

POLITICA DI CYBERSECURITY DEL GRUPPO SCHILLER

Impegno per la cybersecurity

SICUREZZA INFORMATICA

SCHILLER si impegna per la cybersecurity:

- ❖ Il nostro obiettivo è quello di aderire allo standard ISO 27001 e agli altri requisiti applicabili in materia di sicurezza informatica, in modo da gestire e mitigare efficacemente i rischi di cybersecurity in tutte le nostre attività.
- ❖ Ci impegniamo ad adempiere ai nostri obblighi di conformità.
- ❖ Le nostre misure mirano a garantire la protezione delle informazioni personali e delle ePHI in conformità alle leggi sulla privacy applicabili.
- ❖ Ci assicuriamo che la cybersecurity sia perfettamente integrata nei nostri processi aziendali, in modo da mantenere il nostro impegno nei confronti della cybersecurity e della gestione della qualità.
- ❖ Stabiliamo obiettivi compatibili con la direzione strategica e il contesto della nostra organizzazione.
- ❖ Con la protezione dei segreti commerciali e delle informazioni proprietarie da accessi e divulgazioni non autorizzati, rafforziamo il nostro impegno a fornire dispositivi e servizi medici di alta qualità.

MIGLIORAMENTO CONTINUO

SCHILLER si impegna a migliorare continuamente la sicurezza informatica

- Il nostro impegno comprende valutazioni periodiche dei rischi e l'adozione di controlli tecnici e organizzativi adeguati per gestire i rischi di cybersecurity.
- Conduciamo audit e verifiche per valutare costantemente l'idoneità, l'adeguatezza e l'efficacia delle misure di cybersecurity.
- Determiniamo le opportunità di miglioramento e assicuriamo la disponibilità delle risorse necessarie.
- Integriamo pratiche solide di cybersecurity nel nostro sistema di gestione della qualità per mantenere gli standard più elevati dei nostri prodotti e servizi.

SENSIBILIZZAZIONE DEI DIPENDENTI

SCHILLER informa e forma i propri dipendenti sulla cybersecurity

- Ci impegniamo a salvaguardare l'integrità, la riservatezza e la disponibilità delle risorse informative, che comprendono i processi di produzione, l'infrastruttura ICT, le informazioni personali, le informazioni sanitarie elettroniche protette (ePHI) e i segreti commerciali.
- Comunichiamo questa politica ai nostri dipendenti.
- Ci assicuriamo che i dipendenti siano consapevoli dei rischi di cybersecurity e dei vantaggi derivanti da un'efficace gestione e mitigazione di tali rischi in tutte le nostre attività.
- I nostri dipendenti comprendono l'importanza della cybersecurity e si attengono ai requisiti applicabili.