


INFORMATION SECURITY POLICY

Date / Data	Write By / Scritta da	Revision
17/02/2025	Federico Pino	1.0
13/02/2026	Federico Pino	1.1

Il presente documento è approvato tramite processo di governance aziendale. La versione controllata è quella archiviata nel sistema documentale.



This document is approved through the corporate governance process. The only controlled version is the one retained in the document management system.

 	Information Security Policy / Politica per la Sicurezza delle Informazioni	D-ITA-INF-01
--	---	---------------------

INFORMATION SECURITY POLICY

Index

Articolo 1 (Introduction).....	3
Articolo 1 (Introduzione).....	3
Article 2 (Objectives).....	4
Articolo 2 (Obiettivi)	4

 	Information Security Policy / Politica per la Sicurezza delle Informazioni	D-ITA-INF-01
--	---	--------------

Articolo 1 (Introduction)

The Information Security Management System is the tool with which Sumitomo Riko Group (hereinafter also SumiRiko) intends to protect the confidentiality, integrity and availability of its information assets, including the sensitive information of its customers and suppliers. The achievement of adequate levels of security allows SumiRiko Italy S.p.A. to mitigate and counteract losses and damages that may have an impact on people, on the image and reputation of the company, on economic and financial aspects, as well as allowing compliance with the contractual and legislative context in force on the protection of information and personal data, with an eye towards the TISAX standard. Compliance with this Information Security Policy is mandatory for all employees, collaborators, suppliers, contractors, partners and external parties who handle information of SumiRiko Italy S.p.A. or its customers.

This Information Security Policy also supports compliance with Directive (EU) 2022/2555 (NIS2), as implemented in Italy by Legislative Decree 138/2024.

Articolo 1 (Introduzione)

Il Sistema di Gestione della Sicurezza delle Informazioni è lo strumento con il quale Sumitomo Riko Group (di seguito anche SumiRiko) intende proteggere la riservatezza, l'integrità e la disponibilità del proprio patrimonio informativo, ivi incluse le informazioni sensibili dei suoi clienti e fornitori.

Il raggiungimento di adeguati livelli di sicurezza, consente a SumiRiko Italy S.p.A. di mitigare e contrastare perdite e danneggiamenti che possano avere impatto sulle persone, sull'immagine e la reputazione aziendale, sugli aspetti di natura economica e finanziaria, oltre a consentire la conformità al contesto contrattuale e legislativo vigente in materia di protezione delle informazioni e dei dati personali, con un occhio di riguardo verso lo standard TISAX.

L'osservanza della presente politica sulla Sicurezza delle Informazioni è obbligatoria per tutti i dipendenti, collaboratori, fornitori, appaltatori, partner e parti esterne che gestiscono informazioni di SumiRiko Italy S.p.A. o dei suoi clienti.

La presente Politica per la Sicurezza delle Informazioni supporta altresì la conformità alla Direttiva (UE) 2022/2555 (NIS2), recepita in Italia dal D.Lgs. 138/2024.

Article 2 (Objectives)

The company puts into practice the following principles:

- Protect company and customer/supplier information acquired, processed or generated as part of the services provided, safeguarding its confidentiality, integrity and availability;
- Ensure proper access to the right information when necessary and prevent unauthorized access, both by those who work in SumiRiko Italy S.p.A. and by those who work on its behalf;
- Outline and implement security measures within the defined scope of the ISMS, to protect information from infringements, misuse and fraud, with an eye to information assets of a prototype nature;
- Define internal and external roles and responsibilities for information security;
- Head of departments are nominated as responsible for the security of information under their assignment.
- Support staff and collaborators with appropriate education and training to raise awareness of cybersecurity in order to minimize risks; Ensure continuity of information security in the event of an unfavorable scenario or if a threat materializes;
- Ensure compliance with the TISAX standard, in its latest version; Maintain compliance with contractual, legislative and regulatory provisions, in particular on information protection;
- Ensure the appropriate custody of the Personal Information of third parties and their management according to the

Articolo 2 (Obiettivi)

La società mette in pratica i seguenti principi:

- Proteggere le informazioni aziendali e dei clienti/fornitori acquisite, trattate o generate nell'ambito dei servizi erogati, salvaguardando la loro riservatezza, l'integrità e la disponibilità;
- Garantire il corretto accesso alle giuste informazioni quando necessario e prevenire l'accesso non autorizzato, sia da parte di chi opera in SumiRiko Italy S.p.A., sia di chi opera per suo conto;
- Delineare e mettere in atto misure di sicurezza dell'ambito definito dell'SGSI, per proteggere le informazioni da infrazioni, uso improprio e frodi, con un occhio di riguardo verso gli asset informativi di natura prototipale;
- Definire ruoli e responsabilità interni ed esterni per la sicurezza delle informazioni;
- I responsabili dei dipartimenti sono nominati responsabili della sicurezza delle informazioni di loro competenza.
- Supportare il personale e i collaboratori con un'adeguata istruzione e formazione per sensibilizzare in materia di sicurezza informatica al fine di minimizzare i rischi;
- Garantire la continuità della sicurezza delle informazioni in caso di scenario sfavorevole o qualora si concretizzi una minaccia;
- Garantire l'ottemperanza allo standard TISAX, nella sua ultima versione;
- Mantenere l'osservanza delle disposizioni contrattuali, legislative e regolamentari, in particolare sulla protezione delle informazioni;
- Garantire la idonea custodia delle informazioni Personali di terzi e loro gestione secondo principi di liceità, proporzionalità e pertinenza.

Gli incidenti di sicurezza informatica significativi sono gestiti e notificati in conformità alle procedure di Incident Management e di notifica NIS2 dedicate.

La Società raggiunge gli obiettivi prefissati di

<p>principles of lawfulness, proportionality and relevance.</p> <p>Significant cybersecurity incidents are managed and notified in accordance with the dedicated Incident Management and NIS2 Incident Notification procedures.</p> <p>The Company achieves its security objectives through a structured risk management approach and by planning appropriate mitigation measures on various fronts. The Management of SumiRiko Italy S.p.A.:</p> <ul style="list-style-type: none"> ✓ is directly responsible for the implementation of the policy and compliance with it by all stakeholders. ✓ shares the principles and objectives of the ISMS and fully supports its implementation and maintenance by providing the necessary resources for this purpose. ✓ provides the necessary feedback for the continuous improvement of the ISMS. ✓ In accordance with Article 20 of the NIS2 Directive, the Management retains ultimate responsibility for cybersecurity, approves the Information Security Risk Assessment and accepts residual risks. <p>With the aim of maximum transparency and collaboration, this Information Security Policy is communicated to all employees and made available to all interested parties as deemed necessary, upon explicit request.</p> <p>This policy is subject to review on a periodic basis and/or in the event of significant changes regarding information security and/or the organizational environment, to ensure its suitability, adequacy and efficiency.</p> <p>This Policy is supported by the Information Security Management System documentation and by specific NIS2 governance documents.</p>	<p>sicurezza delle informazioni tramite un approccio di gestione del rischio strutturato e pianificando opportune misure di mitigazione su diversi fronti.</p> <p>La Direzione di SumiRiko Italy S.p.A.:</p> <ul style="list-style-type: none"> ✓ è direttamente responsabile dell’attuazione della politica e dell’osservanza della stessa da parte di tutte le parti interessate; ✓ condivide i principi e gli obiettivi del SGSI e ne sostiene pienamente la realizzazione e il mantenimento fornendo le risorse necessarie a tale scopo; ✓ fornisce le risorse necessarie al miglioramento continuo del SGSI. ✓ In conformità all’Articolo 20 della Direttiva NIS2, la Direzione mantiene la responsabilità ultima in materia di cybersicurezza, approva il Risk Assessment sulla Sicurezza delle Informazioni e accetta i rischi residui. <p>Con l’obiettivo della massima trasparenza e collaborazione, la presente politica per la Sicurezza delle Informazioni è comunicata a tutti i dipendenti e resa disponibile a tutte le parti interessate per quanto ritenuto necessario, su esplicita richiesta.</p> <p>La presente politica è soggetta a revisioni su base periodica e/o in caso di cambiamenti significativi riguardanti la sicurezza delle informazioni e/o il contesto organizzativo, al fine di garantirne l’idoneità, l’adeguatezza e l’efficienza.</p> <p>La presente Politica è supportata dalla documentazione del Sistema di Gestione della Sicurezza delle Informazioni e dai documenti di governance NIS2 dedicati.</p> <p>Chivasso, 13/02/2025</p> <p>La Direzione di SumiRiko Italy S.p.A.</p>
--	--

Chivasso, 13/02/2026

The Management of SumiRiko Italy S.p.A.