1. INTRODUZIONE 1
1.1 SCOPO 1
1.2 CAMPO DI APPLICAZIONE 2
1. RIFERIMENTI NORMATIVI 2
1.4 ACRONIMI E TERMINOLOGIA 2
2. OBIETTIVI 3
3. IMPEGNO DELLA DIREZIONE 3
4. RUOLI E RESPONSABILITA' DELL'IMS 4
5. ALLEGATI ALLA POLITICA GENERALE 5
5.1. POLITICA DEL GRUPPO SYMPHONIE 5

Proprietà Gruppo Symphonie

1. INTRODUZIONE

1.1 SCOPO

Il Gruppo Symphonie ha deciso di sviluppare un Sistema di Gestione integrato per la Qualità e la Sicurezza delle Informazioni (IMS – Information Management System) conforme agli standard internazionali ISO 9001 e ISO 27001 per ottimizzare i suoi processi, favorire il miglioramento continuo e tutelare il suo patrimonio di conoscenza, i suoi progetti, le sue soluzioni informatiche e più in generale il suo sistema informativo e documentale dalle molteplici minacce interne ed esterne, intenzionali o accidentali che minano la reputazione dell'organizzazione e il suo business.

Il presente documento definisce la politica aziendale integrata per la qualità e la sicurezza delle informazioni dell'intero Gruppo Symphonie.

Il rispetto dei contenuti della presente politica è obbligatorio per tutto il personale di tutte le Local Company del Gruppo e deve far parte delle dichiarazioni di impegno con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto nel trattamento delle informazioni che rientrano nel contesto di applicazione dell'IMS.

1.2 CAMPO DI APPLICAZIONE

L'IMS si applica a tutte le attività, progetti e soluzioni erogate e sviluppate dal Gruppo Symphonie

1. RIFERIMENTI NORMATIVI

- ISO IEC 27000
  Information technology - Security techniques - Information security management systems - Overview and vocabulary
- ISO IEC 27001
  Information technology -- Security techniques -- Information security management systems -- Requirements
- ISO IEC 27002
  Information technology -- Security techniques -- Code of practice for information security controls
- ISO/IEC 27004 "Information technology — Security techniques — Information security management Monitoring, measurement, analysis and evaluation
- ISO 9001
  Quality management systems — Requirements
- Regolamento UE 2016/679
- D. Lgs. 196/2003 armonizzato con il D. Lgs. 101/2018)

1.4 ACRONIMI E TERMINOLOGIA

ACRONIMO	SIGNIFICATO
IMS	Integrated Management System
CEO	Amministratore Delegato
AUD	Responsabile Audit

Proprietà Gruppo Symphonie

DPSCC	Data Protection Security & Continuity Committee
GDPR	General Data Protection Regulation 2016/679
RAS	Responsabile di Asset
RPS	Responsabile Progettazione SW
RSG	Responsabile Sistema Sicurezza delle Informazioni
RIT	Responsabile Sistemi Informativi
SGSI	Sistema di Gestione della Sicurezza delle Informazioni

2. OBIETTIVI

L'obiettivo principale dell'IMS è garantire un adeguato livello qualità dei prodotti servizi e di sicurezza delle informazioni (comprendendo i dati personali) nell'ambito di tutte le fasi del trattamento delle stesse (acquisizione, elaborazione, progettazione, conservazione, trasmissione, eventuale distruzione, ecc.) in linea con l'analisi dei rischi effettuata e con le "best practices" messe in atto dal Gruppo.

L'IMS definisce un insieme di misure organizzative, logistiche, informatiche e comportamentali atte a garantire:

- la confidenzialità e riservatezza delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato e ne ha i privilegi;
- l'integrità delle informazioni: ovvero la qualità e la completezza delle informazioni e l'affidabilità dei metodi per la loro elaborazione;
- la disponibilità delle informazioni: ovvero la garanzia di accesso alle informazioni e alle risorse collegate da parte degli utenti autorizzati nel momento in cui lo richiedono.

Attraverso la comunicazione del presente documento, la direzione del Gruppo intende perseguire i seguenti obiettivi generali:

1. standardizzare una metodologia di analisi del rischio sulla sicurezza delle informazioni;
2. certificare il proprio IMS a tutela e garanzia dei propri clienti, dei propri associati e degli stakeholder in genere.
3. proteggere il proprio patrimonio informativo e le informazioni aziendali;
4. aumentare la consapevolezza e la responsabilità degli associati e dei collaboratori sulle tematiche connesse con la sicurezza delle informazioni;
5. preservare la brand reputation;
6. soddisfare le aspettative dei clienti fornendo soluzioni sw che soddisfino i requisiti richiesti e forniscano idonee garanzie sul livello di affidabilità e sicurezza delle loro informazioni;
7. tutelarsi da eventuali rischi di natura legale (comprendendo eventuali penali contrattuali) dovuti a violazioni sulla sicurezza delle informazioni;
8. conformarsi ai requisiti internazionali sulla sicurezza delle informazioni favorendo al contempo lo sviluppo di nuove opportunità di business;
9. garantire un'integrazione efficace tra i requisiti volontari della ISO 27001 e i requisiti cogenti del Regolamento UE 2016/679 e più in generale della normativa sul trattamento dei dati personali;
10. garantire la compliance ai requisiti normativi cogenti.

Proprietà Gruppo Symphonie

3. IMPEGNO DELLA DIREZIONE

La Direzione del Gruppo verificherà periodicamente e regolarmente (o in concomitanza di cambiamenti significativi normativi e organizzativi) l'efficacia del IMS aggiornando l'analisi dei rischi sulle informazioni al fine di individuare eventuali derive ed adottare le opportune azioni di mitigazione, riesaminando e dove necessario aggiornando la politica.

L'impegno della direzione si concretizza tramite una struttura organizzativa trasversale al Gruppo i cui compiti sono:

- garantire la definizione di obiettivi specifici relativi alla qualità e alla sicurezza delle informazioni in aderenza con le politiche e le strategie del Gruppo;
- garantire un approccio sistematico per l'analisi del rischio sulle informazioni;
- sviluppare un sistema di gestione basato sul monitoraggio di KPI / OKR significativi e oggettivamente misurabili;
- incrementare, in un'ottica di "accountability", i livelli di sicurezza nel trattamento dei dati personali;
- integrare l'approccio "privacy & security by design" nella progettazione del software e nell'erogazione dei servizi;
- favorire un'efficace integrazione tra i requisiti di sicurezza delle informazioni e i requisiti obbligatori della normativa italiana (D. Lgs. 196/2003 armonizzato con il D. Lgs. 101/2018) ed europea (Regolamento UE 2016/679) sul trattamento dei dati personali;
- fornire risorse adeguate per la pianificazione, implementazione, controllo e miglioramento continuo dell'IMS;
- implementare un sistema di rilevazione della soddisfazione del cliente;
- definire i ruoli e le responsabilità aziendali per la progettazione, miglioramento e mantenimento dell'IMS;
- monitorare le prestazioni dell'IMS e assicurare un sistema di risposta veloce ed efficace nella gestione degli incidenti sulla sicurezza delle informazioni;
- monitorare i cambiamenti dell'esposizione alle minacce, rivedendo i criteri per l'accettazione del rischio e i livelli di rischio accettabili;
- garantire programmi di informazione, sensibilizzazione e formazione del personale creando una cultura aziendale sulla sicurezza delle informazioni;
- definire procedure, istruzioni operative e linee guida comportamentali per assicurare la riservatezza, integrità e disponibilità delle informazioni;
- eseguire audit periodici per verificare il rispetto dei requisiti dell'IMS;
- garantire la disponibilità di risorse, umane ed economiche adeguate al raggiungimento degli obiettivi dell'IMS.

Proprietà Gruppo Symphonie

4. RUOLI E RESPONSABILITA' DELL'IMS

Nell'ambito del gruppo le funzioni di staff sono centralizzate sulla capogruppo Symphonie; l'implementazione dell'IMS delle singole Local Company è governata dalla Capogruppo al fine di garantire un'efficace e omogenea applicazione.

Le figure chiave dell'IMS sono:

Amministratore Delegato (CEO)	Definisce la politica dell'IMS (IMS) Autorizza le direttive e i regolamenti interni. Mette a disposizione le risorse per il perseguimento degli obiettivi aziendali Approva l'analisi dei rischi e supervisiona il processo di riesame della direzione definendo strategie, politiche e obiettivi aziendali. Identifica il Responsabile dell'IMS
Responsabile IMS (RSG)	E' la figura direzionale che coordina le attività di progettazione e implementazione del Sistema di Gestione della Qualità e Sicurezza delle Informazioni (IMS) Assicura che l'IMS sia conforme alle normative ISO 9001 e ISO 27001 e riferisce all'Amministratore Delegato sulle prestazioni del sistema. Si adopera per promuovere la competenza e la consapevolezza interna
Responsabile IT (RIT)	E' il Responsabile dei sistemi informativi e supervisiona tutte le attività legate alla sicurezza delle informazioni in ambito telematico definendo le procedure di propria pertinenza (Disaster & Recovery, Backup, ecc.) Supporta attivamente il Responsabile IMS e l'auditor interno nell'analisi dei rischi e nella definizione di programmi di miglioramento a favore dell'integrità, disponibilità e riservatezza delle informazioni E' responsabile delle attività di assistenza tecnica, coordina gli amministratori di sistema e si adopera per mettere in atto tutte le misure di sicurezza informatiche previste dall'IMS Garantisce l'applicazione delle misure di sicurezza sancite dall'art. 32 del Reg. UE 2016/679
Auditor sulla sicurezza delle informazioni (AUD)	Supporta tutte le funzioni nell'implementazione e monitoraggio del sistema secondo i requisiti delle ISO9001 e ISO 27001 Supporta l'organizzazione nell'emissione della documentazione di sistema Supporta l'organizzazione nelle fasi di verifica dell'ente di certificazione terzo
Data Protection Security & Continuity Committee (DPSCC)	Collabora attivamente con il Responsabile dell'IMS sulla sicurezza delle informazioni nelle attività trasversali la privacy e il data protection in genere. Ha un ruolo di primo piano nella definizione delle policy di sicurezza dei dati e delle informazioni per i collaboratori della società. Integra le informazioni acquisite e condivise con l'auditor sulla sicurezza delle informazioni nel sistema di trattamento dei dati personali. Rappresenta l'organismo ufficiale di riferimento sulla compliance normativa legata al trattamento dei dati personali
Responsabile Asset (RAS)	E' responsabile della gestione degli asset della società. Esegue il censimento degli asset e mantiene aggiornato l'inventario degli asset della società
Responsabile Progettazione SW (RPS)	E' responsabile del processo di sviluppo, test, validazione e rilascio del sw. Integra i requisiti di sicurezza e di conformità espressi nella normativa privacy nei requisiti di sviluppo sw promuovendo e garantendo un approccio privacy & security by design.

Proprietà Gruppo Symphonie

5. ALLEGATI ALLA POLITICA GENERALE

5.1. POLITICA DEL GRUPPO SYMPHONIE

Il contesto nel quale operiamo ci impone una spiccata attenzione e sensibilità alla qualità e sicurezza delle informazioni per tutelare la nostra brand reputation, garantire l'aderenza ai requisiti contrattuali e cogenti ed andare incontro alle aspettative dei nostri clienti sempre più esigenti in tal senso.

Gli obiettivi fondamentali sui quali si basa la politica sulla qualità e sicurezza delle informazioni del Gruppo Symphonie sono:

a) la conformità ai requisiti legislativi e/o normativi cogenti;

b) la continua comunicazione, sensibilizzazione e formazione del personale al fine di favorire la consapevolezza e la conoscenza interna sulle tematiche relative alla qualità e alla sicurezza delle informazioni;

c) la scelta di partner affidabili e qualificati che forniscano idonee garanzie di qualità e sicurezza e si allineino agli standard qualitativi del Gruppo;

d) l'adozione di un regolamento informatico interno contenente le linee guida da rispettare in merito al corretto trattamento delle informazioni;

e) la partecipazione attiva di tutti gli associati che in modo propositivo e proattivo sono chiamati a proporre azioni migliorative e segnalare criticità attraverso strumenti dedicati;

f) il puntuale censimento e l'identificazione degli asset aziendali, le informazioni strategiche trattate e gli strumenti utilizzati per i trattamenti;

g) l'adozione di un sistema di classificazione delle informazioni;

h) l'adozione di un sistema di identificazione, analisi e trattamento dei rischi sulla qualità e sicurezza delle informazioni;

i) l'adozione di un sistema di profilazione e controllo degli accessi alle informazioni per evitare che personale non autorizzato possa accedere a dati e/o informazioni non di sua pertinenza;

j) un continuo bilanciamento di interessi tra l'esigenza di condividere la conoscenza all'interno della società e l'esigenza di garantire la sicurezza delle informazioni al fine di non pregiudicare l'efficienza e lo scambio di conoscenza come valore aggiunto nella gestione dei progetti;

k) la chiara definizione di accordi di riservatezza con i partner esterni;

l) la definizione di chiare e vincolanti clausole contrattuali sulla sicurezza delle informazioni con i collaboratori, fornitori e i clienti della società;

m) il rispetto di procedure e sistemi di controllo atti a prevenire l'accesso alle informazioni da parte di terzi non autorizzati;

n) il monitoraggio costante degli indicatori di processo dei partner che mettono a disposizione l'infrastruttura cloud per l'erogazione di servizi in modalità SaaS;

o) un sistema efficiente di Help Desk e supporto informatico nell'affrontare tutte le tematiche "operative" legate alla sicurezza delle informazioni, prevenzione e gestione degli eventuali incidenti;

p) l'adozione di un sistema reattivo di gestione degli incidenti sulla sicurezza delle informazioni integrato con il processo del Data Breach;

q) l'attuazione di misure idonee di sicurezza informatica per garantire: la protezione da codici malevoli (antivirus), la disponibilità delle informazioni (backup & recovery) e la riservatezza delle informazioni (firewall, intrusion prevention system, logging, crittografia, ecc.);

Proprietà Gruppo Symphonie

r) la predisposizione di piani di disaster recovery e business continuity per garantire la continuità operativa in caso di eventi bloccanti imprevisti, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino il più possibile le conseguenze negative;

s) la predisposizione e il continuo aggiornamento di procedure aziendali per lo sviluppo sicuro del software;

t) l'integrazione del'IMS nel CRM/ERP aziendale in conformità con i requisiti espressi dal Reg. UE 2016/679;

u) un approccio basato sui principi di security-privacy by design & by default;

v) la definizione di chiari politiche di data / information retention;

w) la predisposizione di strumenti di monitoraggio, controllo e audit Interni per verificare il rispetto degli obiettivi prefissati;

x) la promozione di programmi di miglioramento continuo del sistema di gestione per qualità e la sicurezza delle informazioni;

y) l'adozione incrementale di politiche specifiche per accompagnare il processo di miglioramento continuo del Gruppo traguardando la sostenibilità

Tali elementi sono volti a promuovere una gestione resiliente delle tematiche connesse con la sicurezza delle informazioni, in grado di "tarare" dinamicamente le azioni di mitigazione all'evolversi delle minacce, garantendo la stabilità del sistema e la disponibilità delle informazioni.

G-CEO 13/10/2023

Proprietà Gruppo Symphonie