Infrastrutture Venete S.r.l.

Regolamento per la sicurezza informatica e l'utilizzo degli strumenti ICT

Approvato con Determina dell'Amministratore Unico	30/06/2026	Prima emissione
		Rev. 00

Sommario

1. FINALITÀ E SISTEMA DEI CONTROLLI

1.1 SCOPO E OBIETTIVI STRATEGICI

Lo scopo del presente Regolamento è preservare il patrimonio ICT di Infrastrutture Venete S.r.l. e fornire agli Utenti le indicazioni vincolanti circa il loro corretto ed appropriato uso, nel pieno rispetto della normativa vigente. In aderenza alle linee di indirizzo della Regione del Veneto, la Società persegue i seguenti obiettivi:

- **Riduzione del rischio informatico:** mitigare l'esposizione alle minacce e alle vulnerabilità dei sistemi, al fine di salvaguardare la disponibilità, l'integrità e la riservatezza (confidenzialità) dei dati gestiti, nonché la continuità operativa dei servizi ferroviari e di navigazione;
- **Conformità Privacy:** garantire il costante rispetto della normativa europea e nazionale vigente in materia di protezione dei dati personali (Regolamento UE 2016/679 - GDPR e D.lgs. 196/2003 e s.m.i.);
- **Tutela del patrimonio aziendale:** garantire l'integrità, la conservazione e la disponibilità dei beni materiali (hardware, postazioni di lavoro, dispositivi mobili, infrastrutture di rete) e immateriali (software, applicativi, banche dati, know-how societario) della Società;
- **Trasparenza operativa:** esplicitare le regole per la corretta e sicura fruizione dei servizi informatici erogati dalla Struttura Affari Generali e ICT – Ufficio ICT, definendone le caratteristiche, i criteri di assegnazione dei dispositivi e le modalità operative adottate dal Servizio di Supporto Tecnico – servizio di assistenza tecnica ***Support osTicket*****,** raggiungibile all'indirizzo: https://infoservizi2.stweb.it/support/

1.2 PRINCIPIO DI ACCOUNTABILITY E TUTELA DEL LAVORATORE

In adempimento al principio di *accountability* (responsabilizzazione) imposto dal GDPR e nel rispetto dell'art. 4 della Legge n. 300/1970 (Statuto dei Lavoratori), la Società adotta misure organizzative e tecniche atte a bilanciare il diritto del datore di lavoro di proteggere la propria organizzazione e i propri asset con il diritto del lavoratore alla riservatezza e alla dignità nei luoghi di lavoro.

Il presente Regolamento assolve agli obblighi informativi richiesti dall'art. 4, comma 3, della Legge 300/1970. Esso fornisce agli Utenti l'adeguata e preventiva informazione circa le modalità d'uso degli strumenti messi a disposizione e le modalità di effettuazione delle verifiche tecniche. Ai sensi della medesima disposizione legislativa, le informazioni raccolte tramite gli strumenti di lavoro e i sistemi di sicurezza informatica (necessari per la protezione del perimetro aziendale) sono utilizzabili a tutti i fini connessi al rapporto di lavoro, inclusi quelli disciplinari, purché nel rispetto delle tutele a protezione dei dati personali e del presente documento.

I dati personali eventualmente raccolti o transitati nel corso delle verifiche tecniche, manutentive o di sicurezza informatica sono trattati nel rispetto del principio di minimizzazione (adeguati, pertinenti e limitati a quanto necessario rispetto alle legittime finalità aziendali). In conformità alle Linee Guida del Garante della Privacy per posta elettronica e internet nonché ai successivi provvedimenti in materia di metadati, i sistemi aziendali di gestione della posta elettronica sono configurati per limitare la conservazione dei log tecnici di trasmissione ai soli tempi strettamente necessari all'erogazione e alla sicurezza del servizio, prevenendo la raccolta prolungata o generalizzata di tali informazioni.

1.3 GRADUALITÀ DEI CONTROLLI E VERIFICHE TECNICHE

Al fine di escludere qualsiasi forma di controllo prolungato, costante o indiscriminato, la Società adotta un sistema di verifiche tecnico-informatiche rigorosamente graduali:

1. **Controlli preliminari anonimi o cumulativi:** in caso di rilevazione di anomalie di sicurezza, saturazione delle risorse di rete o potenziali utilizzi difformi dalle istruzioni, l'Amministratore di Sistema (AdS) effettuerà accertamenti preliminari a livello aggregato o anonimo;
2. **Avvisi generalizzati:** qualora i controlli aggregati confermino l'anomalia, la Società invierà avvisi generalizzati diretti ai dipendenti dell'area o del settore interessato, evidenziando l'utilizzo irregolare rilevato e invitando gli interessati ad attenersi al presente Regolamento;
3. **Verifiche mirate o individuali:** controlli su base più ristretta o individuale potranno essere compiuti esclusivamente in caso di successive e ulteriori anomalie, oppure qualora si rendano indispensabili per specifiche finalità di controllo di qualità, manutenzione ordinaria e straordinaria, risoluzione di guasti tecnici o gestione di incidenti di sicurezza (data breach) che comportino l'obbligo di intervenire tempestivamente sui sistemi.

1.4 DIFFUSIONE DEL DOCUMENTO, VINCOLI COMPORTAMENTALI E CONFORMITÀ

L'utilizzo scorretto, abusivo o illecito delle risorse ICT espone la Società a gravi rischi patrimoniali, penali e reputazionali, e si considera contrario ai doveri fondamentali di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice Civile.

La violazione delle regole contenute nel presente Regolamento darà luogo all'esercizio del potere disciplinare da parte del Datore di Lavoro, che sarà attuato nelle forme previste dall'art. 7 dello Statuto dei Lavoratori e in perfetta conformità con i criteri di gradualità e proporzionalità stabiliti nel Titolo IV del *Regolamento Interno del Personale* di Infrastrutture Venete S.r.l., nonché dalle norme sanzionatorie del *CCNL Autoferrotranvieri* applicato.

Ai fini della piena cogenza ed efficacia del sistema disciplinare, il presente Regolamento viene pubblicato sul sito istituzionale della Società https://www.infrastrutturevenete.it/ e trasmesso tramite il Portale del Dipendente (Intranet aziendale), assolvendo agli obblighi di pubblicità e affissione, unitamente al Codice Disciplinare aziendale vigente.

Infine, il presente documento costituisce parte integrante del sistema di controllo interno e presidio organizzativo della Società atto a prevenire i rischi di reato ex D.Lgs. 8 giugno 2001, n. 231, concorrendo direttamente all'efficacia del Modello di Organizzazione, Gestione e Controllo (MOG) adottato.

2. AMBITO DI APPLICAZIONE

Il presente Regolamento si applica obbligatoriamente e senza eccezioni a tutto il personale dipendente di Infrastrutture Venete S.r.l. — inclusi i dirigenti, i lavoratori somministrati/interinali, i tirocinanti e gli stagisti — nonché ai collaboratori esterni, ai consulenti e ai partner commerciali autorizzati, a qualsiasi titolo, all'accesso o all'utilizzo delle risorse ICT aziendali (nel seguito definiti complessivamente **"Utenti"**). Ciascun Utente, in relazione al proprio profilo autorizzativo e alle mansioni assegnate, è tenuto all'osservanza scrupolosa delle presenti norme.

Le disposizioni si applicano, con livelli di dovere e responsabilità ancora più stringenti, ai soggetti incaricati di mansioni tecniche, di amministrazione o di vigilanza sui sistemi e sulle infrastrutture di rete, coordinati dall'Ufficio ICT. Ricadono in tale perimetro gli Amministratori di Sistema (AdS), gli amministratori di rete, gli amministratori di banche dati e i gestori dei servizi o di sicurezza applicativa, sia interni sia dipendenti di fornitori esterni formalmente designati.

Le regole che disciplinano l'uso delle risorse ICT di IV sono declinate e strutturate su tre versanti sinergici:

- **Versante Organizzativo (Misure Organizzative):** relativo alle procedure di pianificazione e assegnazione dei beni, alla gestione e profilazione degli accessi, al supporto tecnico e alla risposta tempestiva agli incidenti di sicurezza (*data breach*);
- **Versante Tecnologico-Procedurale (Misure Tecnologiche):** relativo alle configurazioni tecniche di sicurezza imposte sui dispositivi, alla protezione delle postazioni di lavoro (PdL), all'uso della crittografia e dei depositi password cifrati (*Vault*), ai sistemi di autenticazione a più fattori (MFA) e ai vincoli di rete e cloud, in conformità alle specifiche di sicurezza aziendali;
- **Versante Comportamentale (Misure Comportamentali):** relativo alle regole di condotta quotidiana esigibili dall'Utente nell'utilizzo del personal computer, della posta elettronica aziendale, della rete Internet, dei canali di comunicazione sociale (*social media*) e degli strumenti di telefonia mobile aziendale.

In coerenza con gli obiettivi di gestione della sicurezza delle informazioni (standard ISO 27001), la protezione dell'intero patrimonio tecnologico e informativo aziendale si fonda sul rispetto e la salvaguardia della triade dei requisiti di sicurezza (RID):

- **Riservatezza (o Confidenzialità):** la garanzia che le informazioni, i documenti e i dati gestiti siano accessibili, conoscibili e fruibili esclusivamente dai soggetti esplicitamente autorizzati e provvisti di reale necessità di sapere (*need to know*);
- **Integrità:** la garanzia della completezza, dell'accuratezza tecnica e dell'inalterabilità delle informazioni, dei flussi di dati e dei codici dei programmi applicativi;
- **Disponibilità:** la garanzia che gli Utenti autorizzati possano accedere tempestivamente e utilizzare le informazioni, i servizi informatici e le risorse tecnologiche ogni qualvolta sia necessario per lo svolgimento delle proprie attività lavorative e per la continuità dei servizi della Società.

3. MISURE ORGANIZZATIVE

3.1 GESTIONE DEGLI EVENTI E DEGLI INCIDENTI INFORMATICI

Le misure organizzative della Società sono orientate alla tempestiva rilevazione, classificazione e gestione degli eventi imprevisti, al fine di mitigare gli impatti operativi e garantire la costante conformità con il quadro normativo nazionale ed europeo.

A. Definizione e contestualizzazione

- **Incidente Informatico:** qualsiasi evento imprevisto e non pianificato rispetto al normale funzionamento di un sistema, di un applicativo o di un'infrastruttura ICT aziendale (sia essa di tipo hardware o software, locale o in Cloud), causato da malfunzionamenti accidentali, eventi naturali, errori umani o attacchi informatici mirati, in grado di compromettere o minacciare la riservatezza, l'integrità o la disponibilità dei dati e la continuità dei servizi della Società.
- **Violazione di Dati Personali (*Data Breach*):** la violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati da IV.
- **Phishing:** una tecnica di inganno informatico attraverso la quale malintenzionati inviano e-mail, messaggi o comunicazioni digitali contraffatte — graficamente simili a quelle di mittenti istituzionali o partner autorevoli — con lo scopo fraudolento di indurre l'Utente a rivelare password aziendali, dati bancari o a scaricare allegati contenenti software malevoli (malware).

B. Obblighi di segnalazione e condotta dell'Utente

Ogni Utente che rilevi un'attività anomala, un sospetto tentativo di *Phishing*, un malfunzionamento sistemico o la presenza di software malevolo sul dispositivo affidatogli, è tassativamente tenuto a:

1. **Inviare una e-mail immediata di allerta all'Ufficio ICT – informatica@infrastruttureveneto.it** inserendo obbligatoriamente nell'oggetto la dicitura *"[URGENTE - SICUREZZA INFORMATICA]"* per consentire l'immediata intercettazione visiva della minaccia;
2. **In alternativa**, qualora il servizio di posta elettronica aziendale non sia accessibile o risulti temporaneamente bloccato dall'attacco in corso, **l'Utente deve aprire tempestivamente un ticket nel portale ufficiale di assistenza tecnica aziendale (*Support osTicket*, raggiungibile all'indirizzo: https://infoservizi2.stweb.it/support/), avendo cura di selezionare l'apposita categoria di priorità assoluta denominata *"Incidenti di Sicurezza / Cybersecurity"***, al fine di evitare che la segnalazione confluisca e si disperda tra le quotidiane richieste di assistenza ordinaria**;**
3. **Nei casi di massima urgenza** (quali attacchi ransomware in corso con evidenza di cifratura dei file, o furto/smarrimento di dispositivi informatici aziendali), effettuare in ogni caso anche una tempestiva **segnalazione telefonica** ai diretti superiori e ai contatti operativi dell'Ufficio ICT, parallelamente all'invio della comunicazione scritta;
4. **non spegnere il computer o il dispositivo interessato** in caso di infezione da virus o attacco informatico in corso. L'Utente deve limitarsi esclusivamente a scollegare il cavo di rete (ove possibile) o a disconnettere il Wi-Fi, per consentire al personale tecnico di eseguire i necessari rilievi e analisi.

All'Utente è fatto divieto assoluto di porre in essere interventi autonomi o tentativi di riparazione, al fine di non alterare o distruggere le evidenze informatiche necessarie alle successive analisi.

C. Flusso di Escalation e Gestione Operativa

L'attivazione delle contromisure segue una precisa linea gerarchica interna aziendale:

- **L'Ufficio ICT** coordina le attività tecniche immediate sul campo e presiede al contenimento della minaccia. Analizza l'evento e ne classifica il livello di gravità (Bassa, Media, Alta, Critica).
- In caso di incidenti a priorità **Alta o Critica**, l'Ufficio ICT ha l'obbligo di investire immediatamente il **Responsabile Affari Generali e ICT**, il quale assume la supervisione della gestione

dello stato di emergenza e provvede a darne tempestiva notizia alla **Direzione Generale (DG)** per l'autorizzazione all'impiego di risorse specialistiche esterne di cybersecurity. Nei casi previsti dalla Legge n. 90/2024, il Responsabile Affari Generali e ICT provvederà alla trasmissione delle notifiche all'Agenzia per la Cybersicurezza Nazionale (ACN) sul portale istituzionale dedicatovi, previa approvazione formale dell'**Amministratore Unico**.

3.2 GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

Qualora l'analisi dell'incidente informatico evidenzi un coinvolgimento, anche solo potenziale, di archivi o dati personali, si attiva senza indugio la catena procedurale interna per il presidio della tutela della privacy:

1. **Segnalazione interna: L'Ufficio ICT**, intercettata l'anomalia sui dati personali dai monitoraggi di sicurezza o a seguito delle segnalazioni d'allerta dell'Utente, provvede al contenimento tecnico immediato e avvisa tempestivamente il **Delegato Privacy**.
2. **Attivazione del Presidio Privacy:** Il **Delegato Privacy** informa tempestivamente il **Data Protection Officer (DPO)** di Infrastrutture Venete S.r.l. e avvia l'istruttoria preliminare volta a verificare i presupposti e l'entità della violazione.
3. **Valutazione del rischio e Notifiche:** Qualora l'istruttoria evidenzi un rischio per i diritti e le libertà delle persone fisiche, il **DPO** effettuerà formalmente la notifica di *Data Breach* al Garante per la Protezione dei Dati Personali per conto dell'**Amministratore Unico** e previa sua autorizzazione. Tale adempimento deve essere eseguito tassativamente tramite la procedura telematica sul portale dell'Autorità **entro 72 ore** dal momento in cui la Società ne è venuta a conoscenza.
4. **Violazioni su servizi Cloud:** Se la violazione interessa dati ospitati su architetture Cloud fornite da terzi, la segnalazione del fornitore esterno (il quale è contrattualmente vincolato a inviarla entro 24 ore dalla rilevazione) viene presa in carico dall'**Ufficio ICT** e trasmessa immediatamente al **Responsabile Affari Generali e ICT** per l'attivazione delle medesime procedure di verifica e notifica descritte.

4. MISURE TECNOLOGICHE E PROCEDURALI

4.1 PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

In attuazione dei principi di protezione dei dati sin dalla fase di progettazione (*Privacy by Design*) e per impostazione predefinita (*Privacy by Default*), Infrastrutture Venete S.r.l. adotta criteri di sicurezza informatica stabili sin dalla fase di pianificazione di qualsiasi nuovo processo, servizio o strumento informatico.

- **Divieto di acquisto e installazione autonoma:** è fatto divieto alle singole Direzioni, Uffici o Unità Operative aziendali di procedere autonomamente — e senza preventivo raccordo — all'acquisto, all'installazione, al noleggio o al download da Internet di soluzioni software, applicativi, programmi o estensioni per i browser web. Qualsiasi esigenza operativa deve essere preventivamente comunicata al Responsabile dell'Ufficio ICT per la necessaria valutazione di compatibilità tecnica, di sicurezza e di conformità alle normative sulla protezione dei dati.
- **Clausole contrattuali obbligatorie per i fornitori:** nei contratti di appalto, di fornitura o di

servizi che implicano lo sviluppo, la manutenzione o la gestione di applicazioni informatiche e banche dati aziendali, le strutture proponenti devono obbligatoriamente prevedere l'inserimento dell'atto di "*Nomina a Responsabile Esterno del Trattamento*" e della specifica regolamentazione delle attività degli "*Amministratori di Sistema*", vincolando i soggetti esterni al rispetto dei più elevati standard di sicurezza informatica.

4.2 TRATTAMENTO DEI DATI IN ARCHITETTURE "CLOUD"

L'adozione e l'utilizzo di servizi, applicativi e piattaforme in Cloud (servizi e programmi accessibili via web e non installati localmente) sono rigorosamente subordinati alle seguenti regole:

- **Approvazione preventiva:** qualora si renda necessario l'utilizzo di servizi in Cloud per specifiche esigenze di lavoro, la richiesta deve essere preventivamente vagliata, verificata e autorizzata per iscritto dal Responsabile Affari Generali e ICT.
- **Localizzazione geografica dei dati:** Salvo motivate e straordinarie ragioni tecniche esplicitamente verificate e autorizzate, la Società si rivolge esclusivamente a fornitori esterni la cui infrastruttura di rete e i cui centri di conservazione dati (*Data Center*) siano localizzati all'interno del territorio dell'Unione Europea, escludendo il rischio di trasferimenti illeciti di informazioni verso paesi terzi non conformi ai requisiti del GDPR.
- L’azienda si riserva di bloccare l’accesso ad applicazioni ritenute non pertinenti all’ambito lavorativo o comunque non adeguate.

4.3 SICUREZZA DELLE POSTAZIONI DI LAVORO E CRITTOGRAFIA

Le Postazioni di Lavoro (siano esse fisse o mobili, inclusi computer desktop, computer portatili e tablet) costituiscono strumenti di lavoro di esclusiva proprietà aziendale e sono configurate a monte per garantire la protezione del perimetro informativo societario.

- **Principio del privilegio minimo:** a tutela della rete aziendale, a tutti gli Utenti viene assegnato un profilo d'uso standard di "non amministratore" (privilegi limitati). Tale configurazione impedisce l'installazione autonoma di software non controllato, riduce significativamente l'attivazione accidentale di virus o programmi malevoli e ne blocca la propagazione.
- **Supporto Tecnico e verifiche di rete:** qualsiasi eccezionale deroga operativa o necessità di installazione di software specifico per motivi di servizio deve essere richiesta esclusivamente all'Ufficio ICT tramite l'apertura di un ticket nel portale *osTicket*. Il personale del Supporto Tecnico è l'unico autorizzato a intervenire sulle configurazioni dei computer; ogni intervento deve essere motivato, limitato nel tempo e seguito dal ripristino immediato del profilo standard non appena esaurita l'esigenza. Il personale dell’ufficio ICT ha la facoltà di verificare periodicamente tutta la Rete Aziendale procedendo, se necessario, anche alla rimozione immediata di eventuali software installati senza licenza o comunque non autorizzati.
- **Crittografia (cifratura) dei dischi e dei supporti:** al fine di proteggere le informazioni in caso di furto o smarrimento del dispositivo, su tutti i computer portatili aziendali è mantenuta attiva e obbligatoria la funzionalità di cifratura automatica del disco fisso. I supporti rimovibili di memoria (quali chiavette USB o hard disk portatili) messi a disposizione dalla Società e utilizzati per il trasferimento di dati personali o informazioni aziendali riservate devono essere sottoposti a cifratura obbligatoria, richiedendo il supporto operativo dell'Ufficio ICT.
- **Regole di salvataggio e tutela dei dati lavorativi**: i dati salvati localmente sulle postazioni di lavoro (es. sul Desktop o nella directory locale C:) non sono soggetti a copia di sicurezza e potrebbero andare persi a seguiti di guasti, furti o smarrimenti. È fatto obbligo agli Utenti di

salvare i propri file e documenti di lavoro esclusivamente sulle cartelle condivise di rete o sullo spazio Google Drive aziendale. Tali repository centralizzati sono gli unici sottoposti a sistemi stabili di salvataggio periodico e backup automatizzato. Il dettaglio delle cartelle da utilizzare per le diverse tipologie di file deve essere concordato con il proprio Responsabile di Unità Operativa o Direttore di Direzione.

4.4 POLITICA DELLE SCRIVANIE E DEI COMPUTER PULITI (CLEAN DESK POLICY)

La protezione delle informazioni impone un controllo rigoroso non solo sugli strumenti digitali, ma anche sull'ambiente fisico di lavoro, a tutela del patrimonio aziendale e dei dati trattati.

- **Condotta quotidiana e blocco dello schermo:** durante ogni assenza temporanea dalla propria postazione, anche se di brevissima durata, l'Utente è tenuto a bloccare lo schermo del proprio computer (utilizzando la combinazione rapida di tasti *Windows + L* o la funzione di blocco equivalente). I computer portatili, i telefoni cellulari e i tablet aziendali non devono mai essere lasciati incustoditi in uffici vuoti, sale riunioni o luoghi accessibili a soggetti esterni estranei alla Società.
- **Divieto di archiviazione di dati personali non lavorativi:** Le postazioni di lavoro, i server e gli spazi di archiviazione in Cloud (Google Drive) sono destinati esclusivamente allo svolgimento delle mansioni professionali. È fatto divieto all'Utente di creare cartelle, salvare file, fotografie, comunicazioni o documenti di natura strettamente personale e non attinenti all'attività lavorativa (con particolare riferimento a dati sensibili, sanitari o finanziari) sui dischi locali dei computer o sulle piattaforme di condivisione aziendali. L'Azienda declina ogni responsabilità per la perdita o il danneggiamento di tali contenuti e si riserva il diritto di rimuoverli qualora rilevati.
- **Gestione della documentazione cartacea:** al termine della giornata lavorativa, o in caso di assenze prolungate, l'Utente ha l'obbligo di rimuovere dalla propria scrivania e riporre all'interno di cassettiere o armadi dotati di serratura tutta la documentazione cartacea, le note, i promemoria o i fogli di lavoro contenenti dati personali, credenziali di accesso o informazioni societarie riservate. I documenti cartacei non più necessari devono essere distrutti tramite gli appositi distruggidocumenti d'ufficio, vietandone l'accumulo o il gettito nei cestini dei rifiuti generici.
- **Responsabilità all'interno delle sale riunioni:** chi organizza, presiede o richiede l'uso di una sala riunioni aziendale ha la diretta responsabilità di verificare che, al termine dell'incontro, non venga dimenticato o lasciato incustodito alcun documento cartaceo, appunto o supporto di memoria rimovibile. È fatto obbligo di cancellare accuratamente le lavagne fisse o mobili utilizzate e assicurarsi che eventuali copie di documenti scartate siano distrutte in modo sicuro.

4.5 SICUREZZA DELLA RETE E DEI SERVER

L'infrastruttura di rete e l'architettura dei server di Infrastrutture Venete S.r.l. sono governate e monitorate centralmente per assicurarne la continuità operativa.

- **Centralizzazione delle risorse:** non è consentita in alcun modo all'Utente l'installazione, la configurazione o la gestione autonoma di apparati server, dispositivi di rete (quali router, switch, ripetitori o antenne Wi-Fi personali) o memorie di archiviazione locale presso gli uffici o le sedi periferiche senza la preventiva ed esplicita autorizzazione scritta del Responsabile Affari Generali e ICT.

- **Tracciabilità degli accessi tecnici:** l'accesso ai sistemi centrali, ai server e agli apparati di rete con privilegi amministrativi da parte del personale tecnico o dei fornitori esterni formalmente designati deve avvenire esclusivamente attraverso sistemi controllati e tracciati, al fine di garantire la registrazione inalterabile delle attività e la revoca immediata delle autorizzazioni in caso di necessità.

4.6 SICUREZZA DELLA NAVIGAZIONE INTERNET

La connessione alla rete Internet aziendale è una risorsa di proprietà della Società, fornita all'Utente esclusivamente per scopi istituzionali e per lo svolgimento delle mansioni professionali.

- **Uso pertinente e filtri di protezione:** l'accesso alla rete Internet deve essere strettamente correlato allo svolgimento delle attività lavorative. A tutela dell'integrità dei sistemi e per prevenire il download involontario di virus, malware o l'esposizione a minacce informatiche, la Società implementa sistemi centralizzati di filtraggio dei contenuti. Tali sistemi bloccano automaticamente l'accesso a categorie di siti web ritenute pericolose, non correlate all'attività d'ufficio o contrarie alle finalità aziendali.
- **Politiche di navigazione eccezionali:** l'Ufficio ICT si riserva la facoltà di definire e applicare politiche di navigazione personalizzate ed eccezionali in base a documentate e motivate esigenze d'ufficio o per specifiche mansioni professionali, escludendo in ogni caso utilizzi impropri o in contrasto con le norme di legge.

4.7 CONSERVAZIONE DEI LOG E ACCESSO AI DATI DEL PERSONALE ASSENTE O CESSATO

La gestione delle tracce informatiche e l'eventuale accesso ai dati contenuti negli strumenti aziendali avvengono nel rigoroso rispetto dello Statuto dei Lavoratori, dei diritti della persona e delle prescrizioni del Garante per la Protezione dei Dati Personali.

- **Cancellazione periodica delle tracce di rete:** i sistemi aziendali registrano i log di rete e di sistema (le tracce informatiche di funzionamento) unicamente per finalità di sicurezza logica, diagnostica tecnica e continuità dei servizi. Tali registrazioni vengono cancellate periodicamente secondo le politiche di conservazione stabilite dalla Società, prolungandone la durata solo in presenza di specifici obblighi normativi o su esplicita richiesta dell'Autorità Giudiziaria.
- **Accesso ai dati in caso di assenza prolungata o cessazione:** Al fine di garantire la continuità amministrativa e operativa della Società e la tutela del patrimonio informativo aziendale, in caso di assenza improvvisa, prolungata o di cessazione del rapporto di lavoro dell'Utente, i colleghi o i superiori non possono accedere autonomamente al computer o ai file dell'interessato. L'accesso ai file contenuti nelle risorse informatiche assegnate all'Utente assente (ivi inclusa la sua cartella di lavoro individuale) può avvenire esclusivamente a fronte di una formale e motivata richiesta scritta del Direttore Generale o del Direttore di Settore competente, indirizzata e autorizzata dal Responsabile Affari Generali e ICT. L'intervento tecnico dell'Ufficio ICT sarà limitato allo stretto necessario, privilegiando il solo trasferimento dei file di natura prettamente professionale e garantendo l'assoluto rispetto della dignità e della sfera personale del lavoratore. **In ogni caso, in virtù del divieto di utilizzo dei sistemi aziendali per finalità strettamente personali, l'Utente non può vantare alcuna aspettativa di riservatezza rispetto a file o cartelle che, in violazione delle disposizioni del presente Regolamento, siano stati indebitamente memorizzati sui dispositivi o sugli spazi di archiviazione societari.** Ciascun accesso straordinario viene registrato e verbalizzato a cura dell'Ufficio ICT.

Le cartelle di lavoro individuali e i file del personale cessato vengono conservati per un periodo massimo di 12 mesi dalla chiusura del rapporto di lavoro per consentire il recupero delle attività lavorative in corso, decorso il quale si provvede alla loro rimozione definitiva o archiviazione storica centralizzata.

4.8 STRUMENTI AMMESSI PER LO SCAMBIO E LA CONDIVISIONE DEI DATI

Il trasferimento, l'invio e la condivisione di file, documenti e informazioni aziendali deve seguire esclusivamente canali sicuri, protetti e tracciabili forniti dalla Società.

- **Canali ufficiali approvati:** lo scambio e la condivisione di dati all'interno degli uffici o verso soggetti esterni (enti, partner, fornitori) deve avvenire unicamente tramite gli strumenti ufficiali messi a disposizione e configurati dall'Ufficio ICT, quali le cartelle di rete protette sui server aziendali o le piattaforme di collaborazione e archiviazione su spazio Google Drive esplicitamente contrattualizzate e approvate dalla Società.
- **Divieto di condivisioni non controllate:** è fatto assoluto divieto all'Utente di attivare funzioni di condivisione di cartelle o file direttamente tra singoli computer sfruttando le funzionalità di rete spontanee dei sistemi operativi. Questo divieto è finalizzato a prevenire gravi vulnerabilità di rete e a mantenere il controllo centralizzato aziendale sui permessi di accesso ai dati.
- **È tassativamente vietato l'utilizzo di supporti di memoria personali o di terzi**. Lo scambio di documenti o file avviene normalmente via Google Drive.

4.9 GESTIONE DELLE UTENZE E DEGLI AMMINISTRATORI DI SISTEMA (AdS)

L'identificazione certa e univoca degli Utenti è il presupposto fondamentale per la sicurezza logica dei sistemi informatici aziendali.

- **Trattamento e custodia delle credenziali:** I codici di identificazione utente (User ID) e le relative password di accesso assegnate sono strettamente personali, riservati, secretati e non cedibili o condivisibili per nessuna ragione (nemmeno tra colleghi dello stesso ufficio o tra superiori e sottoposti). L'Utente è l'unico custode delle proprie credenziali e risponde personalmente di qualsiasi attività o operazione effettuata sul sistema informatico con la propria identità digitale. Qualora vi sia il dubbio che la riservatezza sia stata compromessa, la password deve essere immediatamente sostituita.
  - **Parametri di complessità e rotazione**: le password devono essere modificate obbligatoriamente al primo utilizzo e, successivamente, aggiornate con cadenza trimestrale (ogni 90 giorni). Ogni nuova password deve rispettare rigorosamente i seguenti requisiti minimi di complessità logica:
    - ✓ una lunghezza minima di 12 (dodici) caratteri;
    - ✓ presenza simultanea di almeno un carattere alfabetico maiuscolo, uno minuscolo, un carattere numerico e un carattere speciale (es. !, @, #, $, %, ^, &, *, ecc.).
  - **Divieto di trascrizione e banalizzazione**: le password non devono essere trascritte su carta o memorizzate su supporti elettronici non protetti (è fatto assoluto divieto d'uso di Post-It, agende cartacee, file di testo in chiaro). Devono essere tassativamente evitate password banali o facilmente ricavabili tramite dati personali (es. User ID, date di nascita, nomi di familiari o targhe auto).
  - **Presidi di protezione:** a tutela dei profili, il sistema applica un blocco automatico temporaneo di 30 minuti dopo 5 tentativi falliti di autenticazione, nonché la memorizzazione

dello storico delle ultime 8 password, vietandone il riutilizzo.
    - **Autenticazione a più fattori (MFA)**: laddove tale funzionalità sia tecnicamente prevista, implementata e attivata dall'Ufficio ICT per l'accesso alle piattaforme Cloud, alla posta elettronica o ai sistemi aziendali, gli Utenti hanno l'obbligo di utilizzare i sistemi di Autenticazione a Più Fattori (MFA / secondo fattore di sicurezza tramite applicazione su smartphone o codice) forniti dall'Azienda.

- **Adempimenti per gli Amministratori di Sistema:** per il personale incaricato di mansioni tecniche con privilegi di accesso elevati (siano essi dipendenti interni o tecnici/fornitori esterni), la Società applica scrupolosamente le prescrizioni del Provvedimento del Garante della Privacy. Gli Amministratori di Sistema firmano un atto di designazione individuale, hanno l'obbligo di operare ordinariamente con un account standard "non privilegiato" (attivando il profilo amministrativo solo per il tempo strettamente necessario alle manutenzioni) e i loro log di accesso logico ai sistemi vengono registrati in modo inalterabile e conservati per un periodo non inferiore a 6 mesi per eventuali verifiche del Delegato Privacy.

4.10 MODALITÀ DI UTILIZZO DELLA POSTA ELETTRONICA AZIENDALE

La casella di posta elettronica aziendale è uno strumento di comunicazione ufficiale intestato alla Società ed affidato all'Utente per l'esclusivo svolgimento delle proprie mansioni professionali.

- **Regole di condotta e firma istituzionale:** l'utilizzo della posta elettronica deve conformarsi ai principi della buona educazione digitale. In calce ad ogni messaggio inviato verso l'esterno dell'Azienda, l'Utente deve configurare obbligatoriamente la firma istituzionale standardizzata predisposta dalla Società, comprensiva della nota informativa legale (*Disclaimer Privacy*) volta a informare i terzi circa la riservatezza delle informazioni contenute e il divieto di diffusione non autorizzata.

4.11 GESTIONE IN CASO DI CESSAZIONE DEL RAPPORTO DI LAVORO

- In stretta conformità con le linee guida del Garante Privacy, le procedure aziendali e le necessità di continuità aziendale, al momento della cessazione del rapporto di lavoro o del trasferimento definitivo dell'Utente ad altro Ufficio o Unità Operativa, la Società provvede alla tempestiva disattivazione e al congelamento della casella di posta elettronica individuale per un periodo massimo di **12 mesi,** decorsi i quali l'account verrà definitivamente rimosso. Al fine di garantire la continuità delle attività professionali, all'atto della disattivazione verrà configurato un sistema di risposta automatica (*Messaggio di cortesia*) attivo per un periodo di **90 giorni**, volto a informare i mittenti esterni della disattivazione dell'account e a indicare un indirizzo di posta elettronica istituzionale alternativo dell'Ufficio o della Direzione a cui indirizzare le comunicazioni di lavoro. È tassativamente vietato impostare qualsiasi inoltro automatico dei messaggi in arrivo verso account di altri colleghi (c.d. divieto di *forward* automatico).
- Per questo motivo, a seguito della cessazione del rapporto di lavoro, il dipendente deve provvedere a:

    - eliminare eventuali messaggi di natura personale inviati, ricevuti o archiviati nella propria casella di posta elettronica in violazione della presente Policy;
    - eliminare eventuali contatti personali dalla rubrica del sistema di posta elettronica, dallo smartphone aziendale, memorizzati in violazione della Presente Policy;

- restituire i dati in formato cartaceo, di cui sia venuto in possesso nel corso delle attività;
- restituire gli strumenti aziendali (PC e cellulare) completi con i dati di interesse aziendale;
- restituire una copia dei dati di cui sia venuto in possesso nel corso del rapporto di lavoro e cancellarli da qualunque supporto di sua proprietà o a lui riservato (a titolo di esempio: chiavette, dischi esterni, computer personale, copie in cloud ecc.).

- Nella fattispecie, si precisa che i dati di cui si tratta possono essere riferiti sia a persone fisiche, identificate o identificabili, sia ad altre informazioni come disegni, documenti, codici di accesso e qualunque altro tipo di informazione di tipo industriale dell'Azienda, delle sue controllate/correlate e dei suoi clienti/fornitori.

4.12 ACCESSO REMOTO AI SERVIZI AZIENDALI (SMART WORKING / LAVORO A DISTANZA)

L'accesso alle risorse informatiche, ai server e ai dati aziendali al di fuori del perimetro fisico degli uffici della Società deve avvenire garantendo le medesime condizioni di sicurezza presenti in sede.

- **Canali sicuri di collegamento (VPN):** l'accesso da remoto è consentito esclusivamente agli Utenti esplicitamente autorizzati e deve realizzarsi unicamente ed obbligatoriamente tramite i canali cifrati protetti (*VPN - Virtual Private Network*) o le piattaforme di Desktop Virtuale fornite, installate e configurate dall'Ufficio ICT.
- **Vincoli di comportamento e riservatezza ambientale:** l'Utente che opera in modalità di lavoro a distanza (smart working, trasferta o domicilio) ha la responsabilità personale di verificare che l'ambiente circostante garantisca la totale riservatezza delle sessioni di lavoro, posizionando lo schermo e custodendone l'uso in modo da impedire la visualizzazione o l'accesso ai dati aziendali a soggetti terzi non autorizzati. Per il collegamento remoto è obbligatorio l'utilizzo di sistemi di autenticazione a più fattori.

4.13 UTILIZZO DI DISPOSITIVI E RETI PERSONALI E PRIVATI (BYOD)

- **Accesso con dispositivi privati**: L'utilizzo di personal computer, tablet o smartphone di proprietà privata dell'Utente per scopi lavorativi (regime Bring Your Own Device - BYOD) è vietato, salvo eccezionale e formale autorizzazione scritta del Responsabile Affari Generali e ICT. Qualora esplicitamente autorizzato, l'accesso ai dati e agli applicativi aziendali deve realizzarsi obbligatoriamente ed esclusivamente tramite i canali cifrati protetti (VPN) o le infrastrutture desktop virtuali fornite e configurate dall'Ufficio ICT;
- **Regole di connettività presso le sedi**: All'interno dei locali fisici e delle sedi di Infrastrutture Venete S.r.l., è tassativamente vietata la connessione di personal computer, notebook o strumenti informatici privati e non aziendali alla rete LAN interna di produzione (sia via cavo sia tramite l'aggancio alle reti Wi-Fi aziendali di servizio). Per le necessità di connettività a Internet di dispositivi privati è consentito esclusivamente l'utilizzo della rete Wi-Fi dedicata denominata "Ospiti" (Guest), ove fisicamente presente e attiva;
- **Limitazione di responsabilità**: la Società non risponde in alcun modo di eventuali danni, perdite di dati o malfunzionamenti che dovessero verificarsi sui dispositivi privati dell'Utente a seguito dell'installazione o dell'utilizzo degli applicativi aziendali, rimanendo la manutenzione dell'hardware privato a totale ed esclusivo carico del proprietario.

4.14 UTILIZZO DI STRUMENTI DI INTELLIGENZA ARTIFICIALE (IA)

- **Divieto di caricamento di dati aziendali su piattaforme pubbliche:** è vietato agli Utenti inserire, copiare o caricare informazioni aziendali, dati personali, documenti interni, codici sorgente, atti amministrativi o contrattuali di Infrastrutture Venete S.r.l. all'interno di strumenti di Intelligenza Artificiale generativa accessibili pubblicamente online (quali, a titolo esemplificativo, chatbot, sistemi di traduzione automatica non aziendali o software di elaborazione testi algoritmica), **qualora tali sistemi non siano stati preventivamente autorizzati e contrattualizzati dall'Ufficio ICT**.
- **Tutela del patrimonio informativo:** il caricamento di asset informativi societari su piattaforme esterne prive di tutele contrattuali dedicate costituisce una violazione del dovere di riservatezza e una potenziale compromissione della sicurezza dei dati (*data breach*), oltre a esporre la Società al rischio di violazione delle normative sulla proprietà intellettuale.
- **Linee guida future:** l'introduzione e utilizzo di strumenti di IA per finalità produttive aziendali sarà oggetto di specifica regolamentazione e formazione a cura del Settore Affari Generali e ICT.

4.15 GESTIONE E ASSEGNAZIONE DELLA TELEFONIA MOBILE AZIENDALE

La Struttura Affari Generali e ICT sovraintende alla pianificazione, all'acquisto, all'assegnazione e alla revoca dei dispositivi di telefonia mobile, delle SIM card e degli apparati di connettività mobile (quali router portatili o modem) di proprietà o in uso alla Società.

- **Vincolo di servizio:** l'assegnazione di un dispositivo mobile o di una SIM aziendale è strettamente subordinata a motivate esigenze di servizio, valutate in base al ruolo ricoperto (quali l'esercizio delle funzioni di reperibilità, l'attività del personale tecnico o di linea, il coordinamento della sicurezza delle infrastrutture ferroviarie e navigabili, o ruoli direzionali). I profili di traffico abilitati (nazionali o internazionali) sono definiti dall'Ufficio ICT in base alle effettive necessità operative della mansione.
- **Divieto di cessione e alterazione:** Il dispositivo e la relativa SIM sono strettamente personali e non possono essere ceduti in uso a terzi esterni alla Società. È fatto divieto di alterare la configurazione software predefinita, effettuare procedure di sblocco forzato del sistema operativo (*jailbreak* o *rooting*) o disattivare i sistemi di protezione e monitoraggio installati dalla Società.
- **Misure di protezione del dispositivo:** l'Utente è tenuto a mantenere costantemente attivi i sistemi di protezione e blocco dello schermo sul dispositivo (PIN numerico complesso o autenticazione biometrica ove disponibile). Il dispositivo deve essere custodito con la massima cura.
- **Chiamate e traffico personale:** l'utilizzo della linea telefonica aziendale per comunicazioni personali è tollerato esclusivamente nei limiti della normale ragionevolezza e urgenza. Qualora i contratti aziendali stipulati con l'operatore telefonico prevedano opzioni di fatturazione scissa per il traffico personale, i relativi costi saranno posti a carico del dipendente secondo le modalità concordate con la Direzione Generale.
- **Restituzione dell'asset:** l'Utente ha l'obbligo di restituire tempestivamente il dispositivo, la SIM card e tutti gli accessori ricevuti in dotazione dall'Ufficio ICT al momento del venir meno delle esigenze di servizio che ne avevano giustificato l'assegnazione, in caso di cambio di mansione, sospensione prolungata dall'attività lavorativa o alla cessazione formale del rapporto di lavoro a qualsiasi titolo.

5. MISURE COMPORTAMENTALI E SISTEMA SANZIONATORIO

5.1 PARTECIPAZIONE AI SOCIAL MEDIA E TUTELA REPUTAZIONALE

La Società riconosce e rispetta il diritto di ciascun Utente alla libertà di espressione e alla partecipazione attiva sui Social Media (quali, a titolo esemplificativo, LinkedIn, Facebook, Instagram, X, YouTube) e sulle piattaforme di messaggistica istantanea (WhatsApp). Tuttavia, l'utilizzo di tali canali, sia durante l'orario di lavoro sia nel tempo privato, deve avvenire nel rispetto del dovere di fedeltà, riservatezza e correttezza verso l'Azienda.

- **Divieto di divulgazione di informazioni riservate:** è fatto assoluto divieto agli Utenti di pubblicare, condividere o commentare sui propri profili social personali informazioni, dati, provvedimenti interni, notizie o indiscrezioni riguardanti le attività della Società che non siano ancora state rese pubbliche attraverso i canali ufficiali. Tale divieto si estende in particolare ai dati tecnici, commerciali e di know-how relativi agli asset societari.
- **Uso di immagini, fotografie e loghi aziendali:** non è consentito pubblicare sui social media personali fotografie o video scattati all'interno degli uffici, dei cantieri, delle cabine di guida o delle aree operative societarie se in tali immagini sono visibili loghi di Infrastrutture Venete, documenti di lavoro, schermate di computer aziendali o volti di colleghi e terzi senza il loro esplicito consenso. È altresì vietato l'utilizzo del logo istituzionale della Società per la creazione di profili, pagine o gruppi personali senza una preventiva autorizzazione scritta da parte della Direzione Generale.
- **Separazione tra opinioni personali e posizioni della Società:** nello svolgimento della propria attività sui social network, l'Utente deve chiarire, ove necessario, che le opinioni espresse sono di natura strettamente personale e non rappresentano in alcun modo la posizione ufficiale di Infrastrutture Venete S.r.l. In ogni caso, è fatto divieto di utilizzare espressioni o pubblicare contenuti che possano ledere l'immagine, l'onorabilità e la reputazione della Società, dei suoi vertici, dei colleghi o dei partner istituzionali.
- **Utilizzo dei social media durante l'orario di lavoro:** l'accesso alle piattaforme social personali tramite i computer o i dispositivi mobili aziendali, così come l'uso dei propri dispositivi personali per finalità non lavorative durante l'orario d'ufficio, deve essere limitato a casi eccezionali e non deve in alcun modo pregiudicare il regolare svolgimento delle mansioni professionali o la sicurezza della rete aziendale.

5.2 RESPONSABILITÀ E SISTEMA SANZIONATORIO

- **Inadempimento contrattuale:** il rispetto delle disposizioni del presente Regolamento costituisce adempimento degli obblighi derivanti dal rapporto di lavoro (artt. 2104 e 2105 cod. civ.). L'inosservanza delle regole d'uso delle risorse ICT, l'elusione delle misure di sicurezza informatica o l'adozione di condotte lesive della reputazione aziendale integrano un illecito disciplinare e un danno al patrimonio informativo e materiale della Società.
- **Rinvio al Regolamento Interno del Personale:** qualsiasi violazione accertata (nel rispetto delle garanzie procedurali e dei presupposti statistico-anonimi definiti al paragrafo 2.3) sarà perseguita e sanzionata attraverso i provvedimenti previsti dal **Regolamento Interno del Personale di Infrastrutture Venete S.r.l.**, in stretta applicazione della gradualità e delle sanzioni stabilite dal Contratto Collettivo Nazionale di Lavoro (CCNL) di riferimento in vigore, fatta salva l'attivazione di eventuali azioni civili o penali nei casi previsti dalla legge.

6. RESPONSABILITÀ GIURIDICHE ESTERNE E MODELLO 231

6.1 RESPONSABILITÀ CIVILE E PENALE

Le violazioni delle disposizioni del presente Regolamento, laddove integrino condotte illecite o causino pregiudizi diretti agli asset societari, possono esporre l'Utente a gravi conseguenze di natura giuridica esterna rispetto al rapporto di lavoro. Il dipendente risponde personalmente dinanzi alle Autorità competenti per:

- **Danni patrimoniali:** i danni diretti causati alla Società o a terzi a seguito di utilizzi illeciti, negligenti o non autorizzati delle risorse ICT.
- **Reati :** Le fattispecie di reato configurabili a carico dell'autore materiale della condotta, quali, a titolo esemplificativo, l'accesso abusivo a un system informatico o telematico (art. 615-ter c.p.), la frode informatica (art. 640-ter c.p.) o il danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.), i quali possono comportare, oltre alle responsabilità penali personali, l'applicazione delle sanzioni aziendali ai sensi del D.Lgs. 231/2001.

6.2 PRESIDIO DEL MODELLO ORGANIZZATIVO D.LGS. 231/2001

Le regole comportamentali e tecnologiche formalizzate nel presente documento costituiscono parte integrante e sostanziale del sistema di controllo interno e dei protocolli di prevenzione atti a escludere la responsabilità amministrativa della Società ai sensi del D.Lgs. 8 giugno 2001, n. 231.

- **Prevenzione dei reati informatici:** il rispetto del presente testo mira specificamente a impedire il compimento dei reati informatici e di illecito trattamento dei dati (art. 24-bis D.Lgs. 231/2001) e dei delitti di violazione del diritto d'autore e tutela del software (art. 25-nonies D.Lgs. 231/2001).
- **Flussi verso l'Organismo di Vigilanza:** qualsiasi violazione accertata che possa integrare un rischio ai sensi del Modello Organizzativo aziendale sarà tempestivamente segnalata all'Organismo di Vigilanza (OdV) di Infrastrutture Venete S.r.l. per le valutazioni e i provvedimenti di competenza.

6.3 PRESIDIO WHISTLEBLOWING

Al fine della conformità al D.lgs n. 24 del 2023 (c.d. Decreto Whistleblowing), stante l'implementazione da parte della Società di un proprio canale informatico per la segnalazione di "illeciti Whistleblowing" accessibile da sito internet societario, si ricorda la possibilità di inoltrare – tramite l'anzidetta piattaforma e con garanzia delle tutele di cui al Decreto, in primis riservatezza e divieto di ritorsioni– segnalazioni di fatti che, a proprio parere, possono integrare uno degli illeciti di cui all'art. 24 bis e/o 25 nonies D.Lgs 231/2001.

7. ENTRATA IN VIGORE, PUBBLICITÀ E AGGIORNAMENTO

7.1 ADOZIONE ED ENTRATA IN VIGORE

Il presente Regolamento è adottato formalmente con apposito provvedimento dell'Amministratore Unico ed entra in vigore con efficacia immediata a decorrere dalla data della sua approvazione e pubblicazione.

7.2 ASSOLVIMENTO DEGLI OBBLIGHI INFORMATIVI E PUBBLICITÀ

Al fine di garantire la massima diffusione, la piena conoscibilità e l'opponibilità delle presenti norme a tutto il personale, anche ai sensi e per gli effetti di cui all'art. 4, comma 3, della Legge n. 300/1970 (Statuto dei Lavoratori), la Società provvede alla pubblicità del testo mediante:

- **Pubblicazione e trasmissione tramite il Portale del Dipendente:** il testo integrale del presente Regolamento viene trasmesso a tutti i dipendenti in forza all'atto dell'adozione e pubblicato in via permanente all'interno della Intranet aziendale (Portale del Dipendente). Tale modalità digitale e dematerializzata garantisce la costante accessibilità del documento e sostituisce a tutti gli effetti l'affissione cartacea nei locali aziendali, costituendo presupposto di piena conoscibilità e cogenza delle regole d'uso per tutto il personale
- **Informativa ai nuovi assunti:** copia del presente Regolamento viene consegnata o trasmessa a ogni nuovo Utente all'atto dell'assunzione o della sottoscrizione del contratto di collaborazione, affinché ne prenda formale visione prima dell'attivazione delle credenziali e delle risorse informatiche.

7.3 PROCESSO DI REVISIONE E AGGIORNAMENTO

Il presente documento è soggetto a verifica periodica per garantirne il costante allineamento tecnologico, organizzativo e normativo. Il Settore Affari Generali e ICT si occupa del monitoraggio dell'efficacia delle misure e propone i necessari aggiornamenti o integrazioni in conseguenza di:

- evoluzioni del quadro normativo nazionale ed europeo in materia di cybersecurity, intelligenza artificiale e protezione dei dati personali;
- provvedimenti, linee guida o prescrizioni emanate dall'Autorità Garante per la Protezione dei dati Personali o dall'Agenzia per l'Italia Digitale (AgID);
- mutamenti strutturali nell'architettura tecnologica aziendale, introduzione di nuovi applicativi o variazioni nell'organizzazione interna di Infrastrutture Venete S.r.l..