Ulteriori Politica per la Sicurezza delle Informazioni

Politica per la Classificazione, Etichettatura e Trasferimento delle Informazioni (Punto Tisax 1.3.2)
Riguardo alle informazioni PSE stabilisce i principi chiave per la loro classificazione, etichettatura e trattamento sia in forma elettronica che cartacea.

Politica per la Gestione degli incidenti relativi alla sicurezza delle informazioni (Punto Tisax 1.6.1)
Lo scopo della presente politica è quello di identificare il flusso di lavoro per la gestione degli Incident di sicurezza all'interno dell'organizzazione PSE.

Politica per i dispositivi mobili e il telelavoro (Punto Tisax 2.1.4)
Lo scopo della presente politica è quello di garantire la dovuta attenzione alla sicurezza delle informazioni e dei sistemi accessibili attraverso telelavoro e lavoro mobile, e di ridurre il rischio di violazioni della sicurezza, anche fuori dal posto di lavoro usuale.
Per proteggere dati e informazioni da azioni illegali e/o dannose svolte in modo consapevole o inconsapevole, PSE adotta misure tecniche e organizzative appropriate contro la perdita, il cambiamento, la distruzione o il danneggiamento accidentale e/o intenzionale dei dati personali e, in senso più esteso, dei dati e delle informazioni.
Inoltre PSE istruisce il proprio personale abilitato al telelavoro in modo che sia a conoscenza delle procedure e delle politiche di sicurezza, in termini di piena comprensione e rispetto.

Politica per Piano di continuità operativa PCB e Piano disaster recovery PDR (Punti Tisax 1.6.3 – 5.2.8 – 5.2.9)
Nell'ambito delle attività svolte da PSE, l'erogazione del servizio interno di Information Communication Technologies (ICT) rappresenta una parte essenziale al buon funzionamento dell'azienda stessa, da cui consegue la necessità di garantirne una sua continuità operativa.
Per questa ragione la Società si è dotata di un Piano di Continuità Operativa (BCP: Business Continuity Plan) e Disaster Recovery Plan (DRP) al fine di disporre di procedure atte a gestire e superare condizioni di emergenza e di disastro che impediscono la normale erogazione del servizio medesimo.

Politica per il controllo degli accessi (Punto Tisax 4.1.2)
Scopo della presente politica è quello di limitare l'accesso alle informazioni e ai servizi di elaborazione delle informazioni e prevenire l'accesso non autorizzato a sistemi ed applicazioni.

Politica di gestione delle password (Punto Tisax 4.1.3)
Scopo della presente politica è quello di definire la gestione delle informazioni segrete di autenticazione degli utenti.

Politica sull'uso dei controlli crittografici (Punto Tisax 5.1.1)
L'organizzazione PSE adotta sistemi per assicurare un uso corretto ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni ovunque questo sia necessario e/o possibile.

Politica per il trasferimento delle informazioni (Punto Tisax 5.1.2)
L'organizzazione PSE adotta sistemi di trasferimento delle informazioni, con ausilio di idonei strumenti, atti a preservare l'integrità , la riservatezza e la disponibilità delle informazioni stesse.

Politica per la gestione dei cambiamenti (Punto Tisax 5.2.1)
Scopo di tale politica è quello di definire come vengono controllati i cambiamenti interni a PSE che possono influenzare la sicurezza delle informazioni.

Politica per il controllo contro Malware (Punto Tisax 5.2.3)
Scopo della presente politica è assicurare che le informazioni e le strutture preposte alla loro elaborazione siano protette contro il malware

Politica di Gestione delle vulnerabilità tecniche (Punto Tisax 5.2.5)
Scopo della presente politica è prevenire lo sfruttamento di vulnerabilità tecniche.

Politica di Gestione della sicurezza dei servizi di rete (Punto Tisax 5.3.2)
Scopo di tale politica è quello di assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.

PSE - Viale Umbria 4 - Grezzago (MI) Italia – Data : 25//02/2025 **La Direzione : PSE**