REGOLAMENTO DELL'ORDINE ARCHITETTI PPC DELLA PROVINCIA DI VERONA PER L'UTILIZZO DEL SISTEMA INFORMATICO

PREMESSA

Il Garante per la protezione dei dati personali, con Provvedimento del 01.03.2007 pubblicato sulla G. U. R.I. del 10.03.2007, n. 58, ad oggetto *"Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori"* raccomanda l'adozione da parte dei datori di lavoro pubblici e privati, di un disciplinare interno, definito con il coinvolgimento delle rappresentanze sindacali, in cui siano indicate le regole per l'uso di Internet, della posta elettronica e della tenuta di file della rete interna nel rispetto della Legge 20.05.1970, n. 300 (Statuto dei lavoratori), del Regolamento (UE) n. 2016/679 e del Decreto Legislativo 30.06.2003, n. 196 (Codice in materia di protezione dei dati personali) così come modificato dal d.lsg 101/2018.

Con il presente regolamento sono disciplinate le condizioni di utilizzo delle risorse informatiche di comunicazione che l'Ordine degli Architetti, Pianificatori, Paesaggisti e Conservatori della Provincia di VERONA – di seguito per brevità Ordine degli Architetti PPC di Verona- sito in via Santa Teresa n°2 – 37135 Verona (VR) architettiverona@pec.it mette a disposizione degli operatori per l'esecuzione delle funzioni di competenza.

Sono altresì regolate le modalità con le quali l'Ordine degli Architetti PPC di Verona può accertare e inibire le condotte illecite degli utilizzatori di Internet, della posta elettronica e dell'accesso alle risorse di archiviazione di massa (server – hard disk).

Sono tenuti all'osservanza delle presenti norme i "Responsabili del trattamento", i Dipendenti designati "Incaricati del trattamento" dei dati personali ai sensi del regolamento 2016/679 e del Decreto Legislativo 30.06.2003, n. 196 e s.m.i., nonché ogni altro Responsabile e/o incaricato e autorizzato dall'azienda.

1.UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente 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 dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'amministratore di sistema.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita dell'amministratore di sistema, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informatici dell'Ordine degli Architetti di Verona. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione 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.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'amministratore di sistema.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate 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. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc...), se non con l'autorizzazione espressa dell'amministratore di sistema.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'amministratore di sistema nel caso in cui vengano rilevati dei virus.

2.UTILIZZO DELLA RETE DELL'ORDINE DEGLI ARCHITETTI DI VERONA

Le unità di 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 queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

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

L'amministratore di sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

3.GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'amministratore di sistema. È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al Custode delle Parole chiave all'amministratore di sistema.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Parole chiave, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o persona dalla stessa incaricata.

4.UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

5.UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dall'amministratore di sistema 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 Pc fissi connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili non devono mai restare incustoditi e sul disco devono essere conservati solo i file strettamente necessari.

I PC portatili usati all'esterno dei luoghi di lavoro (in occasione ad esempio di convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

6.USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda 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 la casella di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

È buona norma evitare messaggi completamente 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.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'Ordine degli Architetti di Verona deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).

Per la trasmissione di file all'interno dell'Ordine degli Architetti di Verona è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.

È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo. In particolare, si deve evitare, secondo le regole di buona diligenza, l'apertura e la lettura di messaggi di posta elettronica in arrivo provenienti da mittenti di cui non si conosce con certezza l'identità o che contengano allegati del tipo .exe, com, .vbs, .htm, scr, .bat, .js, .pif.

È vietato inviare catene telematiche (dette di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'amministratore di sistema. Non si devono in alcun caso attivare gli allegati di tali messaggi.

Sono attivati indirizzi di posta elettronica per le strutture aziendali, condivisi dagli operatori assegnati a ciascuna di esse.

La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

Nei messaggi inviati tramite posta elettronica aziendale (di servizio e/o nominative) verrà accluso il seguente testo: "*Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento Aziendale adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente*".

E' ammesso l'utilizzo di sistemi di webmail personali e private con modalità e tempi tali da non incidere negativamente sull'attività di servizio.

7.USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale 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 fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'amministratore di sistema.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

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 (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

8.CONSERVAZIONE DEI DATI

In applicazione dei principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet ed al traffico telematico la cui conservazione non sia necessaria, saranno cancellate entro sei mesi dalla loro produzione.

È consentito il prolungamento dei tempi di conservazione in casi specifici, ad es.: per esigenze tecniche o di sicurezza; per l'indispensabilità dei dati rispetto all'esercizio od alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità giudiziaria o della polizia giudiziaria.

9.SANZIONI DISCIPLINARI

Tutte le violazioni al presente regolamento potranno essere oggetto di procedimento disciplinare, fatte salve le ulteriori responsabilità civili, penali e contabili previste dalla normativa vigente.

10.DISPOSIZIONI FINALI

È fatto obbligo, a chiunque spetti, di osservare e far osservare il presente regolamento.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Per quanto non espressamente previsto nel presente regolamento, si rinvia ai regolamenti aziendali in materia di accesso agli atti, di procedimento amministrativo e di privacy nonché alla normativa nazionale e regionale vigente.

Il presente Regolamento è soggetto a revisione con frequenza annuale.