POLICY AZIENDALE PER LA SICUREZZA DELLE INFORMAZIONI

CLASSIFICAZIONE DEL DOCUMENTO

Contrassegnare il caso di pertinenza:

TIPO	DESCRIZIONE	Flag
PUBBLICO (PUBLIC)	Un documento pubblico può essere modificato solamente da chi ha completato l'iter di redazione, controllo e approvazione, è primariamente destinato ai componenti la lista di distribuzione ma può essere visualizzato da tutti all'interno dell'organizzazione. Può essere divulgato al di fuori dell'organizzazione.	**X**
INTERNO (CONFIDENTIAL)	Un documento interno può essere modificato solamente da chi ha completato l'iter di redazione, controllo e approvazione, è primariamente destinato ai componenti la lista di distribuzione ma può essere visualizzato da tutti all'interno dell'organizzazione. Non può essere divulgato al di fuori dell'organizzazione.	
RISERVATO (RESTRICTED)	Un documento riservato può essere modificato solamente da chi ha completato l'iter di redazione, controllo e approvazione, ed è destinato unicamente ai componenti la lista di distribuzione. Non può essere divulgato al di fuori della lista di distribuzione.	

REDAZIONE ***Responsabile del Sistema di Gestione per la Sicurezza delle Informazioni (RSGSI)***	***APPROVAZIONE*** ***Datore di Lavoro***
Ing. Nicola Carpi 	***Ing. Claudio Contini*** 

Originale archiviato elettronicamente

STATO DEL DOCUMENTO

Ed.	Data	Descrizione revisione
1.0	**20/04/2020**	**Prima emissione**
2.0	**12/01/2022**	**Modifiche a seguito del passaggio da Selta a DigitalPlatforms**
3.0	**21/11/2022**	**Inserita Cloud Policy, a seguito dell'estensione del Sistema di Gestione ISO 27001 agli standard ISO 27017 ed ISO 27018**
4.0	**19/03/2024**	**Aggiornamento e completamento della Politica in relazione all'adozione dello standard ISO 27001:2022 e all'adeguamento della Struttura Organizzativa per la Sicurezza delle Informazioni. Introdotta la figura del CISO (Chief Information Security Officer) con descrizione di mansioni e responsabilità.**

INDICE

1 INTRODUZIONE

La diffusione delle tecnologie ICT a tutti i livelli della società comporta un aumento dei rischi per la sicurezza in termini di perdita di dati, intrusioni, perdita della riservatezza e violazioni della privacy, e ciò vale in particolare per i sistemi informatici, richiedendo pertanto una accurata analisi delle loro debolezze e delle possibilità di un loro utilizzo non sicuro. L'implementazione di un adeguato sistema di protezione delle informazioni si basa su una sistematica analisi delle possibili minacce, e sulla determinazione delle precauzioni da adottare. La presente politica descrive ad alto livello i princìpi e gli obiettivi che l'azienda ha fatto propri al fine di garantire un sistema di gestione che riduca per quanto possibile i rischi associati alle diverse minacce, e sia strumento di miglioramento continuo.

2 RIFERIMENTI NORMATIVI

ISO/IEC 27000:2018	Information Technology – Security Techniques – Information Security Management Systems – Overview and vocabulary
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection – Information Security Management Systems – Requirements
ISO/IEC 27002:2022	Information security, cybersecurity and privacy protection – Information Security Controls
ISO/IEC 27017:2021	Information Technology – Security Techniques – Code of practice for Information Security Controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27018:2020	Information Technology – Security Techniques – Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors

3 POLITICA

3.1 GENERALITA'

DigitalPlatforms S.p.A. ha in carico la seguente missione:

Progettazione, produzione, installazione e assistenza di apparati e sistemi di telecomunicazioni, trasmissioni, telecontrollo, supervisione, automazione, comunicazione aziendale e accesso alle reti. Erogazione di servizi di cloud computing in modalità SaaS mediante utilizzo di datacenter cloud service provider esterni, con dichiarazione di applicabilità estesa ai controlli ISO/IEC 27017 e 27018.

Progettazione, realizzazione, installazione e servizi di consulenza di reti ICT in sicurezza per enti istituzionali e per imprese. Progettazione, produzione e manutenzione di apparati informatici per il trattamento di informazioni classificate (TEMPEST). Consulenza per la misurazione di sistemi e prodotti rispondenti alle normative in ambito NATO.

DigitalPlatforms tratta quindi dati pubblici e riservati, dati anonimi, personali comuni o sensibili, anche ad alta criticità. Essi includono anche quelli relativi al personale e alla tutela della privacy.
Data la potenziale criticità dei dati trattati, in qualunque formato essi siano (informatico e non), è fondamentale che sia loro garantita la massima riservatezza, integrità e disponibilità.

I livelli di sicurezza da garantire devono essere tali da rispettare le clausole contrattuali e la normativa vigente, nonché la coerenza ed il bilanciamento tra:

- Rischio di impresa
- Sostenibilità economica
- Risultati delle analisi e delle valutazioni del rischio
- Politiche, codici di condotta e strategie aziendali nei confronti di dipendenti, clienti e fornitori

Le politiche aziendali, già definite nell'ambito dei Sistemi di Gestione per la Qualità, l'Ambiente e la Sicurezza e Salute dei Lavoratori, sono improntate al costante adeguamento del contesto in cui si opera ed al miglioramento dell'efficacia ed efficienza dei processi, delle prestazioni e dei controlli di sicurezza.

Di seguito sono elencati i diversi principi cardine sui quali è improntata la presente politica:

- **Rispetto dei requisiti legali, delle norme tecniche e delle prescrizioni contrattuali riguardanti la sicurezza delle informazioni.**
- Le informazioni devono essere accessibili solo a coloro che ne hanno necessità (principio *"need to know"*) e nei tempi stabiliti.
- Il personale **deve essere opportunamente coinvolto e formato** in materia di sicurezza delle informazioni, e deve seguire i princìpi etici e comportamentali prescritti e condivisi.
- I Fornitori devono essere opportunamente tenuti sotto controllo; i rapporti tra DigitalPlatforms e le aziende fornitrici di prodotti e servizi devono essere basati su una contrattualistica che tenga conto delle aspettative di entrambe le parti e della chiara definizione degli accordi commerciali, delle tempistiche e dei requisiti e responsabilità tecniche ed organizzative, includenti quelli relativi alla protezione delle informazioni.
- La natura dei servizi erogati richiede già di per sé di tenere in considerazione i requisiti di sicurezza sin dalla contrattazione con i Clienti.

La responsabilità finale della sicurezza delle informazioni è in carico alla Direzione, che delega i Responsabili ad attuare quanto necessario, e secondo specifici Organigrammi, in accordo con il Responsabile dei Sistemi IT ed il Responsabile delle Risorse Umane.
Pur essendo la *governance* delegata a diverse funzioni, la Direzione mantiene la responsabilità per fornire gli indirizzi strategici e fornire le risorse necessarie.

3.2 COMUNICAZIONE E REVISIONE DELLA POLITICA

La Direzione di DigitalPlatforms definisce, divulga e si impegna a far comprendere e mantenere attiva la presente Politica per la Gestione della Sicurezza delle Informazioni. La divulgazione può avvenire tramite affissione in bacheca o tramite pubblicazione sulla intranet aziendale.
Essa è volta a garantire la tutela e la protezione da minacce, di origine interna o esterna, di natura accidentale o intenzionale, alle quali sono soggette le informazioni nell'ambito delle attività che rientrano nel Campo di Applicazione del Sistema di Gestione, in accordo con lo standard ISO/IEC 27001:2022 e con le linee guida dello standard ISO/IEC 27002:2022.
La Politica deve essere applicata a tutti i livelli in azienda, e deve essere parte degli accordi che l'azienda stipula con qualsiasi soggetto interno o esterno che risulti coinvolto nel trattamento delle informazioni che rientrano nel Campo di Applicazione del Sistema di Gestione. A tal fine, la presente Politica deve essere trasmessa, quando necessario, anche alle parti esterne (Clienti, Fornitori, Organi di vigilanza e controllo), interessate alla gestione in sicurezza delle informazioni.

La politica della sicurezza delle informazioni viene riesaminata almeno annualmente per verificare l'adeguatezza, ed aggiornata se necessario.

In particolare, l'aggiornamento della Politica e delle prassi operative è indispensabile laddove in fase di Riesame della Direzione si identifichino:

- Evoluzioni significative del business
- Nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio
- Significativi incidenti di sicurezza
- Nuovi requisiti e pressioni da parte dei mercati di riferimento
- Evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni

In particolare, le attività dell'azienda poggiano sul presupposto di un Sistema ICT sicuro e correttamente funzionante. Quasi tutte le informazioni presenti sono salvate e processate in formato elettronico. Le risorse ICT non sono immuni da vulnerabilità, pertanto è necessario effettuare una dettagliata catalogazione degli asset informatici, nonché una pianificazione e controllo della loro sicurezza.
La Strategia di Sicurezza ICT è divisa nei seguenti ambiti:

- Aspetti organizzativi di Sicurezza ICT (organizzazione, personale)
- Sicurezza delle infrastrutture (per esempio: data center, IDF rooms)
- Sicurezza dei supporti fisici ICT (per esempio: server, clients, componenti di rete)
- Sicurezza della rete (network and system management)
- Account Management, ovvero corretta gestione degli Accessi
- Sicurezza nelle applicazioni (per esempio: E-Mail, etc.)

3.3 SISTEMA DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Il punto di partenza per definire i requisiti di un Sistema di Gestione per la Sicurezza delle Informazioni consiste nell'identificare le possibili minacce presenti. Le minacce sono da un lato dipendenti dall'ambiente operativo, dall'altro dalla sensibilità delle informazioni che vengono gestite.

Esse possono essere suddivise in diverse tipologie di eventi:

1) Modifiche non autorizzate delle informazioni (perdita di Integrità)
2) Accessi non autorizzati alle informazioni (perdita di Riservatezza)
3) Impatti non previsti o non autorizzati sulla funzionalità del Sistema (perdita di Disponibilità)
4) Informazioni provenienti da fonti non affidabili (perdita di Autenticità)
5) Perdita del controllo sui dati personali (perdita di Privacy)

Una corretta gestione delle informazioni, in particolare quelle presenti su supporto informatico, è una condizione basilare per garantire e mantenere gli obiettivi fissati di Integrità, Riservatezza, Disponibilità, Autenticità e Privacy delle Informazioni.

Il mancato soddisfacimento di adeguati livelli di sicurezza porta a conseguenze molto negative:

- Danneggiamento dell'immagine aziendale
- Mancata soddisfazione del Cliente
- Sanzioni dovute al mancato rispetto della normativa vigente
- Fuga di informazioni sensibili e di know-how dall'azienda
- Danni economici e finanziari

Le regole, le procedure, le disposizioni organizzative e le responsabilità definite per conseguire gli obiettivi di Integrità, Riservatezza, Disponibilità, Autenticità e Privacy delle Informazioni, costituiscono la base del Sistema di Gestione implementato dall'azienda.

Per identificare le esigenze per la sicurezza, l'Azienda valuta periodicamente i rischi, allo scopo di determinare il livello di esposizione delle informazioni alle varie minacce presenti. I risultati di tale valutazione determinano le azioni da intraprendere, i controlli e le misure di sicurezza da adottare.

3.4 OBIETTIVI DELLA POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

1) Acquisire piena conoscenza e consapevolezza delle informazioni gestite e valutazione della loro criticità, al fine di determinare ed implementare gli adeguati livelli di protezione.
2) Realizzare una catalogazione degli asset aziendali rilevanti ai fini della gestione delle informazioni, individuando, per ciascuno di essi, un Responsabile.
3) Classificare le informazioni sulla base di determinati livelli di criticità.
4) Garantire l'accesso sicuro alle informazioni, in funzione di determinate matrici di autorizzazione, in modo da prevenirne l'accesso a chi non dispone dei diritti necessari.
5) Garantire l'accesso alle sedi ed ai singoli locali aziendali esclusivamente al Personale Autorizzato, a protezione della sicurezza degli ambienti e degli asset aziendali ivi presenti.
6) Definire procedure per l'utilizzo sicuro dei beni aziendali e delle informazioni, includendo gli aspetti di sicurezza anche in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
7) Implementare un sistema di collaborazione e di consapevolezza tra l'organizzazione e le terze parti interessate, in modo da trattare le informazioni ad adeguati livelli di sicurezza.
8) Riconoscere con tempestività Incidenti e Anomalie, inclusi quelli riguardanti i Sistemi Informativi, gestendoli secondo procedura ed implementando adeguati sistemi di prevenzione.
9) Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con terze parti.
10) Garantire la Business Continuity aziendale ed il Disaster Recovery, attraverso l'adozione e l'applicazione di adeguate procedure di sicurezza.
11) Garantire la riservatezza, l'integrità e la disponibilità dei dati archiviati, accessibili e manipolati utilizzando i servizi di cloud computing.
12) Stabilire un quadro di responsabilità e azioni necessarie per soddisfare i requisiti normativi e le linee guida di sicurezza per il cloud computing.

3.5 ORGANIZZAZIONE PER LA SICUREZZA DELLE INFORMAZIONI

La Direzione di DigitalPlatforms assicura che gli obiettivi della presente politica siano costantemente perseguiti, attraverso l'adozione di un Sistema di Gestione conforme allo standard ISO 27001:2022.
Per garantire il funzionamento di tale Sistema di Gestione, la Direzione di DigitalPlatforms ha definito e stabilito una "Struttura Organizzativa per la Sicurezza delle Informazioni", che riporta le figure chiave per la conduzione ed il miglioramento costante dello Stesso Sistema di Gestione.
Nell'ottica di una sempre maggiore integrazione tra le aziende facenti parte del Gruppo DigitalPlatforms, e allo scopo di rafforzare la conduzione tecnica del Sistema di Gestione, la Direzione ha introdotto, all'interno della Strutture Organizzativa per la Sicurezza delle Informazioni, le seguenti figure, che operano all'interno dello Steering Committee:

3.5.1 CISO (Chief Information Security Officer), Strategy di Gruppo

Questa figura, nominata direttamente dalla Direzione generale di Gruppo, ha la responsabilità ultima della sicurezza delle informazioni e dell'implementazione del relativo Sistema di Gestione (SGSI). Essa deve stabilire le Politiche per la sicurezza delle informazioni ed il presente Organigramma, assegnando i diversi ruoli e responsabilità per garantirne il funzionamento. Effettua periodicamente il riesame del SGSI e mette a disposizione tutte le risorse necessarie per mantenerlo e migliorarlo.
Il CISO di Gruppo ha il compito di assumere decisioni strategiche in merito all'implementazione di nuove prestazioni, servizi ed investimenti in merito alla sicurezza delle informazioni, compresi i prodotti e i servizi che l'azienda fornisce all'esterno, includendo le soluzioni di cloud computing.

3.5.2 CISO (Chief Information Security Officer), DigitalPlatforms S.p.A.

Il CISO (Chief Information Security Officer) ha I seguenti compiti e responsabilità:

- Predisporre, aggiornare e far rispettare le politiche per proteggere l'asset di informazioni della Società
- Predisporre un piano di Cyber Crisis Management ed un piano di Stress Test al fine di mitigare il rischio derivante da attacchi informatici
- Predisporre un Programma di Sicurezza delle Informazioni e Cybersecurity, compreso un Piano di Governance dell'infrastruttura aziendale, insieme con IT Governance, relativamente a processi, procedure e linee guida
- Supervisionare gli Audit di controllo periodici di Information e Cybersecurity, implementando Azioni Correttive e garantendo la compliance alle politiche
- Predisporre e aggiornare il Piano di Business Continuity e Disaster Recovery
- Riesaminare l'infrastruttura ed i sistemi di sicurezza informatica con implementazione di nuovi sistemi, al fine di mantenere l'organizzazione in linea con gli ultimi standard di sicurezza
- Supportare tutte le funzioni interne coinvolte in attività di Sicurezza delle Informazioni
- Valutare il management sullo sviluppo aziendale e sulle necessità di azioni nell'area della sicurezza informatica
- Definire i necessari criteri di sicurezza per la scelta dei fornitori e monitorarne gli indicatori di rischio
- Prevedere un Piano di Formazione della Cybersecurity per dipendenti e collaboratori

Il CISO può avvalersi di risorse interne ed esterne all'azienda per svolgere le attività di cui sopra, ed è dotato di un Budget annuale approvato dalla Direzione per la gestione degli aspetti di Security.