



Information Security Policy

Politica di protezione delle informazioni
IMS_MPO_001-4.0 Information Security Policy

CONTACTS

COMPANY	NAME	ROLE	EMAIL ADDRESS	PHONE
SORINT.SEC	Marco Battaglia	General Manager	marco.battaglia@sec.sorint.it	+39 345 0215949

DOCUMENT REVIEW

VERSION	DATE	AUTHOR	APPROVED BY	ISSUE BY
IMS_MPO_001-1.0 Information Security Policy	02/08/2022	Giuseppe Letizia	Marco Battaglia	-
IMS_MPO_001-2.0 Information Security Policy	22/05/2024	Rita Formisano	Giuseppe Letizia	-
IMS_MPO_001-3.0 Information Security Policy	03/03/2025	Rita Formisano	Giuseppe Letizia	-
IMS_MPO_001-4.0 Information Security Policy	19/03/2026	Rita Formisano	Alex Vavassori	-

CHANGE HISTORY RECORD

VERSION	DATE	CONTENT MODIFIED
1.0	02/08/2022	Document Creation
2.0	17/07/2024	Adeguamento normative ISO 27001/2022 + Paragrafo 11
3.0	03/03/2025	Riferimenti normativi ISO 14001 e ISO 45001
4.0	19/03/2026	Review Annuo + Paragrafo 12

PUBLICATION DATE

VERSION	DATE	DOCUMENTS
1.0	21/11/2022	IMS_MPO_001-1.0 Information Security Policy
2.0	23/07/2024	IMS_MPO_001-2.0 Information Security Policy
3.0	03/07/2025	IMS_MPO_001-3.0 Information Security Policy
4.0	31/03/2026	IMS_MPO_001-4.0 Information Security Policy

SOMMARIO

1	Introduzione	4
1.1	Ambito	4
1.2	Obiettivo	4
2	Riferimenti Normativi	5
2.1	Documenti Applicativi	5
2.2	Documenti di Riferimento	5
3	Implementazione	5
3.1	Guida	5
3.2	Policy di riferimento	5
4	Information Security in Sorint.Sec	5
4.1	Requisiti generali	6
4.2	Responsabilità del Management di Sorint.Sec	6
4.3	Responsabilità dei dipendenti	6
5	Risk Management	7
6	Information Security Review	7
7	Prevenzione, investigazione e report	7
8	Formazione relativa all'information security	7
9	Revisione della documentazione e comunicazione	7
10	Relazione con altre policy	7
11	Sicurezza delle informazioni in caso di disruption	7
12	Impegno della Direzione	8
13	DOCUMENT INFORMATION	9

1 Introduzione

Sorint.SEC 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.SEC 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.

Questa information security policy costituisce una parte fondamentale dell'insieme dei controlli di Sorint.SEC 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 riferimenti alle opportune figure presenti all'interno del Sistema di Gestione della Sicurezza delle informazioni (ISMS) di Sorint.SEC.

1.1 Ambito

Questa policy si applica in relazione con altre policy o procedure a tutte le tipologie di informazioni di Sorint.SEC e dei suoi clienti, ai sistemi che hanno come Owner Sorint.SEC (anche in cloud) e a tutto il personale interno e di terze parti che collabora con l'azienda.

1.2 Obiettivo

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.SEC.

Inoltre, fornisce al Management, la direzione e il supporto per implementare il Sistema di gestione delle informazioni (ISMS) e assicurare che le operazioni rispettino le regole di sicurezza identificate dall'azienda.

2 Riferimenti Normativi

2.1 Documenti Applicativi

Per la consultazione dei documenti applicativi, fare riferimento al Registro di prescrizioni legali e prendere visione della documentazione di supporto relativa alle norme ISO/IEC 27001:2022, ISO 14001:2015, ISO 9001:2015 e ISO 45001:2018.

2.2 Documenti di Riferimento

Per la consultazione dei documenti di riferimento, fare riferimento al Registro di prescrizioni legali e prendere visione della documentazione correlata alle norme ISO/IEC 27001:2022, ISO 14001:2015, ISO 9001:2015 e ISO 45001:2018.

3 Implementazione

È responsabilità di tutto il management Sorint.Sec assicurare l'implementazione e il rispetto dei requisiti della policy. Il Chief information Security Officer (CISO) di Sorint.Sec 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.

3.1 Guida

Per supporto o assistenza è possibile contattare il supporto tecnico all' indirizzo di mail: support@sec.sorint.it
Inoltre, per specifiche richieste relative alle procedure e alle policy del ISMS è possibile far riferimento al CISO all' indirizzo: ciso@sec.sorint.it.

3.2 Policy 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.

4 Information Security in Sorint.Sec

L'informazione 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.

4.1 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.Sec 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.Sec sono tracciati e controllati da una policy di accesso.
- L'accesso fisico agli asset di Sorint.Sec 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.Sec sono gestiti e mantenuti seguendo le raccomandazioni dei fornitori.

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

4.2 Responsabilità del Management di Sorint.Sec

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

4.3 Responsabilità dei dipendenti

Sorint.Sec 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

5 Risk Management

Tutti i processi e le aree di Sorint.Sec sono soggette a periodici assesment 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).

6 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.

7 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, garantendo rispetto nei confronti dell'ambiente e sicurezza in ambito lavorativo. Tutti gli incidenti di sicurezza devono essere prontamente segnalati, gestiti e documentati secondo le procedure definite, al fine di minimizzare e prevenire il ripetersi degli eventi.

8 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.

9 Revisione della documentazione e comunicazione

Questa politica di sicurezza viene rilasciata formalmente dal Chief Information Security Officer (CISO) per conto dell'Executive Board di Sorint.Sec.

La policy e il Sistema di Gestione delle informazioni di Sicurezza (ISMS) sono soggetti a regolare review, 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 Intranet.

10 Relazione con altre policy

La policy di sicurezza è la base per stabilire altre procedure e policy sulla sicurezza delle informazioni più dettagliate. Il set completo della documentazione a supporto dell'Information Security si trova sul portale aziendale.

11 Sicurezza delle informazioni in caso di disruption

Per far fronte a un possibile caso di disruption, come descritto nel punto 5.29 della normativa ISO 27001/2022, Sorint.SEC assicura la continuità del servizio adoperando il piano di DR descritto nella parte di Business Continuity.

Inoltre, per garantire che le informazioni restino al sicuro durante una possibile interruzione, Sorint.Sec utilizza le proprie procedure di Detection e contenimento che permettono di rilevare e mitigare potenziali minacce. Queste procedure sono descritte e dettagliate all'interno dell'operational runbook di Sorint.Sec.

Specifichiamo, però, che tutti i servizi core utilizzati ed erogati da Sorint.Sec sono in cloud.

12 Impegno della Direzione

La Direzione si impegna a garantire la protezione, l'integrità, la disponibilità e la riservatezza delle informazioni gestite dall'organizzazione, assicurando che vengano adottate misure adeguate per prevenire, rilevare e gestire i rischi relativi alla sicurezza delle informazioni. A tal fine, la Direzione supporta l'implementazione e il miglioramento continuo del Sistema di Gestione Integrato, mettendo a disposizione risorse, competenze e strumenti adeguati. Annualmente, la Direzione provvede inoltre a monitorare e riesaminare gli obiettivi, i rischi e l'efficacia delle misure di sicurezza adottate, assicurando che rimangano coerenti con il contesto organizzativo, normativo e tecnologico in evoluzione.

13 DOCUMENT INFORMATION

COPYRIGHT

© Le informazioni contenute in questo documento sono di natura riservata e di proprietà di SORINT.SEC S.r.l., fermo restando che sarà utilizzato per scopi di valutazione. Il Copyright di questo documento è di proprietà di Sorint.SEC S.R.L. Nessuna parte del presente documento può essere riprodotta, memorizzata in un sistema di recupero o trasmessa in qualsiasi forma e con qualsiasi mezzo, inclusi, senza limitazione, elettronico, meccanico, fotocopiatura, registrazione o altro, senza il consenso scritto di Sorint.SEC S.r.l.

Sorint.SEC S.R.L. si adopera per garantire che le informazioni contenute in questo documento siano corrette e, sebbene ogni sforzo sia fatto per garantire l'esattezza di tali informazioni non si assume alcuna responsabilità per eventuali errori od omissioni nella stessa. Tutti i marchi e nomi di prodotti utilizzati nel presente documento sono pertanto riconosciuti.

© The information contained in this document is of a confidential and proprietary nature and is submitted by Sorint.SEC srl on the understanding that it will be used for evaluation purposes only. The copyright to this document is owned by Sorint.SEC srl. No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, including, without limitation, by electronic, mechanical, photocopying, recording or otherwise, without Sorint.SEC srl prior written consent.

Sorint.SEC srl endeavors to ensure that the information contained in this document is correct, and whilst every effort is made to ensure the accuracy of such information it accepts no liability for any error or omission in the same. All trademarks and product names used within this document are hereby acknowledged.



Sorint.SEC S.r.l. Società 51% Controllata da Sorint.Lab S.p.A.
Sede Legale: Via Zanica, 17 – 24050 Grassobbio (Bg), Italy
Sede Operativa: Via Dell'Artigianato – Osio Sotto, 24046 (Bergamo), Italy
COD. FISC., N. REG. IMPR. BG 04010360164, PI 04010360164
CAP. SOC. € 10.000,00 i.v. REA BG 427668

Legale Rappresentante e Amministratore Unico: Luca Pedrazzini
Società Soggetta a Direzione e Coordinamento di Sorint.Lab S.P.A.
Phone: +39 035 0510401
<https://sorintsec.ai>