

Regole aziendali per l'utilizzo dei sistemi informatici

di Priori Claudio - Ikaros Calcio

1

Nelle realtà aziendali si sono diffusi negli ultimi anni tecnologie:

- Informatiche
- Telefoniche

- Innovative tecniche di gestione dell'impresa
- Problematiche di gestione degli strumenti informatici/telefonici forniti dall'azienda ai propri collaboratori

I datori di lavoro sentono la necessità di attuare adeguati sistemi di controllo

- sanzioni per usi scorretti

di Priori Claudio - Ikaros Calcio

2

Usi scorretti

- Espongono l'azienda a rischi:

- patrimoniali
- penali
- violazione del
 - diritto d'autore
 - Privacy

→ problemi alla sicurezza e all'immagine

- Contrari ai doveri di

- diligenza
- fedeltà

previsti dagli artt. 2104 e 2015 del Codice civile.

di Priori Claudio - Ikaros Calcio

3

è necessario garantire

- il diritto del datore di lavoro di proteggere la propria organizzazione
- il diritto del lavoratore a non vedere invasa la propria sfera personale
 - diritto alla riservatezza
 - dignità

Sanciti dallo Statuto dei lavoratori e dal codice sulla privacy.

di Priori Claudio - Ikaros Calcio

4

Le policy aziendali
che dettano le regole sull' uso degli strumenti
informatici e telematici, **non sono sostitutive**
di:
Statuto dei lavoratori
codice sulla privacy.

Utilizzo del Personal Computer 1

- Il PC affidato all' utente è uno strumento di lavoro.
- Ogni utilizzo diverso da quello previsto nella attività lavorativa è vietato perchè:
 - può innescare disservizi
 - costi di manutenzione
 - minacce alla sicurezza
- Il PC deve essere custodito con cura.
- Il personale ICT dell' azienda è autorizzato a compiere interventi sul PC per garantire la sicurezza e la salvaguardi del sistema (aggiornamento software, manutenzione hardware)
 - accesso in qualunque momento dei dati presenti nel PC:
 - archivi di posta
 - verifica dei siti internet visitati

Utilizzo del Personal Computer 2

- Il personale ICT può collegarsi e visualizzare in remoto il desktop delle singole postazioni PC
 - L'utente deve essere avvisato
 - l' intervento deve avere una finalità tecnica:
 - sicurezza contro
 - virus
 - spyware
 - malware
 - assistenza tecnica
- Non è consentito l' utilizzo di programmi diversi da quelli installati ufficialmente dal personale ICT.
 - la normativa a tutela dei diritti d' autore impone la presenza nel sistema di software regolarmente licenziato.
- Non è possibile installare dispositivi di memorizzazione, comunicazione o altro...
- Attenzione all'utilizzo di supporti esterni:
 - In caso di rilevamento virus → avvertire i tecnici ICT.
- Il computer deve essere spento ogni sera prima di lasciare gli uffici.
 - se lasciamo un PC incustodito, acceso e connesso alla rete può essere utilizzato da terzi in modo indebito senza poter poi risalire all' identità del soggetto (savescreen + password).

Gestione ed assegnazione delle credenziali di autenticazione

- Assegnate dal personale ICT, su richiesta del Responsabile dell' ufficio/area nell' ambito del quale andrà ad operare il nuovo utente.
- Le credenziali di autenticazione:
 - User id (identificazione utente)
 - password (parola chiave riservata)
 - non divulgabile
 - almeno 8 caratteri, complessa
 - non per il bios
 - Da modificare:
 - al primo utilizzo
 - ogni 6 mesi
 - Se la password perde la sua riservatezza ci si accorda con il personale ICT.
- Le credenziali di autenticazione vengono custodite dal personale ICT.

Utilizzo della rete

- Per accedere alla rete l'utente deve possedere specifiche credenziali di autenticazione.
- non posso accedere alla rete con credenziali altrui.
- Le cartelle utenti presenti nei server sono:
 - aree di condivisione di informazioni professionali
 - non possono contenere dati personali, non legati alla attività lavorativa
 - sono controllate
 - sono sottoposte a backup periodici(i dischi locali non sono soggetti a salvataggio da parte dei tecnici ICT. La responsabilità è a carico del singolo utente)

Gli utenti devono controllare almeno ogni tre mesi il contenuto delle cartelle per evitare il salvataggio di file **inutili** o **ridondanti**.

Utilizzo e conservazione dei supporti rimovibili

- Tutti i supporti magnetici rimovibili:
 - dischetti
 - CD DVD
 - supporti USB
- che contengono dati sensibili o How-Know aziendale devono:
 - essere trattati con cura per evitare:
 - cancellazioni
 - furti
 - riposti in armadi chiusi
- La distruzione dei supporti deve essere concordata con il personale ICT.
- Non si possono usare supporti personali!
- L'utente è responsabile dei supporti e dei dati in essi contenuti.

Utilizzo dei PC portatili

- L'utente è responsabile del PC portatile e deve custodirlo con diligenza.
- I PC utilizzati all'esterno devono essere sorvegliati per evitare
 - danni
 - sottrazioni

Uso della posta elettronica

- è uno strumento di lavoro
 - gli assegnatari sono responsabili del corretto utilizzo
- è vietato utilizzare la casella di posta per motivi diversi da quelli lavorativi.
 - invio/ricevimento di file allegati contenenti:
 - brani musicali
 - filmati
 - ...
- La casella di posta deve essere mantenuta in ordine:
 - cancellando documenti inutili e allegati ingombranti
- Le comunicazioni con contenuti rilevanti o impegni contrattuali devono essere visionate od autorizzate dal responsabile d'ufficio.
- Massima attenzione nell'aprire i file attachements di posta
 - non eseguire il download di file:
 - eseguibili
 - siti web o ftp sconosciuti.
- In caso di assenza programmata (ferie) o non programmata (malattia) le mail ricevute verranno "girate" ad altro utente al fine di garantire la funzionalità del servizio di posta.
- I messaggi devono contenere una informativa standard sulla natura non personale delle comunicazioni e sul fatto che i contenuti potranno essere letti altri sulla base delle policy aziendali.

Navigazione in Internet

- È proibita la navigazione in Internet per motivi diversi da quelli legati all'attività lavorativa.
- Non è possibile:
 - eseguire il download di software o documenti
 - Eseguire transizioni finanziarie.
 - RegISTRAZIONI a siti, forum, chat line, guestbook ...
...che non siano attinenti all'attività lavorativa.
In caso di dubbio si deve contattare l'ICT.
- I controlli del personale ICT possono avvenire mediante:
 - Controllo dei contenuti dal Proxy Server
 - File di Log della navigazione svolti
 - I dati sopracitati vengono conservati per un tempo definito dell'az.

di Priori Claudio - Ikaros Calcio

13

Protezione antivirus

- Il sistema informatico è protetto da software antivirus aggiornato quotidianamente.
- L'utente deve mantenere comportamenti atti a ridurre il rischio di attacco.
- Nel caso venga rilevata la presenza di un virus, l'utente deve:
 - Sospendere ogni elaborazione in corso
 - Spegner il computer
 - Segnalare subito l'accaduto al personale del Servizio ICT.
- Ogni dispositivo esterno deve essere verificato mediante il programma antivirus prima del suo utilizzo.
 - In caso di virus il dispositivo deve essere consegnato al ICT.

di Priori Claudio - Ikaros Calcio

14

Utilizzo dei telefoni, fax e fotocopiatrici aziendali

- Il telefono aziendale è uno strumento di lavoro:
 - Uso legato solo alla attività lavorativa
 - La ricezione o l'effettuazione di telefonate personali è consentito in caso di necessità o urgenza comprovata.
- Il caso di assegnamento di un tel. Cellulare, l'utente è responsabile del suo utilizzo e custodia.
 - Vietato inviare SMS o MMS di natura personale.
 - L'uso promiscuo è possibile previa autorizzazione.
- È vietato l'uso di fax e fotocopiatrici per uso personale salvo esplicita autorizzazione del personale di ufficio.

di Priori Claudio - Ikaros Calcio

15

Sistemi di controllo graduati

- In caso di anomalie il personale del servizio ICT può:
 - effettuare controlli anonimi nei confronti di
 - Dipendenti
 - settori

di Priori Claudio - Ikaros Calcio

16