REGOLAMENTO PER IL CORRETTO E SICURO TRATTAMENTO DEI DATI PERSONALI
E PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA

Approvato dal Consorzio di bonifica di secondo grado per il Canale Emiliano Romagnolo
in data 23 novembre 2022 con deliberazione n. 56/22/CD.

1 Sommario

1 SEZIONE I – AMBITO GENERALE

1.1 Definizione

Consorzio di bonifica di II grado per il Canale Emiliano Romagnolo con sede in Bologna, via Ernesto Masi n. 8, CF 80007190376, di seguito anche “Consorzio”

Amministratore di sistema: la persona fisica, preposta dal Titolare, cui spetta la gestione della sicurezza del sistema informatico.

Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Comunicazione di dati personali: corrisponde al dare conoscenza dei dati personali a uno o più soggetti determinati, diversi dall'interessato, in base a una precisa finalità e una modalità certa e sicura di trattamento, anche mediante la loro messa a disposizione o consultazione.

Dati che presentano rischi specifici: il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure e accorgimenti a garanzia dell'interessato, ove prescritti.

Dati giudiziari: dati personali relativi a condanne penali e reati, dati idonei a rilevare informazioni riguardo a provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Dati particolari o Categorie particolari di dati personali: dati personali idonei a rivelare l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona.

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo (come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online) oppure a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

Diffusione di dati personali: azione posta in essere quando viene data conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Dipendente/utente: personale del Consorzio assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio, in possesso di specifiche credenziali di autenticazione per accedere ad una qualsiasi risorsa fornita dal Consorzio, nonché personale autonomo che utilizzi temporaneamente le risorse informatiche del Consorzio.

DPO: Lepida S.c.p.A. contattabile all'indirizzo: dpo-team@lepida.it

Interessato: la persona fisica a cui si riferiscono i dati personali.

NDA: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali che le parti si impegnano a mantenere segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

Referente Privacy: Roberto Genovesi, contattabile all'indirizzo: genovesi@consorziocer.it

Reg. UE n. 679/2016 (GDPR): Regolamento Europeo in materia di dati personali e s.m.i. (d'ora in poi anche "GDPR")

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

Risorse informatiche: tutto il parco macchine consortile quali workstation, personal computer, smartphone, notebook, tablet, server, monitor, proiettori e stampanti utilizzati per l'accesso alla rete interna e per l'accesso a Internet nelle varie forme (rete fissa consortile, rete dati mobile ecc.).

Soggetto autorizzato al trattamento: la persona fisica autorizzata dal Titolare a procedere al trattamento, ovvero a compiere operazioni di trattamento dati in base alle regole definite dall'organizzazione.

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Trattamento dei dati personali: qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi 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, la cancellazione o la distruzione.

Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

1.2 Premessa

Nello svolgimento delle proprie mansioni il Consorzio gestisce una serie di "informazioni", proprie e di terzi.

Tali informazioni possono essere considerate, ai sensi del Reg. UE n. 679/2016 (GDPR) e s.m.i., "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea sia digitale, è necessario che il Consorzio adotti una serie di misure di sicurezza tecniche e organizzative.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'organizzazione è chiamata a garantire la riservatezza, o per NDA ("Non Disclosure Agreement" o "Accordo di Riservatezza"), o per una più ampia tutela del patrimonio consortile.

Nel presente regolamento sarà adottato il termine “dati” per intendere l’insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i “dati personali” intesi a norma di legge.

In linea generale ogni dato, nell’accezione più ampia sopra descritta, di cui il soggetto autorizzato viene a conoscenza nell’ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno, anche una volta concluso il rapporto lavorativo con il Consorzio, salvo specifica autorizzazione esplicita del Consorzio stesso.
Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l’attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche, e in particolare l’accesso alla rete Internet dal computer consortile, espone il Consorzio a possibili rischi di un coinvolgimento di rilevanza civile, penale e/o amministrativa, creando problemi alla sicurezza e all’immagine dell’ente stesso.

Premesso che i comportamenti che normalmente si adottano nell’ambito di un rapporto di lavoro, tra i quali rientra l’utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, il Consorzio adotta il presente Regolamento interno per evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature consortili.

Sono destinatari del presente Regolamento tutti gli amministratori e i dipendenti, senza distinzione di ruolo e/o livello, nonché tutti i collaboratori del Consorzio, a prescindere dal rapporto contrattuale con lo stesso intrattenuto (collaboratore a progetto, in stage, consulente, tirocinante ecc.). Tutti i soggetti esterni, persone fisiche o giuridiche, che operano con il Consorzio attraverso un rapporto di collaborazione nell’ambito di convenzioni, protocolli di intesa o incarichi professionali sono tenuti a rispettare ed osservare le presenti disposizioni.
Il mancato rispetto del Regolamento, pertanto, a seconda della natura del rapporto esistente, sarà sanzionato mediante l’applicazione delle sanzioni disciplinari previste dal Titolare, dai CC.CC.NN.LL., dal Codice etico adottato dal Consorzio e più in generale dalla normativa di riferimento.

Una gestione dei dati cartacei, un uso dei personal computer e di altri dispositivi elettronici (di seguito “device”) nonché dei servizi di Internet e della posta elettronica difforme dalle regole contenute nel presente Regolamento potrebbe esporre il Consorzio all’aumento del rischio di accessi non

autorizzati ai dati e/o al sistema informatico consortile, furti o divulgazioni di informazioni riservate, furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico, nonché a problemi legati all'immagine del Consorzio stesso, oltre ad innescare conseguenze di natura penale dovute a violazioni specifiche di disposizioni di legge (come la legge sul diritto d'autore Legge 633/1941).

1.3 Integrazione all'informativa

Il presente Regolamento costituisce un'integrazione alla più generale informativa sul trattamento dei dati personali resa ai sensi dell'art. 13 del GDPR.

1.4 Modalità di pubblicizzazione

Il presente Regolamento è pubblicizzato adeguatamente, anche nel rispetto dello Statuto dei lavoratori.

Il **Consorzio di bonifica di II grado per il Canale Emiliano Romagnolo** dispone che il Regolamento sia:

- inviato a mezzo e-mail a tutti i lavoratori;
- inserito nella piattaforma Ufficio Web in uso al personale con obbligo di spuntare la presa visione;
- inserito nella cartella di rete consortile dedicata alle policy consortili.

1.5 Aggiornamento del Regolamento

Gli aggiornamenti al presente Regolamento saranno resi noti tramite comunicazione ufficiale via e-mail.
Le prescrizioni di seguito esposte si aggiungono e integrano le istruzioni già comunicate tramite posta elettronica a tutti gli Autorizzati al trattamento dei dati in attuazione del Reg. UE n. 679/2016 (GDPR) integrando, inoltre, le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

1.6 Validità

Il presente Regolamento ha validità a partire dalla data di efficacia del provvedimento di approvazione.

1.7 Istruzioni operative per il trattamento delle informazioni

Ogni qualvolta il dipendente, nello svolgimento delle sue mansioni, si trova a trattare dati personali, con strumenti elettronici e non elettronici, deve scrupolosamente attenersi alle seguenti istruzioni:

- Raccogliere i dati e registrarli per gli scopi inerenti unicamente all'attività svolta.
- Verificare che i dati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare del trattamento.
- Mantenere la massima riservatezza sui dati di cui si effettua il trattamento. In particolare, la consegna di schede e documenti contenenti dati personali deve essere effettuata in busta chiusa. La consegna a soggetto diverso dall'interessato, oltre a essere rigorosamente effettuata mediante busta chiusa, deve avvenire unicamente nei confronti di persona munita di documento di riconoscimento e di delega scritta da parte dell'interessato.
- Non utilizzare, comunicare o diffondere alcuno dei dati predetti se non previamente autorizzato in forma scritta dal Titolare del trattamento o dal Responsabile.
- Osservare i criteri stabiliti dall'art. 32 GDPR sulle misure minime di sicurezza per il trattamento dei dati personali e tutte le misure di protezione e sicurezza, già in atto o successivamente disposte, tese ad evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito dei dati personali.
- Non condividere o salvare dati o informazioni di carattere istituzionale in Internet, ad esempio tramite Social Media, forum, chat, blog, siti Internet; non salvare dati personali o istituzionali in sistemi cloud esterni al Consorzio, salvo il caso in cui ciò sia autorizzato dal Titolare del trattamento.

Per quanto concerne gli archivi cartacei, l'accesso è consentito solo se previamente autorizzato dal Titolare del trattamento e deve riguardare i soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati, avendo particolare riguardo a quanto segue:

- I documenti cartacei devono essere prelevati dagli archivi per il tempo strettamente necessario allo svolgimento delle mansioni.
- Atti e documenti contenenti dati particolari o giudiziari devono essere custoditi in contenitori muniti di serratura e devono essere controllati in modo che a tali atti e documenti non possano accedere persone prive di autorizzazione.
- Atti e documenti contenenti dati particolari o giudiziari devono essere restituiti al termine delle operazioni affidate.
- Eventuali fotocopie o copie di documenti devono essere autorizzate e custodite con le stesse modalità dei documenti originali.

Gli archivi cartacei per ogni ufficio saranno chiusi a chiave e custoditi dal responsabile di tale ufficio.

1.8 Titolarità dei dati e dei device

Il Consorzio è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni e i dati contenuti e/o trattati mediante i propri device digitali o archiviati in modo cartaceo nei propri locali.
Il Consorzio è esclusivo titolare e proprietario dei computer e dei device (smartphone, tablet etc.) messi a disposizione dei soggetti autorizzati ai fini dell'attività lavorativa.
L'account "istituzionale" è dotato di credenziali univoche e prevede password di accesso di almeno 12 caratteri, complesse, a scadenza trimestrale e non ripetibili.
L'account istituzionale sarà utilizzato dal soggetto autorizzato esclusivamente per un fine di carattere lavorativo. Gli ambienti interni a computer e device non devono essere, quindi, utilizzati per finalità private e diverse da quelle consortili, se non eccezionalmente e nei limiti evidenziati dal presente Regolamento (vedi punto 3.1 sull'utilizzo promiscuo dei device).
Qualsiasi eventuale tolleranza da parte del Consorzio, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni impartite nel presente Regolamento.

Qualora il soggetto autorizzato tratti in qualsiasi modo informazioni – personali e non – di natura privata all'interno di computer e device consortili, non potrà presumere o ritenere che tali informazioni, registrazioni e dati da lui trattati o memorizzati nell'ambiente consortile (inclusi messaggi di posta elettronica e/o chat inviati o ricevuti, file di immagini, file di filmati o altre tipologie di file) siano privati o personali.

1.9 Presa in consegna delle dotazioni consortili

La consegna delle dotazioni consortili sarà debitamente documentata nel contratto di assunzione qualora la custodia del device dovesse coincidere con l'assunzione, diversamente l'adozione del device sarà documentato con atto separato.
Presso gli uffici dell'Amministrazione, previa richiesta di accesso agli atti tramite invio di una e-mail all'indirizzo genovesi@consorziocer.it , sarà possibile avere verifica del censimento delle dotazioni in custodia.
L'utente è responsabile del personal computer e degli altri dispositivi elettronici assegnatigli dal Consorzio e deve prendersene carico con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Le attrezzature consortili vanno gestite e utilizzate con la massima cura. È compito dell'utente verificare quotidianamente che le stesse si trovino nello stato in cui gli sono state consegnate; eventuali disfunzioni e/o rotture riscontrate vanno immediatamente comunicate al Referente di ufficio che avrà cura di informarne l'Amministratore di sistema.

1.10 Restituzione delle dotazioni consortili

A seguito della cessazione del rapporto lavorativo o di consulenza del soggetto autorizzato con il Consorzio o, comunque, al venir meno, ad insindacabile giudizio del Consorzio, della permanenza dei presupposti per l'utilizzo dei device consortili, gli autorizzati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei device in uso;
2. Divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

1.11 Restituzione dei dati cartacei

A seguito della cessazione del rapporto lavorativo o di consulenza del soggetto autorizzato con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'ente, della permanenza dei presupposti per l'utilizzo di dati cartacei istituzionali, gli autorizzati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei dati cartacei in loro possesso;
2. Divieto assoluto di alterare o manomettere o distruggere i dati cartacei assegnati o renderli inintelligibili tramite qualsiasi processo.

2 SEZIONE II – USO DEL PERSONAL COMPUTER DELL'ENTE

2.1 Modalità d'uso del Personal Computer consortile

Il personal computer, sia fisso sia portatile (da ora in avanti "PC"), assegnato al dipendente è uno strumento di lavoro che contiene tutti i software necessari per svolgere le attività allo stesso affidate. L'utilizzo del PC viene disciplinato nel presente Regolamento affinché l'utente non contribuisca ad innescare disservizi, generare costi di manutenzione e, soprattutto, innescare minacce alla sicurezza.

Il PC affidato all'utente permette l'accesso alla rete consortile solo attraverso specifiche credenziali di autenticazione, come meglio descritto successivamente nella Sezione IV.

La custodia della dotazione consortile fuori dall'ufficio deve avvenire secondo la dovuta diligenza evitando ogni possibile forma di danneggiamento del bene.

Al fine di cercare di ridurre l'efficacia di eventuali attacchi informatici subiti dal Consorzio (es. ransomware, cryptolocker etc.) i file creati, elaborati o modificati sul PC assegnato devono essere sempre salvati a fine giornata sul sistema di repository documentale centralizzato (tutti i dischi di rete e repository in cloud).

Si deve prestare particolare attenzione, durante la custodia del PC portatile, quando lo si lascia in vista in auto, in una stanza, nell'atrio di un albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

In caso di perdita o furto dei PC e degli altri dispositivi elettronici l'utente deve avvisare immediatamente (entro le 24 ore), ai contatti di cui in premessa, il Referente Privacy, il quale si occuperà delle procedure connesse alla Privacy e, successivamente, della denuncia alle Autorità competenti.
Anche di giorno, durante l'orario di lavoro, il collaboratore deve adottare le dovute precauzioni per non minacciare la sicurezza delle informazioni trattate nel corso dell'attività lavorativa.
L'utilizzo del PC consortile per fini personali, durante una eventuale conservazione dell'apparecchio portatile presso il proprio domicilio, deve essere limitato e sempre nel rispetto del Regolamento e della normativa vigente. Qualora degli strumenti consortili venga fatto un uso privato nell'ambiente privato, o un uso privato accidentale nell'ambiente istituzionale, è d'obbligo la cancellazione dei dati contenuti nello strumento, immediata e comunque prima della riconsegna dello stesso per manutenzioni.
Eventuali dati residui che venissero visualizzati accidentalmente dagli Amministratori di sistema saranno in ogni caso trattati con riservatezza.

In particolare, il soggetto autorizzato deve adottare le seguenti misure:

1. Utilizzare principalmente le aree di memoria della rete interna del Consorzio ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri file fuori dalle unità di rete.
2. Spegnere il computer, o curarsi di effettuare il Logout, al termine dell'attività lavorativa o in caso di assenze prolungate, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.
3. Spegnere il PC dopo il Logout.
4. Non utilizzare dispositivi di memorizzazione esterna (pennette USB, hard disk esterni, ecc.) diversi da quelli messi a disposizione dal Consorzio.
5. Mantenere conservati sul desktop solo i dati e le informazioni strettamente necessari per l'attività lavorativa, limitatamente alle situazioni in cui non è possibile usufruire della connessione alla rete consortile o di altro accesso sicuro alla rete interna consortile, o in casi in cui tale connessione sia instabile. I dati e le informazioni conservati sul desktop dovranno essere cancellati dallo stesso e spostati all'interno di apposita cartella di rete consortile non appena possibile.
6. Impostare il blocco del PC tutte le volte che abbandona la postazione di lavoro, onde evitare utilizzi impropri da parte di soggetti non autorizzati.
7. Non dare ad altri utenti accesso al proprio PC a meno di necessità stringenti e sotto il proprio costante controllo.

Nell'utilizzo degli screen saver si invita a non adottare file, immagini e informazioni riconducibili alla propria sfera personale e affettiva**.**

2.2 Divieti espressi sull'utilizzo del Personal Computer

Al soggetto autorizzato è vietato:

1. Gestire, memorizzare (anche temporaneamente) o trattare file, documenti e/o informazioni personali o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa consortili e negli strumenti informatici consortili in genere.
2. Modificare le configurazioni già impostate sul PC, salvo espressa indicazione degli Amministratori di sistema.
3. Installare e/o utilizzare programmi, software e/o sistemi, anche di criptazione, diversi da quelli autorizzati e installati dagli amministrati di sistema senza la preventiva autorizzazione scritta del Consorzio.
4. Registrare file, software o archivi di uso istituzionale su dispositivi personali.
5. Fare copia dei software installati per uso personale.
6. Installare alcun software di cui il Consorzio non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul PC consegnato, diversi da quelli autorizzati e installati dagli amministrati di sistema, senza l'espressa autorizzazione dell'organizzazione. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.
7. Caricare nel PC, sul disco fisso del computer o nel server alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.
8. Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli eventualmente consegnati, senza l'autorizzazione espressa degli Amministratori di sistema.
9. Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell'organizzazione, quali per esempio virus, trojan horses, ecc.
10. Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.
11. Effettuare in proprio attività manutentive, ad eccezione dei soli dipendenti autorizzati con funzione di amministrazione di sistema, che sono autorizzati alle sole attività manutentive di cui al documento "*Elenco ADS autorizzati alle manutenzioni*".
12. Permettere attività manutentive da parte di soggetti non espressamente autorizzati dal Consorzio.

2.3 Protezione dei sistemi da intrusioni informatiche

Il sistema informatico del Consorzio è protetto contro le intrusioni e gli attacchi volti a renderlo insicuro o non disponibile, attraverso i seguenti sistemi di difesa:

- Firewall
- Antivirus/antimalware
- Content filtering

2.3.1 Firewall

Per stabilire efficaci controlli di sicurezza della rete consortile il Consorzio è dotato di un sistema Firewall quale sistema di difesa perimetrale atto a proteggere i sistemi e le informazioni attestati sulla rete stessa. In particolare:

- tutti gli utenti della rete sono identificati e le loro autorizzazioni di accesso sono puntualmente censite;
- vengono adottate opportune policy in base agli utilizzi autorizzati (l'accesso a ogni singola risorsa avviene in conformità alle specifiche necessità collegate alle mansioni dei singoli);
- i dati e i sistemi sono segregati in aree separate della rete consortile, in base al loro livello di criticità.

Sul dispositivo Firewall sono stati attivati appositi blocchi atti a respingere, fra gli altri, anche eventuali attacchi informatici provenienti dal web, aventi come bersaglio i sistemi e i servizi consortili esposti su Internet, a garanzia della continuità operativa degli stessi. Quotidianamente viene inviato agli Amministratori di sistema un rapporto sintetico delle sole attività illecite rilevate e del traffico cumulato, mentre tutte le attività di navigazione effettuate dai singoli utenti vengono archiviate in modo sicuro previa anonimizzazione e pseudonimizzazione, garantendo la privacy dei dipendenti ma consentendo nel contempo l'effettuazione di indagini e attività di informatica forense in caso di necessità.

2.3.2 Protezione dei PC

Tutti i PC in dotazione ai dipendenti presentano la cifratura dei dati archiviati in locale tramite crittografia del disco rigido attuata mediante tecnologia "BitLocker" di Microsoft, atta ad impedire l'accesso alle informazioni in esso contenuti da parte di soggetti terzi non autorizzati nel caso di smarrimento o sottrazione dei dispositivi.

Inoltre, i documenti di ogni singolo utente risultano sincronizzati con il proprio spazio cloud "OneDrive" riservato su "SharePoint" di Microsoft 365, il quale risulta dotato di algoritmi di protezione e ripristino in caso di attività anomale rilevate (modifica, eliminazione, ecc.), permettendo in tal modo la protezione, l'accesso e il recupero dei dati da parte degli utenti anche da altre postazioni qualora risulti impossibile accedere ai propri PC, a garanzia della continuità operativa.

Sulle postazioni di lavoro risulta installato apposito software di sicurezza che consente di effettuare la gestione granulare dei privilegi consentiti agli utenti, bloccando l'esecuzione di qualsiasi processo con privilegi elevati, ad eccezione di quelli preventivamente autorizzati dagli Amministratori di sistema in quanto conformi alle politiche previste in tema di utilizzo dei software e di sicurezza informatica. In tal modo risulta possibile bloccare e prevenire malware che potrebbero danneggiare e compromettere la conformità dei dati e la sicurezza informatica dell'intera infrastruttura informatica.
Limitatamente ai PC in uso ai tecnici che devono poter intervenire anche in condizioni di emergenza sui sistemi PLC degli impianti elettromeccanici telecontrollati, nonché del personale dell'Area Ricerca e Sviluppo agronomico ritenuto assolutamente affidabile, sono stati creati appositi profili di configurazione atti a garantire una maggiore flessibilità all'utente nell'esecuzione dei software anche non preventivamente autorizzati, mantenendo tuttavia la possibilità da parte degli Amministratori di sistema di effettuarne il controllo di conformità ex-post, a tutela del rispetto delle politiche definite.
Le postazioni di lavoro risultano inoltre controllate tramite apposito software di gestione che monitora e controlla costantemente il rispetto dei criteri di sicurezza impostati in tema di installazione di patch e aggiornamenti del sistema operativo e dei software installati, nonché l'esecuzione da remoto di attività di monitoraggio delle periferiche hardware e dei log di sistema, utili in caso di indagini di informatica forense.
Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico consortile mediante virus o mediante ogni altro software aggressivo.
Qualora il software antivirus rilevasse la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso spegnendo il computer e avendo cura di segnalare prontamente l'accaduto agli Amministratori di sistema per l'attivazione delle contromisure necessarie a impedire compromissioni dei dati e della sicurezza dell'infrastruttura informatica.
Ogni dispositivo magnetico di provenienza esterna al Consorzio dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato ai referenti informatici interni. Si ricorda che i virus possono essere trasmessi tramite scambio di file via Internet, via e-mail, scambio di supporti removibili, filesharing, chat, ecc.

Inoltre, all'utente:

1. È vietato accedere alla rete consortile senza servizio antivirus attivo e aggiornato sulla propria postazione, salvo esplicita indicazione degli Amministratori di sistema.
2. È vietato interferire con le attività dell'antivirus consortile.
3. È vietato disattivare l'antivirus e i software di protezione senza l'autorizzazione espressa degli Amministratori di sistema, anche e soprattutto nel caso ciò sia richiesto per l'installazione di software sul computer.

4. È vietato aprire messaggi e-mail provenienti da mittenti sconosciuti o di dubbia provenienza, con oggetti o testi inspiegabili o in qualche modo strani e, soprattutto, cliccare su collegamenti o accedere agli eventuali allegati, provvedendo in caso di ragionevole dubbio a contattare il Responsabile informatico interno e gli Amministratori di sistema prima di intraprendere qualsiasi azione deliberata.
5. Contattare i soli dipendenti autorizzati con funzione di amministrazione di sistema, il cui elenco è consultabile sul documento "*Elenco ADS autorizzati alle manutenzioni*", prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra esposto.

2.3.3 Content filtering

I sistemi di content filtering installati assicurano la protezione da:

- accessi a siti web potenzialmente pericolosi o indesiderati;
- spamming di posta elettronica;
- file pericolosi o indesiderati (eseguibili, filmati, musica, etc.).

Per quanto riguarda l'accesso a siti web, il servizio di Content Filtering è attuato nell'ambito del dispositivo firewall di rete perimetrale.

Tutti i messaggi di posta elettronica vengono preventivamente filtrati tramite apposite piattaforme di sicurezza atte a bloccare i messaggi in arrivo che presentino contenuti ritenuti potenzialmente pericolosi in quanto veicolanti malware attraverso allegati e link a siti malevoli. Successivamente le e-mail recapitate nelle cassette postali dei singoli utenti vengono altresì vagliate dai sistemi di protezione previsti da Outlook di Microsoft 365.

3 SEZIONE III – USO DI ALTRI DEVICE (NOTEBOOK, TABLET, CELLULARE, SMARTPHONE E ALTRI DISPOSITIVI ELETTRONICI)

3.1 L'utilizzo di notebook, tablet o smartphone

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobili") possono essere concessi in uso dal Consorzio ai soggetti autorizzati per ragioni di servizio.

L'autorizzato è responsabile dei device mobili assegnatigli dall'organizzazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai device mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sugli stessi prima della riconsegna. Coloro che hanno in dotazione il device mobile dovranno inserire un codice di sblocco allo stesso, in modo da impedire l'accesso da parte di terzi.

All'interno dei device consortili è autorizzata la conservazione di documenti scaricati come allegati (e-mail, instant messaging, ecc.) il cui contenuto sia di carattere professionale esclusivamente per il tempo strettamente necessario.

Si raccomanda la massima attenzione nell'utilizzo di applicazioni sul proprio dispositivo, in relazione all'eccessivo consumo di traffico dati e alla sicurezza del proprio apparato. Per prevenire eventuali abusi potrà essere prevista una verifica periodica sulla quantità totale del traffico dati generato da ogni utenza.

Si richiede particolare attenzione e buon senso nell'installare applicazioni in quanto alcune di esse potrebbero danneggiare il device dato in dotazione (esempio: virus, ecc.).

Al soggetto autorizzato è vietato lasciare i device mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e/o altri luoghi accessibili al pubblico.

In caso di perdita o furto dei device mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente (entro le 24 ore) l'ente che provvederà – se del caso – a occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l'orario di lavoro, al soggetto autorizzato non è consentito lasciare incustoditi i device mobili.

Il soggetto autorizzato non dovrà mai utilizzare i dispositivi mobili consortili per utilizzi personali, salvo diversa autorizzazione da parte della Direzione generale, in ogni caso senza aggravio di costi per il Consorzio e sotto la personale responsabilità dell'utilizzatore.

Sul dispositivo mobile personale (ovvero non di proprietà consortile) è fatto divieto di installare app o software istituzionali o altrimenti utilizzati per ragioni lavorative, posta elettronica istituzionale compresa, né conservare, scaricare, mantenere o accedere a dati, file e documentazione consortile.

Le condizioni specifiche di utilizzo dei device sono definite nell'atto di consegna del device.

Di seguito vengono elencate brevemente le condizioni generali per l'utilizzo dei device consortili:

1. Non potranno essere utilizzati dal dipendente per uso personale.
2. La concessione del device consortile potrà essere recisa unilateralmente e discrezionalmente dal Consorzio. Tale decisione dovrà essere comunicata al dipendente con almeno 15 (quindici) giorni di preavviso rispetto alla decorrenza operativa.
3. In caso di cessazione del rapporto di lavoro o di consulenza del soggetto autorizzato con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'ente, della permanenza dei presupposti per l'utilizzo del device consortile, a prescindere dalla motivazione il device mobile dovrà essere restituito al Consorzio a seguito di formale richiesta dello stesso (senza preavviso).
4. I device mobili saranno utilizzati esclusivamente per svolgere attività autorizzate e consentite dalla legislazione vigente. Qualora il Consorzio venisse a conoscenza di usi illegittimi degli stessi, provvederà a farne segnalazione alle autorità competenti. Eventuali spese per sanzioni o altro derivanti dalla violazione delle norme di comportamento sono a carico del dipendente. Tale comportamento attiverà le apposite procedure disciplinari ai sensi dei CC.CC.NN.LL. di riferimento.

3.2 Memorie esterne (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.) e cloud

Considerato che i dispositivi di memorizzazione esterna rappresentano un elemento di criticità dal punto di vista della sicurezza informatica, il Consorzio ne limita l'utilizzo ai soli casi in cui non sia possibile utilizzare gli altri strumenti di condivisione disponibili con la piattaforma Microsoft 365, previa autorizzazione della Direzione generale. Pertanto, ai soli soggetti autorizzati può essere consentito l'utilizzo di un dispositivo di memorizzazione esterna di proprietà consortile (quale una chiave USB, un hard disk esterno, una memory card, ecc.), preventivamente crittografata dagli Amministratori di sistema qualora compatibile con la tipologia di utilizzo, su cui copiare temporaneamente dei dati per un facile trasporto o per altri usi (es. macchine fotografiche con memory card, videocamere con dvd, ecc.).

Questi dispositivi, che devono essere gestiti con le stesse accortezze di cui all'articolo precedente, devono essere utilizzati esclusivamente dalle persone a cui sono stati affidati e, in nessun caso, devono essere consegnati a terzi. L'eventuale sottrazione o lo smarrimento devono essere immediatamente comunicati ai referenti informatici e privacy per le verifiche del caso.

Ai soggetti autorizzati è fatto divieto di utilizzo, per ragioni lavorative, di sistemi di archiviazione cloud diversi da quelli che vengono messi a disposizione dal Consorzio.

3.3 Distruzione dei Device

Ogni device e ogni memoria esterna affidati agli autorizzati, (personal computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'ente che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento e le procedure interne adottate in tal senso.
In particolare, il Consorzio provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.
Il Consorzio provvederà inoltre a cancellare i dati contenuti nei device concessi in dotazione dallo stesso. Si raccomanda all'utente di riconsegnare i device depurati da ogni dato, anche personale, interno all'ambiente privato o a quello consortile.

3.4 Protezione dei sistemi da intrusioni informatiche

Oltre a quanto già indicato per i personal computer nel paragrafo 2.3, il Consorzio, attraverso una piattaforma di Mobile Device Management, gestisce in modo centralizzato tablet e smartphone, allo scopo di garantire che l'utilizzo degli stessi sia conforme alle policy consortili. Attraverso

l'installazione di un modulo client si sovrintende ad una serie di operazioni, quali, a titolo esemplificativo e non esaustivo:

- Semplificare la configurazione dei dispositivi, includendo eventuali antivirus;
- Consentire il download solo di app consentite;
- Localizzare un dispositivo smarrito, bloccando e cancellando da remoto i dati presenti;
- Rilevare le modifiche non autorizzate apportate al software di sistema;
- Rilevare se e-mail aziendali vengono inoltrate a domini di posta diversi da quelli autorizzati o se un allegato di posta viene spostato su una scheda rimovibile;

L'applicazione del Mobile Device Management di tablet e smartphone è subordinata alla preventiva adozione di uno specifico disciplinare contenente modalità operative e profili di autorizzazione, approvato dalla Direzione generale.

4 SEZIONE IV – GESTIONE DELLE CREDENZIALI DI ACCESSO E PASSWORD

4.1 Procedura di acquisizione delle credenziali

Gli account di accesso al PC vengono assegnati all'utente dal Legale Rappresentante, anche mediante assistenza resa dall'Amministratore di sistema, all'inizio dell'attività lavorativa.
Gli account sono dotati di credenziali univoche. L'account consortile prevede password di accesso di almeno 12 caratteri, complesse, a scadenza trimestrale e non ripetibili.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dall'Amministratore di sistema, associato a una parola chiave (password) riservata che dovrà essere custodita dal soggetto autorizzato con la massima diligenza e non divulgata. La parola chiave deve essere modificata dal dipendente al primo utilizzo dello strumento elettronico e, successivamente, ogni tre mesi.
Tale procedura sarà facilitata dalla richiesta automatica di modifica da parte del sistema.

4.2 Regole per un corretto utilizzo delle password

Di seguito vengono riportate le informazioni utili per una corretta gestione delle credenziali e per la realizzazione di una parola chiave sicura, in ottemperanza agli obblighi di legge previsti e alle best practices sul tema, anche comunitarie. Si ricorrerà all'uso di tali istruzioni anche per la gestione dei login relativi alla posta elettronica consortile e per tutti gli altri account adottati per finalità lavorative.
In fase di scelta della nuova parola chiave non si possono utilizzare le ultime cinque parole chiave utilizzate, in ordine di tempo, dal dipendente.

La parola chiave deve rispettare le seguenti caratteristiche:

- deve avere una lunghezza minima di 12 caratteri;
- deve contenere almeno una lettera maiuscola (insieme ad altre minuscole o viceversa);
- deve contenere almeno un numero oppure un carattere speciale, escluse lettere accentate;
- non deve contenere riferimenti ai propri dati personali o al nome utente;
- deve essere diversa da quella precedente.

Inoltre, il dipendente non deve:

- salvare la parola chiave in un file del computer;
- trascrivere la parola chiave su post-it;
- rivelare la parola chiave attraverso il telefono a nessuno;
- scrivere la parola chiave in un messaggio di posta elettronica;
- rivelare la parola chiave al superiore;
- parlare di parole chiave di fronte a terzi;
- dare indicazione in merito al formato e alla lunghezza della parola chiave;
- svelare la parola chiave su questionari o su formulari di sicurezza;
- rivelare la parola chiave ai membri della famiglia;
- digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'ente;
- annotare la propria password all'interno dell'ufficio o conservarla on-line;
- comunicare la propria password su questionari e/o moduli;
- utilizzare l'opzione "ricorda password" presente in alcuni programmi.

Invece il dipendente deve:

- in caso di dimenticanza e/o ripristino della password, inoltrare la richiesta agli Amministratori di sistema.

4.3 Gestione delle credenziali

La password assegnata dagli Amministratori di sistema, come precedentemente affermato, dovrà essere cambiata dal dipendente al primo utilizzo.
Le credenziali di autenticazione non utilizzate da almeno sei mesi verranno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Le credenziali sono disattivate anche in caso di perdita della qualità che consente al soggetto autorizzato l'accesso ai dati personali.

Qualora la parola chiave dovesse essere sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con gli Amministratori di sistema designati.
Si fa esplicito divieto di utilizzare strumenti di password manager, ad eccezione di quelli autorizzati dagli Amministratori di sistema

5 SEZIONE V – POSTA ELETTRONICA

5.1 La Posta Elettronica è uno strumento di lavoro

La casella di posta elettronica assegnata al dipendente è uno strumento di lavoro.
Gli utenti in possesso di una casella di posta elettronica consortile sono i diretti responsabili del corretto utilizzo di quest'ultima.
Non è permesso l'utilizzo del servizio di posta elettronica con dominio del Consorzio per scopi privati.
Il Consorzio è tuttavia consapevole che gli utenti possono decidere di utilizzare l'indirizzo di posta elettronica personale per limitati accessi; in questo caso si raccomanda al dipendente di cancellare immediatamente ogni messaggio personale, al fine di evitare eventuale e possibile salvataggio di informazioni personali sul PC o sui device consortili.
L'accesso alla posta elettronica è individuale e personale e può, quindi, avvenire soltanto attraverso l'inserimento delle credenziali di identificazione sincronizzate con quelle degli utenti di dominio, la cui password prevede pertanto analoga scadenza trimestrale.
L'accesso non può essere condiviso o ceduto a soggetti terzi.
Sebbene tutta la posta elettronica in entrata sia controllata da un software antispam è possibile che alcune e-mail di spam superino i filtri impostati sul sistema centrale. È quindi necessario prestare la massima attenzione a e-mail sospette, avvisando gli Amministratori di sistema in caso di dubbi sulla provenienza o sul contenuto delle stesse.
Quanto di seguito indicato è da intendersi applicabile anche all'utilizzo di indirizzi di posta elettronica di natura impersonale (tipo: info, amministrazione, personale, direzione operativa, ecc.). La creazione di questi indirizzi di posta da parte degli Amministratori di sistema deve essere autorizzata dalla Direzione.
In occasione della cessazione del rapporto di lavoro, salvo diverse indicazioni fornite dal Titolare del trattamento, l'e-mail del dipendente sarà disattivata dagli Amministratori di sistema il giorno successivo all'ultimo giorno lavorativo e, qualora richiesto dal Titolare medesimo, verrà predisposto un avviso automatico di chiusura dell'indirizzo e-mail, con segnalazione di un account istituzionale alternativo, rivolto a eventuali terzi (mittenti).
Le copie di sicurezza della casella di posta elettronica disattivata saranno conservate dal Consorzio per un massimo di trenta giorni, al termine dei quali la stessa sarà cancellata automaticamente. Per la durata di tale periodo le uniche persone autorizzate ad accedere al contenuto della casella

saranno gli Amministratori di sistema, specificatamente autorizzati dal Direttore generale e solo qualora intervengano circostanze tali da richiedere necessariamente l'accesso ad informazioni ivi contenute.

5.2 Garanzia della funzionalità del servizio di posta elettronica consortile

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (auto-reply). Nel caso in cui un dipendente si assenti senza aver provveduto ad attivare i suddetti sistemi di inoltro automatico, su richiesta della Direzione generale gli Amministratori di sistema potranno impostare tale messaggio di risposta automatica senza necessità di accesso alla casella di posta.
In alternativa, e in tutte le situazioni in cui sia necessario un presidio della casella e-mail per ragioni di operatività, il soggetto autorizzato deve nominare in forma scritta un collega fiduciario che, in caso di sua assenza, inoltri i file necessari a chi ne abbia urgenza.
Qualora il soggetto autorizzato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'organizzazione, mediante personale appositamente autorizzato, potrà verificare il contenuto dei messaggi di posta elettronica del soggetto autorizzato, informando l'autorizzato stesso e redigendo apposito verbale.
Tutti i messaggi ricevuti, spediti o salvati, potranno essere letti dal Direttore generale e dagli Amministratori di sistema esclusivamente per i seguenti motivi:

1. in situazione di assenza, per garantire una regolare continuità dell'attività lavorativa e solo in caso di necessità e urgenza;
2. segnalazioni di malfunzionamenti da parte del singolo utente;
3. fatti illeciti lesivi al patrimonio e/o immagine riscontrati precedentemente alla verifica;
4. controlli di sicurezza in caso di analisi di e-mail sospette.

In tutti questi casi il dipendente verrà preventivamente informato e, nei limiti del possibile, invitato a partecipare alle operazioni di accesso e selezione delle e-mail.

5.3 Comportamenti non consentiti

Non è consentito all'utilizzatore di posta elettronica:

1. Trasmettere messaggi a gruppi numerosi di persone (es. a tutto un ufficio o ad un'intera divisione) senza l'autorizzazione necessaria della Direzione generale.
2. Sollecitare donazioni di beneficenza o altri comportamenti non legati al lavoro.
3. Utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni al Consorzio informazioni riservate o comunque documenti istituzionali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte.

4. Utilizzare l'indirizzo di posta elettronica consortile per motivi non attinenti allo svolgimento delle mansioni assegnate.
5. Usare il servizio per scopi illegali, per inviare e ricevere materiale pornografico, osceno, volgare, diffamatorio, oltraggioso, discriminatorio, abusivo, pericoloso.
6. Utilizzare l'indirizzo di posta elettronica per la partecipazione a dibattiti, Forum o mailing-list su Internet per motivi non professionali; non è altresì consentito aderire o rispondere a messaggi che invitano ad inoltrare e perpetuare verso ulteriori indirizzi e-mail contenuti o documenti oggetto delle cosiddette "Catene di S. Antonio" (nel caso di ricezione di messaggi di tale tipo si invita a darne comunicazione immediata agli Amministratori di sistema; non si dovrà in alcun caso procedere all'apertura degli allegati di tali messaggi).
7. Effettuare ogni genere di comunicazione finanziaria, ivi comprese le operazioni di remote-banking, acquisti on-line e simili, salvo diversa ed esplicita autorizzazione della Direzione.
8. Simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta non proprie per l'invio di messaggi.
9. Prendere visione della posta altrui.
10. Aprire allegati di posta elettronica ambigui o di incerta provenienza (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati).
11. Modificare la configurazione hardware e software del dispositivo assegnato; né utilizzare sistemi client di posta elettronica non conformi a quelli accettati dal Consorzio.
12. Utilizzare crittosistemi o qualsiasi altro programma di sicurezza e/o crittografia, esclusi quelli esplicitamente previsti dagli Amministratori di sistema.
13. Trasmettere a mezzo posta elettronica dati sensibili, personali e/o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento e della protezione dei dati.
14. Inviare, anche all'interno della rete consortile, materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, libertà religiosa, libertà sessuale o manifestazione del pensiero, anche politico. Qualora il collaboratore riceva messaggi aventi tale contenuto è tenuto a cancellarli immediatamente e a darne comunicazione agli Amministratori di sistema.
15. Qualora il soggetto autorizzato dovesse ricevere messaggi aventi contenuti non autorizzati esposti nei precedenti punti, è tenuto a cancellarli immediatamente e a darne comunicazione al Consorzio, nello specifico al Referente Privacy ai contatti di cui in premessa.
16. Installare, accedere o altrimenti utilizzare il servizio di posta elettronica consortile (anche webmail) tramite device diversi da quelli istituzionali.

5.4 Gestione degli indirizzi di posta elettronica

Le caselle personali degli indirizzi di posta elettronica sono assegnate dagli Amministratori di sistema e hanno la nomenclatura immodificabile.
La “personalizzazione” dell’identificativo non comporta la sua “privatezza”, in quanto si tratta di strumenti di esclusiva proprietà consortile, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.
I messaggi inviati tramite posta elettronica istituzionale (di servizio e/o nominativi) dovranno contenere un testo che si componga di firma specifica del soggetto a cui si riferisce, unitamente al seguente disclaimer privacy:

La comunicazione appena ricevuta proviene da un indirizzo di posta elettronica ad esclusivo uso professionale. Le informazioni contenute in questa e-mail e negli eventuali allegati sono riservate e destinate esclusivamente alla persona sopraindicata. Si notifica a chi legge il presente avviso – se non è l’effettivo destinatario o se la presente comunicazione è pervenuta per errore – che è proibito leggere, copiare, usare o diffondere il contenuto di questa e-mail e degli eventuali documenti allegati senza autorizzazione ai sensi dell'art. 616 del c.p. e ai sensi del Reg. UE n.679/2016 (GDPR). Se la e-mail in oggetto è stata ricevuta per errore, si prega di cancellare e distruggere tutte le copie esistenti e di informare il mittente dell’accaduto.
Si ringrazia anticipatamente per la collaborazione.

5.5 Posta elettronica certificata nominativa

La Direzione generale può assegnare ai dipendenti anche una casella di posta elettronica certificata nominativa, in ragione di determinate mansioni lavorative. Per le caselle di posta elettronica certificata nominative si applicano tutte le disposizioni di cui ai paragrafi precedenti.

5.6 Caselle di posta elettronica del Consorzio

Il Consorzio è dotato anche di caselle di posta elettronica, ordinaria e certificata, per garantire il flusso di comunicazioni in entrata e in uscita e per la funzionalità del portale gare telematiche. Le credenziali per l’utilizzo delle suddette caselle di posta, oltre che agli Amministratori di sistema autorizzati che ne necessitano per garantire il corretto funzionamento del sistema di gestione documentale e del portale delle gare telematiche, sono assegnate ai soli dipendenti incaricati dalla Direzione generale, i quali devono custodirle con la massima attenzione rispettando l’assoluto divieto di condividerle con altri.

6 SEZIONE VI – INTERNET

6.1 Internet è uno strumento di lavoro

L’accesso a Internet (tramite PC, tablet o smartphone consortili) è fornito allo scopo di consentire l’accesso ad eventuali informazioni e contenuti necessari allo svolgimento dell’attività lavorativa. Essendo uno strumento di lavoro, gli utenti a cui si attribuisce l’accesso a Internet sono responsabili del suo corretto utilizzo. La connessione alla rete Internet dal device avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell’attività lavorativa. L’utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.
L’utente si impegna a non cedere, una volta superata la fase di autenticazione, l’uso del proprio dispositivo personale a soggetti non autorizzati, in particolar modo per quanto riguarda l’accesso a Internet e ai servizi di posta elettronica.
Di qualsiasi azione o attività svolta utilizzando il codice identificativo o la password assegnata è responsabile l’utente assegnatario del codice.
I dispositivi di accesso alla rete sono preventivamente individuati e assegnati personalmente a ciascun utente; il collegamento alla rete da un dispositivo diverso da quello assegnato avviene solo in caso di esigenze di servizio preventivamente autorizzate dagli Amministratori di sistema (ad es. utente assegnato a diverse sedi di lavoro) e con l’utilizzo della copia ID utente e password personali.
Eventuali controlli, compiuti dagli Amministratori di sistema, potranno avvenire mediante un sistema di analisi dei contenuti o mediante “file di log” della navigazione svolta nel rispetto delle modalità indicate nel successivo paragrafo 8.2.
Per prevenire abusi nell’uso di Internet il sistema è provvisto di filtri d’accesso.
Eventuali ospiti che abbiano bisogno di utilizzare la rete Internet possono chiedere agli Amministratori di sistema la password della “rete guest” del Consorzio.
Il Consorzio potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all’attività lavorativa attraverso filtri e black list.

6.2 Comportamenti non consentiti concernenti l’utilizzo di Internet

È vietato utilizzare l’accesso a Internet in violazione delle norme in vigore nell’ordinamento giuridico italiano a tutela del diritto d’autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248).
È vietato accedere a siti Internet mediante azioni inibenti i filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dal Consorzio per bloccare accessi non conformi all’attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine.

Di seguito vengono riportate le attività che non sono consentite:

1. Scaricare materiale e programmi in violazione della legislazione sui diritti di autore, appartenenti a persone o aziende, coperti da copyright, brevetto o proprietà intellettuale, ivi compresa l'installazione o la distribuzione di software che non siano specificatamente licenziati per essere utilizzati all'interno del Consorzio.
2. Entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato.
3. Compiere attività che appesantiscano il traffico o i servizi sulla rete e possano causare disturbi al sistema senza valutarne adeguatamente le conseguenze.
4. Utilizzare modem personali o utilizzare qualunque altro dispositivo "Internet-Key" con account personali.
5. Installare o distribuire software che non siano specificatamente licenziati per essere utilizzati all'interno del Consorzio.
6. Navigare su siti e scaricare materiali pericolosi/vietati o aventi contenuti illegali.
7. Effettuare copia non autorizzata di materiale coperto da copyright, comprese la digitalizzazione e la distribuzione di foto da riviste, libri o altre fonti, musica o materiale video.
8. Condividere file in modalità peer-to-peer.
9. Scaricare programmi, anche se privi di licenza o in prova (freeware e shareware), se non in caso di espressa autorizzazione da parte degli Amministratori di sistema. Si ricorda infatti che eseguire il download di file da Internet è un'operazione intrinsecamente pericolosa in quanto può essere il veicolo per l'introduzione di virus e malware.
10. Immettere sulla rete o sui server software dannosi per i sistemi o comunque non autorizzati.
11. Utilizzare l'infrastruttura tecnologica consortile per procurarsi e diffondere materiale in violazione delle normative vigenti.
12. Effettuare attività che possano generare problemi di sicurezza o danneggiare le comunicazioni sulla rete.
13. Eseguire qualsiasi forma di monitoraggio della rete che permetta di catturare dati non espressamente inviati all'host dell'utente (sniffing) a meno che questa attività non faccia parte dei compiti dell'utente e sia quindi formalmente autorizzata dalla Direzione.
14. Aggirare le procedure di autenticazione o la sicurezza di qualunque host, rete, account.
15. Accedere a siti Internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
16. Effettuare transazioni finanziarie ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto.

17. Partecipare a forum non professionali, utilizzare chat line e bacheche elettroniche, partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list non professionali spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa.
18. Memorizzare documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
19. Promuovere guadagno personale attraverso l'uso di Internet o della posta elettronica consortile.
20. Accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'ente stesso.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet nonché un possibile illecito trattamento di dati personali e sensibili, è posta sotto la personale responsabilità del soggetto autorizzato inadempiente.

6.3 VPN

Il collegamento alla rete consortile da remoto attraverso VPN (Virtual Private Network) è autorizzato dal Responsabile del trattamento, con richiesta agli Amministratori di sistema, per esigenze di lavoro nelle modalità previste dal Consorzio. Per motivi di sicurezza tutti gli accessi realizzati dagli utenti da remoto attraverso VPN sono registrati.
Il Consorzio assegna ai soggetti autorizzati esclusivamente VPN univoche.

6.4 Interruzione e cessazione del servizio di posta elettronica e di accesso a Internet

Eventuali interruzioni del servizio sono comunicate agli utenti. Ai sensi del presente Regolamento, l'utilizzo del servizio di accesso a Internet e di utilizzo di posta elettronica cessa d'ufficio nei seguenti casi:

1. Se non sussiste più la condizione di dipendente o collaboratore autorizzato o non è confermata l'autorizzazione all'uso.
2. Se è accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali.
3. Se il Consorzio sospetta manomissioni e/o interventi sull'hardware e/o sul software dell'utente impiegati per la connessione, compiuti da personale non autorizzato.
4. In caso di diffusione o comunicazione, imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo IP e altre informazioni tecniche riservate.

5. In caso di accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale, al sito contattato.
6. In caso di concessione di accesso a Internet diretta o indiretta, a qualsiasi titolo, da parte dell'utente a terzi.
7. In caso di violazione e/o inadempimento imputabile all'utente di quanto stabilito nei precedenti punti.
8. In ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente.

6.5 Connessione alla rete da esterno

L'accesso alla rete consortile dall'esterno è possibile mediante apposito gateway opportunamente configurato dagli Amministratori di sistema, previo inserimento delle proprie credenziali di dominio.
Una volta inserite le credenziali si viene proiettati sulla rete consortile con le medesime limitazioni presenti in caso di accesso dall'interno.

7 SEZIONE VII – GESTIONE DATI, CARTACEI E NON

La presente sezione si ritiene integrata dalle "*Istruzioni alle persone autorizzate al trattamento*" adottate dal Consorzio e rilasciate ai dipendenti.

7.1 Gestione dei dati personali e istituzionali

Il trattamento di qualunque dato e informazione deve prevedere, da parte del collaboratore autorizzato, ogni ragionevole misura per assicurare che tali dati e informazioni rimangano invariati.
I dati e le informazioni potranno essere comunicati a terze parti esclusivamente nell'ambito delle proprie attività lavorative.

7.2 Istruzioni operative per la sicurezza dei dati

Sicurezza significa anche integrità, esattezza e aggiornamento dei dati, nonché trattamenti leciti e conformi alle finalità della raccolta.
Di seguito alcuni suggerimenti relativi al trattamento dei dati:

1. Non procedere alla raccolta e al trattamento dei dati senza che sia stata fornita previamente l'informativa all'interessato o alla persona presso cui si raccolgono i dati, come previsto dall'articolo 13 del GDPR.
2. Procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi.

3. Procedere all’aggiornamento dei dati, ove necessario.
4. Non lasciare memorie esterne, fogli e cartelle e quant’altro a disposizione di estranei.
5. Accedere ai soli dati, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di autorizzazione.
6. Conservare in archivi (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave documenti o atti che contengono dati sensibili o giudiziari, ai sensi dell’art. 4, comma 1 lettere d) ed e) del Codice della Privacy.
7. Conservare in archivi muniti di serratura i supporti non informatici che riproducono dati particolari (sensibili e giudiziari).
8. Spegnere sempre il device a fine giornata lavorativa tranne necessità di accesso da remoto.
9. Qualora si dovessero riscontrare difformità dei dati trattati o nel funzionamento degli elaborati, comunicare la circostanza al Titolare.
10. Non fornire dati o informazioni di carattere sanitario per telefono se non si ha certezza assoluta dell’identità del destinatario.
11. Evitare di inviare via fax documenti in chiaro contenenti dati sanitari: in questo caso si suggerisce di comunicare un codice identificativo del soggetto interessato e quindi inviare la copia della comunicazione contrassegnata dal codice, senza il nominativo dell’interessato.
12. Qualora giungano richieste telefoniche di dati personali da soggetti terzi, chiedere la trasmissione di domanda formale a mezzo pec.
13. I documenti cartacei non più utilizzati devono essere distrutti, o comunque resi illeggibili, prima di essere eliminati o cestinati.
14. Fare pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

7.3 Comportamenti non consentiti

Il soggetto autorizzato al trattamento non deve:

1. Divulgare o comunicare a terzi non autorizzati dati, informazioni, atti, documenti riservati (in qualunque forma) senza espressa autorizzazione del proprio Responsabile e/o della Direzione.
2. Svolgere attività di trattamento di dati e informazioni in qualunque formato (comunicazione, modifica, copia, cancellazione, fornitura ad esterni, video, audio e foto, ecc.) non autorizzata e concordata con il proprio Responsabile del trattamento.

3. Pubblicare in Internet (social media, forum, chat, blog, siti Internet) dati e informazioni di carattere istituzionale non autorizzati e concordati con la Direzione.
4. Salvare dati e informazioni in sistemi cloud (per esempio Dropbox, Google+, Evernote, ecc..) non autorizzati dagli Amministratori di sistema. Sarà la Direzione, in collaborazione con gli Amministratori di sistema, ad individuare le piattaforme cloud ritenute idonee.

8 SEZIONE VIII – APPLICAZIONE E CONTROLLO

8.1 Il controllo

Il Consorzio, in qualità di titolare degli strumenti informatici e dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:
1. Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.
2. Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
3. Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assessment del sistema informatico. Per tali controlli il Consorzio si riserva di avvalersi anche di soggetti esterni.
Si precisa, in ogni caso, che l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.
L'ente informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevano o trasmettano comunicazioni elettroniche di natura personale o privata.
In particolare, eventuali sistemi atti a monitorare violazioni di legge o comportamenti anomali da parte degli autorizzati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

8.2 Modalità di verifica

Gli Amministratori di sistema, utilizzando il proprio login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) sia ai server consortili nonché, previa comunicazione al dipendente, ai computer e device in dotazione, anche da remoto, per effettuare i controlli menzionati al punto 8.1.

Il predetto personale autorizzato ha la facoltà di collegarsi e visualizzare da remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa, nonché la massima sicurezza contro virus, spyware, malware, ecc.
Tale intervento può essere richiesto dal soggetto autorizzato oppure svolto direttamente su iniziativa degli Amministratori di sistema qualora fossero questi ultimi ad individuare un problema nel sistema informatico o telematico.
In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, all'utente verrà data comunicazione dell'operazione.

I controlli, anche saltuari od occasionali, saranno svolti in conformità della legge sia per eseguire verifiche sulla funzionalità e sicurezza del sistema sia per verificare il corretto utilizzo, da parte dei dipendenti, tanto della rete Internet che della posta elettronica nel rispetto delle modalità indicate successivamente.

Nell'esercizio del potere di controllo il Consorzio si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo, rispettando le procedure di informazione/consultazione e informando preventivamente i lavoratori dell'esistenza di dispositivi di controllo atti a raccogliere i dati personali.

I controlli si svolgeranno in forma graduata:

- In via preliminare il Consorzio provvederà ad eseguire controlli su dati aggregati, riferiti all'intera struttura lavorativa ovvero a sue aree, e dunque verrà eseguito un controllo anonimo che può concludersi con un avviso generalizzato relativo a un rilevato utilizzo anomalo degli strumenti consortili e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
- In assenza di successive anomalie non si effettueranno controlli su base individuale.
- Nel perdurare delle anomalie si procederà a controlli su base individuale o per postazioni di lavoro e, in caso di abusi singoli e reiterati, verranno eseguiti 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 sicurezza del sistema – e le relative modalità, inoltrando preventivi avvisi collettivi o individuali).
- In caso di utilizzo indebito di posta elettronica e rete Internet, o di riscontrato e reiterato uso non conforme delle risorse informatiche, gli Amministratori di sistema segnaleranno il comportamento al responsabile dell'area di appartenenza del collaboratore, il quale attiverà la segnalazione per l'avvio del procedimento disciplinare.

Per il personale non dipendente, a cui non sono applicabili i CC.CC.NN.LL., il comportamento andrà segnalato alla Direzione per l'adozione degli atti di specifica competenza.

8.3 Modalità di Conservazione

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente e automaticamente i dati personali relativi agli accessi a Internet e al traffico telematico la cui conservazione non sia necessaria. Queste informazioni sono conservate per sette giorni.
Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione a:

1. Esigenze tecniche o di sicurezza del tutto particolari.
2. Indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria.
3. Obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate e deve essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, ai compiti e alle finalità già esplicitati.

9 SEZIONE IX – GESTIONE DEGLI SPAZI CONSORTILI E NORME DI CONDOTTA

9.1 Accesso agli uffici e alle aree protette

L'accesso agli uffici del Consorzio è permesso solo a personale espressamente autorizzato per precise e motivate finalità lavorative.
L'utilizzo della postazione di lavoro e il conseguente accesso a documenti, atti e archivi è consentito nei limiti della propria mansione. Terminata la giornata di lavoro e/o in periodi di assenza non devono essere lasciati visibili documenti e atti riservati, con particolare riferimento a quelli contenenti dati e informazioni di natura sensibile e/o riservati. Pertanto, si fa richiamo alla "politica della scrivania pulita", chiedendo agli autorizzati di trattare dati cartacei solo se necessario e privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dall'ente.
I principali benefici di una politica della scrivania pulita sono:

1. Il decoro della sede consortile.
2. La riduzione della possibilità che informazioni confidenziali siano viste da persone non abilitate a conoscerle.
3. La riduzione della possibilità che documenti confidenziali siano sottratti all'ente.

9.2 Utilizzo di Stampanti e FAX

Ogni utente che mandi in stampa documentazione riservata dovrà rapidamente entrarne in possesso, per far sì che il materiale riservato non sia oggetto di interesse altrui.
Pertanto, si chiede agli utenti di mantenere il più stretto riserbo relativamente alle informazioni acquisite da stampe prodotte da altri.
Anche la stampante deve essere considerata un dispositivo a uso professionale, per questo motivo si deve limitare l'invio della stampa di materiale personale. Tutti gli strumenti consortili devono essere sempre utilizzati per fini lavorativi.

10 SEZIONE X – BACKUP

Le copie di sicurezza dei documenti e database, archiviate sul file server attestato nel datacenter Lepida di Ravenna (loc. Bassette), nonché dei dati residenti su piattaforma Microsoft 365 (caselle e-mail, OneDrive, SharePoint), vengono effettuate giornalmente su dispositivo NAS on premise custodito dal Consorzio di Bonifica della Romagna presso il data center della sede di Rimini (Via Gugliemo Oberdan, 21) e replicate su analogo sistema di archiviazione installato presso il datacenter di Ravenna (Via Angelo Mariani, 26). Il software di backup consente di effettuare controlli di conformità dei dati onde garantirne la sicurezza. In caso di variazioni, queste verranno inserite in apposita appendice al presente Regolamento o nel disciplinare tecnico di cui al paragrafo 3.4.

11 SEZIONE XI – SOGGETTI PREPOSTI AL TRATTAMENTO E RESPONSABILI

11.1 Individuazione dei Soggetti autorizzati e dei Responsabili

I soggetti preposti agli specifici trattamenti dei dati vengono autorizzati a svolgere solo operazioni strettamente necessarie al perseguimento delle finalità legate allo svolgimento della loro attività lavorativa.
Nessuno dei Responsabili del trattamento con funzioni di amministratore di sistema *individuati in alcuni dei fornitori esterni del Consorzio* ha facoltà di operare un controllo diretto sui dati personali dei dipendenti del Consorzio.
I soggetti che operano quali amministratori di sistema, o le figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, svolgono un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni.

11.2 Modalità di Esercizio dei diritti

Gli interessati hanno il diritto di ottenere dal Consorzio, nei casi previsti, l'accesso ai dati personali e la rettifica, la cancellazione degli stessi, la limitazione del trattamento che li riguarda oppure di opporsi al trattamento (artt. 15 e ss. del Regolamento UE 2016/679).
Il Consorzio si è dotato di specifico Regolamento in tema di diritti degli interessati, disponibile all'indirizzo https://consorziocer.it/it/amministrazione-trasparEnte/altri-contenuti/.
Nella stessa sezione del sito internet del Consorzio è disponibile idonea modulistica per presentare istanza, da indirizzare al Consorzio CER agli indirizzi di posta elettronica ordinaria cer@consorziocer.it oppure a quello di posta certificata cer@pec.consorziocer.it.

11.3 Infrazioni disciplinari

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal Legale Rappresentante e dai vigenti CC.CC.NN.LL., nonché con tutte le azioni civili e penali consentite.