Consorzio di Bonifica
CELLINA MEDUNA

REGOLAMENTO
PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI CONSORTILI

Versione	Approvazione
1.0	Delibera del Consiglio dei Delegati n. 1.042 del 30.04.2024

Sommario

Premessa

Il presente Regolamento intende fornire ai dipendenti e collaboratori del Consorzio di Bonifica Cellina – Meduna (di seguito congiuntamente denominati "**Utenti**" e singolarmente "**Utente**"), le indicazioni per una corretta e adeguata gestione delle informazioni consortili, in particolare attraverso l'uso di strumenti informatici del Consorzio di Bonifica Cellina – Meduna (di seguito denominato "**Consorzio**" o "**Ente**").

Ogni Utente è tenuto a rispettare il Regolamento, che è reso disponibile secondo quanto previsto al successivo punto 1.3.

Gli strumenti informatici utilizzati dall'Utente sono messi a disposizione dall'Ente per rendere la prestazione lavorativa (di seguito per brevità "**Strumenti**") e sono da considerarsi domicilio informatico del Consorzio**.**

I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere dall'uso degli Strumenti, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio consortile.

1 Entrata in vigore del Regolamento e pubblicità

Il presente Regolamento entra in vigore dall'approvazione con delibera del Consiglio dei Delegati n. 1.042 del 30.04.2024

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

Copia del Regolamento, oltre ad essere affisso nella bacheca Consortile, è pubblicato sul sito del Consorzio (www.cbcm.it) nella sezione "Amministrazione Trasparente/Disposizioni Generali/Atti Generali".

2 Principi generali di riservatezza nelle comunicazioni

L'Utente deve attenersi alle seguenti regole di gestione del dato.

È vietato comunicare a soggetti non specificatamente autorizzati dati e informazioni consortili dei quali l'Utente viene a conoscenza nell'esercizio delle proprie attività all'interno dell'Ente; è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia autorizzato a riceverli, eventualmente in caso di dubbio mediante richiesta preventiva al proprio Responsabile di area/funzione.

È vietata l'estrazione di dati cartacei e/o informatici per uso personale.

È vietato effettuare colloqui su questioni che possono essere inerenti informazioni aziendali in presenza di persone non specificatamente incaricate a conoscere tali informazioni.

È vietato lasciare incustodite informazioni consortili quando l'Utente si allontana dalla postazione di lavoro. Ciò vale soprattutto nel caso di Utenti con uffici ad accesso di soggetti esterni.

Per le riunioni è opportuno utilizzare le apposite Sale dedicate.

È necessario segnalare prontamente al proprio referente e al DPO (**dpo@cbcm.it**) ogni sospetto incidente legato ai dati, quali ad esempio accessi non autorizzati, cancellazione involontaria di informazioni, diffusione di dati a terzi non voluta, etc.

3 Regole di utilizzo dei sistemi informatici

STRUMENTI INFORMATICI	• **Usare i dispositivi informatici solo per attività lavorative** • **Non archiviare sui sistemi informatici del Consorzio dati ad uso personale** • **Mantenere i dispositivi assegnati in ordine e con cura** • **Segnalare prontamente al referente IT ogni evidenza o sospetto di malfunzionamento dei dispositivi informatici assegnati o utilizzati, o eventuali avvisi di anomalia visualizzati dal sistema** • **Spegnere il computer al termine della giornata lavorativa** • **Bloccare il proprio desktop ogni volta che ci si assenta dalla propria postazione, anche solo per pochi minuti** • **È fatto divieto di utilizzare strumenti personali per svolgere attività lavorativa** • **Non collegare alcun dispositivo non autorizzato alle proprie postazioni di lavoro** • **Non collegare alcun dispositivo non autorizzato alla rete aziendale e segnalare prontamente ogni eventuale device anomalo che risultasse connesso**

CREDENZIALI DI ACCESSO	• **Le credenziali di accesso vengono rilasciate ad uso esclusivamente personale, e non devono essere condivise con alcuno**
	• **Prestare attenzione durante la digitazione delle credenziali affinché non possano essere osservate da terzi**
	• **Procedere ciclicamente – secondo indicazione del sistema informatico – all'aggiornamento della propria password di accesso**
	• **Utilizzare password diverse su diversi sistemi e in particolare NON usare la stessa password utilizzata in contesto lavorativo su ambienti personali (es. social network)**
	• **Le password devono rispondere a particolari criteri di sicurezza e non devono contenere informazioni relative a dati personali che possano facilitarne l'identificazione da parte di terzi, in particolare:**
	  ○ **evitare di utilizzare password comuni, legate ad aspetti personali (componenti del nucleo familiare, animali domestici, date di nascita) o a oggetti/frasi presenti nei pressi della propria scrivania**
	  ○ **evitare di utilizzare numeri progressivi facilmente intuibili nelle password (es. Password2024)**
	  ○ **buona norma è utilizzare frasi come password, integrandole con numeri e caratteri speciali; ad esempio: "Oggiè1BellaGiornata!" è una password di adeguata sicurezza.**
	• **Le password vanno archiviate con cura, in particolare:**
	  ○ **NON conservare copia delle credenziali in luoghi non sicuri (agende, documenti sul proprio computer, post-it, etc.)**
	  ○ **non mantenere copia cartacea delle CREDENZIALI, se non in luoghi adeguatamente protetti da accessi di terzi**
	  ○ **non mantenere copia delle CREDENZIALI all'interno del proprio computer, se non in file resi opportunamente inaccessibili tramite cifratura**
	  ○ **utilizzare preferibilmente un sistema di gestione delle password (c.d. password manager) messo a disposizione dal Consorzio**

GESTIONE DEI DATI	• **Si raccomanda di non salvare dati in locale sul proprio computer, ma di usare unicamente le cartelle di rete messe a disposizione** • **Evitare l'archiviazione di dati personali o non lavorativi sui computer e sulle cartelle di rete del Consorzio** • **È fatto divieto di utilizzare dispositivi di memorizzazione esterna, quali ad esempio chiavette USB, hard disk portatili, spazi di salvataggio in cloud** • **Limitare l'utilizzo della stampa, solo quando è necessario e unicamente per documenti lavorativi; ritirare immediatamente i documenti dai sistemi di stampa** • **Al fine di limitare l'impatto ambientale, si raccomanda di valutare le effettive esigenze di stampa e di limitare quanto più possibile l'utilizzo di documenti in cartaceo, dando preferenza al trattamento in digitale**

	• **Prestare particolare cura nella gestione dei documenti cartacei, al fine di archiviarli in luogo sicuro e non lasciarli accessibili a terzi non autorizzati** • **Provvedere alla distruzione dei documenti cartacei, utilizzando gli appositi distruggi-documenti, al fine di evitare possibili diffusioni non autorizzate di informazioni** • **Prestare particolare attenzione alle scansioni documentali, archiviando immediatamente il dato nella cartella di destinazione** • **Evitare per quanto possibile l'utilizzo di cartelle condivise o di transito** • **Per lo scambio dati con l'esterno, utilizzare unicamente gli strumenti messi a disposizione dal Consorzio; in particolare, è vietato l'uso di piattaforme di scambio dati quali WeTransfer, DropBox o similari**
PROGRAMMI SOFTWARE CLOUD	• **Utilizzare solo programmi autorizzati e messi a disposizione dal Consorzio** • **È fatto divieto di utilizzare altri software – anche offerti come servizi cloud – sui dispositivi del Consorzio e per svolgere attività lavorativa** • **Non è consentito installare alcun software sul proprio computer; in caso di necessità, rivolgersi unicamente al personale IT interno** • **In caso di bisogno di nuove dotazioni software, fare richiesta per tempo al responsabile IT dell'Ente** • **È fatto divieto di sottoscrivere qualsiasi licenza software senza esplicita autorizzazione del referente IT del Consorzio**
NAVIGAZIONE INTERNET EMAIL	• **La casella mail assegnata dal Consorzio deve essere utilizzata solo a fini lavorativi** • **Effettuare gli opportuni controlli prima dell'invio di una mail all'esterno del Consorzio, rispetto ai corretti destinatari, agli allegati inviati e al testo delle stesse, al fine di ridurre il rischio di incidenti informatici e alla reputazione dell'Ente** • **Conservare con particolare cura le credenziali di accesso alla propria casella email, e utilizzare ove possibile le tecnologie MFA (Autenticazione multi-fattore) messe a disposizione dal Consorzio** • **Prestare massima cura nel controllo delle mail in ingresso, che possono essere fonte di infezione informatica. Non cliccare su eventuali link o pulsanti presenti nelle mail. Porre particolare attenzione ai file allegati alla mail, che potrebbero contenere dei virus. In caso di dubbio, consultare preventivamente il referente IT dell'Ente** • **Procedere con opportuna cancellazione delle mail non di interesse, al fine di limitare lo spazio dati dell'archivio** • **Navigare esclusivamente su siti conosciuti e ritenuti affidabili, esclusivamente per finalità lavorative** • **Evitare ogni scaricamento di file dalla Rete, se non necessario ed esclusivamente da siti ritenuti affidabili** • **Non caricare file del Consorzio su piattaforme cloud, se non preventivamente autorizzati** • **Non è consentito l'utilizzo di piattaforme social in orario lavorativo e con strumenti aziendali, a meno di specifica autorizzazione della Direzione** • **Evitare l'accesso a piattaforme di streaming audio/video, al fine di limitare il consumo di banda a disposizione degli utenti**
DISPOSITIVI MOBILI	• **Smartphone e tablet sono assegnati a solo scopo lavorativo all'utente. Ne è vietato l'utilizzo da parte di soggetti terzi non autorizzati.** • **È vietato il loro utilizzo per esigenze personali, a meno di emergenze o casistiche pre-autorizzate dalla Direzione. Non devono essere utilizzati per archiviare dati personali dell'utente** • **Non installare sui dispositivi applicazioni diverse da quelle pre-installate; in caso di bisogno di software aggiuntivi, rivolgersi al referente IT del Consorzio** • **Non configurare sui dispositivi lavorativi alcun accesso a caselle mail personali o a servizi cloud non preventivamente autorizzati e/o non a scopo lavorativo** • **Segnalare immediatamente ogni evento che possa aver causato il danneggiamento fisico o logico dei dispositivi** • **Porre particolare cura alla gestione dei dispositivi, evitando di adottare comportamenti che possano esporli a rischi di danneggiamento, usura eccessiva o furto**

	• **Evitare il collegamento dei dispositivi assegnati a reti non sicure e/o non conosciute** • **In caso di richiesta della Direzione, sarà compito dell'utente riconsegnare il dispositivo assegnato al Consorzio, senza ingiustificato ritardo e comunque entro una giornata lavorativa dalla richiesta**

4 Verifiche e gestione dell'incidente informatico

Segnalazione anomalie

L'Utente ha il dovere di segnalare prontamente all'Ufficio IT eventuali anomalie funzionali degli Strumenti in uso. Una segnalazione tempestiva da parte dell'Utente è di fondamentale importanza per la corretta gestione delle problematiche di sicurezza/possibili incidenti.

L'Utente ha il compito altresì di segnalare prontamente eventuali anomalie nel trattamento dei dati di cui dovesse venire a conoscenza (es. diffusione interna o esterna non autorizzata dei dati, errata cancellazione di informazioni aziendali, installazione di software anomalo sulle macchine, uso promiscuo dei dispositivi aziendali).

Controlli

L'Ufficio IT ha la possibilità di ispezionare – a scopi di verifica di funzionamento e/o di analisi e gestione di possibili incidenti di sicurezza – gli Strumenti aziendali, anche se assegnati specificatamente ad un Utente.
Tali verifiche e ispezioni possono essere svolte solo a seguito di comunicazione all'Utente.

In caso di presunto incidente di sicurezza, l'Ufficio IT ha la facoltà di richiedere o effettuare una copia forense del dispositivo interessato, con successiva analisi tecnica e conservazione del contenuto, previa notifica all'Utente assegnatario. L'Utente autorizza fin d'ora l'Ufficio IT all'esecuzione di tali verifiche, e opererà in ottica collaborativa a supporto dell'Ufficio, fornendo tutto il supporto eventualmente necessario e mettendo prontamente a disposizione i propri dispositivi.

L'Ufficio IT e il Consorzio si impegnano affinché ogni attività di verifica venga svolta nel solo interesse aziendale e nel pieno rispetto della privacy e dei diritti dell'Utente.

5 Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento.

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

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

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