

DISCIPLINARE INTERNO PER L'UTILIZZO DEL SISTEMA INFORMATICO

INDICE

Premessa

1. Utilizzo del Personal Computer
2. Utilizzo della rete
3. Gestione delle Password
4. Utilizzo dei supporti magnetici
5. Utilizzo di PC portatili
6. Uso della posta elettronica
7. Uso della rete Internet e dei relativi servizi
8. Osservanza delle disposizioni in materia di Privacy.
9. Non osservanza della normativa aziendale.
10. Aggiornamento e revisione

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone il Consiglio dell'Ordine degli Avvocati di vallo della Lucania ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dello stesso ente.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche del COA deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'ente ha adottato un regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

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 l'accesso a servizi specialistici, per lo screen saver e per il collegamento alla rete internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'..... (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...*).

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; lo stesso potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere all'ente, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dal GDPR e dal DLGS. 101/2018 linea guida AGID II, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività istituzionale 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 infezione del sistema con 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 del COA Vallo. 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 (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) 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'Amm.re di Sistema. Il personal computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. 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 disattivato lo schermo ed inserita la relativa password.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio pen drive, HD portatili ecc ...), se non con l'autorizzazione espressa dell'AS. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'AS nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE DEL COA VALLO (ANCHE WI-FI)

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'Amm.re di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi 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.

A 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.

Per l'accesso tramite rete wi-fi, rimane inalterata la prassi fin qui descritta per accesso dell'operatore COA.

L'accesso alla rete wi-fi di altri utenti non legati al COA Vallo da rapporti di collaborazione/dipendenza/consulenza è disciplinato con regolamento a parte.

GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi, sono previste ed attribuite dall'AS. 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 compatibile con le linee dettate dal GDPR con contestuale comunicazione al custode delle parole chiave (AS o dipendente in servizio) *n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al custode; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*

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 (punto 5 del disciplinare tecnico).

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 al DPO o persona dal COA incaricata (*Responsabile, responsabile del trattamento informatico, responsabile dei sistemi informatici ...*)

UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (cd rom, pen drive, HD esterni) 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, qualora esistenti, devono essere custoditi in archivi chiusi a chiave.

UTILIZZO DI EVENTUALI PC PORTATILI

L'utente è responsabile del PC portatile eventualmente assegnatogli da (*individuare la figura e la sua qualificazione: responsabile del trattamento informatico, responsabile dei sistemi informatici aziendali,...*) 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 connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.

USO DELLA POSTA ELETTRONICA (ORDINARIA E PEC)

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 le caselle di posta elettronica istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.

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, o istituzionali per l'ente 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'ente il "know how" tecnico o istituzionale protetto (tutelato in base alle vigenti normative), e che, quindi, viene eventualmente contraddistinto da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'ente, non può essere comunicata all'esterno senza preventiva autorizzazione del Consiglio.

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 RR, ...).

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

È obbligatorio controllare i files attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all' AS. In alcun caso è fatto divieto di attivare gli allegati di tali messaggi.

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' AS.

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 dal Consiglio 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).

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del GDPR 679/2016 e DLgs. 101/20108

NON OSSERVANZA DELLA NORMATIVA AZIENDALE

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

AGGIORNAMENTO E REVISIONE

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

Il presente Regolamento è soggetto a revisione con frequenza annuale.