

Politica - Sicurezza delle informazioni

Estratto

Code:	PO-001
Version:	02
Validity date:	25.02.2025
Classification:	Public
Type:	Policy

	Issuance	Validation	Approval
Role	RSGIS	Risk Management Team	Board of Directors
Name	Uboldi	Lombardini	Bernardini
Signature	<i>(signed in original)</i>	<i>(signed in original)</i>	<i>(signed in original)</i>

1 Scopo

L'Organizzazione di Tecniplast SPA (di seguito -L'Organizzazione-) si è posta l'obiettivo di implementare e attuare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) in conformità con i requisiti dello standard UNI CEI EN ISO/IEC 27001:2022, per garantire le caratteristiche di *Riservatezza*, *Integrità* e *Disponibilità* (RID) delle informazioni trattate nell'ambito del perimetro di certificazione individuato.

La presente politica è intesa quale strumento finalizzato a:

- consentire a tutto il personale coinvolto di comprendere, attuare e sostenere i principi, gli impegni e gli obiettivi stabiliti attraverso le politiche di sicurezza;
- permettere la conoscenza delle modalità organizzative e dei comportamenti adottati per garantire il raggiungimento degli obiettivi per la sicurezza delle informazioni, nell'ambito del perimetro individuato.

2 Principi base

- **Centralità delle Persone** - determinante per l'efficacia dei processi aziendali e la creazione del valore – sensibilizzazione, formazione ed aggiornamento del personale, in modo pertinente alla propria attività lavorativa, definendo le competenze richieste per la gestione dei relativi processi e promuovendo consapevolezza tra le risorse, in merito agli obiettivi specifici per la sicurezza.
- **Gestione, sicurezza e classificazione delle informazioni** - garantire che gli Asset e le informazioni correlate siano opportunamente tracciati e classificati, al fine di facilitare il corretto utilizzo e quindi, l'implementazione di misure di protezione adeguate (es: modalità di condivisione di Informazioni Riservate o Strettamente Riservate).
- **Gestione infrastruttura Informatica** – adozione delle di best practices tecniche e procedurali per garantire la sicurezza informatica in un'ottica di miglioramento continuo per la tutela delle informazioni.
- **Gestione della continuità operativa** – implementazione di un sistema di *Business Continuity*, con lo scopo di fornire le linee guida per la gestione della continuità di business della società, mediante l'analisi ed il trattamento dei rischi, nonché di un *Disaster Recovery Plan*, atto a consentire, nell'ipotesi di evento disastroso, il ripristino tempestivo, o comunque nel minor tempo possibile, delle funzionalità dei servizi erogati.
- **Gestione della sicurezza fisica** – assicurare protezione contro le minacce di eventi naturali, intenzionali ed accidentali che possono arrecare danni alle persone e ai beni aziendali.
- **Promozione della cultura della Sicurezza nei rapporti con dipendenti e collaboratori** - formalizzazione all'interno degli accordi contrattuali con il personale ed i collaboratori, delle reciproche responsabilità (es: autorizzazioni al trattamento, nonché impegni di riservatezza); implementazione di un programma di sensibilizzazione per la sicurezza delle informazioni, anche definendo le regole per il corretto utilizzo dei device in dotazione.
- **Gestione degli aspetti di sicurezza nei rapporti con i fornitori** – mitigazione dei rischi associati all'accesso agli asset da parte delle terze parti e quindi definizione dei requisiti di sicurezza che devono essere rispettati per la regolamentazione dei rapporti con terze parti che, per erogare i servizi concordati, hanno necessità di accedere alle risorse informative della Società.
- **Sicurezza degli accessi logici** – implementazione di un sistema di autenticazione degli utenti, il quale deve prevedere un'adeguata profilatura degli stessi e l'adozione di misure di controllo di natura tecnologica e organizzativa.
- **Gestione degli Incidenti** – implementazione di un sistema efficace di gestione degli incidenti che hanno impatto sulle informazioni e sui dati personali (nomina di un team dedicato, prontezza di azione, analisi d'impatto e di remediation), al fine di preservare la continuità operativa della società.

END OF THE DOCUMENT / FINE DEL DOCUMENTO

(This page intentionally left blank) / (pagina intenzionalmente vuota)