Rev	Date	Description	Requested by	Prepared by	Approved by	Approval Signature
0	27/05/2017	First creation	Filippo Gentili	Simone Zabberoni	Marco Guardigli	

Information Security Management System Policy

L'azienda ottempera la gestione della sicurezza delle informazioni per mezzo di:

- Adozione di politiche per proteggere asset e informazioni da minacce interne/esterne deliberate o accidentali
- Allineare la gestione della sicurezza delle informazioni con il contesto strategico dell'organizzazione e gestire i rischi correlati
- Definire gli obiettivi legati alla sicurezza delle informazioni e stabilire i percorsi per raggiungerli
- Stabilire criteri per l'analisi dei rischi, relativa possibile riduzione, comprensione e accettazione
- Controllare accessi alle informazioni/asset (incluse le reti) basandosi sul business e sui livelli di sicurezza
- Proteggere informazioni e supporti fisici durante eventuali spostamenti e trasferimenti
- Proteggere le informazioni associate all'interconnessione dei sistemi informativi aziendali
- Attivare meccanisimi di protezione sulle informazioni condivise
- Attuare Politiche di "Clear Desk" sia per quanta riguarda i documenti che i supporti rimovibili
- Attuare Politiche di "Clear Screen" sugli strumenti utilizzati per l'erogazione dei servizi
- Implementare appropriate misure di sicurezza sui dispositive mobili e sulle comunicazioni
- Utilizzare appropriate sistemi crittografici per la protezione delle informazioni
- Garantire l'uso corretto, la protezione e la durata delle chiavi crittografiche amministrandone il completo ciclo di vita
- Adottare regole per la corretta gestione dei sistemi necessari al business
- Garantire la protezione delle attività dell'organizzazione accessibili da fornitori e da clienti
- Proibire l'uso di software non autorizzati, rispettare il licensing e le leggi sulla proprietà intellettuale
- Proteggere i dati organizzativi e salvaguardare la privacy
- Mantenere copie di backup delle informazioni, del software e delle immagini del sistema e testare regolarmente il corretto ripristino
- Mantenere registrazioni delle evidenze per un periodo sufficiente prima di eliminarle con attenzione
- Adottare Soluzioni disciplinari per scoraggiare l'uso improprio di sistemi e tecnologie da parte del personale
- Seguire i requisiti applicabili in materia di sicurezza delle informazioni, compresi i requisiti descritti nello standard ISO / IEC 27001: 2017
- Verificare l'efficacia e la corretta applicazione dell'ISMS ad intervalli regolari
- Migliorare e sviluppare continuamente il nostro ISMS.

ISMS Obiettivi

1. Assicurarsi che il nostro Business continui ad operare con il minimo disservizio
2. Assicurasi dell'assoluta integrità delle informazioni prodotte ed utilizzate dalla nostra organizzazione
3. Gestire tutte le informazioni rilevanti con il livello appropriato di riservatezza
4. Addestrare alla sicurezza delle informazioni i neo assunti entro 15 giorni dall'ingresso in azienda
5. Cercare di minimizzare gli incidenti legati alla sicurezza informatica a meno di 3 all'anno.

Date : 01-Jun-2019
Place: Ravenna (Italy)

_____
Marco Guardigli
(Managing Director)

NOTES:

1. Le politiche sopra indicate per la sicurezza delle informazioni sono approvate dal Top Management, pubblicate e communicate a tutti gli impiegati e alle parti esterne interessate

2. Target quantificabili e misurabili vengono utilizzati per raggiungere gli obiettivi di sicurezza delle informazioni. Il top management decide i target annuali all'inizio di ogni anno, che vengono poi comunicati alle persone interessate. I risultati sono rivisti contro gli obiettivi prefissi.

3. Le politiche di cui sopra per la sicurezza dell'informazione sono riesaminate dal Top Management a intervalli programmati (ogni 12 mesi) o se si verificano cambiamenti significativi per garantire la loro continuità di idoneità, adeguatezza ed efficacia.

REFERENCES:

ISO/IEC 27001:2017 Standard: Clauses 5.2 Policy
A.5 Information security policies