REGOLAMENTO PER L'UTILIZZO DEGLI

STRUMENTI INFORMATICI

Consorzio BIM del Chiese

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione		Gloria Tomasini	Responsabile transizione digitale
Approvazione Delibera n. 16	14/07/2020	Assemblea	Organo di indirizzo e di gestione del Consorzio BIM del Chiese

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
Ver 1.0	14/07/2020	Prima emissione	----------

Sommario

Introduzione

Le realtà aziendali private e pubbliche si caratterizzano per l'elevato uso della tecnologia informatica che da un lato ha consentito l'introduzione di innovative tecniche di gestione dell'attività, dall'altro ha dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti al dipendente per lo svolgimento delle proprie mansioni. La progressiva diffusione delle nuove tecnologie informatiche ed in particolare il libero accesso alla rete Internet dai personal computer, espone l'Ente ai rischi derivanti dai problemi alla sicurezza e quindi alla possibile lesione dell'immagine del Consorzio.

In questo senso, viene fortemente sentita dal Consorzio BIM del Chiese la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'Ente a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dalla normativa vigente.

I controlli preventivi e continui sull'uso degli strumenti informatici devono garantire tanto il diritto dell'Ente di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro la cui utilizzazione personale è preclusa; quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità. Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del Consorzio deve sempre ispirarsi al principio della diligenza e correttezza - comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro - il presente regolamento interno è diretto ad evitare che comportamenti talvolta anche inconsapevoli possano innescare problemi con minacce alla sicurezza del trattamento dei dati.

Le prescrizioni qui contenute, non si sostituiscono alle specifiche istruzioni che riguardano l'attuazione della normativa in materia di privacy, ma la integra. Il presente regolamento è pertanto diretto a tutelare il Consorzio BIM del Chiese e ad evitare comportamenti scorretti.

Articolo 1 – Utilizzo del personal computer

Il personal computer affidato al dipendente o al collaboratore del Consorzio è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. L'accesso all'elaboratore è protetto da password, che deve essere custodita dal dipendente con la massima diligenza e non divulgata.

Non è consentito l'uso di programmi diversi da quelli caricati ufficialmente dal Consorzio sui vari elaboratori. Non è consentito installare autonomamente programmi provenienti dall'esterno. Tutte le installazioni devono essere eseguite direttamente dall'amministratore di sistema, ovvero concordate preventivamente con l'amministratore medesimo. Ciò in quanto sussiste il grave pericolo di introdurre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Il personal computer deve essere spento ogni sera prima di lasciare l'ufficio o in caso di assenza prolungata dall'ufficio. In ogni caso 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. Pertanto, ciascun computer, se incustodito, deve sempre essere bloccato.

È vietato l'accesso contemporaneo con lo stesso account da più personal computer.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'amministratore del sistema nel caso in cui siano rivelati virus e seguendo quanto previsto dal presente regolamento relativamente alle procedure di protezione antivirus.

Non è consentita la memorizzazione dei documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Non è consentito all'utente di modificare le caratteristiche impostate sui PC assegnati, i punti rete di accesso e le configurazioni della rete presente nella sede, salvo autorizzazione esplicita dell'amministratore di sistema.

Articolo 2 – Utilizzo della rete

Le aree comuni disponibili in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su questa unità vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con nomi di altri utenti.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con la cancellazione dei file obsoleti od inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante, per problemi di occupazione di spazio, ma soprattutto al fine di garantire l'affidabilità degli eventuali dati forniti a terzi.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

Articolo 3 – Gestione delle password

Le password devono essere lunghe almeno 8 caratteri e formate da combinazioni di lettere maiuscole, lettere minuscole e di numeri, ricordando che le lettere maiuscole/minuscole hanno significati diversi per il sistema e che non è possibile inserire il nome, il cognome e l'utente come password o parte di essa. Possono contenere anche caratteri speciali o di punteggiatura. Le password hanno una durata massima di 6 mesi, trascorsi i quali le password devono essere sostituite e non potranno essere riutilizzate le ultime 24 password.

Qualora si sospetti che la password abbia perso la segretezza, essa deve essere immediatamente sostituita, dandone comunicazione all'amministratore del sistema. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia all'utente stesso.

È dato incarico al Segretario di comunicare tempestivamente eventuali cambi di mansione che comportino modifiche o revoche di autorizzazione all'accesso delle risorse informatiche, sia all'ufficio del personale che all'amministratore di sistema, per iscritto, al fine di rendere possibili le modifiche dei profili di accesso alle risorse e la sostituzione delle password, ove necessario.

Articolo 4 – Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (CD, chiavette, etc.) contenenti dati personali devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare dati memorizzati anche dopo la loro cancellazione logica. I supporti magnetici contenenti dati sensibili devono essere custoditi in archivi chiusi a chiave.

Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa.

Tutti i file di provenienza incerta non devono essere utilizzati/installati/testati.

Articolo 5 – Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli dal Consorzio e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Ai PC portatili si applicano le regole di utilizzo previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso, ove ne sussista la necessità, prima del loro collegamento alla rete ovvero della riconsegna. I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in luogo protetto.

Eventuali configurazioni di tipo Accesso Remoto, dirette verso la rete aziendale o attraverso internet, devono essere autorizzate e predisposte esclusivamente a cura dell'Amministratore di sistema.

Articolo 6 – Uso della posta elettronica

La casella di posta assegnata dal Consorzio BIM del Chiese 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 del Consorzio per l'invio di messaggi personali. È vietato l'utilizzo della casella di posta elettronica per l'invio di messaggi estranei al rapporto di lavoro o alle relazioni tra colleghi.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Per la trasmissione di file all'interno del Consorzio è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo.

Si raccomanda di non eseguire download di file eseguibili o documenti da siti Web non conosciuti.

È vietato inviare catene telematiche (c.d. Catene di Sant'Antonio). Non si devono in alcun caso attivare gli allegati di tali messaggi.

Ogni utente è responsabile del contenuto della propria casella di posta elettronica.

Articolo 7 – Posta elettronica certificata

Il Consorzio BIM del Chiese è dotato di casella di Posta Elettronica Certificata da utilizzare per le comunicazioni ufficiali per le quali sia indispensabile avere un riscontro formale dell'avvenuto invio e della conseguente ricezione. Le mail ricevute attraverso le caselle di posta elettronica certificata devono essere, di norma, protocollate secondo le procedure specificatamente predisposte. Non

verranno protocollate quelle comunicazioni che, pur se ricevute a mezzo PEC, non rivestano carattere di ufficialità tale da giustificare la loro acquisizione al protocollo dell'Ente.

Articolo 8 – Uso della rete Internet e dei relativi servizi

Il personal computer abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È vietato al dipendente lo scarico di software gratuiti prelevati da siti Internet, se non espressamente autorizzato dall'amministratore di sistema.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (nickname). Inoltre, non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore, né visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria.

L'accesso ai social network (Facebook, Twitter, Linkedin e similari) è consentito solo ed esclusivamente per utilizzi che abbiano attinenza diretta con lo svolgimento delle proprie mansioni lavorative.

Articolo 9 – Protezione antivirus

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico del Consorzio derivante da virus o da altro software aggressivo.

Ogni utente è tenuto a controllare il regolare funzionamento e l'aggiornamento periodico del software installato.

Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto all'amministratore di sistema.

Non è consentito l'utilizzo di supporti esterni (cd rom, chiavette usb e similari) di provenienza ignota.

Articolo 10 – Le procedure di backup

L'amministratore di sistema è tenuto ad organizzare le procedure ritenute necessarie e sufficienti per garantire la conservazione ed il ripristino dei dati contenuti nel sistema nel caso si realizzino alcuni dei rischi incombenti sui dati (guasto tecnico, errore umano, dolo).

È compito dell'amministratore di sistema:

a) organizzare le aree soggette a back up aziendale

b) organizzare le procedure di copia periodica dei dati su altri dispositivi

c) organizzare le procedure di ripristino dei dati in caso di guasti

d) organizzare periodicamente i test di controllo sulla effettiva funzionalità delle procedure adottate.

Articolo 11 – Smart working

Per lavorare in smart working è possibile utilizzare il pc fornito dall'ente oppure, previa autorizzazione, il proprio computer personale, come previsto dal DL 18/2020 art. 12, comma 3-bis. Il dispositivo elettronico personale deve essere personalizzabile al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo.

Il dispositivo fornito dall'ente deve essere utilizzato solamente dal dipendente e valgono le stesse disposizioni relative al pc in uso sul luogo di lavoro.

Sia che si utilizzi il dispositivo fornito dall'ente che quello personale, nel lavoro da casa vanno osservate inoltre le seguenti regole:

a) assicurarsi che il sistema operativo e l'antivirus del dispositivo siano sempre aggiornati;
b) non memorizzare le password di accesso all'utilizzo delle risorse dell'ente sulle postazioni personali;
c) evitare di scrivere le password utilizzate su post-it e fogli lasciati in prossimità della postazione;
d) non effettuare salvataggi su dispositivi personali e utilizzare preferibilmente le risorse in cloud messe a disposizione dall'amministrazione;
e) limitare il ricorso a penne USB e flash memory per archiviare dati e documenti;
f) bloccare la postazione in casi di assenza, seppur temporanea;
g) adottare ogni cautela a protezione del dispositivo utilizzato, specialmente in caso di spostamenti;
h) non gettare nella spazzatura documenti cartacei utilizzati per l'attività lavorativa contenenti dati personali se non dopo averli triturati o resi illeggibili;
i) comunicare senza ritardo al referente privacy dell'ente ogni tipo di incidente da cui potrebbe derivare una violazione di dati personali (virus, malfunzionamenti, ricorso ad assistenza per riparazioni, accesso da persone terze anche se famigliari, ecc);
j) non installare software proveniente da fonti non ufficiali (se si utilizza il pc personale, portare ulteriore attenzione al software installato o scaricato per finalità non lavorative);
k) non cliccare su link o allegati contenuti in email sospette;
l) utilizzare l'accesso a connessioni wi-fi adeguatamente protette;
m) se si utilizza un dispositivo personale, assicurarsi di accedere con il proprio utente personale e non permettere l'utilizzo dello stesso alle altre persone che usano il pc.

Articolo 12 – Utilizzo di strumenti diversi

All'interno degli uffici è vietato l'uso di strumenti informatici che non siano quelli messi a disposizione o autorizzati dall'Ente. Il Consorzio BIM del Chiese autorizza l'uso di chiavette USB e dispositivi di firma digitale, previa la scansione per la ricerca di eventuali virus.

Articolo 13 – Cellulari e SIM telefoniche

Le schede telefoniche (SIM) ed i cellulari messi a disposizione dei dipendenti del Consorzio BIM del Chiese devono essere utilizzati per l'attività lavorativa. Questo principio deve essere seguito anche per quanto riguarda l'installazione di app e l'utilizzo di internet dallo smartphone.

Fare molta attenzione a quanto si scarica e viene installato sul cellulare dell'ente, in modo da evitare di scaricare virus o divulgare dati sensibili.

Articolo 14 – Osservanza delle disposizioni in materia di privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e delle misure minime di sicurezza, come indicato nei documenti di individuazione degli incaricati del trattamento dei dati.

I documenti e tutti i materiali presenti sul sistema informatico del Consorzio sono, di norma, liberamente accessibili e non filtrati, ma il loro utilizzo deve avvenire esclusivamente per ragioni d'ufficio, in considerazione del proprio ruolo, nonché dei compiti e delle mansioni affidate. Non sono ammessi accessi impropri. In applicazione delle vigenti disposizioni sulla gestione dei flussi documentali, tutti gli accessi e le operazioni compiute sui documenti gestiti sono registrati nei log di processo, con specifica indicazione dell'utente.

Articolo 15 – Inosservanza del regolamento

Il mancato rispetto delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

Articolo 16 – Aggiornamento e revisione

Tutti gli utenti possono proporre, quando lo ritengano necessario, integrazioni e modifiche al presente Regolamento.

Articolo 17 – Codice disciplinare

Il presente regolamento costituisce integrazione del codice di comportamento dei dipendenti dell'ente e pertanto verrà divulgato e messo a disposizione dei dipendenti secondo le disposizioni vigenti.

Articolo 18 – Regolamento smart working

Il presente regolamento costituisce integrazione del regolamento relativo alla modalità di lavoro in smart working adottato dall'Ente e registrato al protocollo 707 del 24/03/2020. Verrà pertanto divulgato e messo a disposizione dei dipendenti secondo le disposizioni vigenti.