybersecurity e difensivi....16
Art. 23 – Gestione delle risorse informatiche e telematiche in caso di assenza dal lavoro....17
Art. 24 – Gestione delle informazioni alla cessazione del rapporto di lavoro....18
CAPO III - ENTRATA IN VIGORE E ABROGAZIONI....18
Art. 25 – Entrata in vigore e abrogazioni....18
RIFERIMENTI NORMATIVI....19

CAPO I: FINALITÀ - AMBITO DI APPLICAZIONE - PRINCIPI GENERALI

Art. 1 – Finalità

1. Il presente Regolamento definisce le regole atte a salvaguardare la sicurezza del sistema informatico del Comune di Padova e a tutelare la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati, anche personali, da questo prodotti, raccolti o comunque trattati.

Art. 2 – Principi generali

1. Il Comune di Padova considera le risorse applicative, di elaborazione, di storage e i servizi di rete, nonché i dati e le informazioni da questi trattati, parte integrante del proprio patrimonio strumentale, funzionale al raggiungimento delle proprie finalità istituzionali.
2. Il Comune di Padova effettua il trattamento dei dati raccolti nell'ambito delle risorse applicative e dei servizi di rete solo per finalità determinate, esplicite e legittime, nel rispetto dei principi di necessità, pertinenza, correttezza e non eccedenza. I sistemi informativi e i programmi informatici sono pertanto configurati in modo tale da ridurre al minimo l'utilizzo dei dati personali e identificativi.
3. Tutti/e coloro cui è consentito l'accesso alle risorse applicative e ai servizi di rete sono tenuti/e al rispetto delle disposizioni di seguito esposte, che definiscono e integrano i doveri minimi di condotta previsti nel Codice di Comportamento del personale dipendente del Comune di Padova, oltre, comunque, a un comportamento ispirato ai principi di correttezza e diligenza.
4. L'uso degli strumenti informatici non è finalizzato all'esercizio di un controllo a distanza dei/delle lavoratori/lavoratrici da parte del/della datore/datrice di lavoro, ma solo a permettere a quest'ultimo/a di utilizzare sistemi informativi per fare fronte a esigenze produttive o organizzative, di sicurezza informatica e di protezione dei dati personali (vedi art. 4, c. 1 della L. 300/1970 e art. 23 del D.Lgs. 151/2015);
5. Il Comune di Padova garantisce al/alla singolo/a lavoratore/lavoratrice assegnatario/a il controllo sui propri dati personali secondo quanto previsto dagli artt. 15, 16, 17, 18, 20, 21, 77 del Regolamento (UE) 2016/679 e nel rispetto delle "Linee guida del Garante per posta elettronica e internet", pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Art. 3 – Ambito di applicazione

1. Il presente Regolamento si applica a tutti/e coloro cui è consentito l'accesso alle postazioni di lavoro, ai servizi applicativi, di storage, di rete, di sensoristica, di telefonia fissa e mobile e a

qualsiasi dispositivo del Comune di Padova tramite il quale risulti possibile accedere alla rete internet o intranet.

Art. 4 – Definizioni

1. Nell'ambito del presente Regolamento si intende per:
   a. **Amministratori/Amministratrici di Sistema**: figura professionale dedicata alla gestione e alla manutenzione di sistemi di elaborazione con cui vengano effettuati trattamenti di dati, anche personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza;
   b. **Apparati di rete**: apparati di rete wired e wireless per l'interconnessione delle risorse informatiche, compresi gli apparati di interconnessione a internet;
   c. **Assegnatario/a:** dipendenti, amministratori/amministratrici, collaboratori/collaboratrici, stagisti/e o altri/e autorizzati/e cui viene assegnata una dotazione informatica del Comune di Padova;
   d. **Casella di posta elettronica istituzionale**: casella di posta assegnata a una struttura dell'Ente (Settore, U.O.C., U.O.S.) o a uno specifico progetto a cui possono accedere con diverse abilitazioni più soggetti preventivamente autorizzati;
   e. **Casella di posta elettronica istituzionale individuale**: casella di posta elettronica assegnata alla singola persona;
   f. **Dati**: manifestazione concreta di una certa quantità di informazione, per mezzo della sua codifica. Il Comune di Padova produce e tratta diverse tipologie di dato, ognuna con un proprio ciclo di vita e regole di utilizzo in relazione al suo dominio e alla finalità;
   g. **Digital Trainer**: personale dell'Ente con competenze digitali incaricati di supportare i colleghi e il Settore Innovazione e Transizione Digitale (ITD) nell'utilizzo delle risorse informatiche e nel processo di transizione digitale;
   h. **Firma elettronica qualificata** o **Firma digitale**: risultato di una procedura informatica che garantisce l'autenticità, l'integrità e il non ripudio dei documenti informatici; si basa sull'utilizzo di un dispositivo e di un certificato qualificato per firme elettroniche;
   i. **Log**: registrazione sequenziale e cronologica delle operazioni effettuate da un utente, un/una amministratore/amministratrice o automatizzate, man mano che vengono eseguite dal sistema o dall'applicazione;
   j. **Mediatore digitale**: personale dell'Ente con competenze digitali, che collabora e supportare gli uffici dell'Ente e il Settore Innovazione e Transizione Digitale nei progetti di trasformazione digitale;
   k. **Postazioni di lavoro**: servizi applicativi, PC, notebook, tablet, smartphone e tutti i dispositivi hardware utilizzati per l'espletamento delle attività istituzionali;
   l. **Risorse informatiche**: le postazioni di lavoro, i servizi applicativi, le risorse di calcolo e storage e i servizi di rete del Comune di Padova;
   m. **RPD (Responsabile Protezione Dati)** o **DPO (Data Protection Officer)**: figura designata dall'Ente a sensi degli artt. 37-39 del Regolamento (UE) 2016/679, in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati;

n. **RTD**: Responsabile per la Transizione Digitale ai sensi dell'art. 17 del D.Lgs 82/2005 Codice dell'amministrazione digitale;
o. **Server:** risorse di elaborazione centrali (fisiche e virtuali) sia in modalità on-premise (installate presso Data Center dell'Ente) sia presso Cloud Service Provider in modalità IaaS (Infrastrutture as a Service) e PaaS (Platform as a Service);
p. **Servizi applicativi: s**oftware gestionali, servizi di collaborazione (posta elettronica, chat, videoconferenza…), software di calcolo e Data Analytics e ogni altra risorsa utilizzata per il trattamento di dati, sia installati presso sistemi propri dell'Ente (on-premise) sia in modalità SaaS (Software as a Service) o ibrida;
q. **Settore Innovazione e Transizione Digitale:** struttura competente per lo sviluppo e la gestione delle risorse informatiche e telematiche, a supporto del/della Responsabile per la Transizione Digitale;
r. **Storage**: sistemi di memorizzazione dei dati;
s. **Ufficio Privacy**: unità operativa semplice che ha il compito di sovraintendere allo svolgimento delle attività di trattamento di dati personali svolte presso altri settori, al fine di supportare il/la Referente privacy di settore nello svolgimento delle attività di sua competenza e di garantire il rispetto di tutti gli obblighi previsti dal Regolamento (UE) 2016/679 e dalla normativa nazionale in capo al "Titolare del trattamento";

Art. 5 – Accesso alle risorse informatiche e telematiche

1. L'accesso alle risorse informatiche e telematiche del Comune di Padova è consentito, previa identificazione, a dipendenti, amministratori/amministratrici, collaboratori/collaboratrici, stagisti/e o altri/e autorizzati secondo le disposizioni del presente Regolamento.
2. L'autorizzazione all'accesso alle risorse informatiche e telematiche avviene attraverso credenziali che sono assegnate a seguito dell'inserimento nelle anagrafiche del sistema di gestione delle risorse umane o, nel caso di collaboratori/collaboratrici e stagisti/stagiste, tramite atto specifico di nomina e autorizzazione del settore competente.
3. L'accesso è personale, non può essere condiviso o ceduto e il relativo utilizzo è consentito a ciascun/a utente soltanto in conformità alle disposizioni del presente Regolamento e della normativa vigente applicabile.

Art. 6 – Tracciatura (Log) dei sistemi

1. La conservazione dei log è un aspetto cruciale per garantire la sicurezza dei dati personali e dimostrare la conformità alle norme sulla privacy.
2. La raccolta dei log e la loro conservazione si applica alle componenti di Data Center, Networking e Postazioni di Lavoro. I log di navigazione internet e di posta elettronica sono raccolti nel rispetto dei provvedimenti del Garante per la protezione dei dati personali.
3. La conservazione dei log degli amministratori di sistema verrà gestita ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008.

Art. 7 – Disposizioni generali per l'utilizzo delle risorse informatiche e telematiche

1. Le risorse informatiche e telematiche, in quanto essenziali per il Comune di Padova, sono rese disponibili per il conseguimento delle finalità istituzionali dell'Ente. Gli/Le utenti sono tenuti/e a servirsi delle risorse informatiche e telematiche dall'Ente loro assegnate in dotazione prestando il proprio contributo affinché ne sia preservata l'integrità e garantito il buon funzionamento e la corretta custodia.
2. Comportamenti difformi da quanto previsto dal presente Regolamento possono causare gravi rischi alla sicurezza e all'integrità dei sistemi aziendali e possono essere oggetto di valutazione da un punto di vista disciplinare, oltre che da un punto di vista penale. Pertanto, sono vietati:
   a. l'utilizzo delle risorse informatiche e telematiche messe a disposizione dal Comune all'assegnatario/a difforme dagli obblighi di cui agli artt. 2104 "Diligenza del prestatore di lavoro" e 2105 "Obbligo di fedeltà" del Codice civile;
   b. le attività commerciali, o comunque lucrative, non autorizzate, nonché la trasmissione di materiale commerciale e/o pubblicitario non richiesto (spamming) o l'uso delle proprie risorse da parte di terzi per tali attività;
   c. le attività comunque idonee a danneggiare, distruggere, compromettere la sicurezza delle risorse informatiche dell'Ente o dirette a violare la riservatezza e/o cagionare danno a terzi, ivi inclusa la creazione, trasmissione e conservazione di immagini, dati o altro materiale offensivo, diffamatorio, osceno, indecente o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza, la religione, le opinioni politiche o la condizione personale o sociale;
   d. le attività comunque non conformi ai fini istituzionali dell'Ente.

3. È consentito l'utilizzo sporadico delle risorse informatiche per finalità personali purché questo non violi le leggi applicabili e sia compatibile con le disposizioni del presente Regolamento nonché dei vigenti regolamenti del Comune di Padova.

Art. 8 – Disposizioni relative alle risorse di elaborazione centrali, storage e di rete

1. Al fine di garantire la sicurezza delle risorse di elaborazione, storage e di rete è vietato:
   a. connettere risorse informatiche alla rete locale o ad altri servizi che includono la connettività di rete senza l'autorizzazione del Settore Innovazione e Transizione Digitale;
   b. cablare, collegare o modificare apparati di rete senza l'autorizzazione del Settore Innovazione e Transizione Digitale;
   c. utilizzare indirizzi di rete e nomi non espressamente assegnati;

d. installare o modificare le configurazioni dei sistemi, hardware o software, che consentano accesso alle risorse informatiche senza l'autorizzazione del Settore Innovazione e Transizione Digitale;
e. fornire accesso alle risorse informatiche a soggetti non espressamente autorizzati;
f. divulgare informazioni sulla struttura e configurazione delle risorse informatiche, con particolare riferimento a quelle che consentono accesso da remoto (VPN, firewall);
g. accedere senza autorizzazione ai locali dei servizi di calcolo, nonché ai locali e alle aree riservate alle apparecchiature di rete;
h. intraprendere ogni altra azione diretta a degradare le risorse del sistema, impedire ai soggetti autorizzati l'accesso alle risorse o accedere alle risorse informatiche violandone le misure di sicurezza.

Art. 9 – Compiti degli/delle amministratori/amministratrici di sistema

1. Gli/Le amministratori/amministratrici di sistema, oltre all'osservanza di tutte le disposizioni precedenti, sono tenuti/e a:
   a. mantenere i sistemi al livello di sicurezza appropriato al loro uso;
   b. verificare con regolarità l'integrità dei sistemi;
   c. controllare e conservare i log di sistema per il tempo necessario a verificare la conservazione degli standard di sicurezza;
   d. limitare l'uso interno di servizi e programmi che trasmettono in chiaro le password;
   e. segnalare immediatamente al/alla Dirigente del Settore Innovazione e Transizione Digitale sospetti abusi e violazioni della sicurezza e partecipare alla loro gestione;
   f. qualora vi sia il sospetto di accesso o violazione dei dati personali, attenersi a quanto stabilito dalla "Procedura per la gestione degli eventi di data breach ai sensi del Regolamento (UE) 679/2016";
   g. installare e mantenere aggiornati programmi antivirus per i sistemi che lo prevedono;
   h. non visionare i dati personali e della corrispondenza di cui dovessero venire a conoscenza e, comunque, a considerarli strettamente riservati e a non riferire, né duplicare o cedere a persone non autorizzate informazioni sull'esistenza o sul contenuto degli stessi;
   i. in caso di interventi di manutenzione da parte di soggetto esterno all'organizzazione, verificare l'esistenza della nomina di responsabile del trattamento predisposta ai sensi dell'art. 28 del Regolamento (UE) 2016/679 e impedire o limitare, per quanto possibile, l'accesso alle informazioni e ai dati personali presenti nei sistemi amministrati;
   j. seguire e stimolare attività formative in materie tecnico-gestionali e di sicurezza delle reti, nonché in tema di protezione dei dati personali e di segretezza della corrispondenza.

2. I/Le Responsabili dei servizi di Data Center, Networking e Sicurezza informatica sono tenuti/e a:
   a. controllare che gli accessi remoti alle risorse locali avvengano esclusivamente mediante l'uso di protocolli che prevedano l'autenticazione e la cifratura dei dati trasmessi;
   b. accertarsi che le password di amministrazione degli apparati che garantiscono la funzionalità e l'operabilità dei servizi della struttura siano condivise da almeno due

amministratori/amministratrici di sistema e mantenere aggiornato un elenco che sarà conservato in busta chiusa presso luogo sicuro individuato dal/dalla Dirigente del Settore Innovazione e Transizione Digitale;

c. sulle macchine gestite, provvedere a disattivare i servizi non essenziali e a limitare il numero degli utenti privilegiati a quello strettamente necessario per le attività di coordinamento e controllo dei servizi afferenti;
d. effettuare la revisione, almeno annuale, degli account;
e. effettuare il monitoraggio dei sistemi gestiti, registrando gli accessi privilegiati e le eventuali modifiche ai file di sistema;
f. collaborare tra di loro nella progettazione, configurazione e gestione delle reti del Data Center e dei servizi Cloud (Iaas e PaaS);
g. fornire supporto per conservare e incrementare la sicurezza delle risorse affidate agli/alle utenti.

CAPO II: REGOLE SPECIFICHE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE

Art. 10 – Assegnazione postazioni di lavoro

1. Tutte le risorse informatiche classificate come "Postazioni di lavoro" affidate agli/alle assegnatari/e sono strumenti di lavoro e devono essere utilizzati in conformità ai principi generali di cui all'art. 2 del presente Regolamento. Ogni utilizzo non inerente all'attività lavorativa può contribuire a innescare disservizi, traffico telefonico e traffico dati maggiori, costi di manutenzione e, soprattutto, minacce alla sicurezza.
2. Gli strumenti informatici vengono messi a disposizione del/della singolo/a assegnatario/a in relazione al ruolo svolto all'interno dell'Ente, su indicazione del/della Responsabile di settore. L'assegnatario/a deve custodirli e utilizzarli con la massima diligenza.
3. La consegna degli strumenti dà luogo, in capo all'assegnatario/a, a tutte le forme di responsabilità previste dalla legge nei confronti di chi detiene beni della pubblica amministrazione. All'atto della consegna degli strumenti informatici, l'assegnatario/a firma la presa visione e accettazione del presente Regolamento disponibile sulla Intranet e la ricevuta di presa in carico dei beni.
4. È vietato lo scambio di qualsiasi strumento informatico fra assegnatari/e. L'Ente si riserva di effettuare verifiche a campione sulla corrispondenza tra assegnatari e beni assegnati.
5. In caso di mobilità interna, ai fini della sicurezza informatica e della corretta gestione degli strumenti nell'inventario, deve essere attivata l'apposita procedura di trasferimento degli strumenti informatici.
6. In caso di cessazione, si rimanda a quanto prescritto dall'art. 24 del presente Regolamento.
7. Le postazioni di lavoro ad uso condiviso (ad esempio sportelli o stampanti speciali quali plotter) sono assegnate al settore utilizzatore prevalente.

Art. 11 – Assegnazione telefono/tablet di servizio e/o SIM card aziendale

1. L'assegnazione della SIM card e dell'eventuale dispositivo in uso esclusivo sono concessi, su richiesta, a:
   a. Amministratori/Amministratrici, Sindaco/a, Vicesindaco/a, Assessori/e, Segretario/a Generale, Vicesegretario/a Generale, Direttore/Direttrice Generale;
   b. Dirigenti;
   c. Funzionari/e con incarico di Alta Specializzazione e di Elevata Qualificazione, su richiesta specifica del/della proprio/a Dirigente;
   d. Assegnatari/e dell'Amministrazione con reperibilità o in modalità di lavoro con prevalenza di "fuori ufficio", su richiesta specifica del/della proprio/a Dirigente;
   e. Responsabili e gestori dei Servizi e sistemi per telegestione e/o telecontrollo dislocati sul territorio comunale (a titolo di esempio: impianti di generazione e/o distribuzione dell'energia, di calore o di sollevamento di cose e persone e di rilevamento delle presenze).

2. Può essere disposta dal/dalla Dirigente l'assegnazione del dispositivo per le esigenze di uno specifico Servizio o Ufficio, da utilizzarsi alternativamente dall'assegnatario/a del Servizio o Ufficio in ragione degli incarichi temporaneamente affidati (c.d. "utenza in rotazione" o "uso condiviso"). In tal caso il/la Dirigente cui fa capo il Servizio richiedente provvede a monitorare di volta in volta il nominativo dell'assegnatario/a, data di consegna e di riconsegna.
3. Non sono concessi telefoni o tablet di servizio a soggetti esterni all'Amministrazione, fatti salvi i casi previsti da atti, regolamenti o normative vigenti.
4. Il/La responsabile della U.O.S. Telefonia provvede alla fornitura delle SIM card e dei dispositivi e all'attivazione delle relative utenze, in attuazione delle specifiche richieste dei/delle Dirigenti fatte pervenire al Settore Innovazione e Transizione Digitale.
5. A nessun titolo i dispositivi assegnati e le relative SIM card potranno essere ceduti o utilizzati da terzi.

Art. 12 – Rilascio di certificati e dispositivi di firma digitale

1. I ruoli per i quali è previsto il rilascio dei certificati di firma digitale e dell'eventuale dispositivo in uso sono:
   a. Amministratori/Amministratrici, Sindaco/a, Vicesindaco/a, Assessori/e, Segretario/a Generale, Vicesegretario/a Generale, Direttore/Direttrice Generale;
   b. Dirigenti;
   c. Funzionari/e con incarico di Alta Specializzazione e di Elevata Qualificazione;
   d. Soggetti con potere di firma e funzione specifica nell'ambito dell'organizzazione per la quale sia necessario firmare digitalmente i documenti.

2. Nei casi di cui alle lettere c. e d. del comma 1, il certificato e l'eventuale dispositivo vengono rilasciati su indicazione del/della Capo Settore che deve dichiarare la funzione per la quale la firma è richiesta.

3. L'utilizzo del dispositivo di firma digitale si presume riconducibile al titolare di firma; pertanto, in nessun caso i certificati e i dispositivi assegnati potranno essere ceduti o utilizzati da terzi.
4. I certificati di firma sono comprensivi dell'indicazione del nome dell'organizzazione; pertanto, non possono essere utilizzati per motivi estranei alle attività e all'organizzazione del Comune di Padova, salvo casi specificatamente motivati conseguenti allo status di dipendente dell'Amministrazione (ad esempio la partecipazione a commissioni di concorso o gare in altre amministrazioni).
5. In caso di furto o smarrimento del dispositivo di firma digitale si applica quanto previsto dall'art. 14, c. 1, lett. h. del presente Regolamento;
6. Nei casi previsti dal comma 5 e in caso di termine di contratto con l'Ente o di variazione dei dati personali, l'assegnatario/a dovrà fare richiesta di revoca del certificato al Settore Innovazione e Transizione Digitale.

Art. 13 – Assegnazione di servizi applicativi

1. L'utilizzo da parte dell'utente delle risorse informatiche classificate come "Servizi Applicativi", compreso il servizio di posta elettronica, il servizio di condivisione documenti, servizi di collaborazione, l'accesso alla rete aziendale tramite Virtual Private Network (VPN), deve essere autorizzato formalmente dal/dalla Dirigente di settore o dal/dalla suo/a delegato/a e, nel caso di servizi applicativi gestionali o banche dati, dall'eventuale Designato/a del trattamento.

Art. 14 – Utilizzo delle postazioni di lavoro

1. Gli/Le assegnatari/e di postazioni di lavoro sono tenuti/e al rispetto delle disposizioni generali di cui all'art. 2 del presente Regolamento. Di seguito si riportano le indicazioni di comportamento operative, da intendersi esemplificative e non esaustive, al fine del rispetto delle disposizioni generali del presente Regolamento e della norma.
   a. Non è consentito installare autonomamente e utilizzare programmi diversi rispetto a quelli messi a disposizione con la consegna della postazione di lavoro o successivamente autorizzati. L'inosservanza della presente disposizione può comportare rischi di sicurezza informatica (ad esempio malware, virus ecc.), di danneggiamento del sistema per incompatibilità con il software esistente e può esporre l'Ente a responsabilità sia civili che penali in caso di violazione della normativa a tutela dei diritti d'autore sul software.
   b. Non è consentito all'assegnatario/a modificare le caratteristiche impostate sul proprio strumento informatico.
   c. Tutti gli apparati connessi alla rete elettrica, inoltre, devono essere spenti a fine giornata lavorativa prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.
   d. Non è consentita l'installazione sul proprio strumento informatico di alcun dispositivo di memorizzazione esterna personale (ad esempio dispositivi USB).

e. Non è consentita la sincronizzazione sulla propria postazione di lavoro di repository documentali diversi da quelli adottati dall'Amministrazione.
f. Non è consentito l'utilizzo della postazione di lavoro per l'accesso e la fruizione a contenuti non pertinenti, pericolosi o illeciti; inoltre è vietata la visione o il download di contenuti in modalità non conforme al rispetto del diritto d'autore.
g. I log relativi all'utilizzo di strumenti, reperibili nella memoria degli strumenti stessi ovvero sui server o sugli apparati di rete, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo per esigenze organizzative, per la sicurezza del lavoro e per la tutela del patrimonio. I controlli potranno avvenire secondo le modalità previste dal presente Regolamento al successivo art. 22 "Controlli di cybersecurity e difensivi".
h. In caso di furto o smarrimento di PC e dispositivi aziendali assegnati, l'assegnatario/a dovrà contattare immediatamente il Settore Innovazione e Transizione Digitale che provvederà all'attuazione delle misure di sicurezza atte a prevenire l'accesso non autorizzato alle risorse informatiche e telematiche del Comune di Padova. L'assegnatario/a presenterà personalmente formale denuncia di furto o smarrimento agli organi di Polizia. Copia della denuncia dovrà essere trasmessa all'Ufficio Amministrativo del Settore Innovazione e Transizione Digitale del Comune; si provvederà all'assegnazione di un nuovo dispositivo e al ripristino dell'utenza, secondo la disponibilità.
i. Con riguardo in particolare all'utilizzo di dispositivi telefonici e SIM card, l'assegnatario/a riceve, di norma, e su specifica richiesta scritta del/della proprio/a Dirigente:
    i. una SIM card con contratto intestato all'Amministrazione;
    ii. un telefono cellulare o tablet intestato all'Amministrazione;
    iii. accessori del dispositivo (batteria, caricabatteria, auricolare ecc.);
    iv. nei casi autorizzati, una SIM Dati intestata all'Amministrazione per collegamento dati e/o fonia.

2. Ogni assegnatario/a è chiamato/a a fornire il proprio contributo al fine di minimizzare la possibilità che i dati aziendali eccezionalmente e solo temporaneamente contenuti in telefoni cellulari, smartphone e tablet siano esposti a rischi di sicurezza.
3. È fatto divieto di disabilitare e modificare le impostazioni di sicurezza dei dispositivi, per esempio disattivare, anche temporaneamente, il PIN della SIM card, il salvaschermo, l'antivirus, violare l'integrità del sistema operativo e altre misure analoghe.
4. Gli/Le assegnatari/e, affinché possano essere immediatamente rintracciabili nei casi di necessità, hanno l'obbligo di mantenere in funzione il telefono cellulare durante le ore di servizio, durante le ore di reperibilità, ove previste, e in tutti i casi in cui le circostanze concrete lo rendano necessario e opportuno. Sono fatti salvi i casi in cui le condizioni tecniche non lo consentano.
5. I Gestori telefonici inviano periodicamente all'Ente una distinta del traffico telefonico, effettuato dagli/dalle utenti con i numeri di destinazione parzialmente oscurati; l'Ente si riserva la facoltà di addebitare all'utente importi derivanti da telefonate personali;
6. L'Amministrazione non assume alcuna responsabilità per contravvenzioni o sinistri imputabili all'uso del dispositivo telefonico durante la guida di autoveicoli o altro utilizzo improprio.

Art. 15 – Utilizzo degli strumenti stampa

1. L'utilizzo degli strumenti di stampa, quali dispositivi multifunzione, stampanti e plotter, deve avvenire con la massima diligenza ed è vietato per fini personali. Si raccomanda l'utilizzo della stampa solo tramite i dispositivi multifunzione e solo in casi indispensabili. L'Ente si riserva di effettuare verifiche sul corretto utilizzo dei dispositivi multifunzione e sulle stampe effettuate.

Art. 16 – Utilizzo delle credenziali

1. L'accesso ai dispositivi, alla rete e alle applicazioni di trattamento dati richiede il possesso di credenziali composte da un nome utente (User ID univoco) e di una parola chiave segreta (Password) e, ove implementata, la Multi Factor Autentication (ad esempio OTP). Per una corretta e sicura gestione delle proprie password devono essere rispettate le seguenti regole:
   a. le password sono personali e non vanno mai comunicate ad altri;
   b. qualora vi sia il dubbio che la password non sia più segreta, deve essere immediatamente sostituita, attraverso la modalità messa a disposizione dal Settore Innovazione e Transizione Digitale;
   c. le password devono essere lunghe almeno 10 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri;
   d. le password devono essere aggiornate al primo utilizzo e successivamente ogni 90 giorni;
   e. le password non devono essere trascritte su carta o mezzo elettronico (mai, ad esempio, su post-it o agende cartacee, posta elettronica, telefono cellulare);
   f. non devono essere usate password semplici, per esempio, che riprendano il nome, la userid o altri dati facilmente ricavabili (data di nascita, nome del/della coniuge, targa della propria auto…).

2. L'Ente può imporre, con opportune modalità tecniche, l'applicazione di tutte o alcune delle regole precedenti. In ogni caso tutte devono essere applicate con diligenza.

Art. 17 – Utilizzo delle cartelle condivise e delle copie di salvataggio

1. I dati di lavoro dei/delle singoli/e assegnatari/e (sia di produzione individuale che di ufficio/settore) devono essere, di norma, salvati nelle cartelle condivise su piattaforme di memorizzazione messe a disposizione dal Settore Innovazione e Transizione Digitale e non su disco fisso del pc. Questo è necessario perché i dati su PC non sono soggetti a copia di sicurezza e, quindi, potrebbero andare persi a seguito di guasti, furti e smarrimenti.
2. L'organizzazione e la gestione delle cartelle e dei dati memorizzati su piattaforme dedicate alla condivisione e alla conservazione dei documenti di lavoro deve essere conforme alle linee guida fornite dal Settore Innovazione e Transizione Digitale.

Art. 18 – Utilizzo della navigazione su Internet

1. In accordo con le "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007, si precisa quanto segue:
   a. la connessione a internet è un bene aziendale da utilizzare in modo corretto e appropriato;
   b. l'Ente si riserva di bloccare l'accesso a siti ritenuti inappropriati o non attinenti all'ambito lavorativo.

2. È comunque proibito l'accesso a reti per la condivisione di contenuti tipo peer-to-peer, il download di contenuti multimediali se non per finalità istituzionali, il download e l'installazione di software senza esplicita autorizzazione del Settore Innovazione e transizione digitale. La violazione del diritto d'autore (ex L. 633/1941 e successive modificazioni, D.Lgs. 169/1999 e L. 248/2000) costituisce reato.
3. Considerata la specifica natura dei log della navigazione, oltre a quanto previsto dall'art. 6 del presente Regolamento, le modalità di registrazione e conservazione saranno adeguate ai provvedimenti del Garante.

Art. 19 – Utilizzo delle Virtual Private Network (VPN)

1. L'Ente gestisce un servizio che consente ai/alle dipendenti aziendali o operatori/operatrici di terze parti l'accesso alla rete aziendale da postazioni remote.
2. L'accesso è personale ed è realizzato mediante un collegamento protetto su Rete Privata Virtuale (VPN – Virtual Private Network) con autenticazione.
3. Il Servizio VPN tiene traccia di ogni accesso e i log vengono conservati fino a 180 giorni per finalità di accertamento di eventuali reati informatici. Le informazioni contenute nei log sono: username, source IP, stato login, data e ora inizio collegamento.
4. L'utilizzo delle VPN è richiesto dalla Segreteria del settore di appartenenza dell' assegnatario/a ed è previsto esclusivamente per:
   a. modalità di lavoro a distanza (agile e da remoto);
   b. attività in mobilità;
   c. collaboratori/collaboratrici di servizi da remoto.
5. I/Le fornitori/fornitrici possono richiedere il servizio mediante apposito modulo, che dovrà essere inviato al/alla Responsabile Unico del Progetto (RUP) o Direttore/Direttrice dell'esecuzione del contratto (DEC), il/la quale provvederà a inoltrarlo al Settore Innovazione e Transizione Digitale dando il proprio nulla osta a procedere. Il Settore Innovazione e Transizione Digitale procederà a valutare la richiesta e, nel caso di accoglimento, procederà all'attivazione di quanto richiesto. È compito del/della RUP/DEC del contratto comunicare eventuali modifiche o sospensioni relativamente alle utenze richieste.
6. L'utilizzo delle VPN deve avvenire nel rispetto delle seguenti regole:
   a. devono essere attivate solo nel momento del loro utilizzo per lo svolgimento di attività che necessitano dell'accesso alla rete interna dell'Ente e devono essere disattivate al termine delle suddette attività;

b. per ragioni di sicurezza la password di accesso non deve essere memorizzata ma inserita ogni volta.

7. Al cessare delle situazioni previste dal comma 4, la Segreteria del settore di appartenenza dell'assegnatario/a deve darne comunicazione alla U.O.S. HD e Testing software affinché si provveda alla disabilitazione dell'utenza.

Art. 20 – Utilizzo delle caselle di posta elettronica

1. Ad ogni assegnatario/a viene fornito un account e-mail nominativo quale cognomeinizialenome@dominio dell'Ente (ad esempio Rossi Mario avrà rossim@comune.padova.it) o, in caso di omonimia, utilizzando le prime due o più lettere del nome. La casella di posta assegnata è uno strumento di lavoro di esclusiva proprietà aziendale ed è assolutamente vietato ogni utilizzo di tipo privato. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
2. Ad ogni settore verrà attivata una casella di posta elettronica istituzionale; su valutazione del/della Capo Settore è possibile attivare caselle di posta elettronica associate a gruppi di lavoro e/o unità operative, anche intersettoriali, al fine di evitare che i singoli soggetti mantengano l'esclusività su dati di interesse comune ad altri.
3. Per tutte le comunicazioni elettroniche verso l'esterno aventi carattere formale devono essere utilizzate le caselle di posta elettronica di settore/ufficio/progetto;
4. In coerenza con il punto precedente, è opportuno che le pagine informative relative ai servizi pubblicate sul sito istituzionale riportino come canale di contatto gli indirizzi delle caselle di posta elettronica di settore/ufficio/progetto;
5. Le istanze, segnalazioni o comunicazioni di carattere formale che pervengono esclusivamente all'indirizzo di posta elettronica istituzionale individuale devono essere inoltrate alla casella di posta elettronica istituzionale del settore/ufficio/progetto di riferimento.
6. Nei messaggi inviati tramite casella di posta elettronica istituzionale e casella di posta elettronica istituzionale individuale verrà accluso il seguente testo:
   "*Ai sensi del vigente D.Lgs. 196/2003 in materia di privacy e del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, si precisa che le informazioni contenute nel messaggio e negli eventuali allegati sono riservate esclusivamente al/ai destinatario/i indicato/i. Si invita ad astenersi dall'effettuare: inoltri, copie, distribuzioni e divulgazioni non autorizzate del presente messaggio e degli eventuali allegati. Nel caso di erroneo recapito, si chiede cortesemente a chi legge di dare immediata comunicazione al mittente e di cancellare il presente messaggio e gli eventuali allegati.*
   Pursuant to the Legislative Decree 196/2003 on privacy and Regulation (EU) 2016/679 of the European Parliament and the Council, please note that the information contained in this message and any attachments is strictly confidential and intended solely for the designated recipient(s).
   Unauthorized forwarding, copying, distribution, or disclosure of this message and any attachments is strictly prohibited. In case of incorrect delivery, the reader is kindly requested to immediately notify the sender and delete this message along with any attachments."

7. Nei messaggi inviati tramite casella di posta elettronica istituzionale individuale verrà accluso il seguente testo: "*Il presente messaggio ha natura non personale; pertanto, sia il contenuto della presente sia le eventuali risposte potranno essere conosciute nell'organizzazione del Comune di Padova.*".
8. È vietato:
   a. utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione;
   b. inviare catene telematiche; qualora si ricevessero messaggi di tale tipo devono essere subito cancellati e non si devono in alcun caso attivare gli allegati di tali messaggi o cliccare su eventuali link;
   c. inviare materiale con contenuto violento o offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o con contenuto politico. Nel caso di ricezione di messaggi con allegati di dubbia provenienza, questi ultimi devono essere subito cancellati;
   d. inviare messaggi di posta elettronica in nome e per conto di un/una altro/a utente, salvo sua espressa autorizzazione;
   e. l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (ad esempio ferie, malattia, infortunio ecc.). In questa ultima ipotesi, come previsto dall'art. 23, c. 1 del presente Regolamento, occorrerà prevedere l'utilizzo di un messaggio "Out of Office" "Fuori servizio" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo e-mail alternativo, preferibilmente di tipo collettivo.
9. È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi/e. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
10. È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo. In particolare, si deve evitare, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati, a titolo esemplificativo ma non esaustivo, del tipo .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif.
11. L'iscrizione a mailing-list o alle newsletter esterne con l'indirizzo della casella di posta aziendale è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
12. Nel caso di invio a destinatari esterni (persone o Enti qualificati e competenti) di messaggi contenenti allegati con categorie particolari di dati o dati relativi a condanne penali e ai reati o a connesse misure di sicurezza, è necessario adottare strategie di trasmissione che garantiscano la riservatezza, come, a titolo esemplificativo ma non esaustivo: trasmissione a indirizzi accessibili esclusivamente ai soggetti qualificati, repository protetti da password, criptografia dei file. Le password di accesso ai repository o di cifratura devono essere comunicate al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati.
13. Il/La Sindaco/a, gli/le Assessori/e, i/le Consiglieri/e, i/le rappresentanti di consulte, ecc., sono tenuti nell'ambito della loro attività pubblica all'uso delle caselle di posta elettronica istituzionale assegnate all'inizio del mandato. È vietato l'utilizzo di caselle di posta elettronica

private o l'inoltro automatico a queste ultime di messaggi di posta da caselle istituzionali, salvo per casi specificatamente concordati tra gli/le interessati/interessate e gli uffici competenti nell'ambito di comunicazioni afferenti all'espletamento del mandato.

Art. 21 – Acquisizione nuove risorse informatiche e telematiche

1. L'acquisizione di nuove risorse informatiche deve avvenire conformemente al Piano Strategico per la Semplificazione e Transizione Digitale ed essere previsto nel Masterplan, con la sola esclusione dell'acquisto di postazioni di lavoro che ha carattere continuativo in una logica di aggiornamento tecnologico continuo.
2. I procedimenti di acquisizione di risorse informatiche e telematiche devono essere effettuati esclusivamente sulla base di progetti e capitolati concordati e approvati dal Settore Innovazione e Transizione Digitale.
3. Al fine di ottimizzare i processi di acquisto e di gestione, il Settore Innovazione e Transizione Digitale individua le diverse tipologie di postazioni di lavoro sulla base dei seguenti criteri:
   a. tipologia di applicazioni utilizzate (ad esempio personal computer per applicazioni gestionali o grafiche);
   b. esigenze di mobilità.
4. In fase di definizione dei capitolati, le caratteristiche tecniche associate alle singole tipologie di postazioni di lavoro saranno definite sulla base dei seguenti fattori:
   a. requisiti minimi per l'utilizzo delle applicazioni;
   b. stato dell'arte della tecnologia;
   c. costo e risorse finanziarie disponibili.
5. L'aggiornamento delle postazioni di lavoro avverrà secondo un ciclo di annualità che tenga conto dei seguenti fattori:
   a. periodo di ammortamento finanziario;
   b. requisiti minimi delle applicazioni informatiche;
   c. risorse finanziarie disponibili.
6. Ove opportuno e per gli aspetti di competenza potrà essere richiesta all'Ufficio Privacy e al RPD una valutazione di rispondenza degli strumenti alla normativa sul trattamento dei dati personali.
7. Tutti gli acquisti devono essere conformi alle regole in materia di cybersecurity definite dall'Agenzia per l'Italia Digitale (AgID) e dall'Agenzia per la cybersicurezza nazionale (ACN).
8. L'acquisto di servizi e beni informatici dovrà essere effettuato nel rispetto delle disposizioni della L. 4/2004 (Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici).

Art. 22 – Controlli di cybersecurity e difensivi

1. L'Ente effettua monitoraggi non puntuali per verificare l'integrità dei propri sistemi informatici e ai fini di ordinaria manutenzione degli stessi.

2. Solo nel caso in cui le attività di controllo accertassero eventi rilevanti per la sicurezza dei sistemi e dei dati, potranno essere eseguite verifiche puntuali più approfondite, secondo procedure preventivamente concordate con le parti sindacali, onde poter appurare eventuali responsabilità. In tal caso, ai sensi del combinato disposto dei commi 2 e 3 dell'art. 4, della L. 300/1970, l'Ente potrà utilizzare i dati così raccolti, anche ai fini disciplinari. I dati contenuti nei file di log dei sistemi verranno conservati per un periodo massimo di 6 mesi.
3. Qualora sussista un sospetto, l'Ente si riserva, inizialmente, di inviare una diffida collettiva dallo svolgere attività non consentite e, successivamente ed esclusivamente in caso di reiterate anomalie e difformità dalle prescrizioni di cui al presente Regolamento, di effettuare controlli più approfonditi per l'identificazione dell'assegnatario/a, che ha violato le prescrizioni. In presenza di tali circostanze, i dati sull'illecito utilizzo degli strumenti informatici saranno trattati, oltre che dal Settore Innovazione e Transizione Digitale, eventualmente anche dalla Direzione Generale e dall'Avvocatura Civica per eventuali finalità di difesa in giudizio.
4. Con riguardo all'utilizzo corretto delle utenze telefoniche, quando dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo, il Settore Innovazione e Transizione Digitale, d'intesa con il/la Dirigente del servizio da cui l'utilizzatore/utilizzatrice dipende, lo segnala a quest'ultimo/a con richiesta di verifica e di attestazione che le telefonate risultanti dal tabulato analitico siano state effettuate per motivi di servizio.
5. Qualora, a seguito di un controllo, si rilevi un caso di "traffico zero" da parte del telefono cellulare assegnato per un periodo di almeno due bimestri consecutivi, ne viene data immediata comunicazione al/alla Dirigente del settore da cui l'assegnatario/a dipende e viene segnalato all'assegnatario/a medesimo/a, con richiesta di motivazione e di giustificazione del mantenimento dell'utenza.
6. L'Ente, in caso di presunte condotte illecite ascrivibili a singoli/e dipendenti sulla base di indizi concreti acquisiti per il tramite di controlli difensivi, si riserva di accertare e segnalare eventuali abusi commessi senza ottemperare a quanto previsto dal comma 3.

Art. 23 – Gestione delle risorse informatiche e telematiche in caso di assenza dal lavoro

1. Ciascun/a assegnatario/a in caso di assenza (ad esempio per ferie o attività di lavoro fuori sede, congedo o assenza prolungata) provvede ad attivare apposite funzionalità del sistema di posta elettronica che consentano di inviare automaticamente messaggi di risposta contenenti informazioni dei contatti alternativi e sostitutivi.
2. In caso di eventuali assenze non programmate (ad esempio per malattia), qualora, per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi, il/la dipendente interessato/a deve essere messo/a in grado di delegare un altro/a lavoratore/lavoratrice (fiduciario/a) a verificare il contenuto di messaggi e a inoltrare all'Ente quelli ritenuti rilevanti (vedi all. 01_NominaFiduciario). Qualora il/la lavoratore/lavoratrice non possa attivare la procedura sopra descritta e perdurando l'assenza oltre un determinato limite temporale, l'Ente può lecitamente disporre, se necessario, l'attivazione di un analogo accorgimento, previo avviso all'interessato/a e mediante personale appositamente incaricato,

come ad esempio l'amministratore/amministratrice di sistema (vedi all. 02_IstanzaAccessoEmail). Di tale attività dovrà essere redatto apposito verbale e informato il/la dipendente interessato/a alla prima occasione utile (vedi all. 03_VerbaleAccessoEmail).

Art. 24 – Gestione delle informazioni alla cessazione del rapporto di lavoro

1. Alla cessazione del rapporto di lavoro, deve essere avviata l'apposita procedura predisposta che prevede il ritiro della postazione di lavoro e di tutti gli accessori assegnati. Tutti gli strumenti aziendali devono essere restituiti all'Ente nello stesso stato in cui sono stati consegnati, fatto salvo il normale degrado d'uso. A tal fine, l'assegnatario/a deve provvedere a:
   a. eliminare eventuali messaggi di natura personale ricevuti o archiviati nella propria casella di posta elettronica;
   b. eliminare eventuali contatti personali dalla rubrica del sistema di posta elettronica e dallo smartphone aziendale;
   c. restituire gli strumenti aziendali completi di accessori e con tutti i dati di interesse aziendale. Nella fattispecie si precisa che per dati si intendono sia i dati riferiti a persone fisiche, identificate o identificabili, sia altre informazioni come disegni, documenti, codici di accesso e qualunque altro tipo di informazione di proprietà dell'Ente, delle sue partecipate e dei/delle suoi/sue fornitori/fornitrici;
   d. restituire l'eventuale SIM card e il relativo apparato mobile entro i 10 giorni antecedenti la cessazione, senza necessità di formale richiesta da parte dell'Amministrazione al/alla Dirigente del settore presso cui presta servizio; il mancato rispetto dei termini della restituzione comporterà blocco dell'utenza e rivalsa dell'Amministrazione nelle forme previste dalla legge.

2. L'utenza di accesso alla rete e alle applicazioni informatiche, compresa la posta elettronica, viene sospesa il giorno successivo al termine del contratto di lavoro o incarico; per tale ragione, prima della disabilitazione dell'utente, il/la Capo Settore, anche tramite suo incaricato, deve provvedere al necessario recupero dei dati di cui sopra nei tempi e con le modalità ritenute più opportune.
3. Il contenuto della casella di posta elettronica verrà cancellato entro i successivi 30 giorni dal termine del contratto di lavoro o incarico.

CAPO III - ENTRATA IN VIGORE E ABROGAZIONI

Art. 25 – Entrata in vigore e abrogazioni

1. Il presente Regolamento entra in vigore decorsi 15 giorni dalla pubblicazione all'Albo Pretorio del Comune di Padova, da eseguirsi a intervenuta esecutività della deliberazione di Giunta Comunale che lo approva.

2. Dalla data di entrata in vigore del presente Regolamento è abrogato il Regolamento per l'utilizzo degli strumenti informatici e telematici del Comune di Padova, approvato con deliberazione di Giunta Comunale n. 324 del 29 giugno 2010.

RIFERIMENTI NORMATIVI

- Legge 20 maggio 1970, n. 300 - Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento
- Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
- Legge 9 gennaio 2004, n. 4 - Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici
- Decreto Legislativo 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale
- Linee guida del Garante per posta elettronica e internet - 10 marzo 2007
- Decreto del Presidente della Repubblica 16 aprile 2013, n. 62 - Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 – Regolamento generale sulla protezione dei dati personali
- Decreto Legislativo 10 agosto 2018, n. 106 - Attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici
- Provvedimento del Garante per la protezione dei dati personali del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati