D.G.N. APPALTI srl

SEDE OPERATIVA/UFFICI:
Via Pietro De Francisci, 48/50
00165 Roma (RM)

Tel.: +39 0683774107
Fax: +39 0683774106
PEC: dgnappalti@legalmail.it
P.Iva: 12505611009

Policy Aziendale

Premessa

L'utilizzo delle tecnologie informatiche messe a disposizione dall'azienda, ed in particolare il libero accesso alla rete internet dai personal Computer aziendali, espone la società ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'azienda stessa. Inoltre dopo una corretta applicazione del Reg.UE 679/2016 e le norme in esso inserite, diventa necessaria la definizione di regole circa l'utilizzo delle tecnologie informatiche ed il collegamento esterno.

Pertanto il presente regolamento ha lo scopo di disciplinare l'utilizzo delle risorse informatiche e telematiche dell'azienda, tutelandone così il patrimonio e l'immagine, e di informare i lavoratori delle possibili implicazioni legate ad un uso non corretto degli strumenti informatici aziendali.

Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali debba sempre ispirarsi al principio della diligenza e correttezza, si adotta il presente regolamento.

Il Regolamento aziendale, di seguito riportato, viene incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e collaboratori e contiene informazioni utili per comprendere in quale modo il dipendente possa contribuire a garantire la sicurezza informatica di tutta l'Azienda.

Utilizzo del Personal Computer

Non è consentito al personale, senza la preventiva approvazione del Responsabile:

- installare o far installare altri programmi oltre a quelli in dotazione, rimuovere quelli esistenti o modificare la configurazione del sistema;
- installare altre periferiche, schede audio e video, dispositivi di memorizzazione oltre a quelle in dotazione;
- installare e/o utilizzare modem per il collegamento con reti, pubbliche o private, diverse da quelle aziendali;
- collegare alla rete personal computers o altri dispositivi portatili se non quelli assegnati dall'ente stesso.

Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di allontanamento dal posto di lavoro, deve essere inoltre attivato lo screen-saver per evitare l'utilizzo del PC da parte di estranei in caso di brevi assenze dal posto di lavoro, lo screen saver deve essere abilitato con password che sarà la stessa dell'accesso utente del sistema operativo.

Le informazioni salvate sul computer devono essere esclusivamente quelle necessarie al normale svolgersi delle attività lavorative.

E' indispensabile effettuare la pulizia periodica degli archivi con cancellazione dei file obsoleti, inutili o provvisori.

La conservazione dei supporti magnetici deve essere fatta in luogo idoneo. E' vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili.

Le gestioni locali dei dati dovranno scomparire, ove possibile, per essere sostituite da gestioni centralizzate su server.

Gli operatori del sistema informativo possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza sia sui PC degli incaricati sia sulle unità di rete.

L'incaricato aziendale o la società incaricata dall'azienda, nell'ambito della loro attività di gestione del sistema, provvedono a mantenere la corretta configurazione dei personal computers e ad impedire la modifica della stessa, utilizzando le tecniche e gli strumenti opportuni.

Utilizzo della posta elettronica

Si intende per account di posta elettronica l'abilitazione all'utilizzo di una casella personale o non personale sul server della società o sul proprio computer.

- Ognuno, può avanzare richiesta di assegnazione di una casella di posta intestata all'ufficio stesso.
- L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta all'amministratore di sistema.
- Una casella di posta elettronica (account) è caratterizzata da un nome ed una password. La password, generata casualmente, verrà comunicata in forma riservata dal responsabile delle password all'utilizzatore dell'account.
- 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.
- Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli e non cliccare su alcun link, testo o immagine presente.
- Nel caso di messaggi provenienti da mittenti conosciuti che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), non devono essere aperti.

- Evitare che la diffusione incontrollata di "catene " (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rar *.jpg). Nel caso in cui si debba inviare un documento all'esterno dell'azienda è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf). Tale software specifico è fornito previa richiesta.
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare se il sito è affidabile e richiedere l'autorizzazione alla direzione.
- La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
- E' obbligatorio controllare i file eseguibili di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Utilizzo di parole chiave per l'accesso al computer e alle procedure

Ogni dipendente assegnatario di personal computer dovrà scegliere una password per l'utilizzo dell'elaboratore. In tal caso, detta password, scritta su carta e conservata in busta chiusa, dovrà essere consegnata al custode delle password.
Tale password, inoltre, dovrà essere modificata ogni 6 (sei) mesi nel caso vengano trattati dati ordinari, ogni 3 mesi se si trattano dati sensibili o giudiziari.
Qualora gli assegnatari di personal computers utilizzino procedure software che richiedano, per l'accesso, ulteriori password, queste dovranno a loro volta essere gestite come descritto nel punto precedente.

Utilizzo di Internet

- Tutti i personal computers connessi alla rete locale sono dotati di accesso ad internet.
- Il pc abilitato alla navigazione in internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.
- E' assolutamente proibita la navigazione in internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
- E' fatto divieto all'utente il download di software gratuiti da siti internet, se non espressamente autorizzato dall'azienda.
- E' vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche e di registrazioni in guest books anche utilizzando pseudonimi.
- Non è consentita la visione di filmati, l'ascolto di files audio, l'utilizzo di programmi di chat e messaggistica, salvo il fatto che la direzione indichi tali programmi come necessari allo svolgimento dell'attività lavorativa del dipendente.
- E' necessario collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus e segnalare eventuali anomalie che possano mettere a rischio la protezione della macchina.
- I servizi informatici, nell'ambito della loro attività di gestione del sistema, adottano misure di controllo, filtraggio e monitoraggio delle connessioni e dei collegamenti ai siti internet e possono venire a conoscenza di siti e collegamenti visitati dagli utenti abilitati alla navigazione.
- Le anomalie e le minacce alla sicurezza e all'integrità dei dati riscontrate dovranno essere comunicate alla direzione per gli opportuni provvedimenti di competenza.

Protezione virus

I computers sono dotati di programma antivirus.
Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale. Ogni utente è tenuto a verificare la presenza e il regolare funzionamento del software antivirus aziendale. Nel caso in cui il software antivirus rilevi la presenza di un virus senza riuscire ad isolarlo, l'utente dovrà immediatamente: sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto all'amministratore di sistema.
Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.

Diffusione e consultazione

Il presente documento verrà esposto in apposita bacheca e notificato a tutti i dipendenti che utilizzano strumenti informatici per il lavoro d'ufficio a cui sono preposti.
Il presente documento viene controllato e revisionato alla luce di modifiche interne, tecnologiche o di legge.