Regolamento per l'utilizzo dei sistemi informatici, delle Telecomunicazioni fissa e mobile, dei fax e delle fotocopiatrici della società Friuli Venezia Giulia Strade S.p.A.

REGOLAMENTO PRIVACY

Sommario

Sommario 2
1. PREMESSA 3
2. FONTI E RIFERIMENTI NORMATIVI 4
3. ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ 4
4. CAMPO DI APPLICAZIONE 4
5. REGOLE INERENTI LA DOCUMENTAZIONE CARTACEA 5
6. UTILIZZO DEL COMPUTER (FISSO E/O PORTATILE) 5
7. GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI AUTENTIFICATE 6
8. IDENTITÀ DIGITALI PERSONALI 7
9. BADGE PER LA RILEVAZIONE DELLE PRESENZE E PER LA GUIDA DEI VEICOLI AZIENDALI 7
10. UTILIZZO DELLA RETE DI FVGS 7
11. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI 7
12. PROTEZIONE ANTIVIRUS 8
13. UTILIZZO DEI TELEFONI AZIENDALI 8
14. UTILIZZO DEI FAX E DELLE FOTOCOPIATRICI AZIENDALI 9
15. ACCESSO AI DATI TRATTATI DALL'UTENTE 10
16. SISTEMI DI CONTROLLI GRADUALI 10
17. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY E RISERVATEZZA 10
18. SANZIONI 10
19. AGGIORNAMENTO E REVISIONE 11

REGOLAMENTO PRIVACY

1. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone FVGS e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza e all'immagine dell'Azienda stessa. In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare, conseguentemente, eventuali usi scorretti che possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli articoli 2104 e 2105 del Codice Civile.

Premesso, quindi, che 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, FVGS ha adottato il presente Regolamento interno diretto ad evitare che determinati comportamenti possano innescare problemi o minacce alla Sicurezza nel Trattamento dei dati. I controlli sull'uso degli strumenti informatici devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo le dotazioni oggetto del presente Regolamento strumenti di lavoro (per i quali è però ormai previsto e autorizzato anche l'uso promiscuo nel rispetto delle regole di cui al presente Regolamento), quanto il diritto del lavoratore a non vedere invasa la propria sfera personale e il conseguente diritto alla riservatezza e alla dignità, così come sanciti dallo Statuto dei Lavoratori e dalla normativa, nazionale e comunitaria, applicabile in materia di protezione dei dati personali.

Questo Regolamento viene incontro a tali esigenze disciplinando le condizioni per il corretto utilizzo degli strumenti informatici e/o telematici da parte dei dipendenti, in particolare alla luce degli obblighi previsti dalla normativa italiana ed europea in materia sotto richiamata, dalle Linee Guida del Garante della Privacy per Posta Elettronica ed Internet – Delib. dd.01/03/2007 e dalla legislazione cogente in materia di responsabilità amministrativa delle persone giuridiche (D.Lgs. 231/01 e s.m.i.) e fornendo informazioni in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Considerato inoltre che FVGS, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori, telefoni e mezzi di comunicazione efficienti (per es. computer portatili, smartphone, tablet etc.), sono state inserite nel presente Regolamento alcune clausole relative alle modalità e ai doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

Si precisa che l'eventuale esercizio del potere disciplinare avverrà garantendo un'adeguata previa pubblicità al Regolamento e nel rispetto delle disposizioni del CCNL applicato e dell'art. 7 L. 300/70 e s.m.i..

Si ricorda infine che dal 2018 FVGS si è dotata di un *Data Protection Officer*, ai sensi degli artt. 37 e ss. GDPR, che provvede, fra le altre cose, all'aggiornamento del presente Regolamento in eventuale collaborazione con altri uffici societari interessati ed è a disposizione degli utenti per qualsiasi chiarimento e/o necessità all'indirizzo mail dpo@fvgs.it .

A causa dell'emergenza dovuta alla pandemia da Covid-19 la Società aveva tempestivamente attivato la possibilità - per i dipendenti che ne facessero richiesta - di lavorare da casa con la modalità c.d. *smart working* ai sensi dell'art. 4, comma 1, lett. a) del D.P.C.M. 01/03/2020. Pertanto, si intendevano allegate al presente Regolamento, ad integrazione dello stesso, tutte le circolari emesse e/o emanande da FVGS in conseguenza dell'emergenza di cui sopra e nel permanere della stessa fino al suo termine ufficiale.

FVGS ha successivamente attivato lo strumento dello *smart working* ordinario ai sensi dell'art. 29bis del CCNL ANAS applicato; per quanto alla protezione dei dati personali nel lavoro agile, si richiede il massimo rispetto

dell'allegato 1 all'Accordo individuale relativo all'effettuazione dello SWO rubricato *Misure per il corretto trattamento dei dati da parte dei lavoratori agili*, riportato anche tra gli articoli di interesse del presente documento.

2. FONTI E RIFERIMENTI NORMATIVI

- **D.Lgs. n.196/03** – Codice della Privacy (come modificato dal Decreto di adeguamento della normativa nazionale ai principi del GDPR - D.Lgs. n.101/18)
- **Linee Guida del Garante della Privacy per Posta Elettronica ed Internet** – Del. Garante della privacy n.13 dd.01/03/2007
- **D.Lgs. 231/01 e s.m.i.** – Disciplina della Responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica
- **Regolamento Generale sulla Protezione dei dati UE (GDPR) n.679/2016**
- **Delibera della Giunta Regionale n.377/2017** - Progetto di Assessment di Friuli Venezia Giulia Strade redatto da INSIEL S.p.A. – Autorizzazione all'integrazione del Sistema Integrativo di FVG Strade nel Sistema Informativo regionale
- **D.Lgs. n.101/2018** - Decreto di adeguamento della normativa nazionale ai principi del Regolamento Europeo relativo alla protezione delle persone fisiche 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.
- **Delibera della Giunta Regionale n.1109/2019** – D.Lgs. 285/1992 e successive modifiche e integrazioni (Nuovo Codice della Strada). LR 9/2011, Assessment di Friuli Venezia Giulia Strade: implementazione
- **Provvedimento del Garante della Privacy dd.04/12/2019** in materia di disattivazione dell'utenza di dominio e dell'account di posta elettronica aziendale conseguente alla cessazione del rapporto di lavoro per qualsiasi motivo
- **Delibera della Giunta Regionale n.1985/2021** – Aggiornamento dell'indirizzo di cui alla DGR 377/2017. Piano informatico FVGSTRADE: Autorizzazione alla Convenzione diretta tra Fvg Strade ed Insiel

La normativa di interesse è ora agevolmente reperibile in un documento a parte pubblicato sulla pagina Intranet del dpo.

3. ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ

3.1. Il nuovo Regolamento entrerà in vigore il giorno successivo alla data di approvazione da parte del Consiglio di Amministrazione tramite delibera ad hoc. Con l'entrata in vigore, la precedente versione del Regolamento si intende abrogata e sostituita dalla presente.

3.2. Il Regolamento è messo a disposizione degli interessati secondo le modalità definite da FVGS e pubblicato anche nella pagina Intranet del DPO e nel *web kit* del dipendente sulla pagina intranet di HR. Un avviso degli eventuali aggiornamenti è tempestivamente inviato via mail a tutti i dipendenti.

3.3. Il Regolamento ha lo scopo di informare gli interessati anche sulle eventuali finalità e modalità del controllo e sulle specifiche tecnologie adottate per effettuarlo, in particolare qualora, mediante l'individuazione dei contenuti dei siti visitati, determini un trattamento di dati personali, anche sensibili, per i quali va sempre rispettato il principio dell'indispensabilità.

4. CAMPO DI APPLICAZIONE

4.1. Il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto o in *stage*, ecc.).

4.2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in *stage*, agente, ecc.) in possesso di specifiche credenziali di autenticazione.

5. REGOLE INERENTI LA DOCUMENTAZIONE CARTACEA

5.1. Per trasferire da un ufficio all'altro documenti cartacei contenenti dati personali, sensibili e non (ad es. affiliazione sindacale, stato di salute, ecc.), relativi a dipendenti della Società, utenti, imprese e/o persone esterne in modo da non rischiare, a titolo esemplificativo, il trattamento illegittimo e/o la diffusione accidentale degli stessi è necessario inserirli in una cartellina che non permetta di vedere dall'esterno il contenuto della stessa.

5.2. La cartellina contenente i documenti va consegnata al diretto destinatario o, in sua assenza, al compagno di stanza di questi o al diretto superiore, che la custodirà momentaneamente; pertanto, non andrebbero mai lasciate carte sulla scrivania di una persona assente, per evitare che chiunque possa leggere il contenuto delle stesse e che le medesime vadano smarrite o confuse con pratiche diverse; se proprio inevitabile, la documentazione andrà posta in una cartella.

5.3. Le regole del presente articolo valgono all'interno dei locali aziendali, ma devono essere rispettate anche qualora ci si debba recare in luoghi esterni al proprio ufficio, quali ad esempio altre sedi aziendali, tribunali, uffici pubblici di vario tipo e/o altro.

5.4. Durante le assenze momentanee dalla postazione di lavoro si deve evitare di lasciare alla vista di chiunque documenti contenenti dati personali; al termine della giornata lavorativa, inoltre, la scrivania deve essere lasciata il più sgombra possibile, chiudendo negli armadi dotati di chiave, se possibile, tutti i documenti riportanti dati che non dovrebbero essere conosciuti all'esterno dell'ufficio.

5.5. I documenti che costituiscono le pratiche cartacee dei vari uffici vanno conservati nelle cartelline e poi possibilmente negli armadi e/o negli schedari appositi; i documenti che non servono più e che non vengono conservati nei fascicoli di ciascun ufficio vanno eliminati il prima possibile, preferibilmente utilizzando le apparecchiature distruggi-documenti reperibili in ogni sede oppure nelle occasioni in cui l'UO competente provvede allo smaltimento cumulativo di documentazione previa raccolta presso i vari uffici.

6. UTILIZZO DEL COMPUTER (FISSO E/O PORTATILE)

6.1. Il Computer affidato al dipendente è uno strumento di lavoro che, analogamente agli altri dispositivi aziendali, può essere utilizzato in maniera promiscua, nel rispetto delle regole di riservatezza, di custodia e di sicurezza di cui al presente Regolamento.

6.2. Il dipendente è responsabile del computer portatile assegnatogli dal CED e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni e/o sottrazioni. Prima della riconsegna del pc portatile a FVGS al momento della cessazione del rapporto di lavoro vanno rimossi eventuali dati personali ivi memorizzati; in caso il dispositivo possa essere riutilizzato il CED provvederà a resettarlo completamente prima di consegnarlo al nuovo utente.

6.3. Il computer dato in affidamento all'utente permette l'accesso alla rete di FVGS solo attraverso specifiche credenziali di autenticazione, come meglio descritto al successivo punto 4 del presente Regolamento, nonché tramite l'utilizzo della VPN (*Virtual Private Network*) in caso di collegamento da remoto durante la prestazione lavorativa prestata tramite *smart working*.

6.4. Il personale che opera presso il CED della stessa FVGS è autorizzato 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, in considerazione dei divieti di cui (ad esempio) ai successivi punti nn. 8.2 e 9.1, potranno anche comportare l'accesso in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui 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'Azienda, si applica anche in caso di assenza prolungata o impedimento dell'utente e non sia possibile procedere altrimenti.

6.5. Il personale incaricato del CED ha la facoltà di collegarsi e visualizzare in remoto il *desktop* delle singole postazioni 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.

6.6. Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del CED per conto di FVGS, né agli utenti è consentita l'installazione in via autonoma programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni *software* esistenti. L'inosservanza della presente disposizione espone anche la stessa FVGS a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul *software* (che impone l'utilizzo di *software* regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore) vengono sanzionate anche penalmente.

6.7. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del CED nel caso in cui siano rilevati virus e adottando quanto previsto dal punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

6.8. Di norma, il pc deve essere spento ogni giorno prima di lasciare gli uffici, in caso di assenze prolungate dall'ufficio o di suo inutilizzo. Atteso che lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo illegittimo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito si raccomanda di utilizzare sempre il blocco con *screensaver* e obbligo di reintrodurre le credenziali per riprendere il lavoro.

7. GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI AUTENTIFICATE

7.1. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale del CED, previa formale richiesta del Responsabile dell'ufficio/divisione nell'ambito del quale verrà inserito e andrà ad operare il nuovo utente. Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessaria, verrà inoltrata direttamente dal Responsabile dell'ufficio/divisione con il quale il collaboratore si coordina nell'espletamento del proprio incarico.

7.2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal CED associato ad una parola chiave (*password*) fornita dal CED per il primo accesso; in seguito, il sistema chiederà la creazione di una nuova password da parte dell'utente che è riservata e dovrà essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del CED che è il soggetto preposto alla custodia delle credenziali di autenticazione è il personale incaricato del CED di FVGS.

7.3. La *password* deve essere composta da almeno otto caratteri (lettere, maiuscole e minuscole, numeri e/o caratteri speciali) in combinazione fra loro e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

7.4. L'utente incaricato del trattamento deve procedere alla modifica della *password* al primo utilizzo; successivamente deve rinnovarla autonomamente **almeno ogni 90 gg.**

7.5. Qualora la *password* debba venire modificata per qualsiasi ragione (smarrimento, decorso del termine sopra previsto e/o perdita di riservatezza), i dipendenti potranno rivolgersi al CED.

7.6. È assolutamente vietata, e punita ai sensi dell'art. 615 quater c.p. al ricorrere delle condizioni di legge, la detenzione abusiva, la diffusione e l'indebita appropriazione di credenziali di autenticazione.

8. IDENTITÀ DIGITALI PERSONALI

8.1. La firma elettronica fornita da FVGS per lo svolgimento dell'attività professionale è strettamente personale e il suo utilizzo, nel rispetto delle norme in materia, non è delegabile.
8.2. L'accesso ai portali e banche dati pubbliche di interesse aziendale tramite identità digitali personali (per es. SPID, CIE e CNS) è pienamente ammesso in conformità con la normativa vigente.
8.3. Le identità digitali sono strettamente personali e non possono essere utilizzate da un soggetto diverso dalla persona a cui sono state rilasciate.

9. BADGE PER LA RILEVAZIONE DELLE PRESENZE E PER LA GUIDA DEI VEICOLI AZIENDALI

9.1. All'atto dell'assunzione viene consegnato al dipendente un *badge* identificativo (contenente nome, cognome e fotografia dell'interessato), necessario per la rilevazione delle presenze, nonché per la guida dei veicoli aziendali, ai sensi dei protocolli aziendali in tema.
9.2. Detto *badge* è strettamente personale e deve essere custodito con cura, alla pari di tutti gli strumenti consegnati dall'azienda per lo svolgimento della prestazione lavorativa; inoltre, va utilizzato esclusivamente dal dipendente ivi identificato.
9.3. L'eventuale smarrimento deve essere segnalato tempestivamente a HR; alla cessazione del rapporto di lavoro, a prescindere dalla motivazione della stessa, deve essere altresì restituito a detto ufficio.
9.4. Al massimo entro un mese dalla cessazione del rapporto di lavoro, il *badge* viene distrutto in maniera protetta, ossia senza illecita diffusione di dati personali, da HR e/o dal DPO; dell'effettiva distruzione deve essere presa apposita nota nel fascicolo personale del dipendente cessato.
9.5. Qualora *badge* validi e funzionanti, correlati a dipendenti in servizio, debbano essere conservati da HR per qualsiasi motivo e per un tempo limitato (per esempio, nelle more della consegna al dipendente in attesa di prendere servizio), devono essere conservati nella cassaforte a disposizione di detto ufficio o comunque in altro luogo dotato di chiave.

10. UTILIZZO DELLA RETE DI FVGS

10.1. Per l'accesso alla rete di FVGS ciascun utente deve essere in possesso della specifica credenziale di autenticazione.
10.2. È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le password d'ingresso alla rete e ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.
10.3. Le cartelle utenti presenti nei server di FVGS sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere salvato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e *back up* da parte del personale del CED.
10.4. Si ricorda altresì che tutte le unità di memorizzazione locali non sono soggette a back up da parte del personale incaricato del CED e che, pertanto, la responsabilità del salvataggio dei dati ivi contenuti è a carico del singolo utente.
10.5. Il personale del CED può in qualunque momento procedere alla rimozione, sia dai computer degli incaricati sia dalle unità di rete, di ogni file o applicazione che riterrà essere pericolosi per la sicurezza.
10.6. Con regolare periodicità (almeno ogni tre mesi), ciascun utente deve provvedere alla pulizia degli archivi digitali contenuti nel proprio pc, con cancellazione dei file obsoleti o inutili; particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante che occupi inutilmente la memoria del pc.

11. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

11.1. Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.) contenenti dati personali, anche sensibili, nonché informazioni costituenti know-how aziendale, devono essere custoditi e trattati

con particolare cautela onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

11.2. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, anche sensibili, ciascun utente dovrà contattare il personale dell'Ufficio Sistemi Informatici e Telecomunicazioni e seguire le istruzioni da questo impartite. Per poter riutilizzare i supporti di memorizzazione di dati si deve procedere alla cancellazione dei dati precedentemente registrati, in modo da evitare che soggetti terzi possano conoscere o comunque risalire alle informazioni memorizzate in precedenza.

11.3. In ogni caso, i supporti magnetici contenenti dati personali, anche sensibili, devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

11.4. È vietato memorizzare dati aziendali su *cloud* personali.

11.5. 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.

12. PROTEZIONE ANTIVIRUS

12.1. Il sistema informatico di FVGS è protetto da *software* antivirus aggiornato in modo continuativo. Si ricorda tuttavia che ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro *software* aggressivo.

12.2. È comunque vietato:

- utilizzare sistemi wi-fi pubblici che potrebbero veicolare virus e simili (per esempio quelli di stazioni ferroviarie, aeroporti e/o altri luoghi pubblici);
- creare *hot-spot* tramite dispositivi non aziendali e perciò non autorizzati.

12.3. È inoltre sconsigliato usufruire di connessioni *blue tooth.*

12.4. Nel caso il *software* antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer, nonché segnalare prontamente l'accaduto al personale del CED.

12.5. Ogni dispositivo magnetico di provenienza esterna a FVGS 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 CED.

13. UTILIZZO DEI TELEFONI AZIENDALI

13.1. Il telefono aziendale fisso affidato all'utente è uno strumento di lavoro, ma viste le caratteristiche della tariffa telefonica scelta da FVGS nonché la possibilità di inserire nel dispositivo due SIM, una personale e una aziendale, ne è altresì concesso l'uso promiscuo. Lo stesso discorso vale per le APP anche perché le stesse sono indistintamente installate sul telefono e il loro utilizzo, in molti casi, non è scindibile né misurabile tra uso privato e aziendale (a titolo esemplificativo si veda lo *Spid* che permette l'accesso a portali istituzionali sia per scopi aziendali che per scopi privati).

13.2. Il dipendente è tenuto a utilizzare e custodire con la massima diligenza lo *smartphone* e la scheda SIM aziendale assegnati.

13.3. In caso di cessazione del rapporto di lavoro o revoca del terminale, il dipendente (ad esclusione del personale che utilizza il telefono aziendale in modo condiviso) potrà mantenere, a richiesta, l'utilizzo dell'utenza telefonica mobile. In questo caso il CED predisporrà la documentazione necessaria affinché il dipendente diventi titolare della SIM. Se il dipendente non ritenesse di volere mantenere la disponibilità dell'utenza assegnata sarà tenuto a restituire con la massima tempestività al CED la SIM e l'apparato radiomobile fornito, completo di eventuali accessori.

13.4. Al termine del rapporto di lavoro o in caso di ritiro anticipato dello strumento, lo *smartphone* deve essere restituito in buone condizioni con tutti gli accessori forniti.

13.5. In caso di smarrimento e/o furto, il dipendente deve informare immediatamente il CED tramite mail all'indirizzo assistenzainformatica@fvgs.it ed effettuare la relativa denuncia presso le Forze dell'Ordine, fornendone tempestivamente copia al medesimo ufficio; in caso di danneggiamento, il dipendente deve informare immediatamente il CED tramite mail all'indirizzo assistenzainformatica@fvgs.it

13.6. Il backup dei dati contenuti sul telefono aziendale è sempre e comunque a carico del dipendente.

13.7. **Si ricorda che il CED non può intervenire da remoto sui *devices* mobili (*smartphone* e *tablet*) né accedere ai dati contenuti negli stessi**.

13.8. Ferme eventuali responsabilità personali, FVGS si riserva, qualora risultino sussistere problematiche inerenti l'utilizzo del telefono aziendale, sia fisso che mobile, di informare preventivamente il possessore del telefono o del telefonino tali problematiche, affinché possa verificare e, se possibile, porre fine alle stesse. Nel caso le stesse perdurino, potranno essere avviati esami dei tabulati telefonici e della navigazione internet, dovendosi un tanto intendersi quale "controllo difensivo", atto cioè a tutelare esclusivamente l'impiego di un bene aziendale e i costi a ciò relativi. Di quest'ultima attività sarà data notizia ai Dirigenti o Responsabili competenti.

13.9. Per quanto riguarda il personale operativo su strada, si precisa che il telefono cellulare con la relativa utenza è assegnato a fini esclusivamente lavorativi alla squadra nella sua totalità; viene detenuto e utilizzato dal Capo Squadra in quanto persona di riferimento della stessa, non come uno strumento personale; in caso di assenza del Capo Squadra, pertanto, il telefonino deve essere preso in consegna e utilizzato da un altro componente della squadra, designato dal Capo Nucleo e/o dal Capo Centro. Le app di messaggistica istantanea, quali ad esempio *Whatsapp*, possono essere legittimamente utilizzate a fini lavorativi per la trasmissione di dati e informazioni, immagini comprese, fra i membri della squadra e/o il resto del personale di FVGS.

14. UTILIZZO DEI FAX E DELLE FOTOCOPIATRICI AZIENDALI

14.1. È vietato l'utilizzo dei fax e delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

14.2. Sono in uso sia impianti multifunzione il cui utilizzo avviene esclusivamente tramite *badge* aziendale fatto scorrere o appoggiato sul lettore installato a fianco della multifunzione sia fotocopiatrici senza tale dispositivo. A seguito di verifica con il DPO di INSIEL è risultato che le multifunzione con lettore trattano esclusivamente i numeri del *badge* del personale dipendente (ovvero dati pseudonimizzati che non permettono l'immediata identificabilità dell'utente).

14.3. Nell'utilizzare stampanti poste al di fuori della propria postazione lavorativa e diverse da quelle con lettore di badge, è opportuno assicurare una tempestiva acquisizione dei documenti al fine di evitare l'accesso di persone non autorizzate agli stessi.

14.4. Per quanto riguarda l'invio di fax, di recente la RAFVG ha messo a disposizione di FVGS un servizio di fax server che converte i fax in arrivo sulle numerazioni aziendali in e-mail poi inoltrate alle relative caselle di posta elettronica aziendali.

14.5. L'operazione d'invio di un fax è simile a quella dell'invio di una normale mail tramite l'interfaccia di Microsoft Outlook. È sufficiente, quindi, generare un nuovo messaggio di posta elettronica ed indicare, nel campo "A", il numero di fax del destinatario, rispettando il seguente il formato: numero-fax@faxtrieste.regione.fvg.it

14.6. Il documento da spedire funge da allegato a questa mail ed è pertanto obbligatorio inserire nel documento un frontespizio per indicare il mittente, il numero di fax del mittente (per la ricezione di eventuali risposte) e l'oggetto del documento. Il "corpo" della mail non deve contenere alcun testo in quanto, in caso contrario, assieme al documento allegato verrebbe generata e inviata anche una pagina iniziale generica che non contiene alcuna informazione specifica.

14.7. Nell'utilizzo del Fax occorre controllare l'esattezza del numero di telefono inserito prima di inviare il documento e attendere la mail contenente il rapporto di trasmissione per una verifica dell'esattezza della stessa.

15. ACCESSO AI DATI TRATTATI DALL'UTENTE

15.1. È facoltà di FVGS, tramite il personale del CED e previa informativa al DPO al fine della verifica del rispetto della normativa sulla *privacy*, accedere a dati trattati dall'utente, preventivamente informato, 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*, ecc.), motivazioni comunque estranee a qualsiasi finalità di controllo dell'attività lavorativa.

15.2. In adempimento alla normativa vigente i dati acquisiti per il tramite delle attività di cui sopra sono trattati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti e non potranno essere utilizzati come elementi atti a istituire provvedimenti disciplinari e risarcitori previsti dal CCNL applicato, nonché per eventuali azioni civili e penali.

15.3. Il tracciato riguardante le pagine visitate (log) viene conservato per un massimo di 15 giorni, per finalità organizzative, di sicurezza e di verifica delle funzionalità del sistema di protezione. Trascorso tale periodo, il sistema cancellerà in modo automatico tali tracciati.

15.4. I trattamenti connessi al servizio *proxy* sono curati solo da INSIEL S.p.A.. Nessun dato derivante dal servizio proxy può essere comunicato o diffuso, salvo nei casi previsti dalla legge.

16. SISTEMI DI CONTROLLI GRADUALI

16.1. In caso di anomalie, il personale incaricato del CED, previa preventiva informazione all'area di riferimento della stessa, potrà effettuare controlli anonimi che si concluderanno con un avviso generalizzato diretto ai dipendenti del settore in cui è stata rilevata la criticità, nel quale si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Perdurando la situazione anomala tali controlli, nelle forme e per le motivazioni di cui sopra, potranno essere effettuati su base individuale, nel rispetto della normativa che vieta controlli prolungati, costanti o indiscriminati; all'esito degli stessi potrà essere avviato, nei confronti del dipendente interessato, regolare procedimento disciplinare nelle forme e nei modi di cui alla legge ed al CCNL applicato.

17. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY E RISERVATEZZA

17.1. Tutti i dipendenti, autorizzati al trattamento dei dati personali ai sensi di legge tramite apposito atto predisposto dal dpo e controfirmato da ciascuno, devono attenersi alle disposizioni in materia di trattamento dei dati personali previste dalla normativa vigente, aziendale, nazionale ed europea.

17.2. È vietato mettere a disposizione di terzi, senza specifica autorizzazione, conoscenze riguardanti dati tecnici, nonché informazioni tecnologiche, societarie, finanziarie e commerciali della Società.

17.3. È inoltre vietato fornire, sia per via telefonica che di persona, dati inerenti a pratiche trattate dalla Società o a persone che con la stessa abbiano avuto contatti, se non si è sicuri che l'interlocutore sia legittimato a richiederli.

18. SANZIONI

18.1. È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra richiamate, qualora siano ravvisabili profili quantomeno colposi nella condotta osservata, è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari e risarcitori previsti dal CCNL applicato.

18.2. Si ammonisce, altresì, il dipendente a non intercettare, interrompere o impedire le comunicazioni informatiche/telematiche (art. 617 quater c.p.) e a non danneggiare informazioni, dati o programmi informativi nonché i sistemi informatici o telematici aziendali e/o di pubblica utilità (artt. 615 quinquies c.p., 635 bis c.p., 635 ter c.p., 635 quater e 635 quinquies c.p.).

19. AGGIORNAMENTO E REVISIONE

19.1. La presente versione del Regolamento è stata preliminarmente inviata alle OO.SS. in data 02/10/2025. Non essendo stata ricevuta alcuna osservazione, il Regolamento è stato approvato dal Consiglio di Amministrazione durante la seduta del 03/04/2026 ed entra in vigore il giorno successivo alla sua approvazione.