Information Security Policy

Information Security Management System

ISMS_MPO_002-1.6

SORINT.lab S.p.A.
Via Zanica, 17 - 24050 Grassobbio (BG) - Italy | Tel +39 035 697 511 - Fax +39 035 697 590
C.F., N. REG. IMPR. BG 95164770166 | P. IVA 03419770163 - REA BG 376790 | CAP. SOC. € 1.262.500,00 i.v.

DOCUMENT INFORMATION

COPYRIGHT

CONTACTS

COMPANY	NAME	ROLE	EMAIL ADDRESS	PHONE
SORINT.lab	Emilio Tresoldi	CISO	emilio.tresoldi@sorint.com	

DOCUMENT REVIEW

VERSION	DATE	AUTHOR	APPROVED BY	ISSUED BY
1.0	19/12/2016	Emilio Tresoldi	Luca Pedrazzini	Luca Pedrazzini
1.1	16/09/2020	Emilio Tresoldi	Luca Pedrazzini	Luca Pedrazzini
1.2	05/09/2021	Emilio Tresoldi	Luca Pedrazzini	Luca Pedrazzini
1.3	12/09/2022	Emilio Tresoldi	Luca Pedrazzini	Luca Pedrazzini
1.4	12/03/2024	Mario Gandolfi	Luca Pedrazzini	Luca Pedrazzini
1.5	05/06/2024	Mario Gandolfi	Luca Pedrazzini	Luca Pedrazzini
1.6	29/11/2024	Mario Gandolfi	Luca Pedrazzini	Luca Pedrazzini

CHANGE HISTORY RECORD

VERSION	DATE	LAST MODIFIED
1.0	19/12/2016	First Version
1.1	16/09/2020	Update
1.2	05/09/2021	Confirmed
1.3	12/09/2022	Confirmed
1.4	12/03/2024	Update - Estensione SORINT
1.5	05/06/2024	Update – email contacts 2.1
1.6	29/11/2024	Update – estensione a PCI-DSS

REFERRAL DOCUMENTS

VERSION	DATE	DOCUMENT
NA	NA	NA

SUMMARY

1. INTRODUZIONE

SORINT.lab riconosce la necessità di garantire che il proprio business operi fluidamente e senza interruzioni per il creare beneficio ai suoi clienti, agli azionisti ed agli altri stakeholder.

Al fine di fornire un livello di funzionamento continuo, SORINT.lab ha implementato un SGSI – Sistema di Gestione della Sicurezza delle Informazioni (in inglese ISMS - Information Security Management System), in linea con l'International Standard for Information Security, ISO/IEC 27001:2022 e al Payment Card Industry Data Security Standard PCI DSS v4.0.1.

Questa information security policy costituisce una parte fondamentale dell'insieme dei controlli di SORINT.lab per garantire che le informazioni siano protette in modo efficace e per soddisfare gli obblighi verso i clienti, azionisti, dipendenti e fornitori.

Il mancato rispetto di questa policy potrebbe avere un effetto significativo sul funzionamento dell'organizzazione e può provocare perdite finanziarie e una incapacità di fornire un servizio critico ai clienti. Chiunque violi questa policy sarà soggetto ad un procedimento disciplinare, in conformità con la legislazione sul lavoro e dei contratti collettivi. Se è stato commesso un reato potranno essere adottate ulteriori azioni.

Se non si comprendono le implicazioni di questa policy è possibile fare riferimento alle opportune figure presenti all'interno del Sistema di Gestione della Sicurezza delle informazioni (ISMS) di SORINT.lab S.p.a.

1.1. AMBITO

Questa policy si applica in relazione con altre policy o procedure a tutte le tipologie di informazioni di SORINT.lab S.p.a e tutte le società da questa controllate d'ora in avanti denominate SORINT e dei suoi clienti, ai sistemi che hanno come Owner Sorint (anche in cloud) e a tutto il personale interno e di terze parti che collabora con l'azienda.

1.2. OBBIETTIVO

L'obiettivo della policy, supportata da altre policy e procedure, è quello di mantenere la confidenzialità, l'integrità e la disponibilità delle informazioni e dei sistemi a supporto e di fornire chiare e coerenti istruzioni per tutti i processi di Business di SORINT.

Inoltre, fornisce al Management, la direzione e il supporto per implementare il Sistema di gestione delle informazioni (ISMS) e assicurare che le operazioni e lo sviluppo software rispettino le regole di sicurezza identificate dall'azienda compresa la conformità allo standard PCI DSS.

2. IMPLEMENTAZIONE

E' responsabilità di tutto il management SORINT assicurare l'implementazione e il rispetto dei requisiti della policy. Il Chief information Security Officer (CISO) di SORINT è responsabile di assicurare tutte le necessarie comunicazioni, i corsi e il supporto per favorire l'attuazione e il controllo del rispetto di questa policy.

Non conformità o eccezioni a questa politica saranno gestite dal CISO e soggette ad eventuale approvazione, modifica od opportuno piano di trattamento che ne indirizzi le azioni correttive.

2.1. GUIDA

Per supporto o assistenza è possibile contattare il NGMS all' indirizzo di mail: desk@sorint.com o al canale wetalk service_desk. Inoltre, per specifiche richieste relative alle procedure e alle policy del ISMS è possibile far riferimento al CISO all' indirizzo: ciso@sorint.com.

2.2. DOCUMENTI DI RIFERIMENTO

La policy può essere letta congiuntamente all' High Level System Management policy la cui ultima versione è presente sul portale aziendale, unitamente a tutte le altre policy disponibili.

3. INFORMATION SECURITY IN SORINT

L' informazioni deve essere protetta da esposizione indesiderata (Confidentiality), corruzione (Integrity) e dalla mancanza di servizio (Availability) in accordo con le adeguate misure di sicurezza e gli adeguati livelli di protezione.

3.1. REQUISITI GENERALI

Per garantire un'adeguata protezione degli asset informativi Sorint definisce che:

- Tutti i processi di business identificano e classificano le informazioni in termine di Confidenzialità, Integrità, Disponibilità.
- Le informazioni di Sorint o dei propri clienti devono essere processate e conservate solo da SORINT o da servizi autorizzati.
- Le informazioni vengono elaborate e controllate rispettando i requisiti legali, contrattuali e di classificazione.
- I requisiti di sicurezza delle informazioni sono definiti in tutti i progetti, iniziative e negli sviluppi del software.
- Il processo di Recruitment garantisce l'adeguatezza delle risorse rispetto ai requisiti di sicurezza.
- La sicurezza delle informazioni è un requisito contrattuale per tutto il personale interno e di terze parti.
- I possibili rischi associati al lavoro con terze parti sono analizzati e opportunamente gestiti.
- L'installazione, la distribuzione e l'utilizzo del software è controllato da policy e procedure e soggetto ad approvazione.
- Le connessioni di rete sono controllate da policy e soggette ad approvazione.
- Gli accessi logici ai sistemi SORINT sono tracciati e controllati da una policy di accesso.
- L'accesso fisico agli asset di SORINT è riservato e protetto da controlli in accordo con i requisiti di classificazione degli asset.
- I backup dei dati vengono effettuati con frequenza adeguata alla classificazione del dato e viene definito nella politica di backup.
- I sistemi di SORINT sono gestiti e mantenuti seguendo le raccomandazioni dei fornitori.

Le risorse di SORINT non devono essere utilizzate per inappropriate attività considerati illegali, non eticamente corrette o che possono essere offensive.

3.2. SISTEMI DI SVILUPPO E TEST

I processi di sviluppo del software per essere efficienti ed efficaci devono:

- Garantire i principali requisiti di sicurezza legati allo sviluppo software
- Assicurare che le risorse coinvolte nel processo di sviluppo siano adeguatamente formate per effettuare i test
- Assicurare I requisiti di sicurezza in tutte le fasi del processo (sviluppo, preproduzione, produzione)
- Garantire "code ownership" e "intellectual property rights"

3.3. RESPONSABILITA' DEL MANAGEMENT SORINT

Tutti i livelli del management SORINT devono assicurare che la gestione della sicurezza delle informazioni fa parte dei propri obiettivi. Tutti i Manager di SORINT promuovono una politica di incoraggiamento del personale, al fine di segnalare le vulnerabilità e le criticità.

3.4. RESPONSABILITA' DEI DIPENDENTI

SORINT si aspetta che tutto il personale assicuri la protezione delle informazioni e che utilizzi gli strumenti in modo corretto e sicuro. Il mancato rispetto di queste azioni influisce negativamente sul business aziendale e sul raggiungimento degli obiettivi prefissati.

Tutti i dipendenti e le terze parti sono responsabili della confidenzialità delle informazioni di Sorint e dei clienti di Sorint che trattano e ne assicurano la sicurezza:

- Rispettando le policy e le procedure
- Implementando correttamente le procedure operative
- Utilizzando solo software approvato dal management
- Cambiando periodicamente le proprie password e conservandole in sicurezza
- Assicurando che i terminali vengano bloccati quando non si è presenti sulle postazioni di lavoro
- Garantendo la corretta protezione degli strumenti al di fuori della sede di lavoro
- Utilizzando mail, social media e reti pubbliche in modo professionale
- Smaltendo file e documentazioni in modo appropriato secondo le regole e le azioni definite.
- Prevedendo opportune precauzioni contro malware ricevuti via e-mail o attraverso qualche altro media
- Non aggirando i controlli di sicurezza e consentendo eventuali controlli richiesti dalle persone preposte a garantire la sicurezza
- Segnalando attraverso gli opportuni canali informazioni riguardanti vulnerabilità di sicurezza o comportamenti illeciti da parte del personale.

4. RISK MANAGEMENT

Tutti i processi e le aree di SORINT sono soggette a periodici assessment e ad una puntuale gestione del rischio. Le aree con un rischio alto vengono sottoposte all' analisi dell'Information Security Committee dal CISO (Chief Information Security officer)

5. INFORMATION SECURITY REVIEW

Una regolare review degli asset dove sono tenute le informazioni viene effettuata puntualmente per determinare la presenza di eventuali non-conformità o vulnerabilità. La direzione è responsabile della corretta review e audit degli asset.

6. PREVENZIONE, INVESTIGAZIONE E REPORT

Tutti i manager dei vari uffici sono responsabili per la prevenzione degli Incident di Sicurezza e di riportare qualsiasi violazione alle Policy e alle procedure.

7. FORMAZIONE RELATIVA ALL' INFORMATION SECURITY

Un adeguata formazione relativa all' Information Security Management System è prevista per tutti i dipendenti sia in fase di assunzione, che nel corso della vita lavorativa in Sorint per garantire che tutti capiscano i rischi legati alla sicurezza e la necessità di avere misure preventive.

8. REVISIONE DELLA DOCUMENTAZIONE E COMUNICAZIONE

Questa politica di sicurezza viene rilasciata formalmente dal Chief Information Security Officer (CISO) per conto del Executive Board di SORINT.

La policy e il Sistema di Gestione delle informazioni di Sicurezza (ISMS) sono soggetti a regolare review, almeno una volta ogni 12 mesi, ad aggiornamenti e miglioramenti derivanti dai cambiamenti dei rischi interni ed esterni, del business e dei feedback del ISMS.

Il CISO assicura la puntuale circolazione delle policy utilizzando gli strumenti di comunicazione a disposizione dell'azienda e il materiale formativo. Le ultime versioni delle policy, delle procedure e delle guide operative si trovano nell' area Information Security Management System sul portale aziendale CLANn.

9. RELAZIONE CON ALTRE POLICY

La policy di sicurezza è la base per stabilire altre procedure e policy sulla sicurezza delle informazioni piu' dettagliate.

Il set completo della documentazione a supporto dell'Information Security si trova sul portale aziendale Clann nell' area Information Security Systems.