



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

Approvato con deliberazione G.C. n. _____ del __/__/2025

INDICE GENERALE

PREMESSA.....	3
CAPO I: FINALITÀ - AMBITO DI APPLICAZIONE - PRINCIPI GENERALI.....	4
Art. 1 - Finalità.....	4
Art. 2 - Principi generali.....	4
Art. 3 - Ambito di applicazione.....	4
Art. 4 - Definizioni.....	5
Art. 5 - Accesso alle risorse informatiche e telematiche.....	6
Art. 6 -Tracciatura (Log) dei sistemi.....	6
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.....	7
Art. 9 - Compiti degli/delle amministratori/amministratrici di sistema.....	8
CAPO II: REGOLE PER L'UTILIZZO DELLE RISORSE INFORMATICHE E TELEMATICHE.....	9
Art. 10 - Assegnazione postazioni di lavoro.....	9
Art. 11 - Assegnazione telefono/tablet di servizio e/o SIM card aziendale.....	10
Art. 12 - Rilascio di certificati e dispositivi di firma digitale.....	10
Art. 13 - Assegnazione di servizi applicativi.....	11
Art. 14 - Utilizzo delle postazioni di lavoro.....	11
Art. 15 - Utilizzo e conservazione dei supporti rimovibili.....	14
Art. 16 - Utilizzo dei dispositivi mobili - Precauzioni nel lavoro agile.....	15
Art. 17 - Utilizzo di cellulari e smartphone.....	15
Art. 18 - Utilizzo degli strumenti stampa.....	15
Art. 19 - Utilizzo delle credenziali.....	16
Art. 20 - Utilizzo delle cartelle condivise e delle copie di salvataggio.....	17
Art. 21 - Utilizzo della navigazione su Internet.....	17
Art. 22 - Utilizzo delle Virtual Private Network (VPN).....	18
Art. 23 - Utilizzo delle caselle di posta elettronica.....	18
Art. 24 - Acquisizione nuove risorse informatiche e telematiche.....	21
Art. 25 - Controlli di cybersecurity e difensivi.....	22
Art. 26 - Gestione delle risorse informatiche e telematiche in caso di assenza o impedimento.....	23
Art. 27 - Gestione delle informazioni alla cessazione del rapporto di lavoro.....	23
Art. 28 - Protezione antivirus.....	24
Art. 29 - Partecipazioni a social media.....	24
Art. 30 - Open Government.....	25
Art. 31 - Videosorveglianza.....	25
Art. 32 - Pubblicazione notizie ed eventi sui canali elettronici del Comune.....	25
Art. 33 - Assistenza agli utenti e manutenzioni.....	26
Art. 34 - Osservanza delle disposizioni in materia di Privacy.....	27
Art. 35 - Accesso ai dati trattati dall'utente.....	27
Art. 36 - Sistema di controlli gradualali e conservazione dei dati.....	27
Art. 37 - Sanzioni.....	29
CAPO III ENTRATA IN VIGORE, ABROGAZIONI E PUBBLICITA'	30
Art. 38 - Disposizioni finali, entrata in vigore e abrogazioni.....	30
RIFERIMENTI NORMATIVI.....	30

PREMESSA

La diffusione delle tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone il Comune di Rovigo e gli utenti (dipendenti e collaboratori dello stesso) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (sul diritto d'autore e sulla privacy, fra tutte), creando problemi alla sicurezza e all'immagine dell'Ente.

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro. Il presente Regolamento è diretto ad evitare che determinati comportamenti possano innescare problemi o minacce alla sicurezza nel trattamento dei dati, disciplinando le condizioni per il corretto utilizzo degli strumenti informatici e/o telematici, in particolare alla luce degli obblighi previsti dalla normativa italiana ed europea in materia di protezione dei dati personali (Reg. UE 2016/679, D.Lgs. 196/2003 e s.m.i.).

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 Rovigo e a tutelare la riservatezza, l'integrità e la disponibilità delle informazioni e dei dati, anche personali, da questo prodotti, raccolti o comunque trattati.
2. La finalità è quella di promuovere in tutto il personale dell'Ente una corretta "cultura informatica" affinché l'utilizzo degli strumenti informatici e telematici sia conforme alle finalità dell'Ente e nel pieno rispetto della legge.

Art. 2 - Principi generali

1. Il Comune di Rovigo 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 Rovigo 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 Rovigo, oltre, comunque, a un comportamento ispirato ai principi di correttezza e diligenza.
4. La regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei/delle lavoratori/lavoratrici, ma solo a permettere all'Ente 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 Rovigo 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 Rovigo 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 Rovigo;
 - d. **Casella di posta elettronica istituzionale:** casella di posta assegnata a una struttura dell'Ente (Settore, U.O.) 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 Rovigo 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. **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;
 - h. **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;
 - i. **Postazioni di lavoro:** servizi applicativi, PC, notebook, tablet, smartphone e tutti i dispositivi hardware utilizzati per l'espletamento delle attività istituzionali;
 - j. **Risorse informatiche:** le postazioni di lavoro, i servizi applicativi, le risorse di calcolo e storage e i servizi di rete del Comune di Rovigo;
 - k. **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;
 - l. **RTD:** Responsabile per la Transizione Digitale ai sensi dell'art. 17 del D.Lgs 82/2005 Codice dell'amministrazione digitale;
 - m. **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);
 - n. **Servizi applicativi:** software 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;
- o. **Servizio Sistemi Informativi:** struttura competente per lo sviluppo e la gestione delle risorse informatiche e telematiche, a supporto del/della Responsabile per la Transizione Digitale;
 - p. **Storage:** sistemi di memorizzazione dei dati;
 - q. **Ufficio Privacy:** unità operativa che ha il compito di coordinare lo svolgimento delle attività di trattamento di dati personali svolte presso altri settori, al fine di supportarli nello svolgimento delle attività di propria 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";
 - r. **Utente:** ogni dipendente e collaboratore (a prescindere dal rapporto contrattuale) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "incaricato del trattamento".

Art. 5 - Accesso alle risorse informatiche e telematiche

1. L'accesso alle risorse informatiche e telematiche del Comune di Rovigo 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 viene 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 Rovigo, 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 difforni da quanto previsto dal presente Regolamento possono contribuire ad innescare disservizi, costi di manutenzione, 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 Rovigo.

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 Servizio Sistemi Informativi;
 - b. cablare, collegare o modificare apparati di rete senza l'autorizzazione del Servizio Sistemi Informativi;
 - 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 Servizio Sistemi Informativi;
 - 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.
2. All'interno delle sedi del Comune possono essere rese disponibili anche reti senza fili, c.d.

“Wi-Fi”. Tali reti consentono l’accesso alle risorse dell’Ente e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L’accesso mediante rete Wi-Fi viene concesso a consulenti e tecnici che nell’ambito di un rapporto contrattuale con l’Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari del Comune che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L’accesso alla sola rete internet in modalità Wi-Fi viene anche concessa ad utenti esterni generici, laddove ne facciano richiesta, tramite l’emissione di un voucher, ovvero di credenziali monouso a tempo, o con la modalità ritenuta più idonea.

3. Gli Amministratori di Sistema si riservano la facoltà di negare o interrompere l’accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell’Ente.
4. I log relativi all’uso del File System e della intranet dell’Ente, nonché i file salvati o trattati su Server o PC, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso gli Amministratori di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell’Ente.
5. I controlli possono avvenire secondo le disposizioni previste al successivo art. 36 del presente Regolamento. Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d’uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 2016/679 “General Data Protection Regulation”.

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

0. 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 Servizio Sistemi Informativi 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.
1. 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. 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;
 - c. effettuare la revisione, almeno annuale, degli account;
 - d. effettuare il monitoraggio dei sistemi gestiti, registrando gli accessi privilegiati e le eventuali modifiche ai file di sistema;
 - e. collaborare tra di loro nella progettazione, configurazione e gestione delle reti del Data Center e dei servizi Cloud (IaaS e PaaS);
 - f. fornire supporto per conservare e incrementare la sicurezza delle risorse affidate agli/alle utenti.

CAPO II: REGOLE 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, evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale dell'Ufficio Informatica ogni malfunzionamento e/o danneggiamento.
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 non preventivamente autorizzato 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. 27 del presente Regolamento.
7. Le postazioni di lavoro ad uso condiviso (ad esempio sportelli, fotocopiatori/scanner di rete 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, Presidente del Consiglio Comunale, Segretario/a 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 del Servizio Sistemi Informativi 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 Servizio Sistemi Informativi.
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, Presidente del

Consiglio Comunale, Segretario/a 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 Dirigente del 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. 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 e l'assegnatario/a dovrà fare richiesta di revoca del certificato al Servizio Sistemi Informativi.

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 e, nel caso di servizi applicativi gestionali o banche dati, dall'eventuale Designato/a del trattamento.
2. L'accesso alle risorse condivise ed ai software gestionali dell'Ente per mezzo di credenziali è legato ad un sistema di autorizzazione dove vengono definiti dei profili che permettono di definire i diritti e le limitazioni di ogni singolo utente in merito alle operazioni che lo stesso può effettuare sui vari dispositivi e sui vari sistemi software. I profili di autorizzazione, per ciascun utente/incaricato o per classi omogenee di utenti/incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

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, senza preventiva autorizzazione del Servizio Sistemi Informativi.
 - 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 possono avvenire secondo le modalità previste dal presente Regolamento al successivo art. 25 "Controlli di cybersecurity e difensivi".
 - h. In caso di furto o smarrimento di PC e dispositivi aziendali assegnati, l'assegnatario/a deve contattare immediatamente il Servizio Sistemi Informativi che provvede all'attuazione delle misure di sicurezza atte a prevenire l'accesso non autorizzato alle risorse informatiche e telematiche del Comune di Rovigo. L'assegnatario/a presenterà personalmente formale denuncia di furto o smarrimento agli organi di Polizia. Copia della denuncia dovrà essere trasmessa al Servizio Sistemi Informativi 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:
 - una SIM card per collegamento fonia e/o dati con contratto intestato all'Amministrazione;
 - un telefono cellulare, smartphone o tablet intestato all'Amministrazione;
 - accessori del dispositivo (batteria, caricabatteria, auricolare ecc.);
 - nei casi autorizzati, una SIM dati intestata all'Amministrazione per collegamento dati.
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.
7. Gli operatori del Servizio Sistemi Informativi sono autorizzati a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Detti interventi potranno anche comportare l'accesso in qualunque momento ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica dei siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Ente, si applica anche in caso di assenza prolungata o impedimento dell'utente e non sia possibile procedere altrimenti.
8. Il personale del Servizio Sistemi Informativi ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
9. L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la postazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. A maggior tutela degli utenti dovrà essere impostato lo screen saver a tempo con l'obbligo di reintrodurre le credenziali per lo sblocco del terminale. Se più utenti utilizzano la stessa postazione di lavoro per trattare dati personali di terzi, effettuano il "log out" (scollegamento dalla rete) ogni volta che un diverso utente deve utilizzare la propria postazione abituale. Al termine della giornata lavorativa i PC dovranno essere spenti salvo sia necessario che la postazione debba rimanere accesa per permettere il collegamento da remoto in regime di smart working: in tal caso l'utente dovrà effettuare il "log out" prima di allontanarsi dalla postazione.
10. Le informazioni archiviate sul PC locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata.
11. La gestione dei dati su PC è demandata all'utente utilizzatore che dovrà provvedere a memorizzare sulle cartelle di rete dell'Ente dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi.

12. Gli operatori del Servizio Sistemi Informativi o gli Amministratori di Sistema possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza dei PC, della rete locale e dei server dell'Ente, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.
13. È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.
14. È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.
15. È vietato l'utilizzo di supporti di memoria (chiavi USB, dischi fissi esterni, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli strumenti informatici dell'Ente, salvo che il supporto utilizzato sia stato autorizzato dal Servizio Sistemi Informativi. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.
16. È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dal Servizio Sistemi Informativi.
17. È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dal Servizio Sistemi Informativi.
18. Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente al Servizio Sistemi Informativi. Nel caso vengano rilevati dei virus dovranno essere seguite le indicazioni di cui all'art. 28 del presente Regolamento.

Art. 15 - Utilizzo e conservazione dei supporti rimovibili

1. Tutti i supporti di memorizzazione rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili o comunque di carattere riservato, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio Sistemi Informativi e seguire le istruzioni da questo impartite.
3. In ogni caso, i supporti contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
4. Non è consentita l'uscita dalle sedi comunali di hardware e supporti magnetici, ottici o di altra natura e cartacei, se non preventivamente autorizzati.
5. È vietato l'utilizzo di supporti rimovibili personali.
6. L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti. È assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
7. È interdetta l'installazione o l'uso di supporti rimovibili sulle stazioni di lavoro. Per eventuali necessità in proposito occorrerà farsi autorizzare dal Servizio Sistemi Informativi.

Art. 16 - Utilizzo dei dispositivi mobili - Precauzioni nel lavoro agile

1. Il Servizio Sistemi Informativi fornisce su richiesta (e se disponibili) dispositivi mobili quali notebook, cellulari, internet key; fornisce inoltre il necessario supporto agli utenti per il corretto utilizzo di essi.
2. L'utente è responsabile del dispositivo mobile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
3. A tali dispositivi si applicano le regole di utilizzo previste dal presente regolamento con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.
4. Anche per tali dispositivi l'installazione di programmi dovrà essere effettuata a cura del Servizio Sistemi Informativi, al fine di garantire il rispetto dei criteri di sicurezza informatica nell'uso della rete.
5. I dispositivi mobili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
6. Gli utenti devono inoltre comunicare al Servizio Sistemi Informativi eventuali guasti o anomalie, riscontrate nell'uso dei dispositivi, e informare tempestivamente di eventuali smarrimenti o furti.
7. L'utilizzo di tali dispositivi è limitato all'utente o agli utenti assegnatari; è quindi vietato cederne l'uso, anche temporaneo, a terzi se non preventivamente autorizzato.
8. I dati personali e riservati di norma non possono essere registrati su tali dispositivi mobili; diversamente devono essere gestiti con la supervisione del Servizio Sistemi Informativi.
9. Tali disposizioni si applicano anche nei confronti di eventuali incaricati esterni.

Art. 17 - Utilizzo di cellulari e smartphone

1. Il telefono dell'Ente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.
2. Qualora venisse assegnato un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet, se consentita.
3. Per gli smartphone dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dal Servizio Sistemi Informativi.

Art. 18 - Utilizzo degli strumenti stampa

1. L'utilizzo degli strumenti di stampa, quali dispositivi multifunzione condivisi, 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.

2. Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate. In caso di inceppamento o malfunzionamento del dispositivo l'utente deve assicurarsi che il lavoro venga rimosso dalla coda di stampa del dispositivo o attendere presso il dispositivo stesso fino alla risoluzione del problema. In ogni caso, è fatto obbligo di non lasciare le proprie stampe (anche qualora siano bozze o stampe errate) presso i dispositivi multifunzione condivisi.

Art. 19 - Utilizzo delle credenziali

1. L'accesso ai dispositivi, alla rete e alle applicazioni software 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 Authentication (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. ad eccezione delle sole utenze di servizio per alcuni sistemi software centralizzati, tutte le user id dovranno essere nominative e riconducibile ad una persona fisica;
 - c. qualora vi sia il dubbio che la password non sia più segreta, deve essere immediatamente sostituita, attraverso la modalità messa a disposizione dal Servizio Sistemi Informativi;
 - d. le password devono avere lunghezza adeguata e devono contenere lettere (maiuscole e minuscole), caratteri speciali e numeri, anche in combinazione tra loro;
 - e. le password devono essere aggiornate al primo utilizzo e successivamente almeno ogni 90 giorni;
 - f. le password non devono essere trascritte su carta o mezzo elettronico (mai, ad esempio, su post-it o agende cartacee, posta elettronica, telefono cellulare) e devono essere custodite con la massima diligenza;
 - g. non devono essere usate password semplici, per esempio, che riprendano il nome, la userid o altri dati agevolmente riconducibili all'utente o 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, in quanto tengono conto delle vigenti linee guida dell'AgID in materia di sicurezza informatica. Laddove nuove versioni di tali linee guida dovessero introdurre misure diverse e/o più stringenti, le stesse dovranno essere osservate in sostituzione di quelle attuali.
3. L'accesso ai sistemi da parte di persone non autorizzate per mezzo di credenziali custodite in modo incauto può esporre l'utente titolare delle stesse a conseguenze disciplinari, civili e penali.

Art. 20 - 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 Servizio Sistemi Informativi 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 o 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 Servizio Sistemi Informativi.

Art. 21 - 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 e l'upload di contenuti multimediali se non per finalità istituzionali, il download e l'installazione e/o l'utilizzo di software senza esplicita autorizzazione del Servizio Sistemi Informativi. La violazione del diritto d'autore (ex L. 633/1941 e successive modificazioni, D.Lgs. 169/1999 e L. 248/2000) costituisce reato.
3. È proibita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Dirigente competente, con il rispetto delle normali procedure di acquisto.
4. È proibito l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione del Servizio Sistemi Informativi.
5. È proibita la partecipazione a Forum non professionali, ai Social Network (salve esigenze d'ufficio), l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
6. È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali.
7. Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda come, a titolo esemplificativo, filmati (tratti da youtube, siti di informazione, siti di streaming ecc.) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.
8. 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. 22 - 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 dal Dirigente del settore di appartenenza dell'assegnatario/a o da altri autorizzati ed è previsto esclusivamente per:
 - a. modalità di lavoro a distanza (agile o da remoto);
 - b. attività in mobilità;
 - c. collaboratori/collaboratrici di servizi da remoto.
5. I/Le fornitori/fornitrici possono richiedere il servizio al/alla Responsabile Unico del Progetto (RUP) o al/alla Direttore/Direttrice dell'esecuzione del contratto (DEC), il/la quale provvederà a inoltrarlo al Servizio Sistemi Informativi dando il proprio nulla osta a procedere. Il Servizio Sistemi Informativi valuterà la richiesta e, nel caso di accoglimento, attiverà 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, il Dirigente del settore di appartenenza dell'assegnatario/a o chi ne ha fatto richiesta deve darne comunicazione al Servizio Sistemi Informativi affinché si provveda alla disabilitazione dell'utenza.

Art. 23 - Utilizzo delle caselle di posta elettronica

1. Ad ogni assegnatario/a viene fornito un account e-mail nominativo quale nome.cognome@dominioEnte (ad esempio Rossi Mario avrà mario.rossi@comune.rovigo.it) o, in caso di omonimia, aggiungendo un numero. 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 e del contenuto dei messaggi inviati.
2. La "personalizzazione" dell'indirizzo non comporta il suo carattere "privato", in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione del dipendente al

solo fine dello svolgimento delle proprie mansioni lavorative.

3. Ad ogni servizio/ufficio verrà attivata una casella di posta elettronica istituzionale; su valutazione del/della Dirigente è possibile attivare caselle di posta elettronica associate a gruppi di lavoro e/o unità operative, anche intersettoriali, il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo, al fine di evitare che i singoli utenti mantengano l'esclusività su dati di interesse comune ad altri.
4. Per tutte le comunicazioni elettroniche verso l'esterno aventi carattere formale devono essere utilizzate le caselle di posta elettronica di settore/ufficio/progetto.
5. In coerenza con il punto precedente, è opportuno che le pagine informative relative ai servizi pubblicate sul sito web istituzionale riportino come canale di contatto gli indirizzi delle caselle di posta elettronica di settore/ufficio/progetto.
6. 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.
7. Ciascun messaggio in uscita deve consentire la puntuale identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.
8. Nei messaggi inviati tramite casella di posta elettronica istituzionale e casella di posta elettronica istituzionale individuale verrà accluso il seguente testo:

Nota di riservatezza

Il testo e gli eventuali documenti trasmessi con il presente messaggio di posta elettronica contengono informazioni di carattere confidenziale e riservate rivolte esclusivamente al destinatario sopra indicato. Sono rigorosamente vietati la lettura, l'uso, la diffusione, distribuzione o riproduzione da parte di ogni altra persona. Nel caso aveste ricevuto questo messaggio di posta elettronica per errore, siete pregati di segnalarlo immediatamente al mittente e distruggere quanto ricevuto (compresi gli eventuali file allegati) senza farne copia. Qualsiasi utilizzo non autorizzato del contenuto di questo messaggio costituisce violazione dell'obbligo di non prendere cognizione della corrispondenza tra altri soggetti, salvo più grave illecito, ed espone il responsabile alle relative conseguenze. Si informa, inoltre, che il presente indirizzo di posta elettronica è di natura istituzionale; si precisa, pertanto, che le eventuali risposte a questa e-mail potrebbero essere conosciute da altri incaricati appartenenti a questo Ente.

Confidentiality Note

The text and any documents transmitted with this e-mail message contain information of a confidential and privileged nature addressed only to the recipient named above. Reading, use, dissemination, distribution or reproduction by any other person is strictly prohibited. If you have received this e-mail message in error, please report it to the sender immediately and destroy what you have received (including any attached files) without making copies. Any unauthorized use of the contents of this message constitutes a violation of the obligation not to take cognizance of correspondence between other persons, unless more serious offence, and exposes the person responsible to the relevant consequences. It should also be noted that this e-mail address is institutional in nature; therefore, it should be noted that any

responses to this e-mail may be known by other appointees belonging to this Entity.

9. 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 a ciò rilasciata;
 - 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. diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo;
 - e. inviare messaggi di posta elettronica in nome e per conto di un/una altro/a utente, salvo sua espressa autorizzazione;
 - f. 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 quest'ultima ipotesi, come previsto dall'art. 26, 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.
10. 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 di elevate dimensioni.
11. 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 con contenuto sospetto o insolito o che contengano allegati, a titolo esemplificativo ma non esaustivo, del tipo .exe, .com, .vbs, .htm, .scr, .bat, .js, .pif. È necessario, inoltre, porre molta attenzione alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare il Servizio Sistemi Informativi per una valutazione dei singoli casi.
12. 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.
13. Nel caso fosse necessario inviare allegati "pesanti" (sopra i 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi per tempo al Servizio Sistemi Informativi. Nei casi in cui detti allegati siano stati realizzati da professionisti esterni, come nel caso dei progetti, è opportuno prevedere, già all'atto dell'affidamento dell'incarico, la richiesta di produrre documenti già ottimizzati in modo da avere

dimensioni contenute e realizzati in formati adatti alla conservazione sulla base delle vigenti linee guida AgID, senza contenuti dinamici (es. file CAD incapsulato in un file PDF) se non strettamente necessari e con immagini esportate a risoluzioni non superiori a quelle necessarie per la consultazione o la stampa.

14. 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, crittografia 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.
15. 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.
16. La casella di posta elettronica deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato nelle cartelle condivise dell'Ente.
17. I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema.
18. Le comunicazioni anche elettroniche ed i documenti elettronici allegati che possono avere rilevanza procedimentale devono essere trattati come previsto dal manuale di gestione del protocollo informatico e conservati per la durata prevista dalla normativa vigente.

Art. 24 - Acquisizione nuove risorse informatiche e telematiche

1. I procedimenti di acquisizione di risorse informatiche e telematiche, siano essi di natura hardware, software o firmware, devono essere effettuati esclusivamente sulla base di progetti e capitolati concordati e approvati dal Servizio Sistemi Informativi.
2. Al fine di ottimizzare i processi di acquisto e di gestione, il Servizio Sistemi Informativi 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.
3. 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.

4. 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.
5. 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.
6. 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 cybersecurity nazionale (ACN).
7. L'acquisto di servizi e beni informatici dovrà essere effettuato nel rispetto delle disposizioni della Legge n. 4/2004 *“Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici”*.

Art. 25 - 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 Legge n. 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 Servizio Sistemi Informativi, eventualmente anche dal Settore Risorse Umane per eventuali procedimenti disciplinari e dall'Avvocatura Civica per eventuali procedimenti avanti l'Autorità Giudiziaria.
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 Servizio Sistemi Informativi, 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. 26 - Gestione delle risorse informatiche e telematiche in caso di assenza o impedimento

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 di posta elettronica e a inoltrare all'Ente quelli ritenuti rilevanti. Qualora il/la lavoratore/lavoratrice non possa attivare la procedura sopra descritta e perdurando l'assenza oltre un determinato limite temporale, il Dirigente del settore di appartenenza 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 di sistema. Di tale attività dovrà essere redatto apposito verbale e informato il/la dipendente interessato/a alla prima occasione utile.

Art. 27 - Gestione delle informazioni alla cessazione del rapporto di lavoro

1. Alla cessazione del rapporto di lavoro, deve essere avviata l'apposita procedura 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, 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 relativo/a Dirigente, anche tramite suo incaricato, deve provvedere al necessario recupero dei dati di cui sopra nei tempi e con le modalità ritenute più opportune concordate con il Servizio Sistemi Informativi.
3. Il contenuto della casella di posta elettronica verrà cancellato entro i successivi 30 giorni dal termine del contratto di lavoro o incarico.
4. Ai dipendenti cessati sarà comunque garantito l'accesso telematico al portale del dipendente contenente i cedolini paga e le certificazioni uniche.

Art. 28 - Protezione antivirus

1. Il sistema informatico del Comune di Rovigo è protetto da software antivirus costantemente aggiornato. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico comunale mediante virus o mediante ogni altro software aggressivo (evitando, quindi, di compiere quei comportamenti vietati dal presente regolamento e già menzionati: es. navigazione su siti non sicuri, download di file non autorizzati, etc.). È fatto assoluto divieto a ciascun utente di modificare le impostazioni del software antivirus.
2. Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso nonché segnalare prontamente l'accaduto al personale del Servizio Sistemi Informativi.
3. Ogni dispositivo di memorizzazione di provenienza esterna all'Ente dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio Sistemi Informativi.

Art. 29 - Partecipazioni a social media

1. L'utilizzo a fini promozionali di Facebook, Twitter, Instagram, dei blog e dei forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.
2. Pur garantendo il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare la propria immagine ed il patrimonio, anche immateriale, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro salvo che per il personale espressamente autorizzato.
3. A tal fine si richiamano le norme in materia di diritti e doveri del pubblico dipendente, con particolare riferimento al D.P.R. 16 aprile 2013 n. 62 "Codice di comportamento dei dipendenti pubblici" al Codice di comportamento aziendale approvato e pubblicato.
4. Il presente articolo deve essere osservato dall'utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.
5. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la

segretezza sulle informazioni dell'Ente, nel rispetto del segreto d'ufficio, segreto professionale e privacy.

Art. 30 - Open Government

1. Il Comune di Rovigo riconosce ed incoraggia modalità di esercizio delle proprie funzioni basate su modelli, strumenti e tecnologie che consentono all'Amministrazione di essere "aperta" e "trasparente" nei confronti dei cittadini.
2. Ferme restando le disposizioni di legge in materia di Open Government l'incaricato dovrà porre particolare attenzione nella pubblicazione e divulgazione di documenti contenenti dati personali, facendo riferimento ai seguenti principi:
 - è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto (cd. "principi di necessità, pertinenza e non eccedenza"). Di conseguenza, i dati personali che esulano da tale finalità non devono essere inseriti negli atti e nei documenti oggetto di pubblicazione on line. In caso contrario, occorre provvedere, comunque, all'oscuramento delle informazioni che risultano eccedenti o non pertinenti;
 - è, sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute" e "la vita sessuale o l'orientamento sessuale" (art. 9 del GDPR).

Art. 31 - Videosorveglianza

1. Il Comune di Rovigo utilizza sistemi di videosorveglianza a garanzia dei luoghi pubblici per una serie di finalità tra cui la sicurezza pubblica, la tutela del patrimonio pubblico ed il monitoraggio del traffico.
2. Ferme restando le disposizioni del Garante della Privacy in materia di Videosorveglianza, devono essere rispettati i seguenti principi:
 - le finalità e le modalità di gestione del sistema di videosorveglianza cittadina sono definite nel vigente Regolamento per l'utilizzo degli impianti di videosorveglianza;
 - il periodo di conservazione non deve superare 7 giorni, fatte salve esigenze di ulteriore conservazione in relazione a indagini da parte delle forze dell'ordine o della magistratura;
 - le immagini possono essere visionate solo da responsabili o incaricati del trattamento dei dati ai sensi della vigente normativa in materia di protezione dei dati personali.
3. Per quanto non espressamente previsto nel presente articolo, si rinvia alla specifica regolamentazione comunale adottata in materia.

Art. 32 - Pubblicazione notizie ed eventi sui canali elettronici del Comune

1. Il Comune di Rovigo dispone di un proprio portale web istituzionale per la diffusione di informazioni riguardanti gli Organi di governo dell'Ente, gli Uffici, le notizie, gli eventi promossi dall'Amministrazione, etc., oltre a svolgere le funzioni di pubblicità legale

legate all'albo pretorio on-line ed alla sezione Amministrazione Trasparente con i contenuti previsti dal D.Lgs. 14 marzo 2013 n. 33 e s.m.i. in materia di trasparenza.

2. L'Ente gestisce ed organizza il piano editoriale legato alla promozione della città ed ai contenuti di carattere informativo, sia turistico che istituzionale, sui portali e sui canali social.
3. Relativamente alle pagine istituzionali riferite agli Uffici ed ai relativi servizi, l'Ufficio Relazioni con il pubblico è abilitato al caricamento e all'aggiornamento dei contenuti, su richiesta dei singoli uffici, che ne rimangono, comunque, gli unici responsabili.

Art. 33 - Assistenza agli utenti e manutenzioni

1. Il Servizio Sistemi Informativi e gli Amministratori di sistema possono accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:
 - verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;
 - verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
 - richieste di installazione/aggiornamento software e manutenzione preventiva, correttiva, migliorativa e adattiva per hardware, software e firmware.
2. Gli interventi tecnici possono avvenire previo consenso dell'utente quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, il Servizio Sistemi Informativi e gli Amministratori di sistema sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.
3. Gli Amministratori di sistema sono altresì autorizzati ad effettuare interventi di tipo emergenziale senza il consenso dell'utente cui la risorsa è assegnata in caso di osservazione di potenziali pericoli per i sistemi informatici dell'Ente, come, ad esempio, il rilevamento di un virus da parte del sistema antivirus centralizzato, o il rilevamento di attività di rete di tipo malevolo da parte di sistemi di intrusion detection o sulla base dell'analisi dei log del firewall. Gli Amministratori di Sistema potranno in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza del sistema informativo e dei dati, sia sui PC assegnati agli utenti sia sulle unità di rete.
4. L'accesso in teleassistenza sui PC della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dal Servizio Sistemi Informativi o dagli Amministratori di sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.
5. Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente deve presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

Art. 34 - Osservanza delle disposizioni in materia di Privacy

1. È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza ai sensi del D.Lgs. n. 196/2003, del regolamento europeo UE 2016/679 e della circolare Agid 18 aprile 2017 n. 2, ed, in generale, a quanto indicato nella lettera di designazione ad incaricato del trattamento dei dati.
2. In adempimento del provvedimento generale del Garante per la Protezione dei Dati Personali del 1 marzo 2007 avente ad oggetto “Linee guida del Garante per posta elettronica e internet” e ai sensi dell’articolo 13 del regolamento europeo UE 2016/679 vengono di seguito indicate alcune informazioni relative al trattamento dei dati personali dei propri dipendenti e/o collaboratori raccolti in esecuzione del presente Regolamento contenente le regole sull’utilizzo degli strumenti informatici, di internet e della posta elettronica.
3. I dati raccolti saranno trattati esclusivamente per le finalità elencate nel presente regolamento (fra le quali si ricordano a titolo esemplificativo i dati raccolti a seguito di manutenzione degli strumenti informatici nonché quelli raccolti a seguito di controlli per verificare il rispetto da parte degli utenti delle regole qui riprodotte) e saranno trattati con modalità telematiche e/o su supporto cartaceo. Si ricorda agli utenti che il conferimento dei dati per le finalità sopra citate è necessario ai fini dell’utilizzo degli strumenti elettronici forniti in uso all’utente e che di conseguenza l’eventuale rifiuto di fornire tali dati impedirà al Comune di Rovigo di garantire agli utenti l’uso stesso degli strumenti. I dati personali raccolti dall’Ente non saranno oggetto di diffusione e potranno essere comunicati esclusivamente a personale di fiducia dello stesso (come ad esempio società di servizi che forniscono supporto nella manutenzione degli strumenti informatici) legati al Comune da vincoli contrattuali che garantiscono la riservatezza e l’integrità delle informazioni trattate. Tutti i dipendenti e/o collaboratori sono titolari dei diritti previsti all’articolo 13 del regolamento europeo EU 2016/679 che possono essere esercitati con richiesta rivolta al Titolare (Comune di Rovigo) o al relativo Responsabile per la Protezione dei Dati (RPD/DPO).

Art. 35 - Accesso ai dati trattati dall’utente

1. Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione del rinnovo tecnologico del parco macchine aziendale comunque estranei a qualsiasi finalità di controllo dell’attività lavorativa, è facoltà della Dirigenza, tramite il personale dei Sistemi Informativi o di addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

Art. 36 - Sistema di controlli gradualità e conservazione dei dati

1. Poiché in caso di violazioni contrattuali e giuridiche, sia l’Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l’Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l’integrità del

proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2, Legge n. 300/1970), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto dell'art. 2 del presente Regolamento e dei seguenti principi:

- Proporzionalità: il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi;
 - Trasparenza: l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti;
 - Pertinenza e non eccedenza: ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.
2. L'uso degli strumenti informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite del Servizio Sistemi Informativi e degli Amministratori di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi, di seguito descritti, e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

Controlli per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico e per motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.)

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli strumenti e alle risorse informatiche e relative informazioni il Responsabile di Settore, in qualità di delegato del Titolare del trattamento dei dati personali, per il tramite dell'Ufficio Informatica, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo strumento oggetto di controllo):

- a) Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento;
- b) Successivamente, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni contenute negli strumenti informatici con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività

lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo dell'indirizzo IP dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite;

- c) Qualora il rischio di compromissione del sistema informativo dell'Ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedurali descritti ai punti 1 e 2, il Dirigente, in qualità di delegato del Titolare del trattamento dei dati personali, unitamente al Servizio Sistemi Informativi o agli Amministratori di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

Controlli per esigenze produttive e di organizzazione

Per esigenze produttive e di organizzazione si intendono - fra le altre - l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un utente (quali file salvati, posta elettronica, chat, SMS, ecc.) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni il Dirigente, in qualità di delegato del Titolare del trattamento dei dati personali, per il tramite del Servizio Sistemi Informativi, si atterrà alla procedura descritta nell'art. 26 del presente regolamento e a quanto segue.

Il Dirigente deve comunque provare le necessità produttive e di organizzazione che richiedano l'accesso allo strumento.

Il Servizio Sistemi Informativi o l'Amministratore di sistema può accedere alla risorsa con credenziali di amministrazione ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.

Deve essere redatto un verbale che riassume le operazioni eseguite.

In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.

Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo EU 2016/679 "GDPR".

Art. 37 - Sanzioni

1. È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. La mancata osservanza, da parte dei dipendenti del Comune, delle presenti modalità, di utilizzo degli strumenti informatici può dar luogo a procedimenti di carattere disciplinare, fatto salvo che le violazioni non comportino più gravi e/o diverse sanzioni ai sensi della vigente normativa.

CAPO III

ENTRATA IN VIGORE, ABROGAZIONI E PUBBLICITA'

Art. 38 - Disposizioni finali, entrata in vigore e abrogazioni

1. Il presente Regolamento entra in vigore ed acquista piena efficacia dall'esecutività della deliberazione di approvazione.
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 Rovigo, approvato con deliberazione di Giunta Comunale n. 260 del 06 dicembre 2007.
3. Il presente Regolamento abroga ogni altra precedente disposizione di pari grado sulla materia trattata contrastante con le norme in esso contenute.
4. Copia del regolamento, oltre ad essere pubblicato sul sito web istituzionale dell'Ente, sarà disponibile nella intranet aziendale e consegnato a ciascun dipendente al momento della sua assunzione.

RIFERIMENTI NORMATIVI

Il presente Regolamento è redatto sulla base dei seguenti riferimenti normativi:

- Legge 20.5.1970, n. 300 recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento" con particolare riferimento all'art. 4, comma 1, secondo cui la regolamentazione dell'uso degli strumenti informatici non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro, ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali;
- D.Lgs. 30/06/2003 n. 196 recante "Codice in materia di protezione dei dati personali" (come modificato dal Decreto di adeguamento della normativa nazionale ai principi del GDPR - D.Lgs. n. 101/18);
- 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 (CAD);
- "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 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;
- D.Lgs. n. 151/2015 (c.d. Jobs Act) recante "Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183.", con particolare riferimento all'art. 23 che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover

tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa»;

- Regolamento Europeo 679/16 “General Data Protection Regulation” (GDPR); in particolare viene garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 2016/679;
- D.Lgs. 10/08/2018 n. 101 recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e 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).”;
- 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;
- C.C. Art. 2104 “Diligenza del prestatore di lavoro”, il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende;
- C.C. Art. 2105 “Obbligo di fedeltà”, il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio;
- C.C. Art. 2106 “Sanzioni disciplinari”, l'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo alla applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione.