Consorzio di Bonifica Adige Euganeo

DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI CONSORTILI

Versione	1.0
Approvazione	delibera del Consiglio di Amministrazione n.92/2018 del 23/5/2018
Versione	1.1
Approvazione	Delibera del Consiglio di Amministrazione n.107/2022 del 4/8/2022
Versione	1.2
Approvazione	Delibera del Consiglio di Amministrazione n.38/2023 del 9/3/2023
Versione	1.3
Approvazione	Delibera del Consiglio di Amministrazione n.154/2023 del 05/10/2023
Versione	1.4
Approvazione	Delibera del Consiglio di Amministrazione n.60/2024 del 04/04/2024
Versione	1.5
Approvazione	Delibera del Consiglio di Amministrazione n.159/2024 del 10/10/2024
Versione	1.6
Approvazione	Delibera del Consiglio di Amministrazione n.157/2026 del 24/09/2026

Sommario

1. PERCHÉ UN REGOLAMENTO INFORMATICO? 4
2. PRINCIPI GENERALI 4
2.1. Campo di applicazione 4
2.2. Entrata in vigore e Aggiornamenti 5
3. REGOLE DI COMPORTAMENTO GENERALI 5
4. REGOLE OPERATIVE 6
4.1 Uso del Pc 6
4.2 Utilizzo di Pc Portatili 7
4.3. Divieto di utilizzo dei dispositivi personali (PC, Tablet, Smartphone) 7
4.4. Credenziali di autenticazione 7
4.5. Antivirus 8
4.6 Utilizzo e Conservazione dei supporti rimovibili 9
4.7. Utilizzo dei device (smartphone - tablet) 9
4.8 Accesso ed utilizzo della rete aziendale 10
4.9 Uso della connessione VPN per telecontrollo 10
4.10 Uso della rete internet 10
4.11 Uso della posta elettronica 11
4.12 Uso stampanti 13
4.13 Gestione dati 14
4.14 Uso delle applicazioni di messaggistica 14
4.15 Uso della rete wi-fi e gestione degli accessi 14
5. MONITORAGGI E CONTROLLI DELL'ENTE 15
5.1 Accesso ai dati dell'Utente 15
5.2 Controlli 16
6. UTILIZZO DEI GESTIONALI E DEL PROGRAMMA PROTOCOLLO 17
7. UTILIZZO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE 18
8. CESSAZIONE DEL RAPPORTO DI LAVORO 18
9. VIOLAZIONI E SANZIONI DISCIPLINARI 19

1. PERCHÉ UN REGOLAMENTO INFORMATICO?

Il Consorzio di Bonifica Adige Euganeo, nel seguito denominato "Ente", ha ritenuto necessario dotarsi del presente Disciplinare al fine di evidenziare ai propri dipendenti e collaboratori le indicazioni e le misure necessarie e opportune per il corretto e consapevole utilizzo delle risorse informatiche durante l'ambito dell'attività lavorativa, definendone le modalità di utilizzo e ponendo particolare attenzione in materia di sicurezza informatica e protezione dei dati.

2. PRINCIPI GENERALI

L'Ente, in qualità di Titolare del trattamento dei dati personali, ritiene opportuno dotarsi di questo Disciplinare al fine di adempiere agli obblighi fissati dal Regolamento Europeo sul trattamento dei dati personali (GDPR), dal Codice in materia di protezione dei dati personali (D.Lgs.n.196/2003, come mod. dal D.Lgs.n.101/2018 e s.m.i.), nonché dai provvedimenti e ai documenti di indirizzo emanati dall'Autorità Garante per la protezione dei dati personali, con particolare riferimento alle "Linee Guida su Posta elettronica ed Internet" - G.U. n. 58 del 10 marzo 2007.
Ove applicabili, l'Ente si impegna a rispettare gli obblighi della disciplina di settore
I trattamenti effettuati dall'Ente rispettano le garanzie poste in essere dal legislatore in materia di protezione dei dati personali e si svolgono nell'osservanza dei principi sanciti dalla normativa privacy.
L'Ente tratta i dati dei lavoratori nella misura meno invasiva possibile, affidando le attività di monitoraggio esclusivamente a quei soggetti opportunamente preposti ed effettuando eventuali controlli esclusivamente in maniera mirata sull'area di rischio, in particolare, nella figura dell'Amministratore di sistema interno.
Il Consorzio di Bonifica Adige Euganeo è titolare di qualsiasi diritto connesso ai sistemi informativi ed alle risorse informatiche, ai dati, ai contenuti di ogni tipo e genere, elaborati, creati, o modificati nell'ambito delle attività lavorative e tramite l'opera dei suoi dipendenti e collaboratori.
Ogni lavoratore potrà far valere i propri diritti sanciti dalla normativa sul trattamento dei dati personali rivolgendo una specifica richiesta scritta al Titolare del trattamento.

2.1. Campo di applicazione e definizioni

Il presente Disciplinare si applica a tutti i lavoratori e collaboratori, di seguito denominati "Utente", autorizzati all'utilizzo delle risorse informatiche e al trattamento dei dati personali, a prescindere dal rapporto contrattuale intrattenuto con l'Ente (lavoratori somministrati, collaboratori a progetto, stagisti, consulenti, ecc.)

Per Amministratore di sistema si intende il soggetto interno all'Ente, o suo collaboratore, formalmente incaricato della gestione, configurazione, manutenzione e sicurezza delle risorse informatiche, secondo le istruzioni e le autorizzazioni conferite dall'Ente stesso.

Per risorse informatiche si intende qualsiasi strumento informatico, tecnologico e telematico di proprietà dell'Ente, utilizzato dal lavoratore per rendere la prestazione lavorativa. A titolo esemplificativo ma non esaustivo sono risorse informatiche:

personal computer fissi e portatili; tablet; telefoni cellulari; telepass; carte di credito; sistemi di geolocalizzazione installati su veicoli aziendali, indirizzo email aziendale, rete aziendale.

2.2. Entrata in vigore e Aggiornamenti

Il Disciplinare è stato approvato dal Consiglio di Amministrazione con deliberazione n.92/2018 del 23/5/2018 e successivamente aggiornato con le deliberazioni indicate.
Con l'entrata in vigore del presente Disciplinare tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
Al fine di informare i propri dipendenti del contesto del presente Disciplinare, lo stesso sarà:

a) consegnato a ciascun dipendente ed a ciascun collaboratore ad inizio attività;
b) affisso nella bacheca aziendale;
c) pubblicato nel Portale dipendente (Ufficio Web);

L'Ente si riserva la facoltà di apportare, in qualsiasi momento, modifiche al presente documento, dandone comunicazione a tutti gli incaricati con le modalità che riterrà opportune.
Il presente Disciplinare è stato predisposto ad uso esclusivamente interno dell'Ente e, pertanto, non potrà essere riprodotto, divulgato, copiato, utilizzato e/o altrimenti reso pubblico in assenza di una previa approvazione scritta dell'Ente stesso.

3. REGOLE DI COMPORTAMENTO GENERALI

L'Ente, consapevole delle potenzialità offerte dalle risorse informatiche, le mette a disposizione dei propri dipendenti e collaboratori esclusivamente per finalità lavorative. Non è pertanto consentito il loro utilizzo, salvo espressa autorizzazione, per finalità diverse o in modo contrario alla normativa vigente o alle disposizioni del presente Disciplinare.
L'utilizzo delle risorse informatiche deve avvenire nel rispetto dei principi di diligenza, fedeltà e correttezza che caratterizzano il rapporto di lavoro. L'Utente è tenuto ad adottare tutte le cautele necessarie per prevenire possibili conseguenze dannose derivanti da un utilizzo non corretto degli strumenti, considerata la possibile sovrapposizione tra attività lavorativa e sfera personale e privata.
A tal riguardo, l'Ente adotterà ogni accorgimento tecnico necessario a tutelarsi da comportamenti non consentiti, nel rispetto della libertà e della dignità dei lavoratori.
Di seguito sono indicate le principali linee di comportamento cui gli Utenti devono attenersi per un corretto utilizzo delle risorse informatiche:

a) le operazioni di trattamento devono essere effettuate nel rispetto delle misure di sicurezza, garantendo la riservatezza delle informazioni trattate, da considerarsi di norma confidenziali e soggette al segreto d'ufficio;
b) le modalità operative devono prevenire rischi di perdita, distruzione o accesso non autorizzato ai dati, nonché trattamenti non consentiti o non conformi alle finalità per cui i dati sono stati raccolti;
c) non devono essere effettuate operazioni di trattamento per finalità diverse da quelle rientranti nei compiti assegnati dal diretto responsabile;

d) devono essere svolte esclusivamente le operazioni di trattamento strettamente necessarie al perseguimento delle finalità istituzionali;
e) deve essere verificata l'esattezza dei dati trattati e la loro pertinenza rispetto alle finalità perseguite.

In generale, l'Utente è tenuto a osservare le regole di ordinaria diligenza e tutte le misure necessarie a garantire il rispetto della normativa in materia di protezione dei dati e di sicurezza delle informazioni, operando con attenzione in tutte le fasi del trattamento, dall'acquisizione dei dati alla loro conservazione ed eventuale distruzione.

Resta fermo che le valutazioni in merito al rispetto del presente Disciplinare tengono conto delle circostanze concrete e della buona fede dell'Utente.

4. REGOLE OPERATIVE

4.1 Uso del PC

Il Personal Computer (comprese le periferiche ad esso connesse) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto:

a) devono essere custoditi con la massima diligenza;
b) non è consentita la configurazione di account personali (es. account di posta elettronica privati) né l'inserimento di informazioni personali sul personal computer aziendale.
c) l'utilizzo è consentito per finalità lavorative; eventuali utilizzi diversi, di carattere occasionale e accessorio, devono comunque avvenire nel rispetto delle disposizioni del presente Disciplinare e delle misure di sicurezza adottate. Eventuali minacce alla sicurezza (ad esempio mail di phishing, spam, virus in genere) devono essere tempestivamente segnalate all'Ente, come anche il furto, il danneggiamento o lo smarrimento del dispositivo;
d) il personal computer dato in affidamento all'Utente permette l'accesso alla rete dell'Ente solo attraverso specifiche credenziali di autenticazione riservate**.**
e) non è consentito l'utilizzo di programmi diversi da quelli ufficialmente installati dall'Ente, né l'installazione autonoma di software da parte degli Utenti, al fine di evitare l'introduzione di virus informatici o alterazioni del corretto funzionamento dei sistemi;
f) non è consentita la riproduzione o duplicazione di programmi informatici ai sensi della Legge 21/05/2004 n. 128. L'inosservanza della presente disposizione espone lo stesso Ente a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico dell'Ente;
g) non è consentita l'attivazione della password d'accensione (BIOS), né modificare le caratteristiche hardware e software del PC, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, hard disk esterni, chiavette USB), salvo preventiva ed esplicita autorizzazione da parte dell'amministratore di sistema (vedi punto 4.6);

h) l'Utente deve prestare particolare attenzione all'utilizzo di supporti di origine esterna e informare immediatamente l'Amministratore di sistema in caso di rilevamento di anomalie o virus;
i)) i salvataggi dei file devono essere effettuati esclusivamente sui server dell'Ente, evitando il salvataggio sul disco locale del PC o su supporti di archiviazione rimovibili; deve inoltre essere evitata l'archiviazione ridondante dei dati;
j) il Personal Computer deve essere spento al termine della giornata lavorativa, nonché in caso di assenze prolungate o inutilizzo. In ogni caso, è fatto obbligo di non lasciare il dispositivo incustodito e connesso alla rete; è altresì raccomandata l'attivazione dello screen saver protetto da password anche in caso di assenze temporanee dalla postazione di lavoro.
Lo screen saver può essere inserito premendo la combinazione di tasti "ctrl+alt+canc"

4.2 Utilizzo del PC Portatile

Il PC portatile assegnato all'Utente è uno strumento di lavoro ed è soggetto alle stesse regole previste per i personal computer fissi.
In considerazione della sua natura mobile, l'Utente è inoltre tenuto a custodirlo con particolare attenzione durante gli spostamenti e l'utilizzo fuori sede, adottando ogni cautela necessaria per prevenire furti, smarrimenti o accessi non autorizzati.
In caso di furto, smarrimento o danneggiamento del dispositivo, l'Utente è tenuto a darne immediata comunicazione all'Ente.
L'Utente deve inoltre prestare particolare attenzione all'utilizzo di reti esterne o non aziendali, assicurandosi che l'accesso alle risorse dell'Ente avvenga nel rispetto delle misure di sicurezza adottate e delle procedure eventualmente previste.
I PC portatili dovranno essere periodicamente collegati alla rete interna dell'Ente al fine di consentire gli aggiornamenti antivirus.

4.3. Divieto di utilizzo dei dispositivi personali (PC, Tablet, Smartphone)

Per ragioni di sicurezza e tutela dell'Ente e del personale si ritiene necessario che i device personali non contengano alcun tipo di applicazione aziendale, mail e posta elettronica certificata relativa all'Ente oltre che informazioni riservate strettamente ad esso.
Agli Utenti è pertanto vietato l'utilizzo di applicazioni aziendali ~~non personali~~, compresi di servizi di posta elettronica aziendale, su dispositivi personali, diversi da quelli forniti e assegnati dall'Ente al Personale che ne necessita per ragioni di servizio.

4.4. Credenziali di autenticazione

Le credenziali di autenticazione per l'accesso al PC, la connessione alla rete e/o per l'accesso ai diversi applicativi, vengono assegnate all'Utente dall'Ente, tramite l'Amministratore di sistema, in seguito alla sottoscrizione del contratto di assunzione o di collaborazione con l'Ente.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Utente (user id), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'Utente con la massima diligenza, NON divulgata né appuntata in nessun luogo.

La password, che rappresenta la parte segreta delle credenziali, è conosciuta solo dall'Utente, è composta da almeno da 8 caratteri, deve essere formata da lettere (maiuscole o minuscole) e numeri, anche in combinazione fra loro, e non contiene riferimenti facilmente riconducibili all'Utente (nome, cognome, data di nascita ecc.).
Le credenziali di accesso rilasciate non sono conosciute dall' Ente, né dall'Amministratore di sistema, che però è in grado di resettarle e gestirle secondo le modalità previste e formalizzate nel presente Disciplinare.
L'Utente, ha l'obbligo di modificare la password dopo il primo utilizzo e, successivamente con cadenza trimestrale, come da policy aziendale.
Per garantire la segretezza delle credenziali e la sicurezza durante le sessioni di lavoro che comportano il trattamento dei dati, ogni Utente dovrà:
a) Evitare di condividere in qualsiasi modo la password;
b) Non lasciare accessibile l'elaboratore durante una sessione di lavoro;
c) Impostare uno screen saver dotato di password (con tempi di avvio brevi) che blocchi l'accesso all'elaboratore in caso sia necessario allontanarsi dal dispositivo;
d) Qualora l'elaboratore sia utilizzato da più incaricati, ricordarsi, sempre al termine del lavoro effettuato, di disconnettersi dal sistema (dal menù Windows "avvio/start" scegliere "chiudi" e poi "disconnetti Utente").

Le credenziali sono strettamente personali e non possono essere cedute a terzi. Il mantenimento della segretezza delle credenziali è ad esclusivo carico dell'Utente, il quale sarà il solo responsabile per qualsiasi attività posta in essere tramite l'utilizzo delle stesse.
Nei casi in cui necessità ed indefettibili esigenze di servizio rendessero necessario recuperare con urgenza documenti o informazioni in possesso all'Utente, devono applicarsi le specifiche procedure di recupero definite dall'Ente.
L'Utente è tenuto ad avvisare tempestivamente l'Ente, mediante il Referente interno e l'amministratore di sistema. Non devono essere intraprese iniziative personali che possono comportare significativi danni alla sicurezza del sistema informativo dell'Ente e compromettere la riservatezza delle informazioni personali dell'Utente.

4.5. Antivirus

Il sistema informatico ed i pc collegati alla rete dell'Ente sono protetti da software antivirus aggiornati quotidianamente in modo automatico.
È vietato cancellare, riconfigurare o disattivare detto software antivirus.
Ogni Utente è comunque tenuto a comportarsi in modo tale da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus o attraverso qualsiasi altro software "aggressivo".
L'Utente dovrà segnalare eventuali anomalie all'amministratore di sistema o altro referente dell'Ente:
a) qualora vi sia motivo di ritenere che il pc sia stato infettato o che non sia installata l'ultima versione aggiornata dell'antivirus: nel caso di infezione, anche sospetta, l'utente deve immediatamente scollegare il cavo di rete dal dispositivo e disattivare, se presente, il servizio wi-fi;
b) nel caso di riconoscimento di virus, il sistema proporrà un messaggio di avviso, e nei casi in cui il sistema antivirus non fosse in grado di rimuovere il virus;
L'Utente è tenuto ad una verifica periodica manuale dei propri dischi locali attivando la scansione antivirus.

4.6 Supporti rimovibili

Non è consentita la creazione o duplicazione di nuovi supporti magnetici rimovibili (quali CD e DVD).
È consentita la consultazione di supporti magnetici rimovibili già esistenti, esclusivamente per esigenze di servizio e con le necessarie cautele, al fine di evitare rischi per la sicurezza dei sistemi e dei dati.
L'utilizzo di supporti di memorizzazione USB (es. chiavette USB, hard disk esterni) è consentito esclusivamente se forniti dall'Amministratore di sistema e per esigenze di servizio, nel rispetto delle disposizioni del presente Disciplinare.
È vietato l'utilizzo di supporti USB personali.
I dati personali e le informazioni costituenti know-how aziendale eventualmente presenti su supporti rimovibili autorizzati devono essere tempestivamente trasferiti sui sistemi informativi dell'Ente che garantiscono adeguati livelli di sicurezza, evitando la conservazione prolungata su tali supporti.
L'Utente è responsabile della corretta custodia dei supporti autorizzati e dei dati aziendali in essi contenuti.
Per la distruzione o l'inutilizzabilità dei supporti contenenti dati personali, l'Utente è tenuto a contattare l'Amministratore di sistema e a seguire le istruzioni impartite.

4.7. Utilizzo dei device (smartphone - tablet)

I device aziendali affidati all'Utente sono strumenti di lavoro e di norma l'Ente non ne consente un utilizzo promiscuo; l'eventuale utilizzo a titolo personale di tale strumento di lavoro si configura come un benefit e come tale viene appositamente regolamentato.
È in ogni caso vietato l'utilizzo dei device aziendali per la visione, il download o il caricamento di contenuti contrari al buon costume, pornografici o violenti, nonché per il download, la riproduzione o la condivisione di contenuti ottenuti illegalmente in violazione della normativa sul diritto d'autore e del codice penale.
I device aziendali non dovranno essere utilizzati per uso personale inserendo i propri dati personali quali ad esempio la propria mail o scaricando applicazioni esterne all'ambito lavorativo.
È vietato qualsiasi utilizzo che possa generare disservizi, costi di manutenzione, danni all'immagine dell'Ente o, in particolare, rischi per la sicurezza dei sistemi. Eventuali addebiti o sanzioni derivanti da un utilizzo improprio restano a carico dell'Utente responsabile.
I device devono essere custoditi con cura evitando ogni possibile forma di danneggiamento. L'Utente è responsabile dei device assegnati e deve custodirli con diligenza sia fuori dall'Ente sia durante l'utilizzo nel luogo di lavoro.
I device utilizzati fuori dalla sede dell'Ente, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
È vietato cedere a terzi, a qualsiasi titolo, l'uso dello smartphone o dell'utenza assegnata. L'ente si riserva in ogni facoltà di richiedere in qualsiasi momento e per qualsiasi ragione la riconsegna dello smartphone e della relativa utenza assegnata. In caso di furto o smarrimento è obbligatorio informare immediatamente l'Ufficio Impianti e l'amministratore di sistema per le opportune salvaguardie aziendali.

4.8 Accesso ed utilizzo della rete aziendale

Per l'accesso alla rete dell'Ente ciascun Utente deve essere in possesso della specifica Credenziale di Autenticazione (username e password).
È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione Utente diverso da quello assegnato. Le password d'accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. (vedi punto 4.4)
Le cartelle utenti presenti nei server dell'Ente sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte dell'Amministratore di Sistema.
Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato dell'Amministratore di sistema. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.
È vietato connettere in rete stazioni di lavoro o altri dispositivi hardware, se non previa autorizzazione dall'Ente. È vietato monitorare, attraverso qualsiasi dispositivo hardware o software, ciò che transita in rete. È vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonica per l'accesso a banche dati esterne o interne all'azienda.
L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli Utenti sia sulle unità di rete.
Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun Utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o non più necessari ~~inutili~~. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

4.9 Uso della connessione VPN per telecontrollo

L'accesso è concesso solamente tramite rete interna dell'Ente e quindi accessibile dall'esterno solamente tramite connessione VPN. In particolare, ad ogni collaboratore a cui è consentito per ragioni di servizio l'accesso al server del telecontrollo, sono state fornite le credenziali per accedere alla rete interna mediante applicativi: "SonicWall NetExtender" e "Global VPN Client" per computer windows e "SonicWall Mobile Connect" per dispostivi Android e IOS.
Si ricorda che le credenziali sono personali, NON cedibili e non divulgabili (valgono le regole di riferimento del punto 4.4).

4.10 Uso della rete internet

La rete Internet è ~~ormai divenuta~~ uno strumento operativo di comunicazione imprescindibile pertanto costituisce a tutti gli effetti uno strumento aziendale.
Un utilizzo non corretto o indiscriminato può rendere l'Ente vulnerabile sotto il profilo della sicurezza informatica. L'accesso e l'utilizzo di Internet devono pertanto avvenire prevalentemente per finalità connesse all'attività lavorativa; è ammesso un utilizzo occasionale e accessorio purché limitato, non interferente con l'attività lavorativa e conforme alle disposizioni del presente Disciplinare.

L'Utente è tenuto a utilizzare la rete Internet in modo tale da non rivelare o diffondere informazioni riservate o di proprietà dell'Ente, quali, a titolo esemplificativo, informazioni finanziarie, dati relativi ai consorziati e ai contribuenti, informazioni tecniche, software, codici di accesso, dati personali e relazioni di lavoro.

Al fine di tutelare i sistemi informatici dell'Ente e ridurre i rischi connessi alla navigazione in Internet, sono adottate specifiche misure tecniche di sicurezza. In particolare, non è consentito l'utilizzo di strumenti ~~o connessioni~~ privati per l'accesso alla rete aziendale.
A titolo esemplificativo e non esaustivo, l'Utente non può utilizzare Internet per:
a) l'upload o il download di software, freeware o shareware, nonché l'utilizzo di documenti provenienti da siti non affidabili o non pertinenti all'attività lavorativa;
b) l'effettuazione di transazioni finanziarie, operazioni di home banking o acquisti online, salvo i casi espressamente autorizzati dall'Ente e nel rispetto delle procedure interne;
c) la registrazione a siti o servizi non connessi all'attività lavorativa;
d) la partecipazione a forum non professionali, l'utilizzo di chat, social network o strumenti analoghi non autorizzati;
e) l'accesso a caselle di posta elettronica personale tramite webmail.

Per prevenire l'accesso a siti non pertinenti o ad alto rischio, l'Ente adotta sistemi automatici di filtraggio e blocco della navigazione (black list), che limitano l'accesso a contenuti illegali, non etici, pornografici, violenti, di gioco e scommesse, peer-to-peer, nonché a siti contenenti malware, spyware, phishing o strumenti di elusione dei controlli.

Resta in ogni caso fermo l'obbligo per l'Utente di evitare l'accesso a siti notoriamente malevoli o potenzialmente pericolosi/non conosciuti e di adottare comportamenti prudenti nella navigazione, anche in presenza di sistemi automatici di protezione. L'Utente è responsabile dell'utilizzo della rete Internet effettuato tramite le risorse informatiche assegnate, nel rispetto delle disposizioni del presente Disciplinare e delle misure di sicurezza adottate dall'Ente.

Eventuali controlli sull'utilizzo della rete Internet possono essere effettuati dall'Amministratore di sistema mediante sistemi di controllo dei contenuti o tramite l'analisi dei file di log della navigazione. Tali controlli non sono continuativi e mirati; i dati raccolti sono conservati per il tempo strettamente necessario al perseguimento delle finalità organizzative e di sicurezza dell'Ente, secondo quanto previsto al successivo Punto 5 e nel rispetto dell'art. 4 dello Statuto dei Lavoratori.

4.11 Uso della posta elettronica

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È vietato utilizzare le caselle di posta elettronica nome.cognome@adigeuganeo.it, nome.cognome.adigeuganeo@gmail.com e quelle condivise tra più utenti per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo ma non esaustivo, l'Utente non potrà utilizzare la posta elettronica per:

a) l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
b) l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list se non legati all'attività lavorativa;
c) la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicare immediatamente all'Amministratore di Sistema. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Ente ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dalla Direzione
È obbligo dell'Utente non utilizzare l'account di posta elettronica come archivio di file ma di trasferire quest'ultimi negli appositi server dedicati (o account di posta condivisi). Analogamente, tutte le conversazioni ufficiali dell'Ente devono essere protocollate tramite apposito gestionale.

Tale disposizione organizzativa è fondamentale per assicurare l'ordinario svolgimento e la continuità delle attività istituzionali nel rispetto delle discipline di protezione dei dati personali e la segretezza della corrispondenza, mediante un sistema di gestione documentale in grado di archiviare e conservare i documenti con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile, in linea con le prescrizioni dell'Autorità Garante per la protezione dei dati personali.

Rischi informatici negli allegati di Posta Elettronica

Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli. (Conosciute come tecniche intrusive di Spamming e phishing)
Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe, .scr, .bat ecc), oppure o file che abbiamo nomi simili a documenti che comunque hanno estensione ZIP o diano parvenza di archivio compresso non devono essere aperti. È obbligatorio quindi porre la massima attenzione nell'aprire i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

L'Utente deve segnalare con immediatezza il sospetto all'amministratore di sistema.

Assenza prolungata dell'Utente

In caso di assenza prolungata, l'Utente potrà delegare il superiore gerarchico a verificare il contenuto dei messaggi ed a gestire quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
Sarà comunque consentito SOLO all'Amministratore di sistema, previa autorizzazione del Direttore, di accedere alla casella di posta elettronica dell'Utente qualora si renda necessario. L'accesso avviene secondo la procedura definita dal Consorzio (vedasi successivo punto 5 del presente Disciplinare). Di tale operazione deve essere data comunicazione all'Utente titolare della casella di posta, che provvede ad aggiornare la propria password.

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenza prolungata dell'Utente (ad es. per malattia) potrà essere attivata a cura dell'Ente un servizio di risposta automatica che invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura.

Cessazione del rapporto lavorativo dell'Utente

In caso di cessazione del rapporto di lavoro dell'utente, il Consorzio provvede alla rimozione dell'account personale assegnato, previa disattivazione dello stesso. Dalla data di cessazione del rapporto di lavoro all'utente è inibita la possibilità di accedervi automaticamente.

La disattivazione avviene a cura del personale del Consorzio preposto alla gestione degli account, secondo modalità tali da inibire in via definitiva la ricezione in entrata di messaggi diretti al predetto account, nonché la conservazione degli stessi.

La disattivazione avviene entro un periodo massimo di 30 giorni dalla data di cessazione ed entro il periodo massimo di 90 giorni il Consorzio provvede alla definitiva e totale cancellazione dell'account personale.

Il Consorzio, contestualmente alla disattivazione dell'indirizzo di posta elettronica, adotta sistemi automatici di risposta volti ad informare i terzi e a fornire a questi indirizzi e-mail alternativi a cui poter inoltrare eventuali comunicazioni di interesse e relative alle attività dell'Ente.

Il Consorzio adotta misure idonee ad impedire la visualizzazione dei messaggi in entrata durante il periodo individuato in cui tale sistema automatico è in funzione.

Qualora l'utente risultasse abilitato all'accesso e all'utilizzo di account condivisi a più collaboratori dell'Ente (es., segreteria@adigeuganeo.it ; ufficioX@adigeuganeo.it), l'accesso a tali account sarà precluso all'utente, tramite aggiornamento delle credenziali a cura del responsabile dell'ufficio.

In considerazione dell'utilizzo condiviso di tale tipologia di account, delle informazioni istituzionali in esso contenute, nonché a tutela delle dell'Ente e delle relative attività, il Consorzio non potrà garantirne l'accesso successivamente alla cessazione del rapporto di lavoro dell'utente.

Configurazione della Posta Elettronica nei dispositivi aziendali

Si rammenta che per ragioni di sicurezza e di tutela dell'Ente e dei dipendenti oltre che per evitare possibili incidenti di sicurezza e divulgazione non autorizzata dei dati, la configurazione della mail aziendale avviene previa abilitazione e riconoscimento del/dei device assegnato/i all'utente (ad es., mediante Id / codice dispositivo).

La procedura di attivazione e configurazione sarà effettuata dall'amministratore di sistema al momento della consegna del device tramite apposito applicativo; sarà quindi inibito l'accesso alla posta elettronica da parte di eventuali dispositivi non riconosciuti e/o privati.

4.12 Uso stampanti

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a:

a) stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;

b) stampare a colori solo se strettamente necessario per il corretto svolgimento della propria attività lavorativa, es. documenti ufficiali da tenere agli atti o da produrre verso l'esterno, non utilizzare stampe a colori per versioni di documenti in bozza;

Qualora l'Utente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà avere cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.
Più precisamente, in caso di stampa di documenti contenenti dati particolari dovrà essere obbligatoriamente attivata dal PC la modalità di "Stampa Protetta", che richiede l'inserimento di un apposito codice ID e che andrà digitato sulla tastiera della stampante per consentire il rilascio riservato a stampa del documento.

4.13 Gestione dati

L'Ente raccomanda di salvare frequentemente i documenti su cui si lavora ed in particolare, quando ci si allontana dalla postazione anche per breve tempo.
Costituisce buona regola la periodica pulizia degli archivi, con cancellazione dei file obsoleti o che hanno alcuna finalità e/o utilità per il business aziendale o perché non utilizzabili, o non più utilizzabili, per le attività/funzioni/mansioni assegnate. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
I dipendenti e collaboratori devono salvare i dati ed i documenti aziendali nell'eventuale sistema documentale.
Il disco rigido di ogni PC, infatti, è destinato a contenere solo il software per il funzionamento della macchina.
Si conferma, in generale, l'obbligatorietà del salvataggio dei dati sulle apposite unità di rete messe a disposizione dell'utenza.
In particolare, si ribadisce il divieto di salvare in locale i file contenenti dati del Catasto e di maggiore importanza per l'Ente e per le sue funzioni operative, come pure l'obbligo di preservare con ogni cura e attenzione l'integrità e la riservatezza dei dati personali particolari.

4.14 Uso delle applicazioni di messaggistica

È consentita l'installazione nei dispositivi aziendali delle applicazioni di messaggistica istantanea: "WhatsApp Messenger" e "Telegram", e delle relative versioni web. L'utilizzo di tali applicazioni deve essere legato esclusivamente a scopi lavorativi.

Il Dipende utilizzatore è responsabile del corretto utilizzo di questi ultimi ed ha l'obbligo di mantenere la sicurezza e la riservatezza delle informazioni aziendali trasmesse, di eliminare messaggi insoliti senza aprirli e di non scaricare allegati sospetti.

4.15 Uso della rete wi-fi e gestione degli accessi

Presso la sede consortile e su alcuni impianti dell'Ente sono disponibili connessioni Internet wi-fi destinate ai dispositivi mobili e agli apparati di automazione aziendali per lo svolgimento dell'attività lavorativa.
È vietata la divulgazione a terzi delle credenziali di accesso alle reti wi-fi, salvo che per esigenze strettamente connesse all'attività lavorativa e previa autorizzazione. In particolare, le credenziali della sottorete wi-fi **"**PRODUZIONE**"** non devono in alcun caso essere comunicate a personale esterno al Consorzio, in quanto consentono l'accesso ai server ospitati presso il CED della sede.

Per il personale esterno che necessiti di accesso a Internet per la condivisione di contenuti, viene preferito l'utilizzo dei PC aziendali disponibili presso le sale riunioni dell'Ente.

5. MONITORAGGI E CONTROLLI DELL'ENTE

5.1 Accesso ai dati dell'Utente

L'Amministratore di Sistema può accedere ai dati trattati dall'Utente (ad es. log di posta elettronica, account di dominio, account di programmi in uso all'Ente, dischi locali, dischi di rete) per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware).
Oltre a ciò l'Amministratore di Sistema, per improrogabili necessità operative è abilitato ad accedere all'account/profilo Utente (ad es. posta elettronica, account di dominio, account di programmi in uso all'Ente, dischi locali) mediante sostituzione della password di accesso.
Di tale avvenuto accesso dovrà comunque essere data comunicazione all'Utente che deve procedere con il cambio della password al successivo accesso.

È comunque obbligo dell'Amministratore di Sistema informare la Direzione, in merito a qualsiasi accesso forzato effettuato per necessità e/o sicurezza su profili di autenticazione dei client.

L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema informativo dell'Ente, nonché il necessario svolgimento delle attività lavorative, ad es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

Il sistema informativo fornisce una serie di informazioni inerenti all'utilizzo dei software e/o dell'hardware di ciascuna postazione di lavoro. In via esemplificativa e non esaustiva il sistema informativo fornisce:
a) log di accesso a internet;
b) log inerenti la posta elettronica e servizi mail to fax;
c) log inerenti l'accesso alle banche dati e agli applicativi;
d) log inerenti la telefonia;
e) log inerenti alle attività eseguite;
f) log di attività di computer (accensione, spegnimento);
g) log di stampa.
L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni, ad esempio:
a) Posta elettronica: secondo le caratteristiche tecniche del sistema in uso - l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto;
b) Navigazione Internet: il nome dell'Utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati.

I file di Log vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e comunque non oltre 6 mesi, fatti salvi in ogni caso specifici obblighi di legge.

Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovrascrittura) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.
L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'Utente all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc.
Sarà cura dell'Utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti, prima di procedere alla restituzione dello strumento.
In ogni caso, l'Ente garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

a) lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
b) riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
c) lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

5.2 Controlli

L'Ente ha l'obbligo di salvaguardare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori, pertanto, si riserva il diritto di effettuare controlli per verificare il rispetto del presente Regolamento.
A tale proposito si sottolinea che le Risorse Informatiche sono di proprietà dell'Ente in quanto strumento di lavoro. È pertanto fatto divieto di utilizzo delle Risorse Informatiche e dell'accesso alla rete internet per fini ed interessi non strettamente coincidenti con quelli dell'Ente stesso.
Con riferimento a tali controlli il presente Disciplinare costituisce preventiva e completa informazione nei confronti dei dipendenti e collaboratori. Disposizione fornite anche mediante apposita informativa privacy predisposta ai sensi degli artt. 12 e 13 del GDPR.
Le verifiche sugli strumenti informatici saranno eseguite dall'Ente nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente Disciplinare, secondo i principi di pertinenza e non eccedenza.
L'Ente, pertanto, si riserva il diritto di controllare, anche in maniera occasionale e/o discontinua il corretto utilizzo degli strumenti di lavoro, implementando, però, ogni misura tecnologica volta a minimizzare il più possibile l'uso di dati identificativi dei lavoratori, nei modi e nei limiti esplicitati di seguito e nel successivo paragrafo.
In nessun caso tali controlli verranno impiegati per un monitoraggio dell'efficienza dell'attività lavorativa del singolo individuo come prescritto dall'art. 4 Statuto dei lavoratori.
Ove necessari, i controlli si svolgeranno in forma graduata:

a) in via preliminare l'Ente provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura ovvero a sue aree e dunque un controllo anonimo che può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con invito ad attenersi scrupolosamente ai compiti assegnati ad alle istruzioni impartite;
b) in assenza di successive anomalie non si effettueranno controlli su base individuale. In tali casi, il controllo si concluderà con un avviso ai dipendenti interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Nel caso vengano rilevate continue anomalie si procederà a controlli su base individuale o per postazione di lavoro e in caso di abusi di singoli e reiterati si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro (indicando le ragioni legittime, specifiche e non generiche, per cui i controlli verrebbero effettuati – anche per verifiche sulla funzionalità e di sicurezza del sistema – inoltrando preventivi avvisi collettivi o individuali).
Le attività sull'uso del servizio di accesso ad Internet vengono automaticamente registrate in forma elettronica attraverso i c.d. "log di sistema". Questi sistemi software sono programmati e configurati in modo da cancellare periodicamente e automaticamente, attraverso procedure di sovrascrittura dei log file, i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia più necessaria.
Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Ente, tramite il personale del Servizio IT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali ed ai documenti ivi contenuti, nonché agli account email ed ai tabulati del traffico telefonico.

6. UTILIZZO DEI GESTIONALI E DEL PROGRAMMA PROTOCOLLO

L'accesso ai gestionali dell'Ente è regolamentato da Credenziali di Autentificazione (username e password) comunicate dall'Amministratore di Sistema al momento della creazione dell'utenza e a cui fanno riferimento tutte le norme adottate nel punto 4.4.
Ciascun utente accede, visualizza ed opera esclusivamente su comunicazioni, documenti, dati e informazioni strettamente necessarie alle mansioni e alle attività assegnate, in coerenza al lavoro svolto.
Tutti i gestionali devono essere adoperati con diligenza per evitare incidenti di sicurezza.
Per la gestione del programma protocollo, ogni utente dovrà attenersi ai seguenti punti:

a) i documenti protocollati dovranno essere visionati esclusivamente in base al proprio settore di competenza, ad esclusione dell'Amministratore di Sistema e dell'ufficio Protocollo, abilitati ad accedere a tutta la documentazione;
b) utilizzare con diligenza la modalità di protocollazione in uscita tramite PEC e mail, in riferimento a tutte le modalità citate al punto 4.11;

c) utilizzare con diligenza la modalità di protocollazione in entrata per evitare la protocollazione di file dannosi alla sicurezza dell'Ente, in riferimento a tutte le modalità citate al punto 4.11;
d) procedere alla protocollazione solo previo autorizzazione del Direttore o altra figura di volta in volta indicata;

7. UTILIZZO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE

È consentito l'utilizzo da parte dell'Utente di sistemi di Intelligenza Artificiale, di seguito IA, esclusivamente tramite account e strumenti forniti dall'amministratore di sistema:
Gemini Pro (licenza personale con pacchetto G-suite) e Chat GPT Team (in condivisione tra Utenti).
Non è autorizzata la registrazione ad altri sistemi o soluzioni di intelligenza artificiale oltre a quelli espressamente indicati dall'Ente. Viene consentito l'uso, senza registrazione, di altre soluzioni di intelligenza artificiale affinché non vengano inserite informazioni e dati riguardante l'ente
L'utilizzo di tali strumenti è consentito esclusivamente per finalità lavorative ed è vietato l'uso per scopi personali o comunque estranei all'attività istituzionale dell'Ente.
L'Utente è tenuto ad utilizzare i sistemi di IA previa adeguata formazione e con la piena consapevolezza dei rischi connessi ad un utilizzo improprio.
È vietato in ogni caso delegare a sistemi di IA decisioni operative, gestionali o strategiche. Ogni contenuto, informazione e output prodotto mediante l'uso di sistemi di IA deve essere attentamente verificato, validato e approvato dall'Utente, che ne rimane l'unico responsabile, assumendosi ogni responsabilità in merito all'utilizzo e agli effetti delle informazioni generate.
L'Utente deve prestare particolare attenzione all'inserimento nei sistemi di IA di dati personali, dati particolari o informazioni riservate dell'Ente, assicurandosi che il loro utilizzo avvenga nel rispetto della normativa vigente in materia di protezione dei dati personali e delle disposizioni interne, stabilite dall'Ente.

Il mancato rispetto delle misure di sicurezza tecniche e organizzative nei sistemi di intelligenza artificiale, l'alterazione illecita dei sistemi e l'illecito diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale espongono l'Ente a possibili responsabilità e sanzioni, secondo le specifiche disposizioni della disciplina di settore.

8. CESSAZIONE DEL RAPPORTO DI LAVORO

Prima della cessazione del rapporto di lavoro, l'Utente è tenuto a verificare che non vi siano documenti o dati rilevanti salvati localmente sul proprio computer, su account di posta elettronica aziendali (vedasi punto 4.11) o su piattaforme cloud accessibili esclusivamente a lui.
In caso contrario, è obbligatorio che l'Utente provveda a condividere tali documenti e dati con il proprio superiore gerarchico, in modo da garantire la continuità delle attività lavorative.

All'approssimarsi della cessazione, l'Utente dovrà inoltre restituire tutti i dispositivi mobili e le apparecchiature informatiche fornite dall'Ente (es. smartphone, tablet, computer portatili) all'amministratore di sistema.
L'amministratore di sistema verificherà che i dispositivi restituiti siano stati ripristinati alle impostazioni di fabbrica, rimuovendo tutti i dati personali e le configurazioni dell'Utente. Eventuali dati o documenti aziendali salvati sui dispositivi dovranno essere trasferiti su sistemi aziendali appropriati prima del ripristino.

9. VIOLAZIONI E SANZIONI DISCIPLINARI

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Disciplinare. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari previsti dalla normativa vigente e dai vigenti C.C.N.L.; nonché con le azioni civili e penali previste dalla normativa di riferimento.