Politica di sicurezza delle informazioni

Campo di Applicazione

La presente politica stabilisce gli obiettivi strategici, i principi fondamentali e il quadro di riferimento per la gestione della sicurezza delle informazioni all'interno di Avid Technology Srl.

Il suo scopo è proteggere gli asset informativi dell'organizzazione da ogni minaccia, interna o esterna, intenzionale o accidentale, garantendone la riservatezza, l'integrità e la disponibilità. La politica si applica a tutto il personale, ai collaboratori, ai processi di business, ai dati e ai sistemi informativi gestiti dall'azienda, in conformità con i requisiti dello standard ISO/IEC 27001.

Riferimenti Normativi

- **ISO 27001:2022:** Requisiti per i sistemi di gestione della sicurezza delle informazioni.
- **ISO 27002:2022**: Sicurezza delle informazioni, cybersecurity e protezione della privacy – Controlli di sicurezza delle informazioni.
- Requisiti legali, normativi, regolamentari e contrattuali applicabili in materia di sicurezza delle informazioni e protezione dei dati personali.

Termini e Definizioni

- **Riservatezza**: La proprietà che le informazioni non siano rese disponibili o divulgate a persone, entità o processi non autorizzati.
- **Integrità**: La proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità**: La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.
- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)**: Un insieme di policy, procedure, linee guida e risorse associate, gestite collettivamente da un'organizzazione, per proteggere i suoi asset informativi.

Ruoli e Responsabilità

- **Direzione Generale/Amministratore Delegato:** definisce e guida la strategia aziendale per la sicurezza delle informazioni, approva la presente politica e si impegna a fornire le risorse necessarie per la sua efficace attuazione, mantenimento e miglioramento continuo. Fissa gli obiettivi, garantisce la coerenza con le strategie aziendali e assicura un adeguato budget per la sicurezza

- **Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (RSGSI)**: assicura la pubblicazione, la comunicazione e la revisione della politica di sicurezza. È responsabile dell'integrazione dei suoi principi nelle attività quotidiane e del corretto funzionamento del SGSI in conformità alla norma di riferimento.
- **Direzione Risorse Umane**: collabora alla definizione e alla comunicazione delle responsabilità individuali in materia di sicurezza delle informazioni, assicurandone l'integrazione nelle mansioni e la consapevolezza del personale durante l'intero ciclo di vita del rapporto di lavoro.
- **Personale Dipendente:** deve rispettare le procedure di sicurezza e segnalare eventuali anomalie o debolezze di sicurezza.
- **Soggetti Esterni (Fornitori e Collaboratori):** devono garantire il rispetto dei requisiti di sicurezza previsti, anche mediante la sottoscrizione di un “patto di riservatezza”.

Obiettivi di sicurezza delle informazioni

Avid Technology Srl definisce e sostiene i seguenti obiettivi strategici per la sicurezza delle informazioni, in linea con il contesto aziendale e gli indirizzi strategici definiti nella "POL Politica del sistema di gestione":

- **Riservatezza**: Garantire che l'accesso alle informazioni, inclusi i dati di progetto, la proprietà intellettuale e le informazioni dei clienti, sia consentito esclusivamente al personale autorizzato.
- **Integrità**: assicurare l'accuratezza, la completezza e la validità delle informazioni e dei sistemi di elaborazione in ogni fase del loro ciclo di vita. L'integrità dei dati è fondamentale per la progettazione e la realizzazione di infrastrutture tecnologiche affidabili e per la corretta gestione dei sistemi hardware e software commercializzati.
- **Disponibilità**: garantire che le informazioni, i sistemi e le infrastrutture tecnologiche siano sempre accessibili e utilizzabili quando richiesto dai processi di business, dai clienti e dalle parti interessate.
- **Conformità**: rispettare tutti i requisiti legali, normativi, regolamentari e contrattuali applicabili in materia di sicurezza delle informazioni e protezione dei dati personali, inclusi gli obblighi derivanti da accordi con clienti e fornitori.
- **Gestione del Rischio**: implementare e mantenere un processo sistematico di gestione del rischio per la sicurezza delle informazioni, come descritto nella "PRO Procedura di gestione dei rischi", al fine di identificare, valutare e trattare le minacce agli asset informativi in modo proporzionato ed efficace.
- **Miglioramento Continuo**: promuovere il miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) attraverso il monitoraggio delle prestazioni, gli audit e il riesame periodico, in conformità con lo standard ISO/IEC 27001.

Il raggiungimento di questi obiettivi è responsabilità di tutto il personale ed è supportato attivamente dall'Amministratore Delegato attraverso la fornitura delle risorse necessarie.

Principi fondamentali di sicurezza delle informazioni

Impegno della Direzione e Gestione della Politica

La presente politica è approvata dall'Amministratore Delegato, che si impegna a garantirne l'applicazione e a fornire le risorse necessarie per il suo mantenimento.

Il Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (RSGSI) ha la responsabilità di:

- Pubblicare e comunicare la presente politica a tutto il personale e alle parti interessate rilevanti.
- Assicurare che i principi qui contenuti siano compresi e integrati nelle attività quotidiane.
- Rivedere questa politica con cadenza almeno annuale, o a seguito di cambiamenti significativi che possano impattare il SGSI, in accordo con la "PRO Procedura di gestione del cambiamento" e la "PRO Gestione riesame della direzione".

La gestione documentale della presente politica e dei documenti correlati segue le direttive della "PRO Procedura di gestione delle informazioni documentate".

Responsabilità Condivisa della Sicurezza

La sicurezza delle informazioni è una responsabilità condivisa che coinvolge l'intera organizzazione. Sebbene ruoli specifici abbiano compiti definiti, ogni membro del personale è responsabile della protezione degli asset informativi a cui ha accesso.

- Le responsabilità specifiche in materia di sicurezza sono formalizzate e assegnate nella "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni".
- La Direzione Risorse Umane, in collaborazione con il RSGSI, deve assicurare che le responsabilità di sicurezza siano integrate nelle mansioni del personale e comunicate durante l'intero ciclo di vita del rapporto di lavoro, come stabilito nella "PRO Procedura di gestione delle risorse umane".
- Tutto il personale è tenuto a rispettare le direttive contenute nel "Codice di condotta" aziendale.

Uso Accettabile delle Risorse Aziendali

Tutti gli asset informativi di Avid Technology Srl, inclusi hardware, software, dati, reti e sistemi, devono essere utilizzati esclusivamente per scopi aziendali autorizzati e in modo responsabile e sicuro.

- L'accesso e l'utilizzo delle risorse sono concessi sulla base del principio del minimo privilegio e delle necessità operative legate al proprio ruolo.

- Le regole dettagliate per l'uso corretto e sicuro delle risorse aziendali sono definite nella "POL Politica di sicurezza operativa", alla quale tutto il personale è tenuto a conformarsi.

Protezione degli Asset e delle Informazioni

Avid Technology Srl adotta il principio della "difesa in profondità" per proteggere i propri asset informativi da accessi non autorizzati, divulgazione, modifica, distruzione o furto.

- **Protezione Fisica e Logica**: gli asset devono essere protetti da minacce fisiche e logiche, sia all'interno che all'esterno delle sedi aziendali. La loro gestione, configurazione e smaltimento devono seguire la "PRO Procedura di configurazione, gestione e smaltimento degli asset".
- **Clear Desk e Clear Screen**: tutto il personale deve assicurare che le informazioni sensibili, in formato cartaceo o su supporti rimovibili, non siano lasciate incustodite sulle postazioni di lavoro. Le postazioni informatiche devono essere protette da un blocco schermo automatico che si attiva dopo un massimo di 10 minuti di inattività.
- **Sicurezza degli Asset Fuori Sede**: gli asset aziendali utilizzati al di fuori delle sedi, inclusi quelli impiegati in modalità di lavoro agile, devono essere protetti con la stessa diligenza di quelli in ufficio. Il personale è tenuto a seguire le direttive specifiche per la sicurezza nel lavoro da remoto.
- **Classificazione delle Informazioni**: le informazioni devono essere gestite e protette in base al loro livello di criticità, come definito nella "POL Politica di classificazione ed etichettatura delle informazioni".

Segnalazione degli Eventi e delle Debolezze di Sicurezza

Tutto il personale e i collaboratori hanno l'obbligo di segnalare tempestivamente qualsiasi evento di sicurezza delle informazioni, sospetto o confermato, e qualsiasi debolezza identificata nei sistemi o nei processi.

- La segnalazione deve avvenire attraverso i canali ufficiali designati dal RSGSI.
- La gestione degli eventi e degli incidenti segnalati è disciplinata dalla "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni", che ne garantisce l'analisi, il contenimento e la risoluzione.

Archiviazione e Aggiornamenti

Il presente documento è gestito in conformità alla "PRO Procedura di gestione delle informazioni documentate". Viene riesaminato con cadenza almeno annuale e aggiornato ogni qualvolta si verifichino cambiamenti organizzativi, tecnologici o normativi significativi, sotto la supervisione del RSGSI e con l'approvazione dell'Amministratore Delegato.

Data di ultima revisione è il 17/10/2025.