UNIONE DEI COMUNI DELLA VALSAVIORE
c/o Municipio di Cedegolo – Piazza Roma, 1 – 25051 Cedegolo (BS)
Tel. 0364/61100 – Fax 0364/61100 – C.F. 90009010175 – P.I. 02148860980
info@unionevalsaviore.bs.it - unione.valsaviore@pec.regione.lombardia.it

LINEE GUIDA PER L'UTENTE SULL'UTILIZZO DEGLI STRUMENTI INFORMATICI

Approvato con Delibera di Giunta n.50 del 27.12.2025

Sommario

1. Premessa

Le presenti Linee Guida sono predisposte al fine di promuovere un utilizzo corretto, consapevole e sicuro degli strumenti informatici messi a disposizione dall'Ente (d'ora in avanti anche semplicemente Organizzazione), in coerenza con i principi di legalità, trasparenza, efficienza e tutela dei dati personali.

L'infrastruttura tecnologica dell'Ente costituisce un bene pubblico, strumentale all'erogazione di servizi alla popolazione, alla gestione dei procedimenti amministrativi e alla comunicazione interna ed esterna. Un uso appropriato delle risorse informatiche contribuisce a garantire la continuità operativa, la sicurezza delle informazioni trattate e la conformità alle normative vigenti, tra cui il Regolamento Generale UE/2016/679 sulla privacy (GDPR), il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005 e s.m.i.), Linee Guida dell'AgID e la regolamentazione tecnica dell'Agenzia per la Cybersicurezza Nazionale (ACN). Le indicazioni ivi contenute sono in linea con il Vademecum_cybersecurity di base emesso da ACN nel mese di luglio 2025.

Tali strumenti, che comprendono hardware, software, reti e servizi digitali, rappresentano una risorsa strategica e imprescindibile per lo svolgimento delle attività lavorative e per il mantenimento di un ambiente operativo sicuro, efficiente e conforme alle normative vigenti.

Ciascun utente ha il dovere di attenersi alle indicazioni e prescrizioni riportate nel presente documento per tutelare l'integrità dei dati, garantire la continuità operativa e prevenire comportamenti che possano compromettere la sicurezza informatica, la riservatezza delle informazioni e/o l'immagine dell'Organizzazione.

2. Ambito di applicazione

Le presenti Linee Guida si applicano a tutti gli utenti interni ed esterni all'Organizzazione che, a qualsiasi titolo, accedano, utilizzino o gestiscano gli strumenti informatici e i servizi digitali dell'organizzazione. Sono quindi tenuti a rispettarle:

- i dipendenti a tempo determinato o indeterminato;
- i collaboratori esterni e consulenti;
- i tirocinanti, stagisti e volontari;
- eventuali terze parti autorizzate (fornitori, partner, etc.).

Tali indicazioni si applicano all'utilizzo di postazioni di lavoro (fisse o mobili), reti, dispositivi mobili, applicativi gestionali, servizi cloud, account di posta elettronica e ogni altro strumento informatico fornito o autorizzato dall'Organizzazione, sia all'interno dei locali che in modalità remota.

Ogni utente (d'ora in avanti anche semplicemente operatore) è responsabile della propria postazione informatica, della propria casella di posta elettronica, compreso il contenuto dei messaggi, e in generale di tutti gli strumenti informatici messi a disposizione dall'Organizzazione.

3. Uso degli strumenti dell'Organizzazione

Gli strumenti elettronici messi a disposizione dall'Organizzazione sono finalizzati esclusivamente allo svolgimento delle attività lavorative e devono essere utilizzati con diligenza e responsabilità. A fine giornata o comunque al termine della propria sessione lavorativa, ogni utente è tenuto a **chiudere eventuali applicativi aperti** e a **disconnettere correttamente le credenziali di accesso utilizzate**. Analogamente, in caso di assenze prolungate dall'ufficio o di inutilizzo degli strumenti, è obbligatorio provvedere allo **spegnimento dei dispositivi elettronici**.

L'uso degli strumenti messi a disposizione deve inoltre rispettare rigorosamente le politiche di sicurezza dell'Organizzazione.

Pertanto è vietato:

- installare programmi non autorizzati;
- utilizzare programmi diversi da quelli ufficialmente autorizzati e installati;

- alterare le configurazioni di sistema;
- impiegare dispositivi non approvati dall'Organizzazione;
- trasferire all'esterno, anche fisicamente, apparecchiature, informazioni o software di proprietà dell'Organizzazione senza aver ottenuto un'esplicita autorizzazione preventiva;
- violare la sicurezza, trasferire, comunicare, diffondere, intercettare, accedere a dati per i quali non si ha una specifica autorizzazione;

Ogni tentativo di accedere, trasferire, diffondere o intercettare dati senza specifica autorizzazione DEVE considerarsi una violazione grave delle norme interne, oltre a poter configurare fattispecie penalmente rilevanti per l'utente che le attua.
Qualsiasi esigenza relativa all'adozione di nuovi strumenti hardware o software DEVE essere richiesta al Segretario dell'Ente, il quale valuta e autorizza ogni eventuale implementazione.
Per motivi di sicurezza, anche fisica del personale, la strumentazione elettronica di tipo non mobile (a titolo esemplificativo e non esaustivo computer desktop, stampanti, monitor), non può essere rimossa/scollegata/spostata salvo previa autorizzazione dell'ufficio competente.

4. Utilizzo di strumenti informatici

4.1. Protezione dei Sistemi

Al fine di garantire la sicurezza dei dati e prevenire accessi non autorizzati o danni causati da software malevoli, l'Organizzazione adotta una serie di strumenti di protezione aggiornati e costantemente monitorati.
In particolare:

- **software antivirus:** tutte le postazioni di lavoro e i server sono dotati, ove tecnicamente possibile, di un software antivirus con protezione in tempo reale, aggiornamento automatico delle definizioni e funzionalità avanzate come il sistema di prevenzione delle intrusioni;

- **controllo della navigazione in Internet**: è attivo un sistema di filtraggio dei contenuti web, che limita l'accesso a siti non pertinenti all'attività lavorativa o potenzialmente pericolosi, contribuendo a ridurre il rischio di infezioni o distrazioni;

- **servizio Antispam**: le caselle di posta elettronica ordinaria (peo) sono protette da un filtro antispam gestito direttamente dal fornitore del servizio, con l'obiettivo di limitare la ricezione di messaggi indesiderati o potenzialmente dannosi.

Le soluzioni hardware e software adottate sono soggette a manutenzione e aggiornamento costante da parte dell'Organizzazione, in modo da assicurare la massima efficacia contro le minacce informatiche che sono in continua evoluzione.
Gli operatori sono tenuti a non disattivare o modificare tali strumenti in alcun modo e a segnalare tempestivamente eventuali anomalie o malfunzionamenti riscontrati.

4.2 Regole per la corretta tenuta della postazione di lavoro

La postazione di lavoro deve essere accudita e custodita rispettando le regole della diligenza e della buona condotta, e ciò rende ciascun operatore responsabile della corretta tenuta della propria postazione di lavoro.
Ogni utilizzo non corretto degli strumenti informatici della postazione di lavoro può causare disservizi, costi di manutenzione, minacce di sicurezza, danni a persone o al patrimonio informativo dell'Organizzazione. Da ciò deriva che ciascun utente è tenuto a rispettare la configurazione degli strumenti applicativi messi a disposizione dall'Organizzazione per lo svolgimento della propria mansione.
Al fine di evitare accessi illeciti a dati personali, l'operatore è tenuto a:

- adottare politiche delle «schermo pulito»;
- non lasciare incustodita la postazione con documentazione visibile ad altri;
- eseguire la procedura di logout dall'applicativo e/o dal sistema operativo tramite la funzione del blocca/disconnetti;
- attivare lo screensaver il cui sblocco è reso possibile attraverso l'inserimento della propria password.

5. Gestione accessi

Per proteggere i dati e i sistemi informatici dell'Organizzazione, è fondamentale che ciascun utente adotti comportamenti responsabili durante l'utilizzo delle risorse informatiche messe a disposizione.
In particolare, ogni volta che l'utente si allontana dalla propria postazione di lavoro, anche solo temporaneamente, è tenuto a:

- bloccare la sessione con password; lasciare un computer incustodito e connesso alla rete può comportare un uso improprio da parte di terzi, con conseguenze potenzialmente gravi e difficilmente tracciabili;
- non comunicare o condividere con terzi le proprie credenziali di accesso (username e password); l'utente è personalmente responsabile della corretta tenuta delle proprie credenziali;
- non consentire l'accesso alla rete informatica dell'Organizzazione o la condivisione della connessione con persone non autorizzate, così come l'accesso fisico alle aree in cui si svolgono attività di trattamento dati a soggetti esterni non autorizzati.

L'accesso ad aree (fisiche/virtuali) e/o sistemi che contengono informazioni sensibili o particolarmente critiche, è consentito solo agli operatori specificamente autorizzati.

5.1 Requisiti per la creazione di una password sicura

Per garantire un elevato livello di sicurezza, le password devono rispettare le seguenti caratteristiche.

	
DEVONO contenere almeno 14 caratteri.	NON DEVONO essere facilmente riconducibili all'utente (es. nomi, date di nascita, dati personali).
DEVONO includere una lettera maiuscola, una minuscola, un numero e un carattere speciale.	NON DEVONO contenere porzioni del nome utente.
DEVONO essere modificate periodicamente ogni 3 mesi.	La stessa password NON DEVE essere riutilizzata per almeno 12 cicli di sostituzione.
DEVE essere utilizzata una password diversa per tutti i siti dove l'utente ha attivato un account.	NON è possibile cambiare password più di una volta ogni 24 ore.

Le credenziali non gestibili tramite questo sistema sono registrate, autorizzate e giustificate in apposita documentazione.

5.2 Corretta tenuta delle credenziali di autenticazione

L'utente è tenuto a rispettare le indicazioni che seguono per gestire correttamente le proprie credenziali di autenticazione (username e password) utilizzate per l'accesso sia ai sistemi interni all'organizzazione (gestionali, server, pc, account di posta elettronica) sia per l'accesso alle piattaforme o ai servizi di soggetti esterni (PA, gestori di pubblici

servizi, ecc.). Al fine di evitare l'accesso a dati personali e/o informazioni di proprietà dell'Organizzazione da parte di altri soggetti, l'utente dovrà adottare i seguenti comportamenti.

	NON ANNOTARE le credenziali in post-it tenuti in vista sulla propria scrivania.
	NON TENERE/ANNOTARE le credenziali sotto la tastiera del pc o in altri luoghi visibili e facilmente accessibili.
	NON RIPORTARE le credenziali su file excel archiviati sul desktop senza alcuna protezione specifica del file excel.
	NON CONDIVIDERE le credenziali di accesso con i colleghi per agevolare le attività lavorative in caso di propria assenza. Si ricorda a tal fine che le credenziali sono personali e sono forme di autenticazione della propria identità informatica, considerate dal legislatore italiano come firma elettronica semplice.

5.3 Misure di sicurezza sugli accessi implementate dall'Organizzazione

Le credenziali inutilizzate vengono automaticamente disattivate dopo 3 mesi. Dove ciò non sia possibile, viene effettuata una verifica semestrale delle utenze attive.

In caso di perdita di validità (ad esempio cessazione del rapporto di lavoro), le credenziali vengono prontamente disattivate, previa autorizzazione del responsabile.
Dopo 5 tentativi errati di accesso, l'account viene bloccato per 30 minuti.

Se un sistema (computer, software, ecc.) resta inattivo per oltre 30 minuti, viene automaticamente bloccato o disconnesso, e per riprendere l'attività è necessario reinserire le proprie credenziali.

5.4 Corretta tenuta dei dispostivi di firma digitale

L'utente dotato dall'Organizzazione di dispositivi di firma digitale è tenuto ad una corretta conservazione dei dispositivi di firma che consiste nel:

- custodire il dispositivo di firma in luogo sicuro e non facilmente accessibile;
- custodire il PIN e il PUK in un luogo sicuro, diverso da quello del dispositivo di firma;
- non affidare la tenuta del dispositivo di firma a un soggetto terzo.

6. Posta Elettronica

6.1 Principi generali

La posta elettronica DEVE ESSERE utilizzata per l'invio di comunicazioni, informazioni e documenti sia all'interno dell'Organizzazione, sia nei rapporti con i soggetti esterni, sia con altre Pubbliche Amministrazioni e per le finalità istituzionale dell'Organizzazione. Le comunicazioni formali e la trasmissione di documenti informatici, il cui contenuto impegni l'Ente verso terzi, avvengono tramite le caselle di posta elettronica legate al sistema di protocollo informatico dell'Organizzazione (per la corretta gestione dei documenti informatici ricevuti/inviati tramite i canali di

posta elettronica, si devono applicare le procedure descritte nel Manuale di Gestione Documentale dell'Organizzazione).
Attraverso le caselle e-mail gli utenti rappresentano pubblicamente l'Organizzazione e per tale motivo viene richiesto di utilizzarle in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine dell'Organizzazione.

6.2 Utilizzo della posta elettronica dell'ufficio

L'Organizzazione ha messo a disposizione per ciascuna struttura organizzativa caselle di posta elettronica ordinaria (peo) condivise con più utenti, al fine di preservare la continuità dell'attività operativa anche in assenza di uno o più utenti.
L'utente è responsabile del corretto utilizzo delle caselle di posta elettronica che gli sono state assegnate.
Pertanto l'utente DEVE:

- conservare la password nella massima riservatezza e con la massima diligenza (sul punto valgono tutte le prescrizioni riportate al paragrafo dedicato);
- mantenere la casella di posta e gli spazi di archiviazione in ordine, cancellando documenti inutili e allegati ingombranti:
- non utilizzare la casella come uno strumento di archiviazione dei documenti (repository);
- monitorare periodicamente la percentuale di occupazione della casella e dell'archiviazione, provvedendo a rimuovere comunicazioni e allegati comunque non più necessari; i documenti prodotti nell'ambito dell'attività amministrativa dell'ufficio e quelli che impegnano l'Ente verso terzi DEVONO essere registrati nel sistema di gestione documentale dell'organizzazione;
- prestare massima attenzione agli allegati provenienti da mittenti sconosciuti che non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi;
- rispondere alle e-mail pervenute solo da mittenti conosciuti e di cui si abbia certezza della provenienza;
- considerare come certamente pericolosa ogni comunicazione sospetta, anche solo all'apparenza, evitando di inoltrarla (assistenza tecnica e sistemi informativi inclusi) e procedere alla sua cancellazione;
- evitare di cliccare su link ipertestuali (ad esempio www……) direttamente dal testo della email e in esso contenuti, e da cui possono attivarsi attacchi informatici alla rete dell'Organizzazione.

6.3 Utilizzo delle caselle di posta elettronica nominativa

Gli utenti che sono dotati di caselle di posta elettronica nominativa DEVONO farne un uso diligente poiché è uno strumento di proprietà dell'Ente, concesso in uso esclusivamente per finalità professionali, in coerenza con le mansioni affidate. Lo strumento non è da considerarsi personale e dunque da utilizzare per fini privati ed extra-lavorativi, quindi è VIETATO:

- iscriversi a siti non istituzionali;
- fare acquisti on line;
- inviare o ricevere materiale offensivo, discriminatorio, pornografico o illecito;
- inviare email di massa non autorizzate o effettuare attività di spam;
- condividere informazioni riservate attinenti alla propria mansione lavorativa con soggetti non autorizzati.

Ogni iscrizione a portali esterni espone l'Organizzazione a rischi di tracciamento, spam e attacchi mirati.

6.4 Utilizzo della posta elettronica su dispositivi personali

È VIETATO per l'utente salvare/memorizzare sul proprio dispositivo ad uso privato o su altri propri dispositivi ad uso privato qualunque contenuto gestito tramite l'account email assegnato dall'Organizzazione e/o inviarlo a soggetti terzi tramite canali social o con altri mezzi.

In caso contrario l'Organizzazione si riserva qualsiasi azione nei confronti dell'utente, considerando anche la personale responsabilità dei danni eventualmente provocati dall'utente.

6.5 Come riconoscere email sospette

Al fine di preservare la sicurezza del patrimonio informativo dell'organizzazione e di garantire la tutela dei dati personali ivi contenuti, l'utente È TENUTO:

- a collegarsi a link verso siti internet contenuti all'interno di messaggi se non vi sia una comprovata sicurezza sul contenuto degli stessi;
- a fare attenzione alle email che riceve, anche se provenienti da indirizzi email conosciuti: verificare la presenza di errori ortografici, di link da aprire, di richieste di inserimento di credenziali, di allegati dal nome sospetto.

7. Accesso alla casella di posta elettronica dell'utente (lavoratore) assente

Sono a disposizione di ciascun utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che in caso di assenze programmate consentano di inviare automaticamente messaggi di risposta. Tali messaggi dovranno contenere l'indirizzo e-mail di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza dell'utente.

Nel caso in cui l'Ente ha necessità di conoscere il contenuto dei messaggi di posta elettronica dell'utente (lavoratore) resosi assente per cause improvvise, e/o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

- richiesta formale e motivata per attività indifferibili avanzata per iscritto da parte del superiore gerarchico del lavoratore assente;
- l'accesso al contenuto dei messaggi sarà poi effettuato per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato per iscritto dall'utente assente;
- qualora non fosse nominato alcun fiduciario sarà l'Amministratore di Sistema dell'Organizzazione ad effettuare l'accesso alla casella e-mail.

Di tale attività sarà redatto apposito verbale e informato l'utente interessato alla prima occasione utile nel rispetto della vigente normativa sulla privacy.
Nel momento in cui il lavoratore riprenderà servizio, dovrà essergli data la possibilità di cambiare la propria password così da rientrarne nel possesso.

In caso di aspettativa o di comando presso altra amministrazione, il dipendente dovrà impostare un messaggio automatico con l'indicazione dei recapiti a cui rivolgersi nel caso in cui riceva comunicazioni. Per tutta la durata del comando o dell'aspettativa l'account di posta elettronica non sarà accessibile, salvo diversa valutazione organizzativa. Durante tale periodo non sarà consentito l'accesso da parte dell'Organizzazione, salvo necessità documentate e autorizzate dal Segretario dell'Ente.

8. Supporti esterni e dispositivi portatili

È VIETATO l'utilizzo dei dispostivi mobili (es. laptop, tablet, ecc.) ed esterni (es. hard disk, chiavette, ecc.) personali e privati dell'utente per svolgere le mansioni lavorative assegnategli dall'Organizzazione.
È consentito all'utente di utilizzare i supporti e i dispositivi portatili messi unicamente a disposizione dall'Organizzazione, con la PREVIA autorizzazione scritta ed espressa da parte del Responsabile del Servizio.
L'utente deve utilizzare i supporti e i dispositivi che gli sono stati assegnati esclusivamente per l'espletamento delle proprie mansioni lavorative osservando le seguenti regole:

- non è consentito modificare la configurazione hardware e software del proprio dispositivo;
- non è consentito installare autonomamente programmi informatici, applicativi e ogni altro software non autorizzato espressamente dall'Organizzazione;
- non è consentito all'utente caricare o inserire all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta (foto, video) o scaricare app relative a social network (es. whatsapp) legato al numero di cellulare personale privato;
- custodire con diligenza e in luogo protetto durante gli spostamenti computer e altri dispositivi portatili assegnati;
- utilizzare i supporti e i dispositivi solo per il trasferimento temporaneo di dati e documenti; non devono essere utilizzati per l'archiviazione a lungo termine; una volta terminata l'esigenza, i dati e i documenti salvati su supporti e dispositivi mobili dovranno essere archiviati sui sistemi dell'Organizzazione (server, gestionali, ecc).

In caso di perdita, sottrazione e/o furto del supporto e/o dispositivo dovrà essere contattato tempestivamente il Responsabile del Servizio per attivare tutte le misure tecnico-organizzative di sicurezza al fine di impedire un accesso illecito da parte soggetti terzi non autorizzati e per verificare la possibilità di una probabile violazione dei dati personali, attivando, di conseguenza, la procedura di "data breach".

9. Utilizzo telefoni cellulari

L'utente munito del telefono cellullare fornito dall'Organizzazione DEVE utilizzare lo strumento solo ed esclusivamente per le finalità previste dall'attività lavorativa.

	
ATTIVARE blocco/sblocco schermo temporizzato con pin	NON UTILIZZARE per blocco/sblocco schermo temporizzato l'impronta digitale, il riconoscimento facciale (dati biometrici in generale).
RIVERSARE su server dell'Organizzazione video/immagini raccolti per fini lavorativi. Evitare di utilizzare whatsapp, dropbox o sistemi similari.	NON MEMORIZZARE immagini/video personali e NON RIPORTARE numeri di telefono di propri familiari e/o contatti privati (conoscenti, amici, etc.).
NON lasciare il dispositivo incustodito	NON SCARICARE App per uso personale (social network, home banking, posta elettronica personale, acquisti) a meno che non lo preveda la funzione svolta all'interno dell'Organizzazione.
MANTENERE un tono della conversazione adeguato al luogo e se possibile allontanarsi in luoghi con adeguata riservatezza.	NON EFFETTUARE backup automatici su piattaforme come google, whatsapp o sistemi similari.

10. Telelavoro

L'utente che abbia un accordo individuale per lo svolgimento della propria mansione lavorativa attraverso la formula del telelavoro deve attenersi a quanto indicato nel presente documento relativamente all'utilizzo degli strumenti elettronici e della casella di posta elettronica ordinaria.

Ulteriormente, l'utente in telelavoro dovrà attenersi alle seguenti istruzioni:

- utilizzare la dotazione concessa in uso dall'Organizzazione esclusivamente per le attività inerenti il rapporto di lavoro e la mansione lavorativa assegnata;
- non manomettere in alcun modo gli apparati;
- non sostituire la dotazione con altre apparecchiature o dispositivi tecnologici;
- non utilizzare collegamenti alternativi o complementari;
- non consentire ad altri l'utilizzo della dotazione.

11. Politiche Archiviazione Dati e Documenti

Dati e documenti informatici di qualsiasi genere inerenti le attività lavorative DEVONO ESSERE archiviati e memorizzati negli strumenti messi a disposizione dall'Organizzazione (Sistema di gestione documentale, software gestionali in uso).
Nelle aree/cartelle di condivisione di dati e documenti tra uffici è necessario che l'utente proceda alla rimozione di quanto condiviso non appena terminate la necessità, al fine di evitare l'accesso a dati anche personali e documenti a soggetti, anche interni all'Organizzazione, non autorizzati.
È vietato produrre copie informatiche di documenti e dati dell'Organizzazione su dotazioni informatiche differenti da quelle messe a disposizione da quest'ultima.
È altresì vietato produrre copie cartacee di documenti e dati informatici. Qualora si ravvisasse la necessità, l'utente è tenuto all'eliminazione delle stesse a conclusione dell'utilizzo e comunque a seguire le istruzioni date per la custodia e sicurezza della documentazione cartacea.
È inoltre vietato:

- utilizzare gli strumenti informatici dell'Organizzazione al fine di custodire, far circolare o promuovere materiale non autorizzato o di carattere personale;
- conservare o mettere a disposizione di terzi materiale protetto dalla legge sul diritto d'autore di qualsiasi genere di cui l'Organizzazione non abbia acquisito i diritti;
- utilizzare la strumentazione informatica per la realizzazione, archiviazione e/o invio di documenti di natura oltraggiosa e/o discriminatoria.

Eventuali materiali di queste tipologie, individuati da parte del personale incaricato della manutenzione e verifica degli strumenti informativi, potrà essere rimosso dagli strumenti informatici dell'Organizzazione senza necessità di autorizzazione e/o notifica al creatore e/o proprietario.

12. Navigazione Internet

L'accesso a Internet rappresenta uno strumento fondamentale per lo svolgimento delle attività lavorative quotidiane. La rete viene utilizzata per comunicare, reperire informazioni, scambiare documenti e accedere a servizi indispensabili per il proprio ruolo. Per questo motivo, l'Organizzazione mette a disposizione dei propri utenti l'accesso a Internet, esclusivamente per finalità strettamente legate allo svolgimento delle mansioni lavorative.
Eventuali utilizzi personali della rete devono essere sempre preventivamente autorizzati, in modo espresso, dall'Organizzazione.
Per garantire un uso corretto e sicuro della rete, non è consentito:

- utilizzare Internet per scopi non pertinenti al lavoro senza autorizzazione;
- accedere a siti con contenuti inappropriati, discriminatori, offensivi o contrari ai principi di rispetto delle persone (es. contenuti discriminatori per sesso, religione, razza, opinioni politiche o sindacali).

L'Organizzazione ha attivato un sistema di sicurezza che può bloccare automaticamente l'accesso a siti considerati inappropriati o potenzialmente pericolosi, sulla base di categorie predefinite o liste di esclusione (blacklist).
Per ridurre i rischi durante la navigazione occorre prestare attenzione prima di cliccare su link sospetti, passando il cursore sul link per visualizzare la destinazione effettiva nella barra del browser. Se il collegamento punta a un file eseguibile (.exe, .scr, ecc.) o a un sito sconosciuto, è VIETATO aprirlo.

Nel caso il software antivirus segnali la presenza di una minaccia o un virus, l'utente dovrà interrompere immediatamente ogni attività e contattare le Società che effettuano manutenzione ed assistenza per le opportune verifiche.
L'utente è direttamente responsabile dell'utilizzo che fa della rete: questo comprende i siti visitati, i contenuti scaricati e le informazioni che eventualmente sono condivise online.
Per garantire la sicurezza e il buon funzionamento del sistema informatico, l'Organizzazione può effettuare controlli sulla navigazione. Tali controlli seguono principi di rispetto, proporzionalità e tutela della privacy, e possono includere:

- la registrazione anonima degli accessi tramite sistemi tecnici (es. proxy server);
- la consultazione di tali dati da parte dell'Amministratore di sistema solo in caso di necessità;
- in presenza di sospetti concreti e previa comunicazione agli utenti, l'attivazione temporanea di controlli più puntuali con tracciamento utente-sito.

L'Organizzazione può effettuare controlli a campione, sempre nel rispetto della normativa vigente, per finalità legate alla sicurezza, alla produttività e alla tutela del patrimonio informativo. I dati raccolti saranno trattati in forma anonima salvo nei casi previsti dalla legge, come obblighi giudiziari o necessità di tutela legale.
Infine, non verranno mai effettuati controlli prolungati, indiscriminati o invasivi: ogni attività di verifica è svolta con senso di responsabilità, nel rispetto della dignità e dei diritti dell'utente, ed in linea con i principi di proporzionalità, necessità e pertinenza in tema di trattamento di dati personali.

13. Anomalie e incidenti

Nel corso dell'attività lavorativa, può capitare di notare un comportamento anomalo del sistema informatico: ad esempio un rallentamento improvviso, un errore inaspettato, l'accesso non autorizzato a dati, o semplicemente qualcosa che "non torna". Segnalare subito queste situazioni è fondamentale per proteggere i dati e garantire la sicurezza dell'intera rete dell'Organizzazione.
Se si nota qualcosa di anomalo/strano - anche se può sembrare un piccolo dettaglio - l'utente DEVE comunicarlo il prima possibile al Responsabile di Servizio il quale provvederà a segnalare l'anomalia riscontrata alle Società esterne incaricate all'assistenza e/o manutenzione. Quando possibile, è preferibile una segnalazione scritta (es. e-mail), così da avere una traccia chiara e tempestiva dell'evento.
Sarà poi compito del personale incaricato analizzare il problema, con l'eventuale supporto dell'utente, e agire rapidamente per riportare la situazione alla normalità, in totale sicurezza.
In casi più gravi, come ad esempio una perdita di dati personali, accessi non autorizzati o modifiche accidentali, siamo di fronte a quella che viene definita una violazione dei dati personali (o data breach). In questi casi è ancora più importante agire con prontezza: avvisare immediatamente il responsabile individuato dall'Organizzazione, che attiverà la procedura specifica prevista per questo tipo di situazioni.