

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Indice

1. Premessa	3
2. Principi di sicurezza informatica	3
Obiettivi	3
Framework	3
Ambiti di intervento	4
3. Misure di sicurezza	4
4. Ruoli e responsabilità	5
Head of IT Infrastructure	5
Data Protection Officer	6
Staff	6

1. Premessa

L'informazione è una delle componenti del business che ha un valore strategico per l'azienda e che, conseguentemente, deve essere adeguatamente protetta. La sicurezza delle informazioni ha come fine la protezione dell'informazione rispetto ad un'ampia gamma di attacchi per garantire la continuità del business e minimizzare i danni e le interruzioni.

L'informazione può esistere sotto diverse forme: stampata o scritta su carta, memorizzata elettronicamente, trasmessa per posta o con mezzi elettronici, registrata o trasmessa verbalmente. In ogni caso, ancorché possa essere trattata in tutte le forme sopra elencate, l'informazione deve sempre essere protetta secondo le seguenti procedure e le norme vigenti.

Il presente documento raccoglie le regole generali emanate in coerenza con gli obiettivi di mantenimento della sicurezza delle informazioni e protezione dei dati, risulta altresì strumento atto a fornire al Titolare del trattamento dei dati garanzie in merito all'esistenza e attuazione di misure tecniche e organizzative idonee ad assicurare il rispetto delle disposizioni in materia di trattamento dei dati personali.

2. Principi di sicurezza informatica

Obiettivi

La Policy si pone l'obiettivo di gestire la sicurezza delle informazioni, fornendo un servizio sicuro e affidabile a clienti, utenti finali, personale, e altre parti interessate, garantendo

- **Confidenzialità:** garantisce che l'informazione sia accessibile solamente a coloro che hanno l'autorizzazione ad accedervi;
- **Integrità:** garantisce l'accuratezza e la completezza dell'informazione e dei metodi di elaborazione;
- **Disponibilità:** garantisce che gli utenti autorizzati possano accedere all'informazione quando vi è necessità;

in considerazione delle disposizioni legali, normative e contrattuali pertinenti.

Framework

L'approccio alla gestione della sicurezza delle informazioni, in linea con lo standard internazionale per la sicurezza delle informazioni, ISO/IEC 27001:2022, si basa su cinque componenti chiave, ovvero:

1. **Identificare:** garantire una visione documentata dei dati detenuti, archiviati ed elaborati, consentendo la protezione delle risorse di dati.
2. **Proteggere:** garantire che gli standard minimi di controllo della sicurezza delle informazioni siano ben progettati e funzionino in modo efficace per proteggere i dati.
3. **Rilevare:** garantire il rilevamento delle minacce informatiche, intese come il rilevamento delle intrusioni, la prevenzione della perdita di dati e l'intelligence sulle minacce.
4. **Rispondere:** garantire che gli incidenti siano identificati, registrati e segnalati, con processi di rimedio proporzionati e allocazione delle risorse.
5. **Recuperare:** garantire che sia in atto un efficace quadro di gestione delle crisi informatiche con pianificazione e test di scenari dedicati.

Ambiti di intervento

POLITICHE DI SICUREZZA DELLE INFORMAZIONI

assicurare che siano in atto politiche, standard, procedure e note guida sulla sicurezza delle informazioni, politiche approvate dal Consiglio e comunicate chiaramente a tutti i dipendenti.

CONSAPEVOLEZZA

garantire la consapevolezza e la comprensione della salvaguardia delle informazioni tramite programmi di formazione e sensibilizzazione e la condivisione delle politiche di sicurezza informatica.

CLASSIFICAZIONE DELLE INFORMAZIONI

identificare le informazioni critiche e determinare il livello di protezione appropriato richiesto per preservare la riservatezza, l'integrità e la disponibilità delle informazioni

CONTROLLO DEGLI ACCESSI

garantire il controllo degli accessi (con privilegi frequentemente rivisti) e la responsabilità del personale per la gestione delle proprie password

CRITTOGRAFIA

la crittografia deve essere utilizzata in modo efficace per proteggere la riservatezza, l'autenticità e l'integrità delle informazioni

SICUREZZA FISICA E AMBIENTALE

assicurare che siano in atto misure di sicurezza fisica in tutte le sedi degli uffici per impedire l'accesso non autorizzato a informazioni sensibili

SICUREZZA DELLE OPERAZIONI

assicurare la protezione delle strutture di elaborazione dati da malware, perdita di dati e sfruttamento di vulnerabilità tecniche

SICUREZZA DELLE COMUNICAZIONI

assicura la sicurezza di tutte le informazioni trasferite, sia internamente che esternamente.

ACQUISIZIONE, SVILUPPO E MANUTENZIONE DEL SISTEMA

considerare la sicurezza delle informazioni nel ciclo di vita dello sviluppo dei sistemi informativi e proteggere i dati durante tutto il processo di test

ESTERNALIZZAZIONE DEI SERVIZI

Gestire la sicurezza delle informazioni nella catena di approvvigionamento esterno

GESTIONE DEGLI INCIDENTI DI SICUREZZA DELLE INFORMAZIONI

assicurare la gestione coerente ed efficace degli incidenti di sicurezza e delle vulnerabilità

ASPETTI DI SICUREZZA DELLE INFORMAZIONI DELLA GESTIONE DELLA CONTINUITÀ AZIENDALE

garantire che la sicurezza delle informazioni durante l'interruzione sia gestita secondo gli obiettivi di continuità aziendale e di disaster recovery

CONFORMITÀ

proteggere le informazioni in conformità con i requisiti legali, statutari, normativi e contrattuali

3. Misure di sicurezza

La Politica per la Sicurezza delle Informazioni e i seguenti Standard sono in vigore per supportare i requisiti specifici del Framework di Sicurezza delle Informazioni e devono essere letti congiuntamente alla presente Politica:

1. Data Protection Policy

gestione dei processi e delle procedure in riferimento al trattamento dei dati personali e particolari, in considerazione delle leggi pertinenti sulla protezione dei dati, in primo luogo il Regolamento Generale sulla protezione dei Dati (GDPR).

2. Information asset management

gestione efficiente delle apparecchiature IT durante il ciclo di vita, per garantire il loro funzionamento dall'acquisto alla dismissione, gestione delle patch e monitoraggio della sicurezza.

3. Classificazione e gestione delle informazioni

gestione della protezione delle informazioni nell'intero ciclo di vita, dalla loro origine alla loro distruzione, valutazione e gestione del rischio associato all'accesso non autorizzato, la divulgazione, la modifica o altri usi impropri.

4. Gestione degli incidenti e data breach

criteri generali e soluzioni adottate per la gestione degli incidenti di sicurezza di natura informatica aventi impatti diretti e/o potenziali sui sistemi e sul business aziendale. Misure organizzative atte a garantire la corretta identificazione, comunicazione e reazione.

5. Gestione dei fornitori terzi

gestione dei rapporti con i fornitori, all'avvio e durante l'intero periodo contrattuale; valutazione del potenziale impatto del rischio associato alla condivisione delle informazioni della società e/o dei dati dei clienti.

6. Regolamento per l'utilizzo degli asset

utilizzo dei beni aziendali, gestione dei programmi, assistenza e aggiornamento, gestione delle password, utilizzo della rete e della posta elettronica aziendale, remote working

7. Sicurezza fisica dell'ufficio

quadro di controlli interni in grado di garantire un livello adeguato di processi, strutture, attrezzature e sistemi per la sicurezza fisica dell'ufficio, delle informazioni archiviate e delle apparecchiature installate.

8. Autenticazione e controllo degli accessi

insieme di processi per l'adeguata governance delle risorse che a vario titolo accedono ai sistemi aziendali, al fine di preservare in ultima istanza la sicurezza dei dati e delle informazioni. Gestione delle password e profilazione dell'utente nel rispetto del principio del minimo privilegio "need to know".

9. Gestione della sicurezza delle operazioni IT

controlli tesi a contribuire ad attenuare i rischi tecnici associati alla gestione della sicurezza delle informazioni: gestione delle modifiche, protezione da malware, gestione delle vulnerabilità tecniche, crittografia, sicurezza generale della rete e continuità aziendale.

4. Ruoli e responsabilità

Head of IT Infrastructure

- Effettuare valutazioni tecniche della vulnerabilità dei sistemi e dei processi IT, identificare potenziali vulnerabilità e garantire che le lacune individuate vengano corrette;
- Coordinare l'aggiornamento delle policy di sicurezza delle informazioni e gli standard, le procedure e le linee guida di accompagnamento;

	SISTEMA DI GESTIONE INTEGRATO	Indirizzi strategici della Direzione <i>Leadership e impegno</i> POL SGQ_03_ISMS_INFO_SECURITY Ed 1.0 del 01/08/2025
---	--	--

- Rispondere e indagare sugli incidenti di sicurezza delle informazioni;
- Coordinare le revisioni periodiche della sicurezza delle informazioni di sistemi, processi e infrastrutture;
- Supervisionare i requisiti di manutenzione della tecnologia di sicurezza su firewall, patch, antivirus, ecc.;
- Fornire consulenza sulla sicurezza per appalti, progetti e nuove iniziative;
- Implementare un programma di penetration test.

Data Protection Officer

Il DPO svolgerà i seguenti compiti in piena autonomia e indipendenza ai sensi dell'articolo 39 del GDPR:

- Informare, consigliare e formulare raccomandazioni in merito alla conformità al GDPR. Nell'ambito di questi compiti di monitoraggio della conformità, il DPO sarà tenuto a:
 - ✓ Raccogliere informazioni per identificare le attività di trattamento; e
 - ✓ Analizzare e verificare la conformità delle attività di trattamento.
- Promuovere una cultura della protezione dei dati all'interno del Gruppo e contribuire all'implementazione degli elementi essenziali del GDPR;
- Offrire consulenza in caso di violazione dei dati personali o altro incidente relativo ai dati personali;
- Cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento

Staff

Tutto il personale ha la responsabilità di garantire il rispetto dei principi e dei controlli di sicurezza delle informazioni delineati nella presente Politica, nonché di segnalare tempestivamente sospette violazioni della presente Politica al responsabile di linea, al Responsabile della Sicurezza delle Informazioni, al DPO o all'helpdesk IT.

Tutte le gravi violazioni della presente Politica, della Politica di Gruppo sulla Protezione dei Dati e degli Standard associati saranno oggetto di indagine. Qualora le indagini rivelino comportamenti scorretti, potranno essere adottati provvedimenti disciplinari in linea con le procedure disciplinari.