POLICY DI SICUREZZA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone DIREZIONE DIDATTICA TODI ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa. Premesso che l'utilizzo delle risorse informatiche e telematiche aziendali deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente sono basilari in un rapporto di lavoro, DIREZIONE DIDATTICA TODI ha adottato il presente regolamento alla luce del nuovo regolamento europeo, per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

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 contiene informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza informatica di tutta l'Azienda. Tale prescrizione si aggiunge e integra le norme già previste dal contratto di lavoro nonché dal "GDPR" adottato dal 25 maggio 2018.

1 Utilizzo del Personal Computer

1.1 Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

1.2 Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte della DIREZIONE DIDATTICA TODI.

1.3 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte della DIREZIONE DIDATTICA TODI.

1.4 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio.

1.5 Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa.

1.6 Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili (.tmp) Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante (principio della non eccedenza).

1.7 La tutela della gestione locale di dati su stazioni di lavoro personali - personal computer che gestiscono localmente documenti e/o dati - è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo. E' comunque vietato l'uso di supporti di archiviazione removibili per la memorizzazione dei dati sensibili se non dotati si sistema di sicurezza (impronta digitale o altri dispositivi di criptazione) e comunque previa autorizzazione del Data Processor.

1.8 Le gestioni locali dei dati dovranno scomparire per essere sostituite da gestioni centralizzate su server entro e non oltre il 2019.

1.9 Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'azienda.

1.10 Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della legge n.128 del 21.05.2004.

1.11 Gli incaricati di DIREZIONE DIDATTICA TODI ad eseguire la manutenzione e gli interventi IT 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.

2. Utilizzo della rete di DIREZIONE DIDATTICA TODI

2.1 L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale (username e password).
2.2 E' fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati.
2.3 E' vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione dell'azienda.
2.4 E' vietato condividere cartelle in rete sia dotate di password, sia sprovviste di password se non dietro esplicita e formale autorizzazione dell'azienda.

3. Gestione delle Password

3.1 Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite da DIREZIONE DIDATTICA TODI.
3.2 L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
3.3 L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: 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.
3.4 La password deve essere immediatamente sostituita, dandone comunicazione a DIREZIONE DIDATTICA TODI, nel caso si sospetti che la stessa abbia perso la segretezza.

4. Utilizzo di dispositivi mobili e USB

4.1 L'utente è responsabile del dispositivi mobili e USB assegnatigli dall'Azienda e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
4.2 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.
4.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi in un luogo protetto.
4.4 Il portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari.
4.5 Nel caso di accesso alla rete aziendale tramite RAS (Remote Access Server) / Accesso Remoto utilizzare l'accesso in forma esclusivamente personale utilizzare la password in modo rigoroso.
4.6 Disconnettersi dal sistema RAS al termine della sessione di lavoro e non memorizzare la password.
4.7 Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'antivirus.

5. Uso della posta elettronica.

5.1 L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del a DIREZIONE DIDATTICA TODI.
5.2 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 (art. 615 comma 5 e segg. c.p.).
5.3 Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.
5.4 Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.
5.5 Interrompere immediatamente tutte le "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata)per evitare la raccolta abusiva di indirizzi di posta.

5.6 Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.rar *.jpg).
5.7 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 di DIREZIONE DIDATTICA TODI su tutte le postazioni.
5.8 L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
5.9 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
5.10 Per la trasmissione di file all'interno di DIREZIONE DIDATTICA TODI è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati che non devono mai superare i 10 MB.

6. Uso della rete Internet e dei relativi servizi
6.1 L'abilitazione alla posta esterna e ad Internet deve essere preceduta da regolare richiesta a DIREZIONE DIDATTICA TODI.
6.2 II PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.
6.3 E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
6.4 Non possono essere utilizzate vie private per il collegamento alla rete.
6.5 E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato di DIREZIONE DIDATTICA TODI.
6.6 E' 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).

7 Protezione antivirus
7.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc..).
7.2 Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale.
7.3 Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente: sospendere ogni elaborazione in corso senza spegnere il computer segnalare l'accaduto al Data Processor o ai suoi subordinati.
7.4 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.

8 Osservanza delle disposizioni in materia di Privacy
8.1 E' obbligatorio attenersi alle disposizioni di cui al General Data Protection Regulation nonché ai mansionari consegnati ad ogni dipendente incaricato al trattamento dei dati, che sono stati adeguatamente edotti tramite apposite sessioni di formazione.

9 Non osservanza della normativa aziendale
9.1 Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali previste dalle leggi (art. 171-ter - art. 248/00 - art. 547 - art.594 e 595 - art. 600-ter e seg. - art. 615 ter - art. 615 quater- art. 615-quinques - art. 617 quater - art. 617 quinquies - art. 617 sexies - art. 635-bis - art. 640 e 640 ter).