

# POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

L'obiettivo primario della Direzione è definire le politiche per la sicurezza delle informazioni, diffonderle e condividerle all'interno dell'organizzazione, promuovere e supportarle verso l'esterno.

Le politiche per la sicurezza delle informazioni sono sviluppate in conformità a:

- requisiti di business
- regolamenti, norme, prescrizioni legislative
- prescrizioni cliente – contrattuali
- prescrizioni interne
- valutazione del rischio in relazione alle informazioni gestite

## Obiettivi della Direzione:

- Definire i criteri ed attuare una metodologia per la valutazione dei rischi sulla sicurezza delle informazioni, determinando quindi i livelli di rischio accettabile ed i protocolli di intervento, laddove necessari;
- Monitorare e controllare i processi dell'organizzazione al fine di valutarne la comprensione delle politiche, garantire l'adeguatezza e il miglioramento continuo del Sistema di gestione mediante opportuni indicatori e la definizione di obiettivi e traguardi di sviluppo;
- Definire ed attribuire le responsabilità in relazione alle mansioni ed alla tipologia delle informazioni;
- Definire regole per l'accesso alle reti ed ai servizi di rete in relazione alle attività svolte ed alla classificazione degli asset;
- Attuare piani di reazioni in caso di scostamenti;
- Riesaminare periodicamente il sistema ed investire nel continuo ammodernamento della struttura informatica.

## Politiche operative:

- **Attuazione delle politiche:** i dipendenti, i collaboratori, i fornitori, i partner e tutte le altre terze parti coinvolti nelle attività di Elmeg adempiono ai loro obblighi e responsabilità individuali, al fine di proteggere le informazioni, i beni e le risorse;
- **Controllo degli accessi:** l'accesso alle informazioni, beni e risorse vengono controllati e monitorati; l'accesso è autorizzato solo per le informazioni necessarie (need to know); mentre l'accesso è autorizzato solo per le informazioni riguardanti specifiche attività previamente autorizzate;
- **Sicurezza fisica, ambientale e logica:** l'accesso alle informazioni, ai beni ed alle risorse viene affidato a personale autorizzato, formato e competente. Inoltre, un sistema di monitoraggio controlla il processo di accesso e di autorizzazione. All'interno dello stabilimento, l'accesso a canali di comunicazione pubblica (es. wi-fi), è permesso attraverso una rete dedicata agli ospiti ("Guest"). I locali, destinati ad avere apparecchiature informatiche oppure archiviazioni, sono identificati e protetti dagli accessi indesiderati.
- **Sicurezza dei dati nella progettazione, sviluppo ed industrializzazione del prodotto:** le informazioni interne ed esterne vengono gestite da personale appositamente formato e consapevole dell'importanza delle informazioni gestite.
- **External hosting:** i dati classificati come interni, possono essere archiviati mediante hosting esterno certificato Tisax (label Livello 3).
- **Protezione da malware:** il sistema di sicurezza prevede diversi livelli di filtraggio, attraverso firewall perimetrale e antivirus operativo sui singoli asset;
- **Protezione e salvataggio dei dati (backup):** tutte le informazioni vengono protette da perdite volontarie ed involontarie, attraverso l'attuazione di procedure di salvataggio. Elmeg ha sviluppato un sistema di salvataggio a che garantisce il tempestivo controllo, attraverso la rendicontazione degli eventi delle attività eseguite;
- **Privacy e protezione dei dati personali:** Elmeg si impegna ad attuare quanto previsto dalle normative locali e regolamenti EU in materia;
- **Rapporti con i fornitori, le società di servizi:** la Direzione coinvolge e responsabilizza i propri fornitori e le terze parti con cui collabora mediante specifici accordi di Non Disclosure Agreement (NDA).

La Direzione

Gianluca Giordano

