POLITICA UTILIZZO ACCETTABILE

Un sistema di sicurezza efficace è fondato su un lavoro di squadra, con la partecipazione ed il sostegno di ogni dipendente e ogni affiliato che si occupa di informazioni e/o dei sistemi di informazione. È responsabilità di ogni utente del computer conoscere queste linee guida e svolgere la propria attività di conseguenza.

SCOPO

Lo scopo di questa politica è quello di delineare l'uso accettabile di apparecchiature informatiche dell'organizzazione. Queste regole sono in vigore per proteggere il personale dai rischi di un uso improprio degli assets dell'organizzazione:

- ⇒ Non conformità legislativa
- ⇒ Attacchi di virus
- ⇒ Compromissione dei sistemi e servizi di rete

CAMPO DI APPLICAZIONE

Questa politica si applica ai dipendenti, collaboratori, consulenti, lavoratori temporanei, incluso tutto il personale affiliato a terze parti e a tutte le attrezzature di proprietà o in leasing dell'organizzazione.

MODALITÀ OPERATIVE

Uso Generale e Proprietà

- ⇒ Si ha la responsabilità di segnalare tempestivamente il furto, la perdita o la divulgazione non autorizzata di informazioni riservate.
- ⇒ Si può accedere, utilizzare o condividere informazioni di proprietà dell'organizzazione solo nella misura in cui è autorizzato e necessario per eseguire le proprie funzioni.
- ⇒ I dipendenti sono responsabili nell'uso personale dei dispositivi e, in caso di incertezza della politica da adottare, devono consultare il proprio supervisore o manager.
- ⇒ Per garantire la sicurezza e la costante manutenzione della rete, soggetti autorizzati all'interno dell'impresa possono monitorare le attrezzature, i sistemi e il traffico di rete in qualsiasi momento.
- ⇒ Le informazioni cartacee devono essere conservate in luogo/struttura adeguatamente protetta.
- ⇒ L'organizzazione si riserva il diritto di eseguire audit di sistemi e reti su base periodica per garantirne la conformità con questa politica.

Sicurezza e Proprietà delle Informazioni

- ⇒ Tutti i cellulari e i computer che si connettono alla rete interna devono rispettare la politica dell'Access Control.
- ⇒ Sia a livello di Sistema, che a livello di utente, le password devono essere conformi alla Politica delle Password. Fornire l'accesso a un altro individuo, deliberatamente o per propria mancanza, è vietato.
- ⇒ Tutti i dispositivi di elaborazione devono essere protetti in base alla politica "Clear Desk, Clear Screen".
- ⇒ i Dipendenti devono prestare estrema attenzione durante l'apertura di allegati di posta elettronica ricevuti da mittenti sconosciuti: potrebbero contenere malware.

Uso Inaccettabile
Le seguenti attività sono, in generale, vietate, tranne specifiche esenzioni, concesse per svolgere legittime responsabilità lavorative.
In nessun caso un dipendente è autorizzato a svolgere qualsiasi attività illecita ai sensi della legge locale, statale o internazionale, utilizzando risorse di proprietà dell'organizzazione.

Di seguito è riportato un elenco – da non considerarsi in alcun modo esaustivo - di attività che rientrano nella categoria di utilizzo inaccettabile nel tentativo di fornire un quadro di riferimento:

1. Le violazioni dei diritti di qualsiasi interessato al trattamento protetti da copyright, segreto commerciale, brevetti o altri diritti di proprietà intellettuale, o simili leggi o regolamenti, tra cui, ma non limitato a, l'installazione e/o la distribuzione "pirata" o senza adeguata licenza d'uso del software.
2. La copia non autorizzata di materiale protetto da copyright, tra cui, ma non limitato a, la digitalizzazione e la distribuzione di fotografie da riviste, libri o altro materiale protetto da copyright, musica protetta da copyright, e l'installazione di qualsiasi software protetto da copyright, per cui l'organizzazione o l'utente finale non dispone di una licenza attiva, è severamente proibito.
3. L'accesso ai dati di un server o di un account per qualsiasi scopo diverso da quello lavorativo, anche se si dispone di accesso autorizzato, è vietato.
4. L'esportazione di software, informazioni tecniche, software o tecnologia di cifratura, in violazione di norme internazionali o regionali, è illegale.
5. L'introduzione di programmi malevoli in rete o nel server (ad esempio, virus, cavalli di Troia, e-mail, etc.).
6. Rivelare la password del tuo account ad altri o consentire l'uso del proprio account da parte di altri. Questo include la famiglia, quando si lavora a casa.
7. Utilizzare un asset dell'impresa per attivamente ottenere o trasmettere materiale che viola le leggi concernenti le molestie sessuali o l'ambiente di lavoro ostile.
8. Fare offerte fraudolente di prodotti, oggetti o servizi provenienti da un qualsiasi account dell'organizzazione.
9. La realizzazione di violazioni della sicurezza o di interruzioni dell'attività di rete.
   Le violazioni della sicurezza comprendono, ma non sono limitate a:
   - l'accesso ai dati di cui il dipendente non è un destinatario.
   - l'accesso a un server o a un account a cui il dipendente non è espressamente autorizzato.

   Ai fini della presente politica, l'"interruzione delle attività" include, ma non è limitata a:
   - Denail of service: malfunzionamento dovuto ad un attacco informatico che impedisce al sistema di svolgere la propria attività ordinaria
10. La scansione delle porte o scansione di sicurezza, è espressamente vietata senza la preventiva segnalazione.
11. L'esecuzione di qualsiasi forma di monitoraggio della rete che è in grado di intercettare i dati non destinati al dipendente, a meno che faccia parte dell'attività lavorativa.
12. Fornire informazioni in merito o gli elenchi dei dipendenti a soggetti esterni.