Garda Chiese
consorzio di bonifica

Corso V. Emanuele II, 122 - 46100 MANTOVA
Telefono 0376321278 email: info@gardachiese.it
PEC: cb.gardachiese-bonifica@pec.regione.lombardia.it
Codice Fiscale: 01706580204

REGOLAMENTO SULL'UTILIZZO DI STRUMENTI INFORMATICI, STRUMENTI DI TELEFONIA MOBILE, INTERNET E POSTA ELETTRONICA

Approvato dal Consiglio di Amministrazione con delibera n. 109 del 22/03/2024

Sommario

Art. 1 - Oggetto

Il presente Regolamento disciplina l'utilizzo di strumenti informatici, di telefonia mobile, di internet e posta elettronica all'interno del Consorzio di bonifica Garda Chiese.

La progressiva diffusione delle tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone il Consorzio e gli utenti a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando potenziali problemi alla sicurezza ed all'immagine dell'Ente stesso.

L'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro. Il Consorzio di Bonifica Garda Chiese adotta il presente Regolamento interno diretto ad evitare anche comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Il regolamento si applica a ciascun "utente", ovvero chiunque sia in possesso di specifiche credenziali di autenticazione al dominio, al Cloud e alla mail o disponga di dispositivi aziendali: allo stato attuale sono utenti tutti i dipendenti del Consorzio, senza distinzione di ruolo e/o livello e il presidente.

Art. 2 - Entrata in vigore del regolamento e pubblicità

Il presente regolamento entrerà in vigore il giorno di pubblicazione della delibera di approvazione.

Copia del regolamento viene consegnata a tutti gli interessati e illustrata mediante idonei incontri di formazione.

Art. 3 – Il servizio ICT

All'interno del Consorzio, nell'ambito dello Staff della Direzione Generale, è definito il servizio *Information and Communication Tecnology* (nel seguito per brevità "Servizio ICT") (i responsabili sono i sigg.rri Stefano Balestra e Matteo Peretti), che:

- gestisce la funzionalità di tutti i dispositivi e delle infrastrutture di rete;

- monitora la sicurezza dei dispositivi e degli accessi remoti (cyber security);

- gestisce il Clouding e l'interazione con sistemi terzi;

- gestisce l'hosting del sito www.gardachiese.it tramite fornitori terzi;

- fornisce il necessario supporto agli utenti per il corretto utilizzo di tutti gli strumenti.

Il servizio ICT è autorizzato a compiere interventi nel sistema informatico diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento dei sistemi operativi e delle patch di sicurezza, manutenzione dell'infrastruttura di rete e collegamento ad Internet, etc.). Detti interventi potranno anche comportare l'accesso in occasione dei controlli necessari ai fini della corretta manutenzione ed uso degli strumenti elettronici: ciò consentirà l'eventuale accesso ai dati residenti su ciascun dispositivo. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività del Consorzio, si applica anche in caso di assenza prolungata od impedimento dell'utente.

Il servizio ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole stazioni di lavoro al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata e/o autorizzazione dell'utente o, in caso di oggettiva necessità ed urgenza, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Art. 4 - Utilizzo degli strumenti di lavoro

Gli strumenti di lavoro (dispositivi fissi e mobili ed infrastrutture di rete, compresi gli accessi remoti ed il Cloud) affidati a ciascun utente sono da intendersi come strettamente connessi alla propria funzione.

I dati risiedono nel Cloud al quale è possibile accedere con sistemi di accesso sicuro (VPN) con dispositivi aziendali. L'accesso alla rete aziendale ed agli strumenti presenti presso gli uffici (ad es. stampanti, plotter, NAS, etc.) è legato al riconoscimento dell'utente su dominio tramite le singole credenziali assegnate.

Gli strumenti di lavoro devono essere custoditi con cura evitando ogni possibile forma di danneggiamento, di manomissione o esposizione al rischio.

Non è consentita l'installazione di programmi dannosi o con licenze non ufficiali.

L'inosservanza della presente disposizione espone il Consorzio a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

Salvo preventiva espressa autorizzazione del personale del Servizio ICT, non è consentito all'utente apportare modifiche strutturali sul dispositivo: le stesse potrebbero arrecare danni al dispositivo, alla sua funzionalità o alla sua sicurezza.

Ogni utente deve prestare la massima attenzione all'utilizzo in sicurezza dei supporti di origine esterna (chiavette usb, hard disk, etc.), non collegandoli a strumenti non aziendali ed avvertendo immediatamente il personale del Servizio ICT nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo articolo 110 del presente Regolamento relativo alle procedure di protezione antivirus.

Gli smartphone sono da intendersi come dispositivi usb esterni. L'azione di collegarli alle porte usb del dispositivo aziendale al fine di ricaricarne la batteria espone quest'ultimo ad un rischio informatico. Si invita pertanto ad utilizzare i dispositivi assegnati con la funzione di caricabatterie.

I dispositivi mobili non dovranno essere lasciati negli uffici in caso di programmate assenze prolungate.

Art. 5 - Gestione ed assegnazione delle credenziali di autenticazione

Le credenziali di autenticazione per l'accesso al dominio e al Cloud vengono assegnate a ciascun utente dal personale del Servizio ICT.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'autorizzato con la massima diligenza e non divulgata.

È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni tre mesi come previsto dal sistema informativo installato in Consorzio. Il sistema avvertirà l'utente della scadenza della password e della necessità di modifica della stessa. È importante che ogni nuova password sia unica e non sia stata utilizzata in precedenza.

La password, formata da lettere (maiuscole o minuscole), numeri e simboli in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

Nel caso in cui l'utente non ricordi la password o la ritenga non più riservata, deve chiedere supporto al servizio ICT, che potrà eseguire una procedura guidata di reset della password, che include passaggi di verifica dell'identità.

Art. 6 - Utilizzo dell'infrastruttura di rete

L'accesso al dominio è consentito agli utenti in possesso di credenziali di autenticazione assegnate in fase di assunzione. È assolutamente proibito entrare nel dominio con credenziali di altri utenti.

Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità. Su queste unità vengono svolte regolari attività di verifica, amministrazione e back-up da parte del personale del Servizio ICT. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato del Servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

Il personale del Servizio ICT, in caso di identificazione di file o applicazioni in genere pericolose per la sicurezza della rete e/o dei singoli PC, potrà procedere alla rimozione degli stessi, previa comunicazione all'utente incaricato.

È opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla 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.

Art. 7 - Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti esterni (supporti USB, hard disk, etc.) devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. È buona norma non utilizzare questi supporti su dispositivi non aziendali.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili contenenti dati particolari, ciascun utente dovrà contattare il personale del Servizio ICT e seguire le istruzioni da questo impartite.

In ogni caso, i supporti esterni contenenti dati personali di natura particolare devono essere dagli utenti adeguatamente custoditi.

E’ vietato l’utilizzo di supporti rimovibili personali su dispositivi aziendali.

L’utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

Art. 8 - Utilizzo dei dispositivi mobili

L’assegnazione dei dispositivi mobili (notebook, cellulari, modem portatili, tablet) è prevista per il presidente e i dipendenti consortili in base a:

a) Esigenze di reperibilità;

b) Servizi fuori sede;

c) Particolari esigenze tecniche di comunicazione.

L’assegnazione delle apparecchiature è disposta dal Direttore Generale, a seguito di richiesta del Capo Settore di appartenenza.

L’utilizzatore prenderà in consegna l’apparecchiatura previa sottoscrizione di dichiarazione di conoscenza delle disposizioni del presente Regolamento

Al momento dell’assegnazione delle apparecchiature, saranno forniti tutti gli accessori di base utili per il corretto funzionamento degli apparati (es: batteria, carica batterie, auricolare, ecc,). Il Servizio ICT fornisce inoltre il necessario supporto agli utenti per il corretto utilizzo di essi.

L'utente è responsabile del dispositivo mobile assegnatogli dal Servizio ICT e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Il Consorzio non assume alcuna responsabilità per contravvenzioni o sinistri imputabili all’uso delle apparecchiature durante la guida di autoveicoli o altro utilizzo improprio.

Le apparecchiature sono di uso personale, e non possono essere cedute a terzi a nessun titolo.

Gli utilizzatori dei telefoni cellulari, affinché possano essere immediatamente rintracciabili nei casi di necessità, hanno l’obbligo di mantenere in funzione il telefono cellulare durante le ore di servizio, durante le ore di reperibilità, ove previste, ed in tutti i casi in cui le circostanze concrete lo rendano opportuno.

La durata delle connessioni internet per il traffico dati deve essere la più contenuta possibile in relazione alle esigenze di servizio, preferendo altresì la funzione dei messaggi di testo in caso di brevi comunicazioni.

In caso di malfunzionamento, l’utilizzatore dovrà consegnare l’apparecchiatura completa all’Ufficio ICT che provvederà alle verifiche di competenza.

In caso di furto o smarrimento dell’apparecchio, l’assegnatario dovrà darne immediata comunicazione all’Ufficio ICT ai fini dell’immediato blocco dell’utenza. Prima di effettuare la denuncia, sarà necessario contattare l’Ufficio ICT per ottenere i dati necessari alla denuncia. L’assegnatario dovrà successivamente presentare la formale denuncia di furto o smarrimento alla competente Autorità fornendo:

- marca, modello e serial number del dispositivo;

- codice IMEI del dispositivo;

- numero di telefono.

Il Consorzio si riserva la facoltà di revocare o sospendere l'assegnazione delle apparecchiature di telefonia mobile per inutilizzo, per esigenze aziendali e comunque per qualsiasi altra motivazione, con obbligo per l'utilizzatore di immediata riconsegna del bene all'Ufficio ICT.

In caso di guasto/smarrimento si provvederà alla sostituzione del cellulare, tramite l'Ufficio ICT. Nel caso si verifichi in corso d'anno più di una sostituzione, sarà richiesto il rimborso al dipendente di quota parte del costo di acquisto nel seguente modo: 20% per la 2^ sostituzione in corso d'anno, 50% per eventuale successiva, 100% per eventuali ulteriori.

In caso di cessazione dell'attività istituzionale/lavorativa a qualsiasi titolo, le apparecchiature devono essere riconsegnate all'Ufficio ICT.

È facoltà del dipendente o dell'amministratore richiedere il riscatto del dispositivo e la portabilità del numero di telefono: l'eventuale autorizzazione è demandata al Direttore Generale.

Tutte le disposizioni del presente articolo si applicano indistintamente ad ogni tipo di apparecchiatura affidata agli utilizzatori (cellulari, smartphone, chiavette, tablet e computer).

Art. 9 - Uso della posta elettronica

La casella di posta elettronica **cognome@gardachiese.it** assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica per motivi diversi da quelli strettamente legati all'attività lavorativa; a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per: l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp4) non legati all'attività lavorativa; l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Il servizio di posta elettronica è accessibile da Cloud con software Outlook o tramite Webmail inserendo le proprie credenziali.

È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Il Server di posta elettronica esegue la scansione delle mail in entrata per rilevare la presenza di eventuali messaggi dannosi: quando viene rilevato un messaggio potenzialmente dannoso, il servizio invia un alert sulla casella di posta elettronica e mette il messaggio in quarantena. Per visualizzare o rilasciare il messaggio, si prega di contattare il servizio ICT.

Al fine di garantire la funzionalità del servizio di posta elettronica del Consorzio e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) dovrà essere impostato dall'utente per inviare automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto dell'Ente.

In caso di ricezione accidentale di messaggi di valenza ufficiale, è buona norma avvisare il mittente dell'errore.

È inoltre espressamente vietato, salvo autorizzazione espressa del proprio Responsabile, salvare/stampare/inoltrare e portare fuori dai luoghi di lavoro documentazione strettamente connessa all'operatività del Consorzio. A titolo esemplificativo e non esaustivo è vietato:

- ✓ stampare e-mail aziendali per scopi personali;
- ✓ inviare informazioni riservate ad indirizzi di posta personali;
- ✓ fotocopiare/scansionare documentazione aziendale per scopi personali;
- ✓ inoltrare a terzi estranei al Consorzio documentazione interna/informazioni ricevute per mezzo di strumenti informatici o via cartacea, salvo che non sia funzionale allo svolgimento di prestazioni professionali.

Art. 10 - Navigazione in internet

I dispositivi in uso consentono la navigazione su internet per fini istituzionali. È vietata la navigazione in Internet per scopi personali (lettura di quotidiani, ricerca di informazioni, etc.).

È vietato l'utilizzo di Internet per:

- l'upload o il download di software potenzialmente dannosi o con licenze non ufficiali nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà essere a tal fine contattato il personale del Servizio ICT);
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat-line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dalla Direzione.

Art. 11 - Protezione antivirus

Il sistema informatico del Consorzio è protetto da software antivirus. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (evitando, quindi, di compiere quei comportamenti vietati dal presente regolamento e già menzionati: es. navigazione su siti non sicuri, download di file da siti non sicuri, etc.).

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso nonché segnalare prontamente l'accaduto al personale del Servizio ICT.

È buona norma non utilizzare supporti di provenienza esterna al Consorzio. In caso di necessità, contattare il Servizio ICT che procederà alla scansione del supporto prima dell'utilizzo su dispositivi aziendali.

Art. 12 - Cybersecurity

Al fine di garantire la riservatezza, l'integrità e la disponibilità (RID) dei dati personali trattati, si riporta di seguito un elenco di comportamenti atti a ridurre il rischio di perdita o distruzione dei dati stessi.

- Quando si naviga in Internet, verificare di non accedere a siti identificati dal Browser come non sicuri;
- È vietato utilizzare credenziali o e mail aziendali per accedere a servizi per scopo personale (registrazioni a siti, shopping on line, etc.);
- Quando si abbandona il dispositivo, anche per un ridotto lasso di tempo, è opportuno bloccarne l'accesso. Controllare che siano attivi gli screensaver e impostare le loro password per proteggere le postazioni durante l'assenza dell'utente.
- Impostare sempre PIN o Password di sicurezza sui propri dispositivi per tenerli protetti.
- Usare password uniche, casuali e lunghe: la robustezza di una password è data sia dal tipo di caratteri usati (numeri, lettere, simboli), sia dalla lunghezza, che rende un eventuale attacco brute-force dispendioso in termini di tempo e risorse, quindi difficile da portare a compimento.
- Ricordarsi di cambiare le password spesso senza utilizzare modifiche che prevedano l'uso di numeri incrementali.
- Non condividere mai le password e i propri dispositivi, smartphone, PC, tablet etc. con altre persone (anche se ritenute affidabili): non è garantito che abbiano la vostra stessa percezione del pericolo e non mettano quindi in atto comportamenti rischiosi.
- Inoltre, in caso di criticità, potrebbe essere davvero difficile poter reclamare la propria estraneità o buona fede, ritrovandosi considerati corresponsabili di eventuali danni, per negligenza.
- Non inserire mai chiavette USB se non si è davvero certi del contenuto: se è attivo l'automatismo di default, potrebbe essere avviato un programma malevolo, presente nella chiavetta, che potrebbe infettare il PC. Fate attenzione anche quando collegate lo smartphone con il cavo USB, anche in questo caso, potrebbe essere avviato un malware o al contrario potrebbe essere iniettato codice malevolo dal PC allo smartphone. Se possibile mantenere sempre disattivata l'opzione di avvio automatico che si attiva al momento dell'inserimento
- Non prendere mai l'iniziativa di gettare gli HDD o gli SSD guasti: gli stessi vanno consegnati all'Ufficio ICT.
- Evitare di aprire allegati sospetti anche se provengono da fonti apparentemente affidabili: uno degli attacchi più in voga (e in crescita) è proprio quello di far recapitare ai dipendenti di un'azienda e-mail con allegati malevoli, facendo credere che il mittente sia un collega.
- Se è presente nel PC aziendale qualche programma di collegamento remoto (Supremo o Teamviewer o Anydesk), usato con lo scopo di assistenza remota, verificare che non sia impostato l'avvio automatico e che sia attivata l'opzione di notifica.
- Impostare le opzioni in modo da evitare l'uso da parte degli applicativi del microfono e della webcam: attivare questi dispositivi solo quando servono davvero per poi disattivarli subito dopo.
- Non installare applicativi se non dopo aver chiesto il permesso di farlo, e farlo solo se sono davvero utili al lavoro che si deve svolgere. Potendo scegliere, adoperare comunque solo applicativi "*portatili*", quelli cioè che funzionano anche senza doverli installare.
- Controllare di utilizzare browser aggiornati all'ultima versione: vecchie edizioni possono contenere bug ed essere la porta di virus. Nel caso servisse un aggiornamento e non è possibile farlo in autonomia, richiedere un intervento ad hoc.
- Attivare il Wi-Fi o il Bluetooth nei dispositivi solo quando richiesto o necessario, non utilizzare Wi-Fi liberi o in centri commerciali, stazioni o aeroporti.

Art. 13 - Osservanza delle disposizioni in materia di protezione dei dati

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicato nella lettera di designazione a "persona autorizzata al trattamento dei dati" ai sensi del Regolamento UE 679/2016.

In adempimento del provvedimento generale del Garante per la Protezione dei Dati Personali del 1 marzo 2007 avente ad oggetto "Linee guida del Garante per posta elettronica e internet" e ai sensi dell'articolo 13 del Regolamento UE 679/2016 **il Consorzio di bonifica Garda Chiese** desidera fornire ai propri dipendenti e/o collaboratori alcune informazioni relative al trattamento dei dati personali raccolti in esecuzione del presente Regolamento contenente le regole sull'utilizzo degli strumenti informatici, di internet e della posta elettronica.

I dati raccolti saranno trattati esclusivamente per le finalità elencate nel seguente regolamento (fra le quali si ricordano a titolo esemplificativo i dati raccolti a seguito di manutenzione degli strumenti informatici nonché quelli raccolti a seguito di controlli per verificare il rispetto da parte degli utenti delle regole qui riprodotte) e saranno trattati con modalità telematiche. Si ricorda agli utenti che il conferimento dei dati per le finalità sopra citate è necessario ai fini dell'utilizzo degli strumenti elettronici forniti in uso all'utente e che di conseguenza l'eventuale rifiuto di fornire tali dati impedirà al Consorzio di garantire agli utenti l'uso stesso degli strumenti. I dati personali raccolti dal Consorzio non saranno oggetto di diffusione e potranno essere comunicati esclusivamente a personale interno o esterno autorizzato al trattamento (come ad esempio società di servizi che forniscono supporto nella manutenzione degli strumenti informatici) legati al Consorzio da stretti vincoli contrattuali che garantiscono la riservatezza e l'integrità delle informazioni trattate.

Art. 14 - Accesso ai dati trattati dall'utente

L'accesso ai dispositivi aziendali e ai dati contenuti può avvenire per motivi tecnici e/o manutentivi o con l'obiettivo di preservare la sicurezza dei dispositivi e dei dati contenuti.

L'accesso ai dispositivi è comunque estraneo a qualsiasi finalità di controllo dell'attività lavorativa.

Il Titolare del Trattamento, in quanto responsabile del mantenimento della sicurezza dei dati e delle informazioni, ha predisposto un'infrastruttura informatica con lo scopo di prevenire possibili attacchi informatici dall'esterno.

Per prevenire un problema di esposizione al rischio interno all'Ente, è importante evitare comportamenti rischiosi da parte di ciascun utente.

A tal fine si avvale legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4 comma 2), di sistemi che consentono indirettamente un controllo a distanza (controlli preterintenzionali) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori; e ciò, anche in presenza di attività di controllo discontinue.

In particolare tale attività di controllo potrà essere esercitata nel caso in cui si rivelino anomalie di funzionamento o si rendano necessarie attività di manutenzione o, comunque, in tutte le ipotesi in cui sia a rischio la sicurezza dei citati beni consortili e/o la sicurezza sul lavoro in generale.

In seguito ad interventi formativi in materia di Cybersecurity, il Consorzio si avvale della possibilità di effettuare test a campione al fine di monitorare la sensibilità degli atteggiamenti degli utenti rispetto alla tematica condivisa.

Il personale incaricato del servizio ICT effettuerà comunicazioni generalizzate dirette ai dipendenti dell'area o del settore in cui è stato rilevato il comportamento non sicuro.

Il Consorzio non utilizza sistemi hardware e/o software idonei ad effettuare un controllo a distanza delle attività lavorative, in particolare mediante:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica;
- l'accesso alla cronologia di navigazione;
- la lettura o la registrazione dei caratteri inseriti tramite la tastiera e analogo dispositivo;

Art. 15 – Formazione e prevenzione

Le attività di formazione rivestono un ruolo importante nell'educare gli utenti sull'utilizzo appropriato degli strumenti informatici forniti, minimizzando così i rischi derivanti da un loro impiego non ottimale. Il Consorzio si impegna all'istruzione degli utenti sulle migliori pratiche da adottare, attraverso il reparto ICT e organizzando specifici programmi di formazione, con lo scopo di migliorare la consapevolezza e l'autonomia degli utenti e creare un ambiente lavorativo digitalmente più sicuro.

Art. 16 - Sanzioni

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 sono perseguibili nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL e dal Codice etico e comportamentale, nonché con tutte le azioni civili e penali consentite.

Art. 17 – Norme finali

Le disposizioni del presente regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete consortile da postazioni esterne all'ufficio.

Sono fatte salve diverse disposizioni scritte eventualmente emanate dal Consorzio la fine di disciplinare particolari situazioni contingenti.