

UTILIZZO SISTEMA INFORMATICO

TABELLA REVISIONI				
N° REV.	DATA EMISSIONE	DESCRIZIONE	RIF. PARAGR.	RIF. PAGINA
00	30.03.2018	Prima Emissione	Tutti	Tutte

VERIFICATO E APPROVATO
DALLA DIREZIONE

EMESSO DAL RESPONSABILE
GESTIONE QUALITA'

30.03.2018

FIRMA

FIRMA

DATA

1. SCOPO

La presente istruzione operativa ha lo scopo di informare e regolamentare l'utilizzo del sistema informatico aziendale. La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone la SAGI SERVICE SRL ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa. Premesso quindi che l'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, SAGI SERVICE SRL ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

2. 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.

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 del responsabile incaricato dall'azienda, 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 della SAGI SERVICE SRL. 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 del responsabile incaricato dall'azienda.

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.

3. UTILIZZO DELLA RETE DI SAGI SERVICE

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.

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.

4. GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal Custode delle Parole chiave (vedi nomina). È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni tre mesi con contestuale comunicazione al Custode delle Parole chiave.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri, devono essere composte da almeno otto caratteri e non devono 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.

5. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili contenenti dati particolari o giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato.

Eventuali supporti magnetici contenenti dati particolari e giudiziari devono essere custoditi in archivi chiusi a chiave.

6. UTILIZZO DEI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli 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.

7. 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.

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.

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.

Per la trasmissione di file all'interno della SAGI SERVICE SRL 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).

8. 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 dal responsabile indicato dall'azienda.

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).

9. SALVATAGGIO DEI DATI

I dati inerenti all'attività lavorativa dovranno essere salvati all'interno del SERVER dedicato.

Per tali dati è stata prevista una procedura automatizzata di backup giornaliero su spazio FTP aziendale, mentre mensilmente si dovrà procedere a effettuare un backup su supporto mobile, il quale poi verrà custodito in un archivio sotto chiave.

10. 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.