Key Information from the General Security Policies of the Sava Insurance Group

Ljubljana, April 2025

Contents

1 INTRODUCTION

This document summarises the key general security policies of the Sava Insurance Group (SIG), adapted for public disclosure for supplier-related purposes. It is intended for all contractual partners who, in the course of their work and the performance of contractual services, have access to or use any of the SIG ICT resources (e.g., applications, telecommunications means, databases, etc.).

This summary includes the following content:

- proper use of all information or ICT resources,
- management of information or ICT resources,
- electronic operations,
- protection of equipment and information or ICT resources.

By accepting the General Security Policies of SIG, the supplier (the contractual partner) undertakes to comply with the IT security requirements in accordance with the applicable best practices, minimum standards and professional principles, and applicable regulations when fulfilling its contractual obligations.

2 PURPOSE AND SCOPE OF SECURITY POLICIES

The purpose of the SIG security policies is to:

- ensure the secure and appropriate use of ICT resources,
- familiarise users with the risks related to the use of ICT resources,
- define measures to protect information from unauthorised disclosure or misuse.

Contractual users use all SIG ICT resources with due care, efficiency and responsibility.

SIG protects its employees and property to the greatest extent possible against illegal or harmful intentional or unintentional activities by individuals.

Inappropriate use of IT exposes SIG and its users to risks such as computer virus infections affecting IT systems, threats to network systems and services, and misuse of information and data stored in the SIG information systems.

3 GENERAL REQUIREMENTS

- The supplier complies with all applicable laws and regulations, including the General Data Protection Regulation (GDPR) and the Digital Operational Resilience Act for the financial sector (DORA).
- The supplier appoints a contact person for security communications and incident response.

4 ACCESS MANAGEMENT

- The supplier establishes strict controls to prevent unauthorised access to the SIG ICT systems.
- The supplier ensures that only authorised, properly verified and trained personnel have access to the SIG ICT systems.
- Access management applies to all forms of access to ICT resources, including but not limited to:
  - user access via graphical user interfaces (GUI),
  - access via application programming interfaces (API),
  - system/service access (service accounts),

  - administrative and privileged access,
  - scripts, cron jobs and automated integrations,
  - remote access (VPN, RDP, SSH, etc.),
  - access via mobile devices or the cloud.
- Access protection to the SIG ICT systems includes but is not limited to multi-factor authentication (MFA) and the principle of least privilege.
- All access to the SIG systems or data is logged and monitored to ensure audit trails.
- The supplier maintains and regularly reviews an up-to-date list of authorised personnel with access rights to the SIG ICT systems.

5 DATA PROTECTION

- The supplier ensures the integrity, confidentiality and availability of data.
- All data are encrypted during transmission using TLS 1.2 or higher cryptographic protocol.
- All data at rest, including backups, are encrypted using AES-256 or an equivalent standard.
- The supplier ensures that the computers used to perform the contracted service are regularly updated with security patches, installed with only legitimate software and protected by regularly updated antivirus software.
- The supplier minimises data processing and storage and only processes and stores data that are strictly necessary to perform the contractual obligations.
- The supplier avoids unnecessary storage of data and ensures that data are deleted or anonymised as soon as storage is no longer required.
- Upon termination of the contractual relationship, the supplier securely deletes the data or returns them in full to SIG.

6 INCIDENT MANAGEMENT

- The supplier has an incident management policy in place that covers the detection, reporting and resolution of security incidents.
- The supplier’s security incidents affecting SIG are reported to SIG within 24 hours.
- The supplier enables SIG to participate in the resolution of incidents affecting its ICT systems, including providing access to relevant documentation.

7 RESILIENCE AND CONTINUITY

- The supplier has a business continuity plan (BCP) and a disaster recovery plan (DRP), both of which are periodically tested.
- These plans are tested annually, and the results are made available to SIG upon request.

8 MANAGEMENT OF SUBCONTRACTORS RELATED TO THE CONTRACTED SERVICE

- The supplier obtains written approval from the client (SIG) before engaging subcontractors or third parties.
- The supplier ensures that all subcontractors meet the same requirements that apply to the supplier.

9 AUDIT AND RISK ASSESSMENT

- The supplier carries out regular risk assessments related to its services and engages the client (SIG) as appropriate.

- The client (SIG) will conduct its own supplier risk assessment, which may include issuing security questionnaires and conducting independent reviews of security measures.
- Upon request by the client, the supplier provides SIG with audit and test reports, responds to security questionnaires and reasonably cooperates in independent reviews.
- The client (SIG) reserves the right to perform regular audits and independent reviews of the supplier’s security measures.
- Upon request by the client, the supplier provides SIG with evidence of compliance, such as certificates, reports or results of security tests.

10 TRAINING AND AWARENESS

- The supplier regularly trains its employees working for the client (SIG) on information security best practices and other content as requested by SIG.

11 TERMINATION OF COOPERATION

- Upon termination of the contract, the supplier ensures the secure disconnection of services from the SIG ICT systems, including the deactivation of access and the secure deletion of all SIG data.
- After termination of the contract, the supplier provides a statement or other proof of data deletion.

12 UPDATES AND CHANGES

- SIG reserves the right to update this document to reflect changes in risks, technologies or regulations. The supplier will be notified of updates and will ensure compliance within a reasonable timeframe.

13 DEFINITIONS AND ACRONYMS

No.	Term/acronym	Description
3	**SIG**	Sava Insurance Group
4	**ICT**	Information and Communication Technology – a technology that enables the collection, processing and exchange of data
5	**MFA**	Multi-Factor Authentication – a multi-level authentication method that increases access security
7	**AES-256**	Advanced Encryption Standard (256-bit) – a cryptographic encryption algorithm used to protect data at rest
8	**TLS 1.2**	Transport Layer Security 1.2 – a cryptographic protocol for secure communication over networks