CONSORZIO DI BONIFICA TERRITORI DEL MINCIO
Via Principe Amedeo, 29 - 46100 Mantova (MN)
Tel 0376.321312 Fax 0376.222852
C.F. 02384350209 www.territoridelmincio.it
aderente
ASSOCIAZIONE NAZIONALE CONSORZI GESTIONE E TUTELA DEL TERRITORIO E ACQUE IRRIGUE

DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI CONSORTILI

Revisione n. 0 del 27/11/2024
Approvato con Deliberazione del Consiglio di Amministrazione n. 51 del 27/11/2024

Sommario

Premessa

Il presente Disciplinare intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, del **Consorzio di bonifica Territori del Mincio** le indicazioni per una corretta e adeguata gestione delle informazioni consortili, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.

Ogni dipendente e collaboratore è tenuto a rispettare il Disciplinare, che è reso disponibile secondo quanto previsto al successivo punto 1.8 "Decorrenza e pubblicità".

Si specifica che tutti gli strumenti utilizzati dal lavoratore (hardware, software, risorse, e-mail, ecc.) sono messi a disposizione dall'Ente esclusivamente per rendere la prestazione lavorativa.

I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere dall'uso degli Strumenti, sono utilizzate per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio consortile. Per tutela del patrimonio consortile si intende altresì la sicurezza informatica e la tutela del sistema informatico consortile. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Disciplinare costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", come modificato dal d.lgs. 10 agosto 2018, n. 101, recante *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)"* (in G.U. 4 settembre 2018 n.205) e del "Regolamento (UE) 2016/679" *del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* ("Regolamento generale sulla protezione dei dati" o "*General Data Protection Regulation*" o "GDPR").

Si precisa, infine, che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

Il presente Disciplinare è adottato ai sensi del vigente art. 4 comma 3 della L. 300/70, come modificato dal D.Lgs. n. 151/2015 e s.m.i., e delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007 e fornisce informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli.

1. Introduzione

1.1. Definizioni

Ai fini del presente Disciplinare i termini sotto riportati hanno il seguente significato:

- ***Ente*** o ***Consorzio di Bonifica*** o ***Consorzio*** o ***Titolare del trattamento***: Consorzio di bonifica Territori del Mincio;
- ***Intranet:*** rete locale di tutte le componenti Hardware/Software ad accesso esclusivo del Consorzio;
- ***Internet***: rete mondiale degli elaboratori ad accesso pubblico;
- ***Web***: servizio di accesso ai contenuti (dati, servizi di elaborazione, etc.) di Internet;
- ***Web Browser***: programma che consente di "navigare" nel Web;
- ***Ufficio Web***: piattaforma HR *web oriented* dedicata ai dipendenti e ai collaboratori del Consorzio;
- ***Personale***: personale con rapporto di lavoro dipendente o collaboratori del Consorzio;
- ***Utente*** o ***Utilizzatore:*** qualsiasi dipendente o collaboratore del Consorzio, sia esso interno oppure esterno dotato di apposite credenziali di accesso ai sistemi informatici;
- ***Strumenti informatici*** o ***Strumenti elettronici:*** le dotazioni aziendali, ovvero quegli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa. A titolo esemplificativo e non esaustivo, si intendono come tali: le postazioni di lavoro fisse (quali pc desktop e simili) e mobili (pc portatili), pc, notebook, smartphone, servizi, software o applicativi, anche per la sicurezza, e-mail client, Internet browser, Software di messaggistica interna, Server, Firewall, antivirus, sistemi di logging, di inibizione di accesso indiscriminato alla Rete, programmi di produttività individuale, procedure gestionali;
- ***Dispositivi:*** telefono, Smartphone, tablet, Notebook, assegnati dal Consorzio all'Utente, nonché ogni applicazione in essi installata;
- ***Strumenti di stampa:*** costituiscono una sotto-categoria degli Strumenti informatici / Strumenti elettronici, a titolo esemplificativo e non esaustivo, multifunzione, Fotocopiatrici, Scanner, Plotter e altri strumenti, a disposizione dell'Utente per rendere la prestazione lavorativa;
- ***Supporti di memoria:*** a titolo esemplificativo e non esaustivo, chiavi USB, CD, DVD o altri supporti per il salvataggio di dati trattati tramite gli strumenti aziendali;
- ***Credenziali di autenticazione:*** codice per l'identificazione dell'Utente (user id), assegnato dall'Amministratore di Sistema all'Utente, associato ad una password riservata;
- ***File System*** o ***Rete Intranet:*** a titolo esemplificativo e non esaustivo Server, cartelle condivise, stampanti condivise, ecc.;
- ***Risorse Informatiche:*** ogni strumento informatico, dispositivo, strumenti di stampa, supporti di memoria e file system come sopra descritti;
- ***Incaricato*** o ***Autorizzato*** o ***Addetto***: dipendente o collaboratore (anche Utente o Utilizzatore) del Consorzio espressamente autorizzato al trattamento di dati personali per conto del Titolare del trattamento ai sensi dell'art. 29 Regolamento (UE) 2016/679 e dell'art. 2 quater-decies del Codice Privacy (D.lgs. n. 196/2003 come modificato dal D.lgs. n. 101/2018);
- ***Visitatore:*** soggetto esterno (cliente, fornitore, consulente, trasportatore, ecc.) all'Ente;
- ***Amministratore di sistema:*** figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
- ***Policies:*** insieme di regole adottate unilateralmente dall'Ente per disciplinare la condotta di dipendenti e collaboratori; l'insieme delle Policies dell'Ente costituisce il Regolamento. La singola **Policy** è individuata nel presente Regolamento, ad es., "7 Social Media & Social Network";

- ***Paragrafo:*** sottosezione di una Policy del Regolamento (nel presente Regolamento individuata, ad es., "Finalità ed ambito di applicazione");
- ***Trattamento di dati personali:*** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicati a dati personali o insieme di dati personali, come la raccolta, la registrazione l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione o la cancellazione (Cfr. Art. 4, Regolamento (UE) 2016/679);
- ***C.C.N.L***.: Contratto Collettivo Nazionale di Lavoro per i dipendenti dai Consorzi di Bonifica e di Miglioramento Fondiario applicato dall'Ente;
- ***Reg. (UE) 2016/679*** *o* ***Regolamento*** *o* ***Reg.*** *o* ***GDPR:*** 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);
- ***Codice:*** Decreto legislativo del 30 giugno 2003, n. 196 recante il "*Codice in materia di protezione dei dati personali*", integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018 n. 101.

1.2. Finalità ed ambito di applicazione

Il presente Disciplinare si applica ad ogni Utente assegnatario di beni e risorse informatiche del Consorzio ovvero Utilizzatore di servizi e risorse informative di pertinenza del Consorzio.

Costituiscono per i dipendenti dell'Ente parte integrante del contratto di lavoro individuale.

Lo scopo del Disciplinare è di stabilire criteri comportamentali con riguardo all'utilizzo delle risorse informatiche del Consorzio in sinergia e coerenti con il Codice Etico e di Comportamento, nonché lo Statuto dell'Ente.

Il Disciplinare assicura che tutte le attività dell'Ente siano gestite secondo i principi generali di sicurezza delle informazioni consortili e dei dati trattati sotto la responsabilità del Consorzio, in qualità di Titolare del trattamento ai sensi del Regolamento (UE) 2016/679.

Il Personale è pertanto tenuto a rispettare il presente Disciplinare, che è reso disponibile secondo quanto previsto al successivo paragrafo 1.8.

1.3. Obiettivi

Il Disciplinare ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo degli Strumenti Informatici all'interno dell'organizzazione consortile. Con il presente Disciplinare il Consorzio intende fornire le indicazioni per una corretta e adeguata gestione delle informazioni dell'Ente, in particolare attraverso un uso consapevole di sistemi, applicazioni e strumenti informatici assegnati al Personale.

Il Presente Disciplinare intende tutelare i beni dell'Ente ed evitare condotte inconsapevoli e/o scorrette da parte degli Utenti che potrebbero esporre il Consorzio a problematiche di sicurezza, di reputazione e danni patrimoniali cagionati anche a terzi e perseguire l'ulteriore finalità di prevenire eventuali comportamenti illeciti del Personale.

L'insieme delle Policies, che possono includere anche prescrizioni, istruzioni operative ed accorgimenti, sono ispirate ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro e di collaborazione, in sinergia con il Codice Etico e di Comportamento dell'Ente.

Attraverso l'adozione di adeguate misure di sicurezza, l'Ente persegue l'obiettivo di assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati, sia nelle proprie attività interne, sia nelle attività istituzionali svolte in

favore dei consorziati e contribuenti del comprensorio consortile di riferimento. Il Consorzio intende anche prevenire utilizzi indebiti che possono essere fonte di responsabilità per l'Ente *(Cfr. Provvedimento Garante, par. 1.1, lett. b)*.

Le prescrizioni del presente Disciplinare devono essere applicate rigorosamente, ove e per quanto compatibili, anche nello svolgimento della prestazione di lavoro da remoto (in modalità telelavoro o smart-working) e all'esterno dei locali del Consorzio.

1.4. Principi generali in materia di protezione dei dati personali

Le disposizioni del presente Disciplinare sono finalizzate a garantire che i trattamenti di dati personali effettuati dal Consorzio siano orientati al rispetto di alcune fondamentali garanzie in materia di protezione dei dati e siano svolte nell'osservanza di alcuni principi generali, tra cui:

- il *principio di necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (cfr. *principio di "minimizzazione dei dati"* ai sensi dell'articolo 5, paragrafo 1, lettera c) del Regolamento);
- il *principio di correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note al Personale dell'Ente (cfr. *principi di "liceità, correttezza e trasparenza"* ai sensi dell'articolo 5, paragrafo 1, lettera a) del Regolamento);
- il *principio di limitazione delle finalità*, secondo cui i trattamenti devono essere effettuati per finalità determinate, esplicite, legittime, ai sensi dell'articolo 5, paragrafo 1, lettera b) del Regolamento, osservando il *principio di limitazione e non eccedenza*.

1.5. Titolarità degli Strumenti e delle risorse informatiche

Gli Strumenti informatici utilizzati per svolgere la prestazione di lavoro sono forniti dal Consorzio al Personale per rendere la prestazione lavorativa. Tali Strumenti informatici, nonché le relative Reti aziendali a cui è possibile accedere tramite gli Strumenti, sono di proprietà dell'Ente.

L'utilizzo degli Strumenti informatici, pertanto, è consentito **esclusivamente** per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere, ovvero per scopi istituzionali e di servizio afferenti all'attività svolta in favore dell'Ente, e comunque per l'esclusivo perseguimento degli obiettivi del Consorzio.

1.6. Responsabilità personale dell'Utente

Ogni Utente è personalmente responsabile dell'utilizzo dei sistemi, dei beni e delle risorse informatiche che gli sono affidate al momento dell'instaurazione e nel corso del rapporto di lavoro o di collaborazione con l'Ente, nonché dei relativi dati trattati nell'ambito delle attività assegnate.

A tal fine ogni Utente, nel rispetto dei principi di fiducia, diligenza e correttezza sottesi ed espressamente previsti al rapporto instaurato con l'Ente, è tenuto a tutelare, per quanto di propria competenza e secondo la propria responsabilità, il patrimonio consortile da utilizzi impropri, scorretti, comunque non autorizzati, da abusi o danni, anche derivanti da negligenza, imperizia, imprudenza, mera disattenzione. L'obiettivo condiviso da tutto il Personale all'interno dell'Ente è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali, anche in considerazione dei compiti istituzionali assegnati dalla legge nazionale e regionale al Consorzio.

Ogni Utente, pertanto, è tenuto in relazione al proprio ruolo nell'organizzazione del Consorzio e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica dell'Ente, riportando senza ritardo al proprio Responsabile e/o Capo Settore e all'Amministratore di sistema eventuali rischi di cui è o viene a conoscenza, ovvero di violazioni del presente Disciplinare. Tali segnalazioni saranno trattate in modo confidenziale dal Consorzio e a piena tutela del segnalante.

Nell'ottica del miglioramento continuo di procedure, processi e prassi interne all'Ente, che possono ulteriormente valorizzare i servizi e le attività istituzionali dell'Ente, il Consorzio incentiva e riconosce suggerimenti, segnalazioni di criticità e proposte di azioni di miglioramento da parte del Personale, ovvero emergono nell'ambito dello svolgimento quotidiano delle attività dell'Ente.

1.7. Controlli

Negli Strumenti informatici dell'Ente, assegnati o comunque concessi in uso agli Utenti, non sono installati o configurati apparati hardware o software aventi come scopo il controllo a distanza dell'attività dei lavoratori. Sono escluse pertanto forme di controllo datoriali aventi direttamente ad oggetto l'attività lavorativa del Personale.

I controlli posti in essere dall'Ente sono sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali del Personale, comprese le disposizioni di settore che tutelano la dignità delle persone sul luogo di lavoro, e non sono comunque costanti, prolungati ed indiscriminati.

Il Consorzio, nel riservarsi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli Utenti dei beni e delle risorse informatiche dell'Ente, agisce in base al principio della "gradualità" dei controlli, secondo la procedura descritta nella successiva Policy 6, nel pieno rispetto dell'articolo 114 del Codice in materia di protezione dei dati personali.

1.8. Decorrenza e pubblicità

Il presente Disciplinare entra in vigore il 1° gennaio 2025. Il presente Disciplinare resta in vigore fino a revoca o successive revisioni.

Con l'entrata in vigore del Disciplinare tutte le norme e le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

L'adozione del presente Disciplinare verrà comunicata a tutti gli Utenti mediante pubblicazione di apposita comunicazione sulla piattaforma "Ufficio Web", ed invio di una copia via e-mail.

Qualora qualcuno degli Utenti non fosse raggiungibile via e- mail, il Consorzio consegnerà a quest'ultimo una copia cartacea del disciplinare

Copia del presente Disciplinare, inoltre, verrà consegnata in sede di assunzione e di inserimento ai nuovi dipendenti e ai nuovi collaboratori dell'Ente.

2. Riservatezza nelle comunicazioni

2.1. Principi generali e istruzioni operative

Il Personale si attiene alle seguenti istruzioni di trattamento, finalizzate a garantire la riservatezza o confidenzialità, a seconda del caso, delle informazioni trattate nell'ambito dello svolgimento delle proprie mansioni all'interno dell'organizzazione dell'Ente. In particolare:

a) È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, particolari, giudiziari, o altri dati, elementi e informazioni consortili dei quali l'Utente viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di Area/Funzione.
b) Il generale divieto di comunicazione di cui sopra deve essere rispettato in tutte le comunicazioni che intercorrono nell'ambito delle proprie attività di lavoro, siano esse comunicazioni interne verso colleghi/altri collaboratori, ovvero soggetti esterni all'Ente (quali, a titolo esemplificativo e non esaustivo, contribuenti-consorziati, fornitori, consulenti, cittadini, altri soggetti terzi) e prescinde dalla modalità e dagli strumenti di comunicazione utilizzati. Il divieto, pertanto, si applica sia nelle comunicazioni *de visu*, sia nelle comunicazioni mediante strumenti informatici, quali telefono e Pc.
c) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.
d) È vietato effettuare colloqui con utenti o colleghi su questioni che possono essere inerenti informazioni o dati personali in presenza di persone non specificatamente incaricate a conoscere tali informazioni. Nelle ipotesi in cui siano presenti dette persone non incaricate, è necessario interrompere la comunicazione, riprendendola in luogo diverso e più riservato o attendere che i soggetti estranei non siano più presenti.
e) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni consortili quando l'Incaricato si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Tale istruzione deve essere scrupolosamente osservata sia durante la giornata di lavoro, sia al termine della stessa, al momento dell'uscita di locali dell'Ente. L'Incaricato deve riporre il materiale all'interno di armadi o cassettiere, coerentemente con le altre disposizioni in materia di gestione della documentazione in formato cartaceo.
f) Per le riunioni interne e gli incontri in presenza con Fornitori, Consulenti e Collaboratori dell'Ente è opportuno utilizzare, ove possibile, dei locali riservati (es. uffici, sale riunioni ecc…).
g) Per le riunioni interne e gli incontri svolti in modalità da remoto mediante Strumenti e Piattaforme di Videoconferenza, sono applicate, ove compatibili, le prescrizioni della presente Policy.
h) Per le comunicazioni telefoniche sono applicate, ove compatibili, le prescrizioni della presente Policy.

3. Trattamenti con Strumenti elettronici

3.1. Utilizzo degli Strumenti

Il Personale è consapevole che gli Strumenti forniti devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. L'utilizzo è strettamente personale e limitato al solo Utente assegnatario; ne è pertanto precluso l'utilizzo da parte di terzi o altri colleghi, salvo espressa e preventiva autorizzazione del Responsabile di funzione. È vietato qualsiasi altro utilizzo, a scopo o vantaggio personale o di altri.

Ciascun Utente si deve attenere alle seguenti regole di utilizzo degli Strumenti elettronici:

a) Gli Strumenti devono essere custoditi con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento. Ogni malfunzionamento e/o danneggiamento agli Strumenti deve essere tempestivamente comunicato dall'Utilizzatore all'amministratore di sistema / Responsabile di Funzione.
b) Il Personal Computer deve essere spento al termine della giornata lavorativa oppure se ci si assenta dall'ufficio per un periodo di tempo prolungato (ad esempio, per un appuntamento o un'attività fuori sede). Negli altri casi di inutilizzo e allontanamento dalla postazione, anche se per brevi periodi, è comunque necessario attivare sistemi di blocco dello schermo premendo la combinazione di tasti "windows+L" (nella maggior parte delle tastiere il tasto windows riporta il simbolo di Windows "⊞" e si trova tra i tasti ctrl e alt sinistri).
c) Non devono essere lasciati lavori incompiuti sullo schermo. È buona norma non lasciare documenti aperti e visibili sullo schermo del PC quando ci si allontana anche solo temporaneamente dalla postazione di lavoro oppure quando si riceve il pubblico, clienti/fornitori e colleghi.
d) È vietato l'utilizzo di supporti di memoria (chiavi USB, Hard Disk rimovibili, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti consortili, salvo che il supporto utilizzato sia stato fornito dall'Amministratore di sistema o comunque autorizzato dal proprio Responsabile di Funzione. In tal caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative, escludendo un utilizzo promiscuo dello stesso anche per finalità personali e comunque estranee alle attività lavorative.
e) Gli Strumenti sono accessibili esclusivamente attraverso specifiche credenziali di autenticazione come meglio descritto nella successiva Policy 5 del presente Disciplinare.
f) È vietata l'installazione e l'utilizzo di programmi e applicativi diversi da quelli ufficialmente approvati dall'amministratore di sistema per conto del Consorzio. È espressamente vietato agli Utenti di installare programmi non attendibili, non licenziati o qualunque software contraffatto, sussistendo infatti il grave pericolo di introdurre malware e virus informatici in genere, di alterare la funzionalità delle applicazioni software esistenti, vanificando l'efficacia delle misure di sicurezza implementate dall'Ente e di violare eventuali diritti di terzi su tali software.
g) Salvo preventiva ed espressa autorizzazione dell'Amministratore di sistema, non è consentito all'Utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro come a titolo esemplificativo e non esaustivo, chiavette Internet, masterizzatori, modem, altri supporti simili.
h) Gli Strumenti in dotazione devono essere custoditi dal Personale con diligenza, anche in relazione al rischio di possibili furti. In particolare, è vietato lasciare tali strumenti incustoditi ed in vista all'interno di veicoli, aziendali o personali.

3.2. Uso del File System consortile e degli Account Consortili

Il Personale è consapevole che le risorse del File System (server, cartelle condivise, stampanti condivise, ecc.) e della rete Intranet del Consorzio di Bonifica e gli Account Consortili dei sistemi Operativi sono necessari per rendere la prestazione lavorativa.

Ciascun Utente si deve attenere alle seguenti regole di utilizzo del File System e della Rete Intranet.

a) L'Utente deve salvare file, documenti elettronici, dati ed informazioni sul Server consortile, per ragioni di sicurezza informatica e per esigenze di organizzazione e pianificazione delle attività dell'Ufficio / Settore, astenendosi dal salvataggio in locale (su desktop, sulla cartella "documenti" del proprio Strumento, altre posizioni in locale del dispositivo).
b) È raccomandata all'Utente particolare attenzione alle cartelle "download" e "posta interna" presenti in locale sul proprio dispositivo. Tali cartelle vengono svuotate automaticamente con cadenza mensile: eventuali file scaricati in queste cartelle di cui è importante conservare una copia devono pertanto essere tempestivamente trasferiti sul server aziendale.
c) In caso di danneggiamento, malfunzionamenti in genere, furto e/o sottrazione degli Strumenti assegnati, il salvataggio di documentazione e file in locale espone a potenziale perdita irreversibile della documentazione in oggetto, in quanto esclusa dalla replica di back-up prevista per i file salvati in Rete.
d) È vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti assegnati, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Amministratore di Sistema o dal Servizio IT a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti, viene rimosso secondo le regole previste nel presente Disciplinare, ferma ogni ulteriore responsabilità civile, penale e disciplinare di cui l'Utente può essere chiamato a rispondere.
e) Senza preventiva autorizzazione del Responsabile di Funzione, all'Utente è vietato trasferire documenti elettronici dai sistemi informatici e Strumenti Aziendali a device esterni (hard disk, chiavette USB, MicroSD, altri supporti di memorizzazione).
f) Il salvataggio di documenti elettronici aziendali deve avvenire in conformità alle indicazioni fornite all'Utente tramite il presente Disciplinare ed eventualmente in altro modo comunicate dal Responsabile di Funzione e/o dall'Amministratore di Sistema.
   Il salvataggio di documenti aziendali (ad esempio, trasmessi via mail, salvati sui Server del Consorzio, condivisi tra più collaboratori / Uffici / Settori) può avvenire su eventuali Repository esterne autorizzate dal Consorzio anche tramite l'Amministratore di sistema (ad esempio, OneDrive), ovvero inviandoli a terzi via posta elettronica o con altri sistemi. Eventuali necessità ed esigenze specifiche (ad esempio, progetti condivisi con altre organizzazioni) devono essere di volta in volta condivise dall'Utente con il proprio Responsabile di Funzione e, se del caso, previo confronto con l'Amministratore di sistema.
g) Con regolare periodicità (almeno una volta al mese), ciascun Utente provvede alla pulizia degli archivi, dei DataBase, delle cartelle di Rete di competenza, con cancellazione di file obsoleti o inutili. L'Utente deve prestare particolare attenzione alla duplicazione dei dati (ad esempio, salvataggio di uno stesso documento in differenti Cartelle di Rete, essendo infatti necessario evitare un'archiviazione ridondante, specie di file non più necessari.
h) È vietato accedere alla rete consortile con Strumenti personali, salvo diversa autorizzazione ovvero salvo l'utilizzo di reti o infrastrutture a ciò dedicate.
i) È vietato accedere alla rete Intranet con un codice d'identificazione Utente diverso da quello individualmente assegnato. Le credenziali (username e password) di accesso alla Rete, agli applicativi e ai programmi utilizzati nello svolgimento delle proprie attività sono segrete e devono essere gestite secondo le procedure impartite dal Consorzio anche tramite il presente Disciplinare (Policy 5 e nella Lettera / Atto di incarico – autorizzazione al trattamento ed eventuali successive integrazioni).

3.3. Rete aziendale del Consorzio

Ciascun Utente per lo svolgimento della prestazione di lavoro in presenza / presso la sede dell'Ente alla Rete aziendale del Consorzio, tramite cavo di rete disponibile presso la postazione di lavoro assegnata, oppure tramite connessione Wi-Fi.

In caso di mancato funzionamento ovvero disservizio, l'Utente deve procedere a comunicare quanto prima possibile il fatto all'amministratore di sistema e al Settore IT.

3.4. Connessione Remota

Quando autorizzato l'accesso alla Rete aziendale del Consorzio da remoto, ovvero dall'esterno della Sede del Consorzio, avviene tramite il portale https://internal.territoridelmincio.it utilizzando le credenziali personali assegnate (nome utente e password).

3.5. Wifi Aziendale

Presso la Sede del Consorzio è disponibile la connessione Wifi "Vodafone-tmincio" e relative estensioni ("_NORD", "_SUD" e "_GIU") a disposizione del Personale e dei Visitatori che, nel corso della loro presenza in Sede, necessitassero dell'accesso alla Rete per motivi validi e legittimi (a titolo esemplificativo e non esaustivo, presentazioni, progetti condivisi, attività formative di docenti ed altri professionisti, altre attività simili). L'accesso avviene tramite la password fornita dall'amministratore di sistema.

Nota Bene: non è possibile accedere alla rete aziendale tramite questa connessione.

3.6. Uso dell'indirizzo di Posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" adottate dall'Autorità Garante per la protezione dei dati personali e pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

L'Utente si deve attenere alle seguenti regole di Utilizzo dell'indirizzo di Posta elettronica assegnato.

a) La casella di posta elettronica assegnata all'Utente è di proprietà del **Consorzio di Bonifica Territori del Mincio**, ancorché sia strutturata riportando i dati anagrafici (*es., m.rossi@territoridelmincio.it*) dell'Utente assegnatario ed è concessa esclusivamente quale strumento di lavoro.
   L'Utente è consapevole che il contenuto delle comunicazioni inviate tramite l'e-mail aziendale assegnata rientrano nel normale scambio di corrispondenza che l'Ente intrattiene nello svolgimento delle proprie attività istituzionali e pertanto, devono ritenersi relative all'Ente stesso, rappresentato nel frangente dal singolo funzionario.
b) È vietato utilizzare indirizzi di posta elettronica personali (account mail del tipo Gmail, Hotmail, Libero, altri servizi di posta elettronica, specie se gratuiti) per finalità lavorative.
c) È vietato utilizzare le caselle di posta elettronica consortile per motivi diversi da quelli strettamente connessi all'attività lavorativa, in particolare per l'invio e la ricezione di messaggi che non abbiano contenuto e rilevanza istituzionale, giuridica e commerciale. A titolo puramente esemplificativo, all'utente è fatto divieto di utilizzare l'indirizzo di posta elettronica assegnato per:
   - l'invio e/o il ricevimento di allegati contenenti contenuti multimediali (immagini, foto, filmati o brani musicali) non correlati all'attività lavorativa;
   - l'invio e/o il ricevimento di messaggi personali, legati alla famiglia, amicizie, associazioni, acquisti di beni o servizi online, partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
   - la partecipazione a catene telematiche o di Sant'Antonio. Se si dovessero peraltro ricevere messaggi di tale tipologia, l'Utente deve comunicare immediatamente al personale del Servizio IT e/o amministratore

di sistema. L'Utente non dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi, in quanto possono costituire ragionevolmente virus informatici o altre tipologie di malware. L'Utente può procedere ad una prima verifica della fonte di provenienza della comunicazione ritenuta sospetta, posizionando il cursore in prossimità degli stessi e verificando il link esteso che compare in sovraimpressione. L'Utente non deve procedere con proprie iniziative, ma attenersi in modo scrupoloso alle ulteriori istruzioni fornite di volta in volta dall'amministratore di sistema e dal Servizio IT.

d) È vietato utilizzare la casella di posta elettronica consortile quale username / nome utente (ovvero come indirizzo mail di riferimento) per Servizi non inerenti l'attività lavorativa (es. per account di social network, servizi di e-commerce, registrazione a siti web, altri indirizzi simili), salvo autorizzazione dell'amministratore di sistema e/o del Responsabile di Funzione.
e) La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili, obsoleti e soprattutto gli allegati ingombranti in termini di peso complessivo del file, dopo avere salvato gli stessi, se del caso, nelle cartelle di Rete.
f) Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il **Consorzio di Bonifica Territori del Mincio** ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata a ciascun Utente dal Responsabile di Area/Funzione.
g) Ciascun Utente deve controllare con attenzione gli allegati di posta elettronica ricevuti prima del loro utilizzo, avendo cura di verificare prima dell'apertura degli stessi ogni elemento sospetto che possa indurre l'Utente a ritenere che si tratti di un virus informatico o altro malware. Sono segnalate agli Utenti le seguenti casistiche più frequenti:
   - il mittente e/o l'indirizzo e-mail del mittente è sconosciuto e/o sospetto (es., l'indirizzo del mittente si compone di soli caratteri alfa-numerici);

   il testo della mail presenta grossolani ed evidenti errori di battitura, un testo poco comprensibile / senza senso compiuto;<u>In caso di dubbio l'Utente deve immediatamente segnalare il sospetto all'Amministratore di sistema ed osservare in modo scrupoloso le istruzioni da questo fornite</u>.

h) È vietato effettuare l'apertura di file allegati alla posta elettronica che siano eseguibili (.exe), cartelle compresse (.zip; .rar; altre estensioni simili), soprattutto se provenienti da istituzioni bancarie o società di servizi (quali Enel, Eni, Wind, Telecom, Poste, altre società simili).
i) Al fine di garantire la funzionalità del servizio di posta elettronica consortile e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenza improvvisa / non programmata dell'Utente assegnatario invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto individuato o altre utili modalità di contatto dell'Organizzazione (es., numero di telefono dell'Ente). In particolare
   - in caso di <u>assenza programmata</u> (ad es., ferie) la funzionalità deve essere attivata <u>direttamente dall'Utente</u>;
   - in caso di <u>assenza non programmata</u> (ad es., per malattia) la stessa funzionalità verrà attivata a cura dell'amministratore di sistema e/o del Servizio IT.

<u>Il Consorzio, per il tramite dell'Amministratore di sistema ed il Servizio IT, non controlla sistematicamente il flusso di comunicazioni mail, né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori e metadati, al di là di quanto tecnicamente necessario per svolgere e assicurare il servizio e-mail.</u>

<u>Procedura di chiusura dell'account – indirizzo di posta elettronica consortile assegnato</u>

In caso di cessazione del rapporto di lavoro dell'Utente, il Consorzio provvede alla rimozione dell'account personale assegnato, previa disattivazione dello stesso, secondo la procedura di seguito descritta.

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 (amministratore di sistema e/o Servizio IT), 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 7 giorni dalla data di cessazione ed entro il periodo massimo di 30 giorni il Consorzio provvede alla definitiva e totale cancellazione dell'account personale assegnato.

Il Consorzio, contestualmente alla disattivazione dell'indirizzo di posta elettronica, adotta, dei 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 misura idonee ad impedire la visualizzazione dei messaggi in entrata ad altri incaricati, a tutela della riservatezza della corrispondenza dell'Utente cessato e di eventuali terzi.

Qualora l'Utente risultasse abilitato all'accesso e all'utilizzo di account condivisi a più collaboratori dell'Ente (es., *segreteria@consorzio; ufficioX@consorzio*, altri account simili), l'accesso a tali account sarà precluso all'Utente,per effetto della procedura qui illustrata.

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

3.7. Uso della rete Internet e dei relativi servizi

L'Utente si deve attenere alle seguenti regole di utilizzo della Rete Internet e dei relativi servizi:

a. gli Strumenti assegnati al singolo Utente possono essere abilitati alla navigazione in Internet. La rete Internet costituisce uno strumento consortile utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa durante l'orario di lavoro.
b. Per la navigazione su Internet è necessario utilizzare esclusivamente i browser messi a disposizione dall'Ente;
c. Al fine di evitare l'accesso a siti e pagine web non sicure, in ossequio ai principi di prevenzione illustrati nelle "Linee guida del Garante per posta elettronica e internet" dell'Autorità Garante per la protezione dei dati personali, il **Consorzio di Bonifica Territori del Mincio** potrà adottare un sistema di blocco o filtro automatico che previene l'accesso a determinati siti inseriti in una black list. Eventuali richieste di accesso a siti "bloccati" dovranno, in tal caso, essere inoltrate all'Amministratore di sistema che le valuterà unitamente al Referente interno la richiesta.

L'Ente, per il tramite dell'Amministratore di sistema e/o il Servizio IT, non effettua la memorizzazione sistematica ed il controllo delle pagine web visualizzate dal singolo Utente, né controlla con sistemi automatici i dati di navigazione dello stesso.

Si informa tuttavia che al fine di garantire il Servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio consortile, l'Ente può registrare e conservare per 180 giorni i dati di navigazione (file di log riferiti al traffico web) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di Utenti, mediante opportune aggregazioni.

Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente.

In tali casi i controlli avverranno nelle forme indicate al successivo punto 5 del presente Disciplinare.

3.8. Telefonia cellulare, Smartphone, Tablet, SIM

L'Utente è consapevole che il telefono, lo smartphone, il tablet, la SIM assegnati nonché ogni applicazione in essi installata sono di proprietà del **Consorzio di Bonifica Territori del Mincio** e vengono affidati all'Utente per rendere la prestazione lavorativa.

L'Utente si deve attenere alle seguenti regole di utilizzo degli Strumenti di telefonia:

a. è vietato effettuare comunicazioni nonché inviare o ricevere SMS o altre comunicazioni elettroniche a carattere personale o comunque non strettamente inerenti l'attività lavorativa.
b. L'eventuale uso promiscuo (anche per fini personali) degli Strumenti di telefonia è possibile soltanto in presenza di preventivo accordo e in conformità delle istruzioni al riguardo impartite dall'amministratore di sistema e/o dal Servizio IT.
c. La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di ragionevole necessità ed urgenza.
d. Salvo quanto previsto alla precedente lettera b), all'Utente è vietata l'installazione di Applicazioni non strettamente inerenti l'attività lavorativa e la sincronizzazione di qualsiasi file personale (sia proveniente da Applicazioni, che foto, filmati, contatti, chat, ecc.) con l'Account Consortile con cui è stato attivato lo Strumento (vedasi il precedente paragrafo 3.2).
e. L'Utente è responsabile del corretto utilizzo e della custodia degli Strumenti di telefonia che gli sono affidati.

Il Consorzio informa che il telefono, smartphone, tablet o altro dispositivo portatile vengono attivati con Account Consortili (vedasi il precedente paragrafo 3.2) di proprietà dell'Ente e concessi in uso temporaneo all'Utente.

Le informazioni relative all'utilizzo degli Strumenti di telefonia, nonché i file mediante gli stessi trattati (documenti, foto, video, messaggi, ecc.) sono registrati nella memoria degli Strumenti stessi ovvero possono lasciare traccia su Server e router consortili, nelle relative bollette pervenute all'Ente ovvero nelle "aree personali" dei siti dei fornitori dei servizi di telefonia, ovvero sono trattati negli account di attivazione del dispositivo (es. microsoft, google, apple, etc.).

L'Ente non controlla sistematicamente tali informazioni, né sono installati software o sistemi in grado di monitorare l'uso degli Strumenti in questione.

In caso di restituzione degli Strumenti, in caso di cessazione dell'Utente ovvero altre esigenze (sostituzione, malfunzionamento, ecc.), gli stessi saranno resettati a cura dell'amministratore di sistema e/o Settore IT.

I controlli sugli Strumenti di telefonia possono avvenire secondo le disposizioni previste successivo punto 5 del presente Disciplinare.

3.9. Strumenti di stampa

L'Utente è consapevole che gli Strumenti di stampa sono di proprietà del Consorzio di Bonifica Territori del Mincio e sono a disposizione del Personale per rendere la prestazione lavorativa; pertanto ne viene concesso l'uso esclusivamente per tale fine.

L'Utente si deve attenere alle seguenti regole di utilizzo degli Strumenti di stampa:

a. è vietato l'utilizzo degli Strumenti di stampa per fini e scopi personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Area / Funzione.

b. È necessario prestare attenzione alle fotocopie ed alle stampe di documenti: copie mal riuscite, inutilizzate, minute, appunti, ecc., devono essere eliminate utilizzandola macchina distruggi-documenti.
c. È raccomandato all'Utente di prestare particolare attenzione anche nell'eventuale utilizzo di carta da riciclo e successivi utilizzi, qualora i fogli utilizzati contengano dati personali e/o informazioni aziendali riservate.
d. Evitare di lasciare per lungo tempo e oltre il termine della giornata di lavoro stampe contenenti dati personali e/o informazioni riservate, in posizioni facilmente accessibili e di passaggio.

All'Utente è raccomandato di riporre in armadi e/o cassettiere chiuse a chiave eventuali pratiche in corso di svolgimento e non concluse al termine della giornata, avendo cura di osservare, ove compatibili, le istruzioni operative volte ad assicurare la necessaria riservatezza (vedasi, in particolare, le istruzioni operative di trattamento formalizzate a ciascun Utente nella *Lettera / Atto di incarico – autorizzazione al trattamento*).

4. Amministratore di sistema

Il presente Paragrafo è redatto anche in ossequio al Provvedimento dell'Autorità Garante in materia "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 (pubblicato in G.U. n. 300 del 24 dicembre 2008 e s.m.i.).

La funzione di Amministratore di sistema è interna all'organizzazione del **Consorzio di Bonifica Territori del Mincio**, in quanto svolta da personale in forza all'Ente espressamente individuato e in tal senso designato.

In particolare, il personale con funzione di Amministratore di sistema interno si occupa della gestione, del supporto, della manutenzione e dell'aggiornamento di hardware, software e degli altri applicativi utilizzati dal Personale nello svolgimento delle attività di lavoro e istituzionali dell'Ente.

L'attribuzione delle funzioni di Amministratore di sistema avviene in seguito alla valutazione dell'esperienza, delle capacità e dell'affidabilità del soggetto in tal senso designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

La designazione quale Amministratore di sistema è in ogni caso individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

L'identità dell'Amministratore di sistema deve essere resa nota nell'ambito dell'organizzazione dell'Ente. Pertanto, nell'Organigramma consortile, pubblicato in Ufficio Web, è disponibile il nominativo dell'Amministratore di sistema.

L'operato degli Amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Consorzio, titolare del trattamento, in modo da controllarne, anche in ottica accountability, la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Il Consorzio adotta sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) ha caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un congruo periodo, non inferiore a sei mesi.

5. Credenziali di autenticazione agli Strumenti e ai servizi consortili

5.1. Principi generali

Le credenziali di autenticazione agli Strumenti e agli altri Servizi consortili consistono in:

1. un codice per l'identificazione dell'Utente (user ID), assegnato a cura dell'amministratore di sistema,
2. una password che l'Utente deve custodire con la massima diligenza, segretezza e osservando le specifiche prescrizioni della presente Policy.
3. uno o più dispositivi per l'autenticazione a più fattori (e-mail personali, app per la generazione di OTP, SMS ecc…)

È specificato che la password è personale, riservata e non conosciuta dall'Amministratore di sistema interno e dal Consorzio.

L'Utente non deve comunicare ad altri le proprie credenziali. Qualora si rendesse necessario far accedere collaboratori o soggetti terzi per esigenze di sicurezza informatica, attività di aggiornamento dei sistemi / applicativi, manutenzione, supporto o risoluzione di problematiche in genere in genere, l'Utente deve procedere ad inserimento della password, avendo particolare cura di non essere osservato durante la digitazione della stessa. Se necessario, per l'eventuale accesso di terzi ai sistemi informativi protetti da una propria password, l'Utente può rivolgere specifica richiesta all'Amministratore di sistema e/o al Settore IT.

Il rilascio, la modifica o la cancellazione di credenziali di autenticazione che permettono l'accesso a Strumenti, Posta elettronica, Rete, Server dell'Ente, ecc., vengono effettuati dall'amministratore di sistema e/o dal personale del Servizio IT, previa richiesta della Direzione o eventuale altro Responsabile.

L'Utente assegnatario delle credenziali è tenuto all'aggiornamento periodico della password di accesso, secondo le politiche di gestione dell'Ente.

L'Utente è tenuto all'immediata sostituzione della password in caso di sospetto che la stessa abbia perso la propria riservatezza, secondo le modalità descritte nel presente Disciplinare, d'intesa con l'amministratore di sistema e/o il personale del Settore IT.

L'Utente è obbligato alla conservazione delle credenziali all'interno del programma di gestione delle stesse messo a disposizione dall'Ente (Keepass).

E' espressamente vietato, pertanto, l'utilizzo di ogni altro metodo di conservazione/archiviazione "in chiaro" delle credenziali (es. fogli excel, fogli di carta ecc….).

L'Utente si obbliga, pertanto, a trasferire all'interno del software fornito dall'Ente le proprie credenziali provvedendo alla distruzione e/o cancellazione degli eventuali supporti di memorizzazione non autorizzati.

Le credenziali di accesso rilasciate non sono conosciute dagli Amministratori di Sistema, che però è in grado di resettarle e gestirle secondo le modalità previste e formalizzate nel presente Disciplinare.

5.2. Istruzioni operative per la gestione delle credenziali di autenticazione

L'Utente si deve attenere alle seguenti regole di utilizzo in merito alla gestione delle credenziali di autenticazione:

a. Modificare alla prima connessione la password che l'Amministratore di sistema e/o il Settore IT fornisce di default ("password scaduta").
b. È fatto assoluto divieto di trascrivere la password nei pressi della postazione di lavoro (con comportamenti non adeguati quali la trascrizione in post-it affisso al monitor del PC assegnato, presso la propria postazione di lavoro, memo dell'agenda, cassetto della scrivania).

c. La password deve essere composta da almeno 10 caratteri scelti tra almeno tre di questi gruppi: maiuscole, minuscole, numeri, caratteri non alfanumerici, non può contenere il nome utente e deve essere significativamente diversa dalle ultime 5 password al fine di assicurare opportuni criteri di complessità volti a precluderne la conoscibilità.
d. È necessario prestare particolare attenzione a non essere osservati mentre si digita la password o qualunque altro codice di accesso ai sistemi informatici del Consorzio. Infatti, anche se molti programmi non ripetono in chiaro la password sullo schermo, l'attenta osservazione da parte altrui dei tasti digitati può condurre all'individuazione della password.
e. È necessario procedere alla modifica della password al primo utilizzo (si veda lettera a) delle presenti istruzioni operative) ed ogni qualvolta richiesto dal sistema. Si informa che il sistema assegna di default un termine di validità della password: qualora l'Utente non provveda a variare la propria password prima della scadenza, l'accesso al personal computer e/o ai sistemi informativi dell'Ente verrà temporaneamente bloccato.
   La scadenza della password degli account è impostata a 3 mesi per tutti gli Utenti privi di autenticazione a più fattori.
   La necessità di procedere ad aggiornamento della password è segnalata all'Utente dal sistema operativo per il tramite di notifica automatizzata 5 giorni prima della scadenza.
   È raccomandato all'Utente di procedere al cambio password prima della scadenza della stessa, al fine di non riscontrare problematiche di accesso alle risorse informatiche del Consorzio.
f. L'Utente deve procedere ad immediata modifica della password nel caso di sospetto che la riservatezza della password sia compromessa, in coerenza con le previsioni della presente Policy.
g. Qualora la password dovesse venire sostituita a seguito di perdita della riservatezza, l'Utente deve procedere a sostituzione secondo le modalità definite dal Consorzio.
h. L'Utente non deve permettere che altri Utenti (es., colleghi) operino con il proprio identificativo Utente e le proprie credenziali riservate. Nelle sole ipotesi espressamente individuate e nei soli casi in cui si renda assolutamente necessario procedere in tal senso, verrà seguita la procedura per la forzatura delle credenziali di accesso, a cura dell'Amministratore di sistema, secondo la procedura descritta al successivo paragrafo 6.2 del presente Disciplinare, cui si rimanda.

6. Controlli sugli Strumenti

6.1. Principi generali

L'utilizzo da parte dell'Utente degli Strumenti Informatici assegnati può lasciare traccia delle informazioni sul relativo uso.

La presente Policy assolve agli obblighi di informativa di cui al Punto 6.1 delle "Linee guida del Garante per posta elettronica ed internet" dell'Autorità Garante per la protezione dei dati. Informazioni sul trattamento di dati personali sono dettagliate anche nell'informativa ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 per dipendenti e collaboratori dell'Ente.

Tali informazioni, che possono contenere dati personali eventualmente anche riservati dell'Utente, possono essere oggetto di controlli incidentali da parte dell'Ente, anche per il tramite dell'Amministratore di sistema e/o del personale del Settore IT, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio consortile, nonché per la sicurezza e la salvaguardia del sistema informatico consortile, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.).

Tali interventi di controllo (di seguito descritti) possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta dall'Utente con gli Strumenti.

In via generale, i controlli previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa in materia (articolo 4 della Legge n. 300/1970 e s.m.i.; art. 114 del Codice in materia di protezione dei dati personali)

6.2. Controlli per la tutela del patrimonio consortile, per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).

Qualora risulti necessario l'accesso alle risorse informatiche, il Titolare del trattamento dei dati personali, per il tramite dell'Amministratore di sistema e del Servizio IT, si atterrà alla procedura di seguito descritta (se e in quanto compatibile con lo Strumento oggetto di controllo).

1. Avviso generico da parte dell'Ente a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Disciplinare.
2. Successivamente, dopo almeno 5 giorni, se il comportamento anomalo persiste, la Direzione potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni, con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP o dell'account, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

Il controllo avviene nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Disciplinare. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Titolare del trattamento e dall'Amministratore di Sistema che ha svolto l'attività.

In caso di nuovo accesso da parte dell'utente allo Strumento oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).

Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Disciplinare costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e del Regolamento (UE) 2016/679.

6.3. **Controlli per esigenze produttive e di organizzazione**

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, SMS ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni. il Responsabile del trattamento dei dati personali, per il tramite dell'Ufficio IT, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

1. Redazione di un atto da parte del Direttore e/o Capo Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
2. Incarico all'Amministratore di sistema e al Referente interno in materia di protezione dei dati di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.

3. Redazione di un verbale che riassuma i passaggi precedenti.
4. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
5. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Disciplinare costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e del Regolamento (UE) 2016/679.

6.4. Controlli non ammessi

L'Ente non può in nessun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa del Personale. Per tali si intendono, a titolo meramente esemplificativo e non esaustivo:

- la lettura e la registrazione sistematica di messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica aziendale;
- la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza delle stesse;
- la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- l'analisi dei dispositivi per l'accesso alla rete internet e l'accesso alla rete consortile.

Non sono ammessi controlli ingiustificati, discriminatori e altrimenti lesivi della dignità e della personalità del lavoratore.

7. Social Media & Social Network

L'utilizzo a fini promozionali e commerciali di Social Media e Social Network quali, a titolo esemplificativo e non esaustivo, Facebook, Twitter, Linkedin, dei Blog e dei Forum, anche professionali (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio consortile, anche immateriale, quanto i propri collaboratori, i propri utenti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

Il presente articolo deve essere osservato dall'Utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.

La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni consortili considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione.

L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori consortili, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro consortili, se non con il preventivo consenso del Responsabile d'ufficio.

Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

8. Utilizzo di sistemi e tecnologie di intelligenza artificiale generativa

Per “intelligenza artificiale generativa" si intende ogni sistema o software che utilizza algoritmi di machine learning per creare contenuti (testi, immagini, suoni, codice, ecc.) a partire da dati di input quali, ad esempio, ChatGPT, Copilot e Gemini.

L’utilizzo di tali strumenti è consentito esclusivamente per attività che rientrano nell’ambito delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere e che siano conformi agli obiettivi dell’Ente.

Ove disponibili, l’Utente dovrà utilizzare esclusivamente gli strumenti di intelligenza artificiale generativa acquistati in licenza dall’Ente (https://copilot.cloud.microsoft) e messi a disposizione del proprio Personale.

In ogni caso, durante l’utilizzo di tali strumenti è vietato immettere dati personali comuni, particolari, giudiziari, o altri dati, elementi e informazioni riservate relative all’attività dell’Ente dei quali l’Utente viene a conoscenza nell’esercizio delle proprie funzioni e mansioni all’interno dell’Ente.

In caso di dubbio circa gli strumenti di intelligenza artificiale generativa utilizzabili e/o le informazioni di cui è consentito l’inserimento, l’Utente dovrà accertarsi mediante richiesta preventiva al proprio Responsabile di Area/Funzione all’Ufficio IT.

È inoltre responsabilità di ciascun Utente verificare, prima del loro utilizzo nell’ambito di documenti o attività ufficiali dell’Ente, che i risultati ottenuti tramite tali strumenti siano accurati, pertinenti, etici, conformi alle leggi vigenti (a titolo esemplificativo quelle in materia di trattamento dati personali, diritto d’autore, proprietà intellettuale), non offensivi, non discriminatori e conformi agli obiettivi aziendali.

9. Sanzioni

È fatto obbligo a tutto il Personale di osservare le disposizioni portate a conoscenza con il presente Disciplinare.

Eventuali violazioni del presente Disciplinare da parte dei dipendenti nonché di altre norme previste dal CCNL applicato, a seconda della gravità della infrazione, comportano l’adozione dei seguenti provvedimenti:

- censura scritta;
- sospensione dal servizio;
- licenziamento in tronco;
- licenziamento di diritto.

Rimane comunque riservato il diritto di intraprendere azioni civili e penali nei confronti dei responsabili di qualsivoglia violazione a danno del Consorzio.

È richiamato in questa sede il Codice Etico e di Comportamento adottato ai sensi del D. Lgs. 231/2001 e pubblicato sul sito del Consorzio all’indirizzo https://www.territoridelmincio.it/amministrazione-trasparente/disposizioni-generali/74-atti-generali.

10. Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Disciplinare. Le proposte verranno esaminate dal Consorzio, in concerto con l'Amministratore di sistema e il Servizio IT.

Il presente Disciplinare è soggetto a revisione con frequenza periodica, secondo necessità (con cadenza almeno di una volta l'anno).