AZIENDA PROVINCIALE TRASPORTI S.P.A.

REGOLAMENTO

Regolamento Aziendale Sistemi Informativi

REV 01 – 29 SETTEMBRE 2025

1. Definizioni

Al fine di evitare ambiguità ed incomprensioni vengono fornite le definizioni di alcuni termini utilizzati nel presente regolamento.

- **Azienda**: Azienda Provinciale Trasporti Spa, identificata con C.F./P.IVA 00505830315, con sede legale in Via Caduti di An Nasiriyah n.6, 34170 Gorizia (GO), ed eventuali acronimi ed abbreviazioni;
- **Beni Aziendali**: da intendersi come nozione afferente all'art. 2555 del Codice civile (da leggersi come ogni bene mobile e immobile utili all'esercizio dell'impresa);
- **Ufficio Servizi Informativi** (abbreviato anche in Ufficio IT): Ufficio affluente alla Direzione Area Procurement, Infrastrutture e Sviluppo, chiamato "ICT Infomobilità" nell'organigramma aziendale;
- **Responsabile dell'Ufficio Servizi Informativi**: sig. Tolazzi Renzo, contattabile all'indirizzo e-mail renzo.tolazzi@aptgorizia.it e ai recapiti telefonici aziendali 0481.593505 e/o 335.8713823;
- **Consorzio**: l'Azienda per l'esercizio del trasporto pubblico locale è consorziata a TPL FVG S.c.a r.l., identificato con C.F/P.IVA 01024770313, con sede legale in Via Caduti di An Nasiriyah n.6, 34170 Gorizia (GO) ed eventuali suoi acronimi ed abbreviazioni;
- **Dispositivo Elettronico**: strumento lavorativo elettronico, ivi inclusi smartphone, tablet, computer, ecc....;
- **MDM**: Mobile Device Management, gestione remota e centralizzata dei dispositivi aziendali quali smartphone e postazioni similari;
- **Personal Computer**: netbook, notebook, workstation e qualunque sinonimo di pc e computer;
- **VPN**: Virtual Private Network - tecnologia che consente l'accesso all'infrastruttura aziendale da un'altra rete esterna tramite una connessione privata;
- **2FA**: autenticazione a due fattori (credenziali di accesso come nome utente e password a cui si aggiunge un codice temporaneo);
- **MFA**: autenticazione a due o più fattori (come 2FA ma può prevedere l'utilizzo di livelli aggiuntivi di sicurezza come l'inserimento di una smart card o di altri segreti);
- **Dati Biometrici**: sono dati considerati a trattamento speciale ai fini del GDPR, si tratta di tutti i dati che analizzano il comportamento fisico, fisiologico o comportamentale dell'utente (di norma ci si riferisce alla scansione delle impronte digitali o del volto);
- **AI / IA**: intelligenza artificiale, nell'ambito di applicazione del presente documento si include qualsiasi tipo di intelligenza artificiale ivi compresa l'intelligenza artificiale generativa e dei processi decisioni automatizzati;
- **IAG**: intelligenza artificiale generativa
- **OTP**: One Time Password, codice monouso solitamente numerico casuale e temporaneo usato spesso nell'autenticazione a due fattori;
- **BYOD**: Bring Your Own Device, l'utilizzo di dispositivi personali non affidati dall'azienda per fini legati alla professione o utilizzati in ambito lavorativo;
- **Account di posta nominativo**: account di posta elettronica, al fine del regolamento si intende di natura professionale e lavorativa, fornito dall'Azienda ad uno specifico dipendente che lo indentifica univocamente, questo tipo di account non è condiviso con altri utenti aziendali.

2. Premesse

Tenendo conto del ruolo centrale che viene ricoperto a vario titolo dalle tecnologie informatiche nei processi aziendali, l'utilizzo sicuro ed efficace di questi importanti strumenti è fondamentale per garantire la continuità operativa, la protezione del patrimonio aziendale, la tutela dei diritti di tutti gli interessati e il rispetto delle normative vigenti. La sempre maggiore esposizione a rischi informatici che includono crimini e frodi informatiche ma non solo, tra cui vale la pena citare come ad esempio il furto e lo smarrimento di dati, unitamente all'obbligo legale di agire con tutti gli strumenti necessari per la tutela degli interessi aziendali e nella difesa delle informazioni trattate, rende doverosa e di primaria importanza l'adozione di un Regolamento aziendale interno al SGI utile a fornire indicazioni e regole armonizzate da seguire per ridurre al minimo i rischi e le esposizioni sopracitate.

3. Scopo del Regolamento

Lo scopo del presente documento è quello di normare e regolamentare l'utilizzo degli strumenti, dei servizi e dei beni aziendali, tangibili o intangibili messi a disposizione direttamente o indirettamente dall'Azienda a chiunque venga incaricato a qualunque titolo di svolgere mansioni per conto dell'Azienda stessa. Per strumenti, servizi e beni aziendali si intendono:

- la postazione di lavoro, che comprende dispositivi fissi o mobili quali ad esempio Personal Computer, Smartphone, Tablet;
- le risorse di rete che comprendono gli archivi, le informazioni, i software, le basi di dati, ed eventuali altri applicativi disponibili in rete eventualmente necessari per l'esecuzione della prestazione lavorativa;
- le credenziali ed altri segreti utilizzati per l'accesso e l'autorizzazione alle risorse aziendali.

4. Ambito di Applicazione

Il presente regolamento si applica a tutti i soggetti che a qualunque titolo utilizzano i servizi informativi aziendali e i relativi dispositivi messi a disposizione dall'Azienda, ivi compresi:

- membri del Consiglio di Amministrazione
- membri del Collegio Sindacale
- membri dell' Organismo di Vigilanza
- Direttore Generale
- personale dipendente
- stagisti, tirocinanti
- collaboratori esterni, consulenti e fornitori
- eventuali altri utenti temporanei o con accessi limitati.

Rientrano nell'ambito di applicazione tutti i dispositivi elettronici ed i servizi che - anche indirettamente - sfruttano l'infrastruttura informativa offerta dall'Azienda, ovvero, a titolo esemplificativo ma non esaustivo:

- computer fissi e portatili, smartphone, tablet e altri dispositivi;
- reti aziendali, connessioni private virtuali (VPN), accessi Wi-Fi;
- sistemi operativi, software gestionali, applicativi software, applicativi web, posta elettronica;
- account professionali assegnati al singolo dipendente, account professionali condivisi tra più dipendenti, credenziali di accesso e altri segreti del contesto digitale aziendale;

- dati trattati, archiviati, trasmessi e rielaborati attraverso i sistemi aziendali.

Le disposizioni si applicano sia all'interno dei locali aziendali, sia in modalità remota.

5. Riferimenti Normativi

Il presente regolamento adotta una serie di riferimenti normativi che vengono citati di seguito:

- **G.D.P.R** - Regolamento Generale sulla Protezione dei Dati Personali - Regolamento n. 2016/679 del Parlamento Europeo e del Consiglio;
- **Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022**, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione;
- **Decreto NIS2 - Normativa Network and Information Security** - Decreto legislativo del 4 settembre 2024, n. 138;
- **AI Act** - **Regolamento sull'Intelligenza Artificiale** - Regolamento n.2024/1689 del Paramento Europeo e del Consiglio; 2025-08-28 Regolamento Sistema Informativo Aziendale - APT Gorizia 5/14
- Eventuali altri atti con forza di legge dell'Unione Europea e della Repubblica Italiana;
- Eventuali alti atti con forza di legge della Regione Autonoma Friuli-Venezia Giulia;
- **Regolamento Aziendale dei Sistemi Informativi di TPL FVG S.c.a.r.l.** - Protocollo n.2025/0001409 del 14/04/2025;
- Eventuali altri atti contenenti misure integrative o sovrapponibili dell'Azienda.

6. Principi generali

L'utilizzo dei servizi informativi aziendali deve avvenire nel rispetto dei seguenti principi fondamentali:

- **Riservatezza**: ogni utente è tenuto a proteggere e tutelare, anche preventivamente, le informazioni aziendali da accessi non autorizzati e a non divulgare dette informazioni impropriamente;
- **Integrità**: i dati ed i sistemi aziendali devono essere utilizzati senza alterarne il contenuto ed il funzionamento salvo nei casi in cui tale modifica si renda necessaria per l'espletamento della prestazione lavorativa;
- **Disponibilità**: i servizi aziendali devono essere utilizzati in modo da non comprometterne la continuità operativa;
- **Responsabilità individuale**: l'utente è responsabile di quanto svolto con le proprie credenziali o dal dispositivo assegnatogli;
- **Uso lecito e conforme**: l'uso dei sistemi aziendali deve sempre rispondere ai casi previsti dalla legge e ai regolamenti aziendali od altri atti, regolamenti o normative applicabili; ogni altro caso d'uso è da considerarsi illecito;
- **Minimizzazione degli accessi**: l'accesso ai dati e ai sistemi deve essere limitato allo stretto necessario per svolgere le proprie mansioni;
- **Buona fede**: l'utilizzo dei beni informatici aziendali deve sempre avvenire con cura, buona fede e diligenza.

7. Utilizzo e gestione delle credenziali di accesso

L'acceso ai servizi informativi ed ai dispositivi elettronici è spesso limitato e richiede l'autenticazione del richiedente. L'autenticazione è un processo che avviene tramite l'inserimento delle credenziali di

accesso come un nome utente o una password o altri segreti quali i codici OTP (temporanei), l'inserimento di smart card in appositi lettori o l'approvazione dell'accesso tramite un secondo dispositivo elettronico come ad esempio uno smartphone aziendale. Le disposizioni qui contenute sanciscono i comportamenti da mantenere per la gestione e l'utilizzo delle **credenziali di accesso** assegnate al singolo beneficiario:

- fornite ai dipendenti costituiscono a tutti gli effetti strumenti utilizzati dal lavoratore e sono il presupposto necessario per l'utilizzo dei sistemi informativi messi a disposizione per rendere la prestazione lavorativa;
- sono informazioni di cui almeno una parte segreta (ad esempio nome utente e password) e possono anche essere generate in forma temporanea e dinamica (codice OTP) o eventualmente suddivise su più dispositivi (MFA tramite altro dispositivo) o accessori (token fisici). Possono eventualmente essere integrate o parzialmente sostituite con dati biometrici dell'utente;
- vanno conservate con la massima diligenza, non vanno mai condivise con altri soggetti ivi compresi altri colleghi di lavoro e superiori gerarchici di qualsiasi livello;
- non devono essere mai archiviate in testo semplice, riportate verbalmente o fisicamente (come, ad esempio, su post-it) e non bisogna dare indicazioni in merito al formato, alla lunghezza e alla complessità delle credenziali stesse;
- quando devono essere modificate dall'utilizzatore, devono essere uniche (quindi mai utilizzate in precedenza) e con un buon grado di complessità, inoltre vanno cambiate quando richiesto dalle politiche del servizio o dell'infrastruttura;
- vanno combinate con l'autenticazione 2FA/MFA quando possibile o se richiesto. L'Azienda si impegna a predisporre degli strumenti per l'adozione semplice ed efficace dell'autenticazione 2FA o MFA. L'utente, se lo desidera, può richiedere livelli di sicurezza aggiuntivi che saranno valutati e approvati dall'Ufficio Sistemi Informativi;
- possono essere archiviate digitalmente, all'interno di spazi digitali sicuri della propria postazione di lavoro, su sistemi conformi quali i Password Manager che vanno preventivamente approvati dal Responsabile dell'Ufficio Sistemi Informativi;
- l'azienda di riserva il diritto di sospendere e revocare le credenziali, anche del lavoratore, in caso di cessazione del rapporto lavorativo, sospetto motivato di compromissione o violazione delle regole di sicurezza;
- in caso di smarrimento, sospetto uso improprio, sospetta o avvenuta compromissione delle credenziali di accesso di un qualunque dispositivo o accessorio utilizzato per l'autenticazione a più fattori, l'utente è tenuto a informare immediatamente il responsabile dell'Ufficio Sistemi Informativi e a segnalare e collaborare con le forze dell'ordine qualora richiesto;
- al termine del rapporto lavorativo si applicheranno le seguenti procedure:
    - qualora l'account di posta sia di tipo nominativo lo stesso verrà disattivato immediatamente al termine del rapporto lavorativo e verrà successivamente rimosso dai sistemi dopo 30 gg;
    - qualora l'account di posta sia di tipo nominativo lo stesso viene impostato per inviare un messaggio di risposta automatizzato;
    - il messaggio automatizzato su una casella di posta nominativa disattivata per cessazione del rapporto di lavoro deve necessariamente indicare gli indirizzi e-mail alternativi (es. un indirizzo generico di ufficio o quello del sostituto) per garantire il corretto inoltro delle comunicazioni lavorative;
- la consultazione di un account di posta nominativo in assenza del dipendente non più in organico è possibile unicamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale;

- la consultazione di un account di posta nominativo in assenza del dipendente non più in organico è consentita unicamente al Responsabile dell'Ufficio Servizi Informativi o suo delegato, a fronte di una richiesta scritta proveniente dalla Direzione Generale propriamente motivata;
- il contenuto raccolto da una consultazione di un account di posta nominativo in assenza del dipendente non più in organico è strettamente confidenziale e la copia del contenuto è possibile unicamente se autorizzata dalla Direzione Generale per le finalità precedentemente individuate.

8. Utilizzo dei dispositivi elettronici

8.1 Dispositivi BYOD

Ai fini del Regolamento, un dispositivo BYOD è un qualunque tipo di dispositivo elettronico non affidato dall'azienda all'utilizzatore che viene usato per fini lavorativi. Il dispositivo BYOD è ad esempio uno smartphone acquistato per fini personali su cui viene installato un client per accedere alla posta elettronica aziendale, l'app per effettuare o ricevere chiamate al proprio numero di telefono fisso aziendale, in cui è installato un client o un profilo per l'uso della VPN aziendale o nel quale vi siano archiviati file aziendali.

L'utilizzo di dispositivi BYOD fatte salve le eventuali autorizzazioni ricevute dal Responsabile dell'Ufficio Servizi Informativi, non è ammesso.

Qualora autorizzati i dispositivi BYOD devono limitare allo stretto necessario il proprio utilizzo dei servizi aziendali ed eventuali accessi alle risorse aziendali quali file e contenuti, deve essere limitato e può avvenire solo in ambienti dedicati e protetti. In tal caso, i dispositivi BYOD protetti con opportuno codice di blocco sono autorizzati ad utilizzare le applicazioni interfaccianti con il sistema informativo aziendale quali 3CX, Microsoft Outlook, Microsoft Authenticator e ad accedere alle reti Wi-Fi a loro dedicate (ad esempio il Wi-Fi per gli ospiti o agli operatori di esercizio).

I dispositivi BYOD non sono considerati, salvo diversi accordi tra le parti, dispositivi elettronici soggetti all'MDM. L'esistenza del dispositivo BYOD viene documentata in appositi archivi al fine di mantenere uno storico dei dispositivi in essere.

La proprietà dei dispositivi BYOD rimane in carico all'utilizzatore.

La proprietà delle risorse e dei servizi aziendali accessibile anche indirettamente attraverso i dispositivi BYOD rimane in carico all'Azienda, in accordo con le applicazioni anche di terze parti; l'utilizzatore deve considerare che l'utilizzo di tali beni è concesso - salvo diversamente specificato - con una licenza temporanea, revocabile e non esclusiva.

L'uso dei dispositivi BYOD qualora essi vengano ammessi deve avvenire in buona fede, con diligenza e non deve prevedere la manipolazione o alterazione malevola delle risorse assegnate dall'Azienda.

Qualora il dispositivo BYOD esca dallo Spazio Economico Europeo, l'utilizzo dell'infrastruttura aziendale e dei beni e servizi ad essa riconducibile può avvenire solo previa autorizzazione.

La consultazione della posta elettronica aziendale è ammessa su dispositivi personali (non BYOD) esclusivamente tramite il client web ufficiale di Microsoft Outlook se l'account aziendale associato è dotato dell'autenticazione a due o più fattori. In fase di accesso la funzione "ricordami" deve essere disabilitata, inoltre, a fine consultazione la sessione va obbligatoriamente disconnessa e quindi interrotta.

Il responsabile dell'Ufficio Servizi Informativi può concedere deroghe alle regole presenti in questa sezione per situazioni motivate su richiesta del dipendente.

L'utente è tenuto a informare l'Ufficio Servizi Informativi senza ritardi quando un dispositivo BYOD viene rubato o smarrito.

8.2 Dispositivi assegnati dall'Azienda

I dispositivi elettronici forniti dall'azienda quali i computer (fissi e portatili), laptop, smartphone e tablet, sono strumenti di lavoro e devono essere utilizzati unicamente per finalità professionale, nello specifico per l'espletamento delle mansioni affidate dall'Azienda.

Fanno parte dei dispositivi elettronici assegnati all'utente anche gli accessori e tutti i beni materiali e immateriali forniti con esso, ivi compresi l'assicurazione, la garanzia, i dispositivi sostitutivi, concessioni d'uso e altri diritti sul dispositivo stesso.

Non sono ammesse l'installazione di software o componenti di qualsiasi tipo, né la modifica delle caratteristiche del dispositivo, del sistema operativo, nè l'installazione di accessori o applicativi di qualunque tipo non distribuiti e/o non autorizzati o licenziati dall'Azienda.

I dispositivi elettronici ed i relativi accessori possono essere gestiti e tracciati dall'Azienda quindi localizzati e limitati nel funzionamento, tramite appositi software di gestione denominati MDM, nei limiti previsti dalla normativa vigente e accordi sindacali aziendali in essere.

Alla consegna del dispositivo aziendale in dotazione e degli accessori correlati quando previsti, l'assegnatario è tenuto alla sottoscrizione del documento di presa in consegna oltre alle eventuali altre documentazioni previste per il caso d'uso.

In caso di furto o smarrimento dei dispositivi elettronici affidati è necessario segnalare l'accaduto senza ritardi al Responsabile Ufficio Sistemi Informativi e procedere alla denuncia dell'accaduto presso le Forze dell'Ordine. Quando richiesto, è necessario fornire all'Azienda una copia della documentazione prodotta.

L'utilizzo dei dispositivi elettronici e quindi dei dati in essi contenuti in paesi terzi dove non vi sono le garanzie previste dal Capo V del GDPR, non è ammesso.

Quando al dispositivo è associato un abbonamento per un servizio (ad esempio il piano dati per la sim dello smartphone), l'utilizzatore deve sfruttare l'abbonamento in coerenza dei limiti previsti al fine dell'ottimizzazione e la riduzione dei costi in carico all'Azienda.

I dispositivi elettronici vanno custoditi con la massima cura e diligenza. È compito del beneficiario fare quanto in suo potere per ridurre al minimo furti, danni e accessi non autorizzati al dispositivo.

Ai fini della gestione tramite MDM dei dispositivi elettronici all'utilizzatore potranno essere somministrate disposizioni e guide aggiuntive da sottoscrivere se previsto al momento della presa in consegna del dispositivo.

I dispositivi elettronici vanno spenti al termine del turno o della giornata lavorativa e la sessione di utilizzo va disconnessa, fatto salvo altre disposizioni e situazioni particolari quali ad esempio le funzioni di reperibilità.

Quando l'utilizzatore si allontana dal proprio dispositivo elettronico è sempre tenuto a portare il dispositivo in uno stato di blocco temporaneo (come il logout dalla sessione) così da impedire accessi non autorizzati.

L'utilizzo dei dispositivi elettronici deve avvenire in modo da non ledere la sicurezza o il benessere dei colleghi di lavoro.

8.3 Utilizzo di dispositivi condivisi

Ad integrazione di quanto precedentemente illustrato, alcuni dispositivi elettronici nascono per essere utilizzati in forma collettiva ossia da più utenti all'interno dell'azienda. Le regole qui impartite hanno lo

scopo di supportare il corretto espletamento dell'attività lavorativa da parte di ognuno dei singoli utilizzatori, ognuno dei quali deve:

- **verificare**, prima di iniziare l'utilizzo del dispositivo, che esso sia integro e in uno stato conforme, atto a permettere l'utilizzo del dispositivo stesso in piena sicurezza;
- **segnalare** eventuali anomalie, malfunzionamenti, sospette violazioni riguardo al dispositivo stesso contattando il Responsabile dell'Ufficio Servizi Informativi;
- **autenticare** ogni sessione di lavoro che deve terminare non appena il dispositivo deve essere ceduto ad un collega o non appena la mansione viene espletata;
- **verificare** che non vi siano dati sensibili archiviati in posizioni condivide, quindi accessibili anche da altri utenti.

9. Utilizzo di strumenti di Intelligenza Artificiale

Pur non essendo una tecnologia recente, l'intelligenza artificiale ha conosciuto una rapida diffusione presso il grande pubblico solo negli ultimi anni, in particolare grazie allo sviluppo e all'accessibilità di strumenti basati su intelligenza artificiale generativa (IAG). Tali strumenti, se utilizzati in ambito aziendale senza un adeguato inquadramento, possono comportare rischi significativi, in particolare per quanto riguarda la tutela dei dati riservati e l'affidabilità delle informazioni generate. Alcuni modelli di IA, infatti, apprendono anche dai contenuti forniti dagli utenti durante le sessioni di utilizzo, esponendo potenzialmente l'organizzazione a criticità sul piano della riservatezza. Inoltre, la possibilità che vengano generate risposte scorrette o infondate (le cosiddette "allucinazioni") può indurre in errore l'utilizzatore finale. Alla luce di tali considerazioni, si rende necessario adottare le presenti linee guida, con l'obiettivo di delineare l'uso dell'intelligenza artificiale all'interno dell'Azienda, definendone i limiti, le responsabilità e le buone pratiche operative.

L'Azienda, in quanto Socio consortile di TPL FVG S.c.a r.l, riconosce l'intelligenza artificiale generativa come un'opportunità per migliorare l'attività lavorativa fintantoché la sua adozione avvenga nel pieno rispetto della qualità, dell'integrità professionale e della tutela dei diritti e dei valori umani e dell'ambiente.

L'utilizzo dell'I.A.G. è ammesso nei limiti imposti dalla normativa vigente, unicamente attraverso software e servizi approvati dall'Ufficio Servizi Informativi, e non deve mai riguardare dati confidenziali, sensibili e particolari (ai sensi del GDPR e NIS2).

L'utilizzatore è tenuto a minimizzare lo scambio dei dati con l'I.A.G. e rendere anonimi gli stessi quando possibile.

L'utilizzo di strumenti di IA per fini professionali legati all'espletamento delle proprie funzioni è consentito unicamente su account e dispositivi aziendali o altri dispositivi autorizzati; altri usi dell'IA sono ammessi per fini unicamente personali su dispositivi non aziendali disconnessi dalla infrastruttura aziendale.
L'Azienda si riserva la facoltà di sensibilizzare l'utenza sull'uso sano e responsabile dell'intelligenza artificiale generativa nei processi aziendali e di normarne l'uso allineando il presente Regolamento aziendale alla normative vigenti e future.

10. Prevenzione delle frodi informatiche

Al fine di evitare qualsiasi tipo di incidente informatico tra cui le cd frodi informatiche al presente regolamento vengono esplicitati alcuni comportamenti da mantenere al fine di ridurre i rischi che possano ledere l'utente in sé e l'azienda oltre ad eventuali altri soggetti che potrebbero essere coinvolti anche indirettamente. Per frode informatica si intende qualsiasi azione illecita volta a ottenere un

vantaggio personale o a causare un danno all'Azienda mediante l'uso improprio di strumenti informatici, ivi compresi gli accessi non autorizzati, le alterazioni di dati, le generiche truffe online, la sostituzione di persona, la circonvenzione di qualsiasi tipo anche in situazioni specifiche come il phishing e lo spoofing.

10.1 E-mail e comunicazioni elettroniche

L'utilizzatore dell'indirizzo mail aziendale assegnatogli è tenuto, ovvero deve:

- a verificare sempre l'identità del mittente tramite il controllo della casella di posta mittente e non solo del nome mittente;
- evitare di fornire credenziali, codici o informazioni tramite e-mail. Qualora ci siano dei dubbi potenziali viene raccomandato l'utilizzo di un metodo comunicativo alternativo attendibile, tra cui la verifica di persona;
- a non cliccare su link sospetti, allegati di dubbia natura e di non inoltrare e-mail potenzialmente sospette ad altri soggetti interni o esterni all'Azienda;
- segnalare il possibile phishing o la e-mail dannosa tramite le apposite funzioni del client di posta utilizzato;
- compilare la e-mail apponendo in calce la firma aziendale autorizzata e usare la firma in calce quale elemento distintivo rispetto ai comuni tentativi di phishing pur consapevole che la firma può essere manipolata;
- astenersi dal partecipare alle cosiddette "catene" dandone seguito (come le Catene di Sant'Antonio)
- trasmettere allegati, qualora il caso d'uso si renda necessario, solo previa crittografia dell'allegato stesso con un segreto da comunicare al destinatario con altro mezzo di comunicazione;
- utilizzare client di posta elettronica autorizzati per leggere la posta su dispositivi personali prevista esplicito consenso del Responsabile del Sistema Informativo aziendale;
- utilizzare la posta elettronica aziendale solo per finalità strettamente professionali e dunque considerare malevole tutte le altre finalità di comunicazione per la posta in ingresso;
- evitare assolutamente l'accesso alla posta elettronica con servizi di dubbia autenticità o con servizi non autorizzati.

Al fine di mitigare rischi derivanti dalle truffe informatiche, l'Azienda si riserva la possibilità di condurre corsi o fornire materiale di sensibilizzazione a tutto il personale.

L'Azienda distribuisce materiale illustrativo auto redatto di sensibilizzazione al fine di rafforzare la conoscenza dei dipendenti circa l'uso improprio e ai rischi derivanti all'utilizzo della posta elettronica.

11. Gestione delle emergenze

Al fine di dare attuazione alle procedure di Disaster Recovery e Business Continuity anche in applicazione delle normative attualmente in vigore, si rende necessario formalizzare alcune procedure armonizzate utili alla gestione delle emergenze.

- Ogni utente deve assicurarsi di lavorare su dispositivi elettronici con software aggiornati, licenziati per uso commerciale, genuini ed installati da fonti ufficiali e attendibili. È fatto obbligo di rimuovere i programmi non idonei al lavoro in sicurezza e di non utilizzare dispositivi compromessi.

- In caso di comportamenti anomali dei dispositivi elettronici o degli applicativi utilizzati è necessario documentare l'anomalia e di aprire una segnalazione come da consuetudine con l'Ufficio Servizi Informativi.
- Il responsabile di ogni settore, quando avviene un'incidente informatico che può compromettere l'accesso o la modifica dei dati, deve mettersi in contatto senza ritardi di sorta con il Responsabile dei Servizi Informativi.
- Le credenziali e la postazione potenzialmente a rischio vengono isolate dal resto della rete per permettere ulteriori indagini.

12. Monitoraggio e controlli

Ai fini di verificare la corretta adozione del presente regolamento e lo stato di preparazione dei portatori di interesse in situazioni di emergenza o di attacco informatico, quindi per formazione e sensibilizzazione, è necessario introdurre nel regolamento una sezione che vada a definire le modalità di monitoraggio e controllo.

Nei limiti imposti dalla normativa vigente, l'Azienda, ovvero la Direzione Generale ovvero il Responsabile dell'Ufficio Servizi Informativi, si riserva la possibilità di effettuare sessioni di monitoraggio e controlli mirati in caso di fondato sospetto, ossia sulla base di segnalazioni anche anonime pervenute all'Azienda in forma scritta o di risultati di altre scansioni quali ad esempio ricerche antivirus, log di sessione, log di navigazione, analisi delle immagini e della registrazione dei video del sistema di videosorveglianza, log di accesso ai varchi, scansioni e utilizzi del tesserino aziendale e verifiche sui file aziendali creati dal dipendente custoditi in posizioni condivise.

Qualora vengano riscontrate irregolarità, l'Azienda si riserva la possibilità di avviare sessioni di formazione ad-hoc, rilasciare, diffondere e distribuire materiale informativo e di sensibilizzazione e valutare azioni sanzionatorie nei limiti previsti dalla normativa vigente e dagli accordi in essere.

13. Aggiornamento del Regolamento

Tenendo conto della fluidità del panorama legislativo nazionale e comunitario in materia di innovazione tecnologica, sviluppo, digitalizzazione e transizione digitale, si rende necessario esplicitare le modalità di aggiornamento del presente regolamento ai fini di disporre di strumenti e regole atti a perdurare nel tempo ma anche a variare con rapidità qualora le necessità lo richiedano.

Il presente regolamento sostituisce e integra qualunque altro documento, informativa o direttiva di rango pari o inferiore.

Il presente Regolamento può essere soggetto a revisione ed aggiornamento in qualsiasi momento su indicazione del Responsabile dell'Ufficio Servizi Informativi, ovvero della Direzione Generale, del Consiglio di Amministrazione o dell'OdV.

Eventuali revisioni ed aggiornamenti del presente regolamento entreranno in vigore salvo previa notifica secondo le consuete modalità di pubblicazione e unicamente dopo aver superato l'iter procedurale tradizionale.