REGIONE AUTONOMA
VALLE D'AOSTA/VALLEE D'AOSTE

Manuale sul corretto uso delle risorse IT

Comitato per la sicurezza

9 giugno 2025

INDICE DEI CONTENUTI

TERMINOLOGIA

Definizioni e acronimi (*)

Vocabolo	Definizione
Account	Iscrizione registrata su un server che, tramite l'inserimento delle credenziali di autenticazione, riconosce e identifica un utente e consente ad esso l'accesso alla rete e/o ai servizi
Access Point	Dispositivi che espongono su rete radio la rete locale dell'edificio
Autenticazione forte/ a due fattori (MFA)	Procedura che richiede agli utenti l'immissione di due credenziali per poter accedere al sistema. Le credenziali sono costituite da qualcosa che l'utente ha (es. una smartcard o un token hardware) e qualcosa che sa (es. una password). Per conseguire l'accesso al sistema, l'utente deve essere dotato di entrambi gli elementi
Cancellazione sicura dei dati	Sistema che garantisce che ogni dato sia cancellato e non più recuperabile in alcun modo dai dispositivi informatici
Cloud	Insieme di tecnologie che permettono, tipicamente sotto forma di un servizio offerto da un provider al cliente, di memorizzare/archiviare e/o elaborare dati grazie all'utilizzo di risorse hardware/software distribuite e virtualizzate in rete in un'architettura tipica client-server
Comunicazioni elettroniche (informatiche e telematiche)	L'invio, la ricezione, la manipolazione di informazioni tramite la rete aziendale, internet, videoconferenze e ogni altro servizio di trasferimento di informazioni
Cifratura	Attività di mascheramento dei dati attraverso algoritmi e chiavi di codifica
Copyright/Diritto d'Autore	Norme sul diritto di autore vigenti che disciplinano l'attribuzione di un insieme di facoltà a colui che realizza un'opera dell'ingegno di carattere creativo, con l'intento di riservargli diritti morali ed economici
Credenziali	Dati e/o dispositivi in possesso di un utente, da esso conosciuti o ad esso univocamente correlati, utilizzati per l'autenticazione informatica (ad esempio, nome-utente e relativa password)
Dati Personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Firewall	Sistema perimetrale che garantisce la sicurezza della rete informatica
Hard disk esterni e di rete	Device di memorizzazione magnetica di tipo esterno collegabili o attraverso porte USB o via rete LAN
Keylogger	Programmi in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente si accorga di essere monitorato
LAN	Rete locale di edificio o ufficio per l'interconnessione delle risorse ICT
Log off	Procedura di disconnessione dalla rete o dagli applicativi software

Vocabolo	Definizione
Malware	Software creato allo scopo di causare danni più o meno gravi a un computer, ai dati degli utenti del computer, o a un sistema informatico
Pen drive/USB	Memoria di massa portatile di dimensioni molto contenute che si collega al computer mediante la porta USB
Phishing	Attività illegale utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica, di messaggi istantanei o contatti telefonici
Postazione di Lavoro (PDL)	Insieme integrato di strumenti informatici (hardware e software) messo a disposizione dell'utente per l'elaborazione dei dati utile alle proprie finalità lavorative. La postazione di lavoro può essere fissa o mobile (p.e. personal computer, notebook, palmare), collegata ad una rete o isolata
Smart Card	Supporto magnetico nel quale possono essere conservati dati utili a identificare un utente e a effettuare l'autenticazione a una risorsa informatica; può essere dotata di sola memoria, memoria con logica di sicurezza, memoria con CPU (sim-card)
Smartphone	Dispositivo mobile che abbina funzionalità di telefono cellulare a quelle di gestione di dati personali grazie alla presenza di particolari applicazioni ad hoc
SIM	La SIM, dall'acronimo inglese Subscriber Identity Module (modulo d'identità dell'abbonato), è una carta contenente un chip in cui si trova il numero IMSI (International Mobile Subscriber Identity), che serve come identificatore unico e meccanismo di autenticazione per i sistemi di telefonia mobile. La SIM viene fornita dagli operatori di telefonia mobile ed associa l'utente ed il suo contratto di abbonamento al dispositivo mobile nella quale è inserita
Social Network	Sistemi informatici dove gruppi di individui si connettono tra loro a seconda di diversi legami sociali.
Spam/Spamming	Invio o ricezione indiscriminati di grandi quantità di messaggi di posta indesiderati, comunque non richiesti o senza una debita autorizzazione (generalmente commerciali).
Spoofing	Attacco informatico dove viene impiegata in qualche maniera la falsificazione dell'identità (spoof). Un esempio è quello della falsificazione del mittente nei messaggi di posta elettronica.
Token	Dispositivo fisico nel quale possono essere conservati dati utili ad identificare un utente e a effettuare l'autenticazione ad una risorsa informatica.
Virtual Private Network (VPN)	Tipologia di rete di comunicazione privata aziendale alla quale possono accedere esclusivamente i soggetti autorizzati e autenticati.
WI-FI	Rete radio che collega senza fili le risorse ICT. Il collegamento viene realizzato attraverso dei dispositivi Access Point che espongono su rete radio la rete locale dell'edificio.

*Per la terminologia "privacy", si rinvia alle definizioni dell'articolo 4 del Regolamento (UE) 2016/679

Premessa

Nel contesto odierno, le organizzazioni devono affrontare un **panorama di rischi e minacce cibernetiche sempre più sofisticati** e con un **impatto dannoso** sempre maggiore. La continua evoluzione tecnologica, tra cui l'implementazione di sistemi di intelligenza artificiale (IA) e l'espansione dei servizi cloud, produce significativi vantaggi e benefici, ma allo stesso tempo amplia ulteriormente la superficie di attacco sfruttabile, offrendo ad attori malintenzionati nuove opportunità per compromettere sistemi e dispositivi.

In questo contesto, **il settore delle Pubbliche Amministrazioni è particolarmente esposto e costituisce uno dei più colpiti**, con attacchi generalmente di gravità alta - in base all'impatto e all'estensione degli stessi attacchi - i quali possono causare potenziali danni di tipo economico, operativo e/o reputazionale. Per queste ragioni, è necessario che gli enti pubblici siano al passo con le nuove tecnologie e adottino misure di sicurezza costantemente aggiornate per prevenire e mitigare tali rischi.

Tenendo in considerazione il contesto rappresentato, l'obiettivo del presente documento, redatto in conformità ai principi previsti dal d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e dal Reg. (UE) 2016/679 (Regolamento generale sulla protezione dei dati o GDPR), è fornire le regole per il corretto utilizzo delle dotazioni informatiche della Regione autonoma Valle d'Aosta/Vallée d'Aoste e per l'espletamento dell'attività lavorativa nel rispetto dei principi di necessità, correttezza, pertinenza e non eccedenza del trattamento dei dati personali, compresi quelli inerenti a categorie particolari. A tale riguardo, esistono regole a cui è necessario attenersi per l'utilizzo di tali risorse proprio al fine di garantire il corretto funzionamento dei sistemi, la sicurezza informatica e la protezione dei dati personali trattati, nonché la continuità dell'attività lavorativa e la corretta gestione dei documenti.

1. Scopo e ambito di applicazione

Il presente documento definisce le **regole e le condizioni per l'utilizzo degli strumenti IT da parte del personale della Regione autonoma Valle d'Aosta** (di seguito Amministrazione) e, in quanto compatibili, di tutti coloro che, a vario titolo, utilizzano strumenti IT dell'Ente.

I predetti soggetti sono tenuti ad adottare **comportamenti responsabili e rispettosi** delle procedure operative predisposte per **l'utilizzo degli strumenti IT adoperati nell'esercizio dell'attività lavorativa**, documentando, ove richiesto, il loro impiego. Tali strumenti includono le dotazioni aziendali intese come i beni forniti al lavoratore per rendere la prestazione lavorativa, di cui all'articolo 4, comma 2, dello Statuto dei lavoratori, mezzi indispensabili per adempiere al proprio obbligo contrattuale.[1]
Questi strumenti rappresentano un mezzo di lavoro e il loro utilizzo deve avvenire in funzione esclusiva dello svolgimento degli incarichi affidati, in base a principi di massima correttezza e professionalità e nel rispetto della normativa vigente; ciò poiché ogni uso anomalo può comportare dei rischi per l'Amministrazione e per il lavoratore, che è tenuto al rispetto dell'obbligo di diligenza di cui all'art. 2104 del codice civile ("Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta"), la cui violazione può essere oggetto di procedimento disciplinare nel rispetto della normativa di legge e di contratto vigente.

[1] Il Garante per la protezione dei dati personali, nel Provvedimento n. 303 del 2016, ha definito gli *strumenti di lavoro* ai sensi dell'articolo 4, comma 2, dello Statuto dei Lavoratori i *servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza*; ne sono parte integrante i sistemi e le misure che ne permettono il funzionamento. Le informazioni raccolte attraverso tali strumenti sono utilizzabili per tutti i fini connessi al rapporto di lavoro, come disciplinato dall'articolo 4, comma 3, dello Statuto dei Lavoratori.

2. Norme e standard di riferimento

Per la stesura di questo documento sono state analizzate e prese in considerazione le principali normative di riferimento e i principali standard di settore, affinché sia garantita conformità normativa e attualità delle misure preventive identificate e definite in questo Manuale.

2.1 Riferimenti

I principali riferimenti utilizzati per la stesura del presente documento sono:

- ISO 27001 Information technology -- Security techniques -- Information security management systems – Requirements
- NIST Cybersecurity Framework (CSF) 2.0, "Framework for Improving Critical Infrastructure Cybersecurity" Version 2.0 National Institute of Standards and Technology, 2024
- "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento", LEGGE 20 maggio 1970, n. 300, con le modifiche apportate dalla L. 23 dicembre 2021, n. 238 e dalla Corte costituzionale, con sentenza 7 aprile-19 maggio 2022, n. 125.
- "Framework Nazionale per la Cybersecurity e la Data Protection" v.02, Febbraio 2019
- Decreto legislativo del 17/05/2018 n.65, Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informative nell'Unione
- NIST Cybersecurity Framework, "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.1 National Institute of Standards and Technology, April 16, 2018
- Garante per la protezione dei dati personali: "Trattamento di dati personali effettuato sugli account di posta elettronica aziendale - 1° febbraio 2018"
- Gruppo di lavoro Articolo 29, "Parere 2/2017 sul trattamento dei dati sul posto di lavoro", WP 249 dell'8 giugno 2017
- Garante per la protezione dei dati personali, "Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro - 13 luglio 2016"
- Garante per la protezione dei dati personali: "Trattamento dei dati personali effettuato attraverso la localizzazione di dispositivi smartphone – 18 maggio 2016"
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
- Circolare AgID 2/2017 Misure minime di sicurezza ICT per le pubbliche amministrazioni
- Garante per la protezione dei dati personali; "Trattamento effettuato sulle e-mail di dipendenti ed ex dipendenti - 30 luglio 2015"
- Garante per la protezione dei dati personali, "Vietato il trattamento di dati personali del dipendente ricavati da file e documenti acquisiti nell'ambito di operazioni di backup effettuate sul server aziendale - 7 aprile 2011"

- Garante per la protezione dai dati personali: “Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema” - 27 novembre 2008” (come modificato in base al provvedimento del 25 giugno 2009)
- Garante per la protezione dai dati personali: “Lavoro: le linee guida del Garante per posta elettronica e internet” (Gazzetta Ufficiale n. 58 del 10 marzo 2007)
- Decreto Legislativo 7 marzo 2005, n. 82 “Codice dell'amministrazione digitale (CAD)” e ss.mm.ii.
- Decreto legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali – Codice della Privacy” e ss.mm.ii.
- Gruppo di lavoro Articolo 29, “Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro”, WP 55 del 29 maggio 2002
- Gruppo di lavoro Articolo 29, “Parere 8/2001 sul trattamento dei dati personali nell'ambito dei rapporti di lavoro”, WP 48 del 13 settembre 2001
- Deliberazione della Giunta Regionale n. 1378 del 27 novembre 2023 “Approvazione del codice di comportamento dei dipendenti degli enti di cui all’articolo 1, comma 1, della L.R. 22/2010”
- Deliberazione della Giunta Regionale n. 1167 del 23 settembre 2024 “Approvazione della nuova disciplina del lavoro agile nell’ambito dell’Amministrazione regionale a decorrere dal 1° gennaio 2025. Determinazioni in merito ai contratti individuali di telelavoro domiciliare in scadenza al 31.12.2024”

3. Principi generali

3.1 Considerazioni preliminari

Ogni dipendente deve rispettare tutte le seguenti regole comuni per l'uso accettabile delle risorse IT. E', inoltre, tenuto a osservare eventuali regole integrative, sempre per l'uso accettabile delle risorse IT, definite attraverso politiche dedicate.

I beni dell'Amministrazione - in particolare, gli strumenti di comunicazione, gli apparecchi telefonici e i personal computer (laptop o desktop) collegati in rete - sono assegnati al personale in ragione dell'attività lavorativa e devono, pertanto, essere destinati all'adempimento dei compiti d'ufficio, nonché custoditi e conservati a cura del personale assegnatario.

3.1.1 Risorse informative

- Non è consentito apportare modifiche **non autorizzate alla configurazione hardware e software** delle postazioni di lavoro, compreso installare software non approvato, interferire con le misure di sicurezza aziendali (ad esempio, il software antivirus), aggiungere o collegare dispositivi o periferiche non autorizzati;
- Non è consentito **ostacolare altri dipendenti nell'accesso** alle risorse informative;
- Non è consentito **eseguire volontariamente operazioni che potrebbero condizionare le performance** dei sistemi informativi o renderli indisponibili;
- Non è consentito **effettuare operazioni non autorizzate di scansione di sicurezza**, di **monitoraggio della rete** o di **intercettazione di dati**, qualora esse non facciano parte dei compiti lavorativi assegnati;
- Non è consentito **violare o tentare di violare la sicurezza della rete aziendale** (aggirare o cercare di aggirare, ad esempio, le misure di sicurezza perimetrale);
- Non è consentito **installare apparecchiature atte a intercettare o impedire le comunicazioni relative a un Sistema Informativo** o a effettuare accessi non autorizzati;
- Non è consentito **diffondere** al di fuori dell'Amministrazione, senza autorizzazione, **software** di proprietà della stessa Amministrazione, sia in forma di codice sorgente che di codice eseguibile;
- Non è consentito eseguire un **trattamento di dati personali** senza autorizzazione;
- Non è consentito **divulgare dati personali o comunicarli a soggetti non autorizzati** al loro trattamento;
- Non è consentito **falsificare documenti informatici** pubblici o privati;
- Non è consentito **installare, elaborare, duplicare, detenere, trasferire materiale soggetto a diritto d'autore**, inclusi programmi, documenti, immagini, materiali audio e video al di fuori dei termini delle licenze;
- Non è consentito **installare, elaborare, conservare, trasferire materiale pornografico** in genere, nonché programmi, documenti, immagini, materiali audio e video o informazioni di vario tipo

che offendano il pubblico pudore o che siano diffamatori, osceni, indecenti o lesivi della dignità umana;

- Non è consentito **introdurre volontariamente nella rete dell'Amministrazione codici malevoli** (ad esempio, virus, worm, trojan horse, keylogger);
- Non è consentito **trattare** (conservare, trasmettere, memorizzare, anche temporaneamente) **dati personali utilizzando risorse non autorizzate** (ad esempio, postazioni di internet point o alberghi);
- Non è consentito utilizzare **qualsiasi programma non esplicitamente autorizzato**.

3.1.2 Protezione delle informazioni

- I documenti di lavoro devono essere **salvati sui dischi di rete condivisi** o in altri sistemi messi a disposizione dall'Amministrazione;
- Non è **consentito salvare dati non pertinenti all'attività lavorativa sugli spazi di memoria condivisa,** in particolare se si tratta di foto e file audio/video;
- A garanzia della riservatezza del contenuto dei dati presenti sulle postazioni di lavoro assegnate al personale, l'Amministrazione esegue, in caso di riutilizzo della macchina e attraverso i servizi preposti, la cancellazione sicura dei dati e la successiva reinstallazione del sistema operativo;
- Non è consentito **mascherare o camuffare la propria identità**;
- Non è consentito **utilizzare credenziali di altri dipendenti**, sia fornite volontariamente che conosciute casualmente;
- Non è consentito **cedere l'uso della propria postazione di lavoro** una volta ultimata la fase di accesso con le proprie credenziali;
- Non è consentito **effettuare il salvataggio dei dati aziendali su sistemi di condivisione non aziendali** (ad esempio, sistemi cloud quali Dropbox, Google Drive, OneDrive, etc.) o altrimenti autorizzati;
- È cura del dipendente garantire **l'assenza di dati non pertinenti all'attività lavorativa** sulle postazioni di lavoro e sui dischi di rete condivisi messi a disposizione dell'Amministrazione.

4. Gestione e modalità di utilizzo delle credenziali di accesso

4.1 Generalità

Ciascun dipendente deve proteggere la **riservatezza** e **l'integrità** delle password.

In particolare:

- A ogni dipendente vengono **assegnati preliminarmente una username e una password**., Una volta assegnata, la username non potrà più essere riassegnata ad altri soggetti, nemmeno in tempi successivi, per poter garantire l'archiviazione e la storicizzazione delle utenze, in conformità alla normativa vigente in tema di dati personali;

- La **password di default**, creata per i nuovi dipendenti o assegnata dopo una reimpostazione della stessa, dovrà essere **cambiata dal dipendente al primo accesso**; la sua gestione e la sua conservazione sono demandate direttamente al dipendente;
- Laddove vi sia la ragionevole certezza che l'utenza sia stata utilizzata da persona diversa dal titolare cui è stata attribuita, la stessa dovrà **essere cambiata immediatamente dal dipendente**;
- La **password** utilizzata dal dipendente deve essere considerata uno **strumento strettamente personale** e deve essere mantenuta **riservata**; inoltre deve essere **scelta**, **utilizzata** e **custodita** con la **massima diligenza**. Al pari delle password, i **dispositivi di autenticazione forte** (smart card, token) devono essere **custoditi attentamente**, segnalando tempestivamente la loro **perdita o il loro furto**.

4.2 Utilizzo di identità digitale in ambito lavorativo

Lo SPID, ovvero l'identità digitale di una determinata persona fisica, rappresenta uno strumento abilitante per l'accrescimento delle competenze digitali del personale pubblico, così come anche rappresentato nella circolare n. 3 del 31 maggio 2024 diramata dal Dipartimento Personale e organizzazione.

L'identità digitale associata allo SPID, al pari di quella associata alla CIE (Carta di Identità Elettronica) o alla CNS (Carta Nazionale dei Servizi), consente l'accesso e la fruizione dei servizi della Pubblica Amministrazione in modalità digitale. L'utenza personale, riconoscibile tramite SPID, viene associata, in fase di registrazione alle piattaforme cui si accede nell'esercizio delle funzioni lavorative, al profilo/ruolo professionale in forza del quale si è abilitati a operare.

Per tali ragioni, lo SPID costituisce un necessario strumento di lavoro per tutti i dipendenti regionali che, per il regolare svolgimento dei propri compiti d'ufficio, devono accedere a piattaforme/portali/applicativi che prevedono l'accesso tramite autenticazione mediante SPID. Si ritiene utile precisare, al riguardo, che il possesso di una CIE (o di una CNS, laddove consentito) costituisce fattore abilitante per l'accesso alle piattaforme digitali al pari dello SPID.

4.3 Disposizioni e Raccomandazioni

Per una corretta gestione delle credenziali di accesso, è necessario attenersi alle seguenti disposizioni generali:

- **Modificare la password di default** comunicata al momento dell'attivazione di un servizio;
- Mantenere le **password riservate**, assicurandosi che non siano divulgate ad altri soggetti;
- **Non cedere a terzi i dispositivi eventualmente consegnati** per l'autenticazione forte;
- Digitare le password in modo tale da **non renderle visibili a terzi**;
- **Evitare di tenere una registrazione** (ad esempio, su carta, file software o dispositivo portatile) **delle credenziali di autenticazione**, a meno che esse non siano memorizzate in modo sicuro e il metodo di memorizzazione sia stato approvato per l'uso (ad esempio, il password manager "Keepass");
- **Non usare le stesse credenziali di autenticazione per scopi lavorativi e non** (ad esempio, e-mail a uso personale, internet banking e social network);

- Cambiare immediatamente le password in caso di sospetto che esse siano note a terzi o di possibile compromissione e segnalare tempestivamente la presunta violazione;
- Non utilizzare la funzione "ricorda password" nei sistemi di autenticazione che propongono tale funzionalità;

Si fa presente che, nel caso di mancato utilizzo delle risorse informatiche per lungo tempo, i sistemi prevedono la disabilitazione dell'utenza secondo quanto stabilito dalla normativa sulla privacy e dalle disposizioni specifiche in materia.

Per la definizione delle password utente, è necessario attenersi alle indicazioni dell'Amministrazione e rispettare le disposizioni a tale fine comunicate; in particolare, sono identificate, definite e applicate le seguenti disposizioni per la definizione delle password utente:

Requisito	Descrizione	Caratteristica
Lunghezza minima e massima	Questa impostazione determina il numero minimo di caratteri della password utente.	La password utente deve avere una lunghezza minima di 10 caratteri e massima di 50 caratteri.
Complessità della password	Questa impostazione determina le caratteristiche raccomandate in fase di creazione o modifica della password da parte del dipendente.	Per garantire un'adeguata complessità della password è richiesto l'utilizzo di: • caratteri maiuscoli (dalla A alla Z); • caratteri minuscoli (dalla a alla z); • cifre in base 10 (da 0 a 9); • caratteri non alfabetici (ad esempio, !, $, #, @, %). E' sconsigliato l'utilizzo di: • caratteri numerici o alfabetici consecutivi o identici (ad esempio, ABCD, 1234, AAAA, 1111); • nomi di persone, date di nascita, animali, oggetti o parole che si riferiscano ad informazioni personali.
Storico password non ripetibili	Questa impostazione determina il numero di nuove password uniche che devono essere associate a un account utente prima che una vecchia password possa essere riutilizzata.	Decorso l'utilizzo di 10 password diverse tra loro, è possibile utilizzare una password già impiegata in precedenza.
Validità della password	Questa impostazione determina il periodo di tempo (giorni) durante il quale una password può essere usata prima che il sistema richieda al dipendente di cambiarla.	La password ha una durata minima di 1 giorno e una durata massima di 89 giorni, decorsi i quali dovrà essere cambiata.

Il dipendente può modificare la password accedendo alla specifica funzionalità messa a disposizione sulla homepage della sezione Intranet del sito istituzionale (accessibile anche dal link presente nell'e-mail di notifica di scadenza password).

Il dipendente riceverà periodiche e-mail di notifica all'avvicinarsi della scadenza della password.

5. Protezione, configurazione e restrizioni d'uso della postazione di lavoro

5.1 Disposizioni relative alla postazione di lavoro

5.1.1 Protezione delle informazioni

- In caso di allontanamento, anche temporaneo, la postazione di lavoro deve essere bloccata (mediante la combinazione di tasti Win+L o CTRL+ALT+CANC e Invio). Dopo 15 minuti di inattività viene attivato lo screen saver; il sistema si sblocca solo all'inserimento della password utente;
- Al termine del turno lavorativo, la **postazione di lavoro deve essere spenta unitamente a tutte le periferiche collegate**, salvo specifiche disposizioni temporanee;
- La postazione di lavoro non deve essere utilizzata per **accedere o tentare di accedere a sistemi o a reti**, anche di terzi, **in assenza di esplicita autorizzazione**;
- Nel caso sia necessario lasciare la postazione di lavoro nelle mani di un tecnico dipendente dell'Amministrazione o di terze parti (in presenza o in acceso remoto), per operazioni di manutenzione hardware/software o di sostituzione, il dipendente è tenuto a verificare l'operato del tecnico mantenendo per quanto possibile la propria vigilanza sulle operazioni compiute;
- **L'eventuale utilizzo di dispositivi personali** (ad esempio, notebook, tablet, etc.) per le attività lavorative è ammesso solo se tali dispositivi **non sono collegati direttamente alla rete regionale** e sono dotati di un sistema antivirus aggiornato;
- È ammesso l'utilizzo in ambito extra-lavorativo di dispositivi (ad esempio, notebook e smartphone) forniti dall'Amministrazione, a condizione che ciò non comporti, da parte del dipendente, violazioni di norme di legge o regolamentazioni, con possibili danni economici e di sicurezza per l'Ente.

5.1.2 Configurazione della postazione di lavoro

- Al dipendente non è consentito in alcun modo **modificare l'hardware del computer in dotazione, né il software** con esso fornito. Il software eventualmente installato in maniera non autorizzata, non conforme alle configurazioni standard o potenzialmente pericoloso per l'infrastruttura sarà rimosso. Coloro che installano software senza le necessarie licenze sono soggetti a sanzioni amministrative e penali, in relazione alle norme che tutelano il diritto d'autore.

5.1.3 Restrizioni d'uso della postazione di lavoro

- Il materiale informatico di cui non è più necessario l'utilizzo dovrà essere restituito all'Amministrazione;
- **Gli assegnatari di computer portatili sono tenuti, almeno una volta al mese, a collegarli fisicamente alla rete aziendale**, al fine consentirne l'aggiornamento, l'attivazione delle licenze di utilizzo dei software aziendali installatati (ad esempio, pacchetto Office) e l'aggiornamento automatico del parco macchine. Lunghi periodi di mancato collegamento alla rete potranno compromettere del tutto, o in parte, il normale utilizzo del computer e/o rallentarne le prestazioni. La mancanza di visibilità, da parte dei sistemi centrali, dei computer portatili, così come la lunga inattività dei computer fissi potranno determinare l'esclusione dal dominio e, pertanto, l'inutilizzabilità degli stessi elaboratori.

6. Modalità di utilizzo del collegamento della postazione di lavoro alla rete

6.1 Generalità

La **rete**, nell'interezza dei servizi tramite essa erogati, è **uno strumento di lavoro**, nonché un **bene dell'Amministrazione**. Essa consente il raggiungimento e la fruizione dei sistemi e delle applicazioni informatiche dell'Amministrazione. Il suo utilizzo da parte dei dipendenti deve, pertanto, ispirarsi ai **principi di diligenza e correttezza**, al fine di **minimizzare i rischi di sicurezza informatica e di salvaguardare i livelli di performance dei servizi** tramite essa erogati.
L'accesso alla rete regionale e alla piena fruizione dei servizi disponibili può avvenire attraverso le seguenti modalità:

- **rete LAN** (Local Area Network - rete fissa presente negli uffici regionali);
- **rete WI-FI** (rete mobile, a oggi disponibile in alcune sale riunioni dell'Amministrazione senza accesso alla rete interna).

È, inoltre, possibile accedere **dall'esterno** alla rete regionale mediante un servizio **VPN** (Virtual Private Network) e seguendo le eventuali ulteriori disposizioni fornite dall'Amministrazione (ad esempio, autenticazione multi fattore). In questo caso, l'accesso potrà avvenire tramite:

- **rete dati di telefonia mobile cellulare** (SIM);
- **rete dati internet domestica** (Adsl/fibra);
- **rete dati internet pubblica** (ad esempio, internet provider, altre reti dati aziendali, internet point), anche se ne è consigliato l'utilizzo solo qualora strettamente necessario e con le dovute cautele, al fine di garantire la sicurezza della rete regionale.

6.2 Disposizioni e Raccomandazioni

Ai fini di un **uso corretto** della **rete regionale** sono identificate, definite e applicate le seguenti disposizioni:

- Le postazioni di lavoro sono dotate di specifici **applicativi di sicurezza** per favorire il rispetto delle policy di accesso alla rete;
- Sono effettuati **controlli mirati e regolari atti a limitare la diffusione di malware** all'interno della rete regionale e a rilevare altri problemi di sicurezza informatica;
- Il dipendente viene **abilitato all'accesso alla rete regionale a partire dalle procedure attivate con il suo inserimento nel sistema di gestione del personale (IRIS)**. Per il personale esterno, l'abilitazione avviene tramite richiesta specifica su procedura denominata "Richieste ICT";
- È possibile l'accesso, tramite sistemi di controllo remoto, esclusivamente per attività di manutenzione e assistenza da parte di aziende esterne, solo se preventivamente verificati e autorizzati;
- Non è consentito porre in essere **attività volte a minare l'integrità, la confidenzialità e la disponibilità della rete** di trasmissione dati e dei servizi erogati attraverso di essa;
- Non è consentito trattare, diffondere o comunicare dati personali **in violazione della normativa vigente in materia di protezione dei dati personali**;

- Non è consentito intercettare, impedire o interrompere illecitamente o abusivamente comunicazioni informatiche o telematiche anche con l'installazione di apparecchiature specifiche;
- Non è consentito collegare alla rete dati regionale dispositivi che non siano autorizzati e controllati (ad esempio, personal computer, modem, apparati di rete, access point, hard disk di rete);
- Non è consentito accedere alla rete regionale o da questa ad altri sistemi informatici, sia interni che esterni, con credenziali non proprie;
- Non è consentito accedere, in modo illecito o abusivo, modificare, diffondere, duplicare, detenere, danneggiare o distruggere informazioni, dati e risorse informatiche della rete, ivi comprese le credenziali di accesso a sistemi informatici o telematici;
- Non è consentito diffondere apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- Non è consentito effettuare attività volte ad aggirare o a compromettere i meccanismi di protezione dei sistemi informatici;
- Non è consentito sfruttare vulnerabilità derivanti da difetti di configurazione o da difetti intrinseci a programmi e/o sistemi;
- Non è consentito porre in essere attacchi informatici, attività intrusive o di scansione di rete di qualunque tipo e verso qualunque sistema interno o esterno;
- L'accesso alle banche dati della Regione o di altri enti alle quali si abbia accesso deve avvenire nei limiti e per le sole finalità per le quali l'accesso è stato autorizzato e limitatamente alle mansioni svolte.

7. Modalità di utilizzo della navigazione in internet

7.1 Generalità

Il dipendente che utilizza **Internet,** quale strumento di ausilio allo svolgimento della propria attività lavorativa, assume la **diretta responsabilità** nell'uso corretto di tale strumento e deve, pertanto, **operare nel rispetto delle norme vigenti** ,in modo da non pregiudicare il livello di sicurezza dell'Amministrazione e non esporla a possibili rischi di **indisponibilità temporanea della rete di navigazione, oltre che di responsabilità nei confronti di terzi o danni d'immagine**, compresi quelli derivanti da attività di acquisizione, riproduzione o condivisione abusiva di informazioni (ad esempio, attività di "file sharing" e/o scambio di opere coperte da diritto d'autore).

Il dipendente e il personale esterno sono **responsabili dell'uso del servizio di accesso ad Internet**, dei contenuti oggetto di ricerca, dei siti visitati, delle informazioni condivise e delle modalità di utilizzo, a prescindere dalle misure attuate per limitare l'accesso a risorse web.

7.2 Disposizioni e Raccomandazioni

Ai fini di un uso accettabile della navigazione Internet sono identificate, definite e applicate le **seguenti disposizioni**:

- L'accesso a Internet è **consentito preferenzialmente attraverso la rete aziendale**;
- Fatto salvo quanto previsto dall'articolo 12 del Codice di comportamento[2], l'utilizzo di Internet deve essere **limitato all'ambito lavorativo** e, in particolare, sono vietate tutte le attività che potrebbero **compromettere la sicurezza della rete aziendale** e le sue prestazioni (ad esempio, partecipazione a chat e/o forum non autorizzati, utilizzando anche pseudonimi, peer-to-peer, scaricamento programmi di dubbia provenienza, etc.);
- Il dipendente si impegna a non **effettuare attività contrarie alla morale**, con lo scopo di recare offesa o danno diretto o indiretto ad altre persone o enti esterni. Nello specifico, è vietato consultare siti con contenuti pornografici, osceni, pedofili, discriminatori o razzisti;
- È consentito comunicare e scambiare **dati e informazioni** solo con persone, organizzazioni e organismi che hanno rapporti istituzionali con l'Amministrazione;
- Non è consentito navigare utilizzando **sistemi o programmi che rendano inefficace la tracciabilità**;
- Non è consentito navigare su siti con **contenuti "ad alto rischio"** di presenza di codice maligno;
- Non è consentito effettuare operazioni di **acquisto e trading on line per uso personale**;
- Non è consentito scaricare file multimediali per la **fruizione di contenuto audio/video** non collegati alla propria attività lavorativa;
- Non è consentito **scaricare software**, anche se provvisto di regolare licenza d'uso ("freeware" o "shareware"), in particolare quando la **provenienza non è certa e garantita**;

[2] Approvato con deliberazione della Giunta regionale n. 1378 del 27 novembre 2023 e rettificato con provvedimento dirigenziale n. 1216 dell'11 marzo 2025, limitatamente alla correzione di alcuni errori e refusi.

- Non è consentito condividere, scaricare, inviare, senza l'autorizzazione del rispettivo autore/proprietario o in violazione della licenza d'uso, materiale in formato elettronico regolato dalle leggi per la tutela del diritto d'autore (ad esempio, film, musica, fotografie, software);
- Non è consentito registrarsi a siti che non presentino contenuti legati all'attività lavorativa, in particolare quando è necessario fornire coordinate l'Amministrazione;
- Non è consentito pubblicare informazioni legate all'ambito lavorativo su gruppi di discussione, forum o, più in generale, su siti web, salvo i casi autorizzati.

L'Amministrazione adotta in misura preventiva, in conformità alle *Linee Guida del Garante Privacy per posta elettronica ed internet del 01/03/2007* e al fine di ridurre gli usi impropri della navigazione in Internet, l'uso di filtri (URL Filtering e Content Filtering) che prevengano determinate operazioni reputate incoerenti con l'attività lavorativa o ritenute a rischio per la sicurezza informatica.

8. Modalità di utilizzo della posta elettronica

8.1 Generalità

La **posta elettronica** è uno strumento necessario ai fini dello svolgimento delle attività lavorative; il servizio è disponibile su rete Internet ed è, quindi, accessibile da qualsiasi dispositivo (fornito dall'Amministrazione o personale). Se ne sconsiglia l'utilizzo da reti libere come "internet point" o reti WIFI non attendibili (ad esempio, quelle messe a disposizione presso aeroporti o stazioni ferroviarie).

Il servizio di posta elettronica aziendale è configurato, **per ciascun messaggio,** con un **limite massimo di spazio, di numero degli indirizzi dei destinatari e di dimensione del testo**.

Gli **assegnatari** di un indirizzo di posta elettronica assumono la **diretta responsabilità nell'uso** dello stesso e devono, pertanto, operare in modo da **non pregiudicare la disponibilità e il funzionamento del servizio** e il **livello di sicurezza** delle informazioni, nel rispetto delle **norme vigenti**.

L'autorizzazione all'uso della casella di posta elettronica aziendale è concessa **ai dipendenti limitatamente alla durata del rapporto di lavoro**. Agli utenti che hanno rapporti formalizzati con l'Amministrazione, la casella di posta elettronica viene **concessa limitatamente alla durata di tali rapporti**, tramite richiesta specifica su procedura denominata "Richieste ICT".

Allo scopo di garantire la **riservatezza** dei dati trattati, in linea con la normativa vigente in materia, le informazioni trasmesse attraverso posta elettronica devono essere **inviate solo agli interlocutori necessari** per l'espletamento delle attività lavorative e possono **contenere solo dati relativi** a stati, fatti e qualità personali previsti dalla legge e **indispensabili per il perseguimento delle finalità** per le quali sono acquisiti.

8.2 Disposizioni e Raccomandazioni

L'uso della posta elettronica implica precise **responsabilità individuali** e richiede l'osservanza di **comportamenti e modalità operative opportune**, coerenti con i contenuti delle politiche di sicurezza dell'Amministrazione e con il quadro legislativo, anche al fine di non esporre l'Amministrazione a rischi di indisponibilità del servizio e di perdita di sicurezza delle informazioni, oltre a eventuali responsabilità verso terzi e danni di immagine.

Il dipendente è direttamente responsabile nei confronti dell'Amministrazione e dei terzi **per l'utilizzo della casella di posta** a assegnata.

Ai fini di un uso accettabile della posta elettronica sono identificate, definite e applicate **le seguenti disposizioni**:

- La posta elettronica aziendale è **protetta da alcuni filtri centralizzati** a tutela delle caselle di posta dei dipendenti, al fine di evitare fenomeni quali *spamming* e *phishing*. Tuttavia, si raccomanda di **controllare sempre** con estrema attenzione **l'affidabilità del messaggio**, anche quando esso proviene da un mittente noto;

- Eventuali **e-mail ritenute sospette** devono essere segnalate tramite il service desk regionale;
- Si raccomanda di controllare sempre con estrema attenzione i destinatari delle e-mail, al fine di evitare errori di persona, specie nei casi di omonimia; i messaggi di posta elettronica devono essere inviati **solo a chi effettivamente interessato**, in coerenza con i ruoli e le responsabilità attribuite;
- Si raccomanda l'utilizzo della funzione di copia nascosta (Bcc o Ccn), se la tipologia del messaggio lo consente, per evitare la diffusione di indirizzi di posta elettronica a soggetti esterni;
- Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o categorie particolari di dati personali (articolo 9 del Reg. UE 2016/679) o dati relativi a condanne penali o reati (articolo 10 del Reg. UE 2016/679), è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso criptazione con apposito software (archiviazione e compressione con password). La password di criptazione deve essere comunicata al destinatario possibilmente attraverso un canale diverso dalla e-mail (ad esempio, tramite lettera o telefono) e, comunque, mai unitamente ai dati criptati. In ogni caso, prima dell'invio occorre accertarsi dell'esistenza di una valida base giuridica che consente tale comunicazione allo specifico destinatario;
- Chiunque riceva erroneamente una e-mail (per omonimia o qualsiasi altro motivo), è tenuto ad **avvisare tempestivamente il mittente** della stessa;
- La posta elettronica personale non deve essere usata come "archivio" e, quindi, si consiglia la periodica "pulizia" della propria casella;
- Nel caso di iscrizione a servizi esterni (mailing list, newsgroup, siti, etc.), la **password** utilizzata **dovrà essere diversa** da quella per l'accesso ai servizi interni;
- La casella di posta elettronica può essere consultata direttamente anche da Internet; a tal proposito, per motivi di sicurezza, si raccomanda l'utilizzo **di terminali su cui si ha il controllo**. Infatti, in una macchina estranea alla propria attività lavorativa potrebbero essere installati software in grado di registrare tutte le operazioni effettuate e tutti i tasti premuti all'insaputa del dipendente;
- L'utilizzo delle caselle di posta elettronica "**condivise**" (ossia quelle assegnate direttamente agli uffici e/o specifiche attività) è consentito solo ed esclusivamente per **l'espletamento delle attività lavorative** afferenti al servizio cui le stesse si riferiscono;
- Non è consentito l'invio di **e-mail di dubbia provenienza** (spamming, catene S.Antonio, etc.); oltre al rischio di poter propagare malware, esse possono anche causare interruzioni di servizio (ad esempio, DDoS - Distributed Denial of Service), essendo spesso responsabili di problemi di congestione delle reti;
- Non è consentito l'invio di messaggi di natura **oltraggiosa, intimidatoria e/o discriminatoria**;
- Non è consentito l'invio di messaggi con **contenuti indecorosi, immorali e/o illegali**;
- Non è consentito, in caso di partecipazioni a mailing list o newsgroup, l'utilizzo dell'**account di posta regionale se non per motivi lavorativi**;
- Non è consentito utilizzare la posta elettronica regionale per l'**iscrizione a social network e siti web** non pertinenti all'ambito lavorativo;
- **In caso di assenza del dipendente**, è opportuno procedere all'attivazione della funzione di **risposta automatica**, con invio automatico di un **messaggio di risposta** agli interlocutori **durante**

il periodo di assenza, ove indicare eventuali riferimenti a caselle di gruppo o a caselle di posta di colleghi a cui è possibile rivolgersi;

- Alla cessazione del rapporto di lavoro, la casella di posta elettronica viene disabilitata e i dati ivi contenuti vengono conservati per un periodo massimo di 30 giorni, per consentire al dipendente cessato di poter richiedere all'Amministrazione eventuale copia del relativo contenuto, dopodiché si procederà alla loro cancellazione definitiva;
- Nei casi di sospensione del rapporto di lavoro con l'Amministrazione regionale, conseguente ad aspettativa superiore a 30 giorni, distacco o comando a tempo pieno presso altro ente pubblico o privato o sospensione cautelare in pendenza di procedimento penale, la casella di posta elettronica viene temporaneamente disabilitata per la durata dell'assenza e riabilitata al momento della ripresa del servizio.

Sono attivi il tracciamento e la conservazione dei log di posta elettronica, al massimo per 21 giorni, nel rispetto del provvedimento 364/2024 del Garante della Privacy relativo al "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", del Regolamento (UE) 2016/679 e dello Statuto dei Lavoratori.

Il datore di lavoro potrà richiedere l'attivazione di sistemi automatici volti a informare i terzi dell'avvenuta disattivazione degli account e a fornire a questi ultimi eventuali indirizzi alternativi, oltre a richiedere l'accesso alla casella di posta del dipendente in casi di estrema urgenza (ad esempio, assenza non programmata), previa richiesta scritta e motivata alla struttura informatica competente, nel rispetto dello Statuto dei Lavoratori.

9. Modalità di utilizzo per scambio sicuro di file e protezione da malware

9.1 Generalità

Con l'aumento delle applicazioni e dei collegamenti in rete con il mondo esterno (Internet, scambio file per mezzo posta e dispositivi di memorizzazione) è aumentata anche la possibilità di incorrere in problemi di infezione da malware. Il **malware**, noto anche come *malicious code* o codice malevolo, si riferisce a un programma che viene inserito di nascosto in un altro programma con l'intento di distruggere dati, eseguire programmi distruttivi o intrusivi o, altrimenti, compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o del sistema operativo. Il malware è la **minaccia esterna più comune per la maggior parte delle postazioni di lavoro, causando danni e interruzioni diffusi e richiedendo sforzi di ripristino estesi all'interno della maggior parte delle Amministrazioni.**

9.2 Disposizioni e raccomandazioni

Ai fini di un uso accettabile dello scambio di file e protezione da malware sono identificate, definite e applicate le seguenti disposizioni.

9.2.1 Misure preventive

- È opportuno rilevare e avere consapevolezza che le postazioni di lavoro sono **dotate di un antivirus** per il quale è previsto un aggiornamento automatico costante;
- Nel caso in cui il software antivirus della postazione di lavoro **evidenziasse anomalie**, è necessario aprire una segnalazione tramite il service desk regionale.

9.2.2 Verifiche relative a dispositivi USB e altri elementi multimediali rimovibili

- È necessario controllare CD, DVD, chiavette USB e ogni altro supporto rimovibile di memorizzazione in caso di scambio di dati, effettuando una **scansione dei file in essi contenuti**, mediante il software antivirus, prima che essi siano aperti o eseguiti;
- È necessario diffidare dall'utilizzo di CD, DVD, chiavette USB e ogni altro supporto removibile di memorizzazione proveniente da **fonti ritenute non note o non attendibili**. Evitare, quindi, di connettere i dispositivi di memorizzazione rimovibili trovati al di fuori dell'ufficio o i dispositivi che possono sembrare sospetti;
- Nel caso in cui ci sia il **dubbio o** il **sospetto di un'eventuale infezione,** è necessario aprire una segnalazione tramite il service desk regionale.

9.2.3 Precauzioni di sicurezza nello scambio di file via e-mail

I virus si propagano via e-mail, anche falsificando il mittente (*spoofing*); per cui una e-mail proveniente da un indirizzo familiare, ma con un **contenuto non ortodosso** (ad esempio, insulti, minacce, invito a

eseguire un'azione con urgenza, presenza di testo con errori sia grammaticali che di punteggiatura), nella maggior parte dei casi è falsificata.

Al fine di ridurre il rischio di diffusione di messaggi contenenti malware, alla e-mail in ingresso vengono applicati filtri di controllo degli allegati, oltre a filtri di limitazione anti-spam.

Al fine di limitare e mitigare la diffusione di virus e/o malware all'interno della rete regionale, sono presenti meccanismi di analisi di rete in grado di rilevare e bloccare eventuali connessioni o traffico di rete anomalo.

9.2.4 Ulteriori precauzioni di sicurezza per particolari minacce informatiche

- "Phishing" e "Ransomware"

Il "phishing" è una frode finalizzata all'acquisizione via e-mail, per scopi illegali, di dati personali e riservati; molto spesso, infatti, arrivano nella casella di posta elettronica dei messaggi con i quali si richiede di inserire le proprie credenziali o di cliccare su un determinato link.

Il furto dei dati avviene attraverso l'invio di e-mail contraffatte, anche con grafica, nomi e loghi ufficiali di Società ed Enti, in molti casi anche Banche, Istituti di Credito, Avvocati, etc., che invitano a fornire informazioni personali (ad esempio, i dati della carta di credito) oppure a pagare per riavere informazioni o che richiedono le credenziali per accedere alle aree riservate.

Per accedere a un sito non bisogna mai inserire i propri dati di login, cliccando direttamente sui link proposti all'interno di un'e-mail, ma digitare manualmente (nella barra degli indirizzi del browser) l'indirizzo del sito per essere certi di non incorrere in siti contraffatti.

Nel caso in cui si dovesse ricevere una e-mail sospetta (anche su casella di posta certificata) con oggetto simile a "...notifica sentenza..." oppure "avviso di spazio esaurito sulla casella postale" oppure "fattura n. … del…" oppure "spedizione n. … del …", si raccomanda di non aprirla e, comunque, di non "cliccare" sugli eventuali link e/o allegati. In particolare, questi ultimi possono essere veicolo di infezione del proprio computer, con installazione di codice malevolo che cripta i dati rendendoli praticamente inutilizzabili e richiesta di un riscatto per il ripristino della situazione "ex ante" ("Ransomware").

Spesso il virus si nasconde dietro messaggi di posta elettronica con mittente apparentemente noto, ma a ben vedere associato a un indirizzo e-mail diverso. Se l'indirizzo e-mail del mittente è stato hackerato, mediante una modalità di falsificazione nota come "spoofing", il virus potrebbe nascondersi in e-mail provenienti da indirizzi noti. Nel dubbio, è consigliabile chiedere telefonicamente al mittente se quella e-mail è autentica.

- Cosa fare in caso di sospetta infezione da virus, malware, etc.

In caso di sospetta infezione, si rende necessario aprire tempestivamente una segnalazione al service desk regionale.

Qualora individuata una possibile violazione informatica, ove sia minacciata la riservatezza, l'integrità o la disponibilità dei dati personali, è comunque necessario fare riferimento alla procedura di "Data Breach" adottata con deliberazione della Giunta regionale n. 1066 del 31 agosto 2018.

10. Modalità di utilizzo del software in dotazione

10.1 Generalità

Le **applicazioni software** sono i servizi IT a supporto dei processi di business e di staff, resi disponibili ai dipendenti per l'esecuzione delle attività e delle funzioni lavorative assegnate. Esse sono, quindi, molteplici: dai sistemi amministrativi, a quelli di gestione, controllo, pianificazione, progettazione, esercizio, etc. La loro **protezione** deve essere effettuata a diversi livelli, per prevenire eventi che ne possono bloccare o degradare le prestazioni o minare l'integrità e la confidenzialità delle informazioni. Tutte le applicazioni software sono dotate di un **processo di autenticazione** e il loro utilizzo è consentito esclusivamente per finalità lavorative.

10.2 Disposizioni e Raccomandazioni

L'autorizzazione all'uso delle **applicazioni software** è **concessa**, secondo le modalità correnti, ai dipendenti dell'Amministrazione, limitatamente alla durata del rapporto di lavoro, e al personale esterno che ha rapporti formalizzati con la stessa, limitatamente alla durata del contratto, per lo svolgimento delle mansioni e delle funzioni assegnate.

Il **software è un prodotto tutelato dalla legge sul diritto d'autore, che prevede per i trasgressori sanzioni amministrative e penali.**

Il software in dotazione e installato sulle postazioni di lavoro è concesso in licenza d'uso all'Amministrazione regionale.

Ai fini di un uso accettabile delle applicazioni software sono identificate, definite e applicate le **seguenti disposizioni**:

- Non è consentito installare sulle postazioni di lavoro **software non autorizzato**;
- È raccomandato, al termine delle attività, effettuare il **"*log off*" dall'applicazione**;
- In linea generale, è necessario accedere alle applicazioni software **utilizzando le risorse fornite dall'Amministrazione**;
- È necessario segnalare **eventuali anomalie di funzionamento** tramite il service desk regionale;
- Non è consentito diffondere e utilizzare **informazioni tratte dalle applicazioni software** senza autorizzazione;
- Non è consentito **modificare dati o procedure** senza autorizzazione;
- Non è consentito l'**accesso abusivo ai sistemi informatici** (sia interni che esterni) di qualunque tipo, nonché il danneggiamento di tali sistemi e dei dati in essi contenuti;
- Non sono consentiti **l'appropriazione e l'utilizzo di password altrui** e la diffusione di **programmi che costituiscano un pericolo per la sicurezza** propria o di terzi;
- Non è consentito **installare e utilizzare alcun software che consenta di alterare, intercettare o impedire le comunicazioni informatiche**;
- Non è consentito **falsificare i documenti in formato digitale**.

Saranno possibili **verifiche riguardo al software installato sulle postazioni di lavoro**, al fine di assicurare la conformità alla normativa in vigore e alle policy aziendali e sarà possibile rimuovere il software non autorizzato. Ove ne ricorrano i presupposti, la violazione degli obblighi che precedono può integrare ipotesi di reato perseguibili ai sensi di legge.

11. Modalità di gestione dell'utilizzo di dispositivi mobili e fissi

11.1 Generalità

I **dispositivi mobili (ad esempio, cellulari/smartphone/tablet) e fissi** assegnati ai dipendenti potranno essere **configurati** in modo tale da garantire la protezione dei dispositivi stessi e dell'infrastruttura tecnologica. Al dipendente potrà essere assegnato uno specifico "profilo" finalizzato allo svolgimento delle sue attività lavorative. In particolare, per i dispositivi mobili è prevista la progressiva adozione di sistemi di **EMM** (Enterprise Mobility Management) per la corretta gestione degli stessi dispositivi forniti dall'Amministrazione.

11.2 Disposizioni e raccomandazioni

Ai fini di un uso accettabile dei dispositivi mobili e fissi sono identificate, definite e applicate le seguenti disposizioni:

- Le chiamate effettuate e ricevute tramite i telefoni e le utenze sono destinate a finalità lavorative. L'eventuale utilizzo per altre situazioni deve essere considerato eccezionale;
- In virtù dei costi più significativi, è sempre opportuno limitare le telefonate internazionali allo stretto indispensabile, in particolare se fuori dallo spazio economico europeo;
- Sono in genere bloccate le chiamate verso numerazioni per servizi a valore aggiunto, quali le numerazioni 4xxxx oppure inizianti per 899;
- Sui sistemi è possibile, su richiesta, impostare specifiche limitazioni sulle direttrici di chiamata abilitate.

11.2.1 Disposizioni e raccomandazioni specifiche dei sistemi di telefonia fissa

- Dove presenti sistemi evoluti di comunicazione come le chat, il loro utilizzo dovrà essere circoscritto a per scopi lavorativi e, comunque, dovrà essere impiegato un linguaggio appropriato;
- In genere, non è possibile deviare il proprio numero telefonico interno su numerazioni esterne all'Amministrazione, compreso il proprio numero di cellulare (sia privato che dell'Amministrazione). In caso di necessità sarà possibile richiedere l'installazione di uno specifico software (cd. softphone) sul cellulare aziendale per rispondere in mobilità al numero telefonico interno d'ufficio piuttosto che rispondere dal computer portatile assegnato ai lavoratori agili.

11.2.2 Disposizioni e raccomandazioni specifiche dei sistemi di telefonia mobile e tablet

- L'assegnazione di telefoni mobili/smartphone e di tablet avviene, in genere, al singolo dipendente, che è responsabile del corretto utilizzo degli strumenti e della loro conservazione;
- È raccomandato che sugli strumenti siano attivi sistemi di blocco e/o cifratura per evitare l'accesso dei dati ivi contenuti da parte di terzi; l'utilizzatore è tenuto a rimuovere i sistemi di

blocco e/o cifratura alla riconsegna del bene ai competenti uffici, nonché a cancellare i dati contenuti;

- È raccomandato il mantenimento attivo del PIN della SIM anche eventualmente cambiandolo rispetto a quello definito dal gestore;
- È ammesso, in caso di telefoni mobili/smartphone e relativa utenza telefonica, l'utilizzo per scopi personali previa adesione agli appositi contratti collegati, qualora disponibili, per l'effettuazione delle telefonate e l'utilizzo di internet a proprio carico; è, invece, possibile l'utilizzo nei sistemi dual-SIM della propria SIM personale. È, altresì, possibile utilizzare la SIM dell'Amministrazione su un proprio telefono personale;
- Nel caso di adesione ai contratti di traffico personale è responsabilità del dipendente adottare i meccanismi previsti per differenziare l'utilizzo personale da quello lavorativo, meccanismi che possono variare nel tempo in base ai contratti stipulati e alle evoluzioni tecnologiche (ad esempio, l'uso dei codici previsti davanti ai numeri per effettuare le chiamate, la modifica del punto di accesso per la navigazione Internet);
- Anche per questi strumenti valgono le considerazioni generali relative alla navigazione in internet e all'utilizzo della posta elettronica;
- Considerato che il traffico Internet con tecnologia mobile è in genere limitato, è ancora più opportuno circoscriverne l'utilizzo a quanto necessario per le attività lavorative, anche nel caso di utilizzo di router mobili (c.d. saponette) piuttosto che delle funzioni di hotspot dal telefono;
- Ogni dipendente potrà, se ritenuto necessario, registrare il device sugli store di applicazioni specifiche per il proprio terminale (ad esempio, Google Play Store, Apple App Store), ma è fatto divieto di installare sui device applicazioni non coerenti con l'attività lavorativa e, comunque, applicazioni a pagamento ricorrendo al credito telefonico come strumento di pagamento;
- È compito dell'utilizzatore verificare e aggiornare periodicamente sia le applicazioni installate che l'intero sistema in base ai rilasci eseguiti dagli specifici produttori.

L'Amministrazione procederà progressivamente a dotare, ove possibile, gli apparati mobili di strumenti di gestione dei dispositivi mobili (EMM Enterprise Mobile Management) in grado di limitare alcune funzionalità dei sistemi, nonché di garantire l'aggiornamento degli stessi sistemi e il controllo remoto del device, previa autorizzazione puntuale all'accesso, secondo le medesime indicazioni già fornite per i computer.

Analogamente, l'Amministrazione si riserva l'adozione di filtri (content filtering) anche sulle utenze radiomobili per prevenire operazioni reputate incoerenti con l'attività lavorativa o ritenute a rischio per la sicurezza informatica.

12 Modalità di gestione dei supporti rimovibili di memorizzazione elettronica

- È fatto divieto al dipendente di utilizzare **dispositivi personali rimovibili di memorizzazione**. È consentito l'utilizzo di dispositivi removibili di memorizzazione forniti dall'Amministrazione per motivi strettamente connessi alle esigenze lavorative;
- I **supporti di memorizzazione rimovibili devono essere conservati in luoghi protetti** (ad esempio, armadi con chiave) e gestiti in modo adeguato al livello di classificazione assegnato, prestando particolare attenzione a non lasciarli incustoditi;
- Il **contenuto dei supporti utilizzati deve essere reso illeggibile** prima del loro riutilizzo o della loro riassegnazione/dismissione;
- La **confidenzialità delle informazioni presenti sui supporti deve essere protetta con meccanismi di sicurezza** adeguati al loro livello di classificazione (ad esempio, utilizzo di sistemi di cifratura, archivi protetti con password complesse);
- Il dipendente presta la massima attenzione nel caso di salvataggio di dati su sistemi di condivisione non forniti dall'Amministrazione.

13 Modalità di svolgimento del lavoro agile

13.1 Generalità

L'Amministrazione consente lo **svolgimento delle attività lavorative a distanza** attraverso la **modalità di lavoro agile** (o smart working). Al fine di garantire il raggiungimento dei propri obiettivi, assicurare un elevato standard di sicurezza per accedere e usufruire dei servizi della rete aziendale, con deliberazione della Giunta Regionale n. 1167 del 23 settembre 2024 e sue s.s.m.m.i.i. è stata approvata la nuova disciplina del lavoro agile nell'ambito dell'Amministrazione regionale, con decorrenza 1° gennaio 2025, che contiene tutte le indicazioni specifiche per lo svolgimento di tale modalità lavorativa e alla quale, pertanto, si rinvia per le relative disposizioni e raccomandazioni.

14 Processo di segnalazione

Ove non diversamente indicato, le segnalazioni/richieste di cui al presente documento dovranno essere presentate tramite il service desk regionale.

Gli incidenti e gli eventi di sicurezza vanno segnalati con immediatezza all'insorgere di sospetti e/o non appena confermato il loro effettivo verificarsi.

Chiunque ravvisi, nell'ambito delle proprie mansioni lavorative, dubbi o incertezze inerenti a tematiche di sicurezza informatica, deve segnalarlo tempestivamente anche al dirigente/funzionario responsabile, nonché all'Ufficio Privacy.

Contatti di riferimento del service desk regionale:

✉ Indirizzo e-e-mail	assistenza@invallee.it
Telefono	800 775 318

15 Aggiornamento e modalità di diffusione del documento

Il presente documento è sottoposto a periodico aggiornamento, in relazione all'entrata in vigore di sopravvenute disposizioni e all'evolversi della tecnologia.

Il presente documento è messo a disposizione del personale attraverso pubblicazione nella sezione Intranet del sito istituzionale. Ogni successivo aggiornamento sarà comunicato con le medesime modalità.

Tutto il personale è tenuto a conformarsi alla versione più aggiornata del documento.