

(ALLEGATO I)



REGOLAMENTO ALFA SULL'UTILIZZO DEL SISTEMA INFORMATIVO

**APPROVATO CON
DECRETO DEL DIRETTORE GENERALE
N. 900 DEL 21/05/2019**

INDICE

- Premessa
- Utilizzo del Personal Computer
- Utilizzo della rete
- Gestione delle Password
- Utilizzo dei supporti magnetici
- Utilizzo del Cloud
- Utilizzo di PC portatili
- Uso della posta elettronica
- Uso della rete Internet e dei relativi servizi
- Osservanza delle disposizioni in materia di Privacy.
- Non osservanza della normativa aziendale.
- Aggiornamento e revisione

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone ALFA ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.

Premesso che l'utilizzo delle risorse informatiche e telematiche del nostro Ente deve sempre ispirarsi al principio della diligenza e della correttezza (comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro) Alfa ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

L'Amministratore di Sistema svolgerà l'incarico di supervisione e manutenzione dell'hardware e del software aziendale, ed opererà sempre sotto incarico da parte della direzione.

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.

Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte della direzione.

L'Amministratore di Sistema, 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 aziendale interna ed esterna.

L'Amministratore di Sistema potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere allo stesso Ente, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità impartite, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività 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 di Alfa.

L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre Alfa 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'Amministratore di Sistema.

Il Personal Computer deve essere spento ogni sera 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 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, ...), 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 nel caso in cui vengano rilevati virus.

UTILIZZO DELLA RETE

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 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 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.

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

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 particolari (ovvero dati sensibili e dati giudiziari) la periodicità della variazione deve essere ridotta a tre mesi.

Le password devono essere formate da lettere (maiuscole / 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.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o all'amministratore di sistema.

UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, CD,DVD, hard disk rimovibili, pen drive,...) contenenti dati personali e/o particolari (sensibili) 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 personali e/o particolari devono essere custoditi in archivi chiusi a chiave.

UTILIZZO DEL CLOUD

Il trasferimento di dati verso sistemi cloud deve essere sempre autorizzato dall'amministratore di sistema. L'accidentale trasferimento di dati in server ubicati fuori dall'unione europea potrebbe non essere consentito dal Regolamento 2016/679 (GDPR).

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 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 in azienda, ecc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.

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 le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing 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 per Alfa 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,...) o in alternativa usando il servizio di posta elettronica certificata (PEC).

Per la trasmissione di file all'interno di Alfa 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 (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Pertanto è consigliabile impostare il client di posta elettronica in modo che non effettui in automatico l'anteprima dell'allegato.

È vietato inviare catene telematiche (o 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.

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

DATA BREACH

Alfa, in caso di violazione dei dati sui propri sistemi informativi dispone che:

- Venga comunicata immediatamente al legale rappresentante l'avvenuta violazione, specificandone la natura e su quali supporti si è verificata
- Venga comunicata immediatamente all'Amministratore di Sistema la violazione al fine di poter avviare le opportune indagini per identificare la natura e le modalità del data breach
- L'Amministratore di Sistema compili il Registro delle violazioni con i dati raccolti
- Entro 72 ore venga valutato, insieme all'Amministratore di Sistema, se la violazione comporta un rischio per i diritti e le libertà delle persone fisiche e, in caso positivo, che la violazione venga notificata al Garante per la protezione dei dati personali con le modalità descritte sul sito www.garanteprivacy.it

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e alle misure adeguate di sicurezza messe in atto da Alfa, come indicate dal Regolamento 2016/679 (GDPR), al fine di tutelare la riservatezza, l'integrità e la disponibilità dei dati.

NON OSSERVANZA DELLA NORMATIVA DELL'ENTE

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 dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

La Direzione