INFORMATION SECURITY POLICY

OBIETTIVI

L'obiettivo di Pellegrini, dichiarato attraverso la presente Information Security Policy ed il conseguente sviluppo di un Information Security Management System (ISMS) e di un Business Continuity Management System (BCMS) integrato, è la tutela del patrimonio informativo aziendale, in linea con la propensione al rischio informatico definito a livello aziendale. Tale tutela si ottiene attraverso l'adozione di misure di natura tecnologica, organizzativa e procedurale, commisurate alla criticità ed al valore delle informazioni stesse, atte a garantirne riservatezza, integrità e disponibilità.

PRINCIPI

Pellegrini:

- riconosce l'importanza della salvaguardia del valore aziendale nei suoi aspetti finanziari, fisici, di proprietà intellettuale e di reputazione;
- conduce le proprie attività conformandosi a principi di integrità e lealtà in ogni operazione e transazione, registrandole, autorizzandole e documentandole correttamente;
- garantisce la continuità del servizio, in accordo con le leggi e le normative vigenti;
- ottempera a tutte le leggi e normative che ne disciplinano l'attività ed esige da tutti i propri contraenti, consulenti e dagli altri soggetti terzi con i quali intrattiene relazioni, che si attengano alla medesima condotta;

Premesso quanto sopra, l'Information Security Management System (ISMS) si basa sui seguenti principi:

- l'organizzazione riconosce nel patrimonio informativo a sua disposizione un asset fondamentale; al fine del corretto perseguimento dei propri obiettivi di business si impegna ad adottare gli elementi di sicurezza necessari a garantirne un opportuno livello di protezione, estendendo tali misure fino alla tutela della sicurezza dei propri clienti;
- l'organizzazione ritiene che la corretta protezione di tale patrimonio debba basarsi sull'adozione di un approccio strutturato, completo e continuativo alle tematiche di sicurezza, che, partendo dagli obiettivi aziendali (di sicurezza) e dalle risorse che è necessario proteggere, permetta di individuare e valutare eventuali minacce e di contrapporre loro le opportune misure di mitigazione;
- l'organizzazione riconosce che l'istituzione, l'attuazione, il riesame, il mantenimento ed il miglioramento del sistema riguarda tutti i soggetti interni ed esterni (così come definiti nell'ambito di applicazione) che accedono alle informazioni aziendali, ognuno per quanto di propria competenza. Al fine di definire opportuni presidi di sicurezza, la società ha comunque altresì formalmente assegnato alcune delle responsabilità correlate a specifiche funzioni e soggetti aziendali;
- l'organizzazione si impegna, nei confronti dei soggetti apicali competenti, a fornire le necessarie risorse per una adeguata, corretta ed efficace protezione delle informazioni;
- l'organizzazione è consapevole che l'efficacia di un Information Security Management System (ISMS) dipenda anche dalla creazione di una cultura della sicurezza. Pertanto, si adopera, in merito, attraverso la sensibilizzazione sul tema e processi di formazione ad hoc.

Chief Information Officer
R.Prefumo