Cyber Security and Information Privacy Protection Policy

Content

1 Preamble

Information is a core asset of a modern company and is seen as the new oil, irrespective of what the information is about and of the form it is embodied in. This in combination with SIG's new digital commercial products and solutions like Plant 360 Asset Management or Digital Sleeve Production opens new business fields, but also increases information security and cybersecurity risks. We also need to adequately protect our know-how, intellectual property, and assets. In parallel, customers' and individuals' awareness regarding the treatment of information has raised all over the world. New laws and regulations regarding the treatment of information are appearing rapidly in several countries.

The SIG Cybersecurity and Information Privacy Protection Policy has been developed to outline our commitments, goals and approaches for sustainability topics identified as strategic or material. It is firmly embedded within relevant functions and processes with appropriate measures and controls and defines the basis for our sustainability approach.

2 Scope

The SIG Cybersecurity and Information Privacy Protection Policy applies to SIG Group AG, all of its subsidiaries and controlled entities ("SIG"). The policy addresses information security in both information technology (IT) and operational technology (OT) and focuses on safeguarding SIG's information assets and mitigating cybersecurity risks. Through the security program, we ensure all SIG employees understand and adhere to the principles and commitments outlined in this Policy. We engage with our suppliers and business partners so that they understand, uphold, and promote these principles as well as support SIG's commitments.

3 Core principles

- **Ensure** compliance with applicable local, national, and international laws and regulations, statutory, regulatory, and contractual requirements, especially in terms of privacy and protection of personally identifiable information, intellectual property rights, protection of records, and regulation of cryptographic controls.
- **Set** objectives on relevant cybersecurity and information privacy protection topics, systematically review them, and update them with regards to strategic alignment, risk management, value delivery, resource and performance management, and assurance process integration.
- **Ensure** cybersecurity and information privacy protection objectives are consistent with policies, measurable, practicable and can be communicated effectively.
- **Implement** effective measures to safeguard information assets and mitigate cybersecurity risks in terms of confidentiality, integrity, and availability.
- Clearly **define** roles, requirements and procedures detailing how information security will be maintained within the internal corporation and external services.
- **Commit** to establishing an information security management system that meets applicable international standards and supports company goals.
- **Define** and **enforce** appropriate operational processes to prevent, resolve and mitigate information security and cybersecurity issues and incidents.

4 Topics: Cybersecurity and Information Privacy Protection

SIG is committed to maintaining complete Cybersecurity and Information Privacy Protection throughout our organization. We are committed to establishing and implementing an effective information security management system to safeguard information assets and personal identifiable information, mitigate cybersecurity risks, and meet obligations of key stakeholders including customers, shareholders, employees, and suppliers.

This is relevant for SIG IT and OT security in equipment and products. SIG's Information Security and Privacy Management System is based on the ISO 27001 and ISO 27701 standard. SIG uses these standards to establish, implement, maintain, and continually improve the security and privacy management system. The security and privacy management system preserves the confidentiality, integrity, availability, and privacy of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.

We are continuously testing, managing, and ensuring all relative protocols as part of SIG's commitment to maintain secure information and proper governance through the ever-changing technology environment.

The following chapters outline our position on cybersecurity and information privacy protection issues and guide our actions.

4.1 Information security – system organisational control and human resource security

4.1.1 Relevance

Organisational control and human resource security are essential to ensure qualification and understanding among employees regarding their roles and responsibilities. Regardless of the effectiveness of the technical abilities of an information security management system, security breaches within an organisation may occur if policies are not understood, followed, and managed throughout all departments within the corporation. Therefore, it is imperative for all employees to understand and implement security protocols and active measures.

4.1.2 Overarching commitment

We are committed to implement an information security management system through a cross-functional, coordinated structure that includes all relevant SIG business units, namely SIG Business, IT, Legal, Audit, HR, Facilities and Compliance. We are equally committed to provide company-wide awareness and executive-level support for setting up an information security management system and information security governance to develop, implement and manage a security program that achieves the following outcomes: strategic alignment, risk management, value delivery, resource and performance management, and assurance process integration.

4.1.3 Targets

SIG's goals for information security – system organisational control and human resource security are:

- Percentage of SIG employees completing security awareness training and passing the test: 100%.
- Percentage of SIG employees reviewing information security policies, including the acceptable use of SIG information resources: 100%.

4.1.4 Implementation approach

To ensure information security and cybersecurity concerns are thoroughly managed throughout the business, SIG has established the Security Framework and Security Management and Governance Organisation responsible for minimizing these concerns as such:

Security framework

- Security governance and risks: Implement and improve processes for mature information security governance and risks.
- Security management and operations: Create and improve standard information security management system for business. Prevent, resolve, and mitigate information security and cybersecurity issues and incidents.
- Security technology and innovation: Implement and improve standard for securing IT and OT infrastructure and integrate IT security into new innovative IT and OT services and products.
- Security compliance: Avoid breaches of legal, regulatory, or contractual obligations related to security and integrate IT and OT compliance by design in terms of information security.

Security management and governance organisation

- Information Security Manager (ISM) has been appointed to oversee risk mitigation for IT services through developing, maintaining and supporting security standards, requirements, and guidelines, as well as monitoring and enforcing compliance with such guidelines.
- Information Security Board (ISB) has been established to act as first line of defence in addressing concerns with IT services, including risks, major threats, security incidents. The ISB reviews audit results, feedback, risks assessments and implements initiatives to improve security in the organisation, including changes to operations, trainings or other measures as required.
- Security and Privacy Governance Board has been established for the review of major initiatives to improve security & privacy in the organization. This board also approves of changes in security & privacy policies and approves of contractual changes which related to cybersecurity. In addition, it supports the communication of security & privacy policies in the organization and promotes continuous improvement of Information Security Management and Privacy Information Management System.
- Audit Risk Committee (ARC) has been established to annually review the company's information security practices and risks.

Additionally, employment candidates, employees, and suppliers are subject to background verification proportional to their roles, as permitted by applicable law. SIG employees are required to review information security policies, including the acceptable use of SIG information resources, before accessing information systems. SIG employees receive on-going security awareness training and communications.

4.2 Information security – system access management

4.2.1 Relevance

Protecting data from unauthorised access or control is central to the safety and security of SIG's employees and business partners' information assets. Access management and control prevents sensitive company specific information and personal identifiable information from leaking to unauthorised personnel. Unauthorised access can be caused by mishandling of accounts, access rights and passwords.

4.2.2 Overarching commitment

We are committed to setting and following a standard process of controlling access and managing information assets and personal identifiable information within SIG's information systems.

4.2.3 Targets

SIG's goals for information security – system access management are:

- Percentage of new user creation or change user authorisation completed on-time: 100%.
- Number of inactive users: 0.
- Percentage of user delimitation completed on-time: 100%.

4.2.4 Implementation approach

Access control processes managed at SIG encompass user account and password control, segregation of duties, user entitlement reviews and activity monitoring.

For user account handling, SIG has set standards and protocols. For example, user ID creation and modification must be approved by designated personnel, authentication credentials are deactivated if unused for over six months, and user access to all systems resources is identified and authenticated. Entitlement reviews are also carried out to remove accounts of personnel who have been transferred to another organisation/role and no longer require current access levels to SIG's information systems. SIG has also produced a set of instructions to be followed when creating, changing new accounts, locking/unlocking user accounts and deleting user accounts, which can be referred to in the instruction user access management documentation. The aim of this instruction is to ensure transparency in the process and timely reaction. Passwords settings are governed at the corporate level and are protected using industry standard practices. For example, passwords are automatically required to be renewed every 90 days, with a minimum of 10 characters containing numbers, upper- and lower-case characters and special characters.

Administrators who require a super-user access to systems to perform duties have been given a unique user ID to identify each personnel. Administrators are aware that password sharing is strictly prohibited and subject to regular review.

SIG IT follows a standard process for controlling the inventory of SIG's information assets and personal identifiable information. This process requires all SIG information assets be identified, tracked, secured and identified with an owner. Information asset owners are responsible for maintaining up-to-date information regarding their information assets.

4.3 Information security – system physical and environmental security

4.3.1 Relevance

The protection of SIG's physical environment (i.e., data centres, secure workplaces) is one of the most obvious yet most important tasks. SIG considers physical and environmental security as a significant part of our information security management system. Physical security is required to protect physical data centres where information is stored. A lack of such control can undo the technical and organisational controls in place and put the business and lives at risk.

4.3.2 Overarching commitment

We are committed to ensuring the safety and security of employees', contractors' and business partners' information assets and personal identifiable information. We consider physical access, logical access, and environmental security as significant parts of our information security management system.

4.3.3 Targets

SIG's goals for information security – system physical and environmental security are:

- Percentage of physical and environmental security equipment regularly checked according to defined schedule: 100%.
- Percentage of SIG data centres complying with physical security design standards: 100%.

4.3.4 Implementation approach

Risk assessments are carried out to identify the level of appropriate protection of sensitive SIG specific information and personal identifiable information being stored. Security measures include, but are not limited to, fire alarms, window, and door locks, uniquely identified access passes on doors, CCTV cameras, reception staff and physical protection against fire, flood, and vandalism.

SIG IT has developed a set of directives which set the standard for the physical design of secure area to ensure that it remains secure whilst non-obstructive to the business carried out within it and is followed by the entire corporation. This directive includes topics such as physical security perimeter, physical entry controls, securing offices, rooms, and facilities, protecting against external and environmental threats, equipment sitting and protection, supporting unities and cabling security.

SIG has defined a comprehensive set of physical security measures for equipment which include:

- All paper-based information is assigned to an owner and assigned a level of sensitivity classification. The information must be stored in appropriate devices such as a locked cabinet or safes.
- All computers must be placed in a location that limits risks of hazards and theft.
- All workstations handling sensitive information are located to limit risk of data being seen.
- All equipment is maintained as per the manufacturer's instructions and any required internal procedures.
- All equipment to be disposed must have all its data or software erased or destroyed.
- Equipment delivery must be signed for by authorised individuals and must be complete.

4.4 Information security – systems operations management

4.4.1 Relevance

Systems operations management includes protecting the security of information when it is being handled, disposed, or transferred within or outside of the business and mitigating cybersecurity risks.

The nature of OT systems is changing as the underlying technologies, such as platforms, software, security, and communications are becoming more like IT systems. These changes increase OT vulnerabilities to malware and hackers. This is relevant for the IT and OT security in equipment and products. IT and OT vulnerability is defined as an inherent weakness in information systems, security instructions, internal controls, or implementation that could be exploited by a threat source and may include incidents such as exposure to malware, outdated software, interception of data transfer and permanent loss information. It is essential that effective precautions are taken to protect the corporation against threats from several sources including threat actor groups, competitor organisations, politically motivated groups, rogue employees, nation state sponsored "cyber-warfare" units or individuals exercising curiosity.

4.4.2 Overarching commitment

We are committed to continuously improving alignment and integration between SIG IT and OT security in equipment and products to provide adequate systems operations management and thereby reduce costs and risks as well as enhance performance. Therefore, we commit ourselves to regularly identify vulnerabilities in IT and OT and develop security measures such as software patching, malware protection, disposal management, network security, encryption, and effective back-up systems to ensure information remains in the hands of authenticated users. Likewise, we are committed to ensure the availability of our operational technology, and safety of our people.

4.4.3 Targets

SIG's goals for information security – systems operations management are:

- Percentage of critical and high vulnerability patch successfully applied on-time: 100%.
- Percentage of information security incident ticket completed on-time: 90%.
- Percentage of the plan vulnerability assessment performed: 100%.
- Number of vulnerability assessment (penetration test) performed per annum: 1.

4.4.4 Implementation approach

SIG conducts IT and OT vulnerability assessments on a six-monthly basis to identify exploitable vulnerabilities. These assessments are carried out in-house or by an external company and cover assessments of the security of all routes into the organisation's internal network from the internet, external web servers, business internal servers and a selection of user computers.

Methods of protection because of vulnerability assessments include:

- Software patch update notifications based on vendor releases to close "holes" in the systems.
- Anti-virus software daily quick scans, scans on read/write of files and a weekly full scan.
- Data on hard drives are rewritten over a minimum of three times before disposal.
- Incoming network communications into SIG are controlled using identification, authentication, authorisation, and logging.
- Virtual Private Network (VPN) is used for secured off-site (remote) connections to SIG network.
- Email transmissions, file transfers and internet transmissions are also secured through means of encryption.
- Security events and logs are reviewed in real-time and alert potential threat to security team.
- All information in SIG PC and laptops is encrypted.

4.5 Information security – system change management

4.5.1 Relevance

Change management is important for controlling risks and keeping disruptions to business functions at a minimum. When changes are made to IT and OT systems, there is a risk that a change in one system could cause a disruption in another system, for example through systems incompatibility. Therefore, every change in IT and OT systems must be managed through an approval system. An efficient change management is relevant for SIG as it allows changes to be implemented more quickly, thereby reducing mistakes and costs.

4.5.2 Overarching commitment

We are committed to reducing business disruptions caused by changes in SIG IT and OT security in equipment and products implementing a digital change management system in which all changes must be tested and approved through specific means prior to implementation.

4.5.3 Targets

SIG's goals for information security – system change management are:

- Number of unplanned downtimes caused by not applying change and configuration management processes: Zero.
- Percentage of major changes (projects) going through a quality gate ensuring managed change impact: 100%.

4.5.4 Implementation approach

SIG IT change management follows a standard process for changes to SIG IT and OT applications and infrastructure. There are three types of changes subject to change management procedures: 1) normal, 2) standard, and 3) emergency.

Normal changes are changes to assets within/associated with SIG IT and OT applications infrastructure that require approval and testing prior to implementation. Normal changes require review and approval from the Change Manager on Duty (CMoD). The planner for the change cannot be the same person as the approver for the change.

Standard changes are low risk, low impact pre-approved changes such as adding capacity to a server. During a standard change process, the assigned team must validate that the change is a standard change. If the change appears to be a standard change, planning documentation is required. If the documentation is not included, the change is not considered standard and is redirected through the normal change management process.

Emergency changes are regular impact changes that are urgent to address a production issue. Emergency changes must be tested and documented. Moreover, they may be approved after implementation.

4.6 Information security – system information protection

4.6.1 Relevance

SIG recognises that there are risks associated with employees, contractors, customers and other third parties accessing and handling SIG specific information and personal identifiable information to conduct business. SIG places high value on the protection of data and information of the company, its employees and business partners. Therefore, it is important that all employees, suppliers and other third parties follow a certain protocol to protect different forms of sensitive data.

4.6.2 Overarching commitment

We are committed to protecting SIG specific information including personal identifiable information using controls appropriate to the sensitivity of the information by developing company-wide protocols on classifying, labelling, and handling of different types of (sensitive) information and mediums.

4.6.3 Target

SIG's goal for information security – system information protection is:

- Percentage of information classified and labelled: 100%.

4.6.4 Implementation approach

SIG has a directive on how different types of information should be classified, labelled, and handled, and how personal identifiable information is collected and processed. Information can come in many forms, including physical, virtual, and verbal. Information must be classified based on its level of confidentiality, and this confidentiality level must be labelled as defined in the Information Classification, Labelling and Handling Directive. All classified information must be encrypted to protect against loss or unauthorised access. Additionally, different mediums must be handled in accordance with the protocol, depending on the type of medium and level of confidentiality.

We clearly explain to individuals in plain and simple language how their personal information is collected and used. We also employ rigorous internal control procedures and the use of information technology to ensure that information is protected.

4.7 Information security – system incident management and business continuity

4.7.1 Relevance

Information security incidents include unauthorised intrusions on IT and OT systems, information assets and personal identifiable information owned or managed by SIG. Such incidents could lead to sensitive information leakage and could cause disruptions to business functions or business revenue and therefore must be detected and resolved to maintain business continuity.

4.7.2 Overarching commitment

We are committed to defending, alerting, monitoring, analysing, responding, and handling of any information security incident. Shall such incidents occur, SIG commits to maintaining a framework to minimise the impact of disruptive events on SIG's business operations globally.

4.7.3 Targets

SIG's goals for information security – system incident management and business continuity are:

- Number of information security incident response plan exercised per annum: 1.
- Number of information security-related incidents causing disruption to business-critical processes: Zero.
- **Monetary damage** from cybersecurity incident: 0.

4.7.4 Implementation approach

The SIG Information Security Response Team is responsible for assessing any known threat strings and customising enterprise systems to address these threats across SIG's worldwide network. Such prevention measures are tested by an external expert through penetration testing (ethical hacking) and phishing campaigns.

Information users are required to report all security incidents immediately to the Information Security Incident Response Team. Reports of security incidents are escalated promptly. When a potential information security incident is detected, SIG conducts an event analysis to determine if there is a problem and if so, how critical the problem is. There is a defined reporting and feedback loop.

Each incident is analysed to determine if changes in the existing security practice are necessary. All reported incidents are logged, and the remedial action indicated. Additionally, a full root cause analysis and measures to

prevent re-occurrence are carried out. The Information Security Board is responsible for training on any procedural changes that may be required because of an incident.

Security breaches are investigated promptly. If criminal action is suspected, the Information Security Manager in conjunction with SIG Legal, will determine whether to contact law enforcement and investigative authorities.

To minimise the impact of incidents on business operations, business continuity plans are validated on a regular basis to ensure that solutions are viable at the time of a business disruptive event. Measures to ensure continuity is achieved include:

- Assignment of key responsibilities.
- Notification, escalation, and declaration of processes.
- Recovery Time Objectives and Recovery Point Objectives.
- Continuity plans with documented procedures.
- Training program for preparing all appropriate parties to execute the continuity plans.
- A testing, maintenance, and revision process.

SIG performs system backups of operating systems, recoveries, and offsite tape rotations for critical configuration items or components that are leveraged to administer the environment. SIG executes regularly scheduled backups of the SIG IT and OT infrastructure. SIG validates restoration of data periodically for disaster recovery purposes. The SIG backup and redundancy program undergoes an annual review and validation.

4.8 Information security – system supplier management

4.8.1 Relevance

IT and OT suppliers are used to not only help with the operation of the company but in many cases to deliver services directly to the customer, for example, cloud services. Suppliers must not only deliver good products and services, but also do so in a secure way that does not put SIG's and our customers' data at risk.

4.8.2 Overarching commitment

We are committed to protecting the confidentiality, integrity and availability of IT and OT when communicating with suppliers. We commit to conducting sufficient assessment of suppliers before and during the contract term, followed by complete and secure off-boarding.

4.8.3 Targets

SIG's goals for information security – system supplier management are:

- Percentage of cloud service provider information security assessments complete: 100%.
- Percentage of critical IT and OT suppliers that include information security requirement into contract: 100%.

4.8.4 Implementation approach

SIG ensures sufficient research and assessment is completed to determine whether suppliers can meet SIG's information security requirements before a contract is agreed on. Once a supplier is onboarded, suppliers are assessed on an ongoing basis at a frequency determined by their risk rating. Any concerns discovered during an assessment are tracked to resolution.

Companies often have differing language when defining information technology standards, for example, different meanings for confidentiality level classifications. SIG resolves this by defining such terms in the Supplier Information Security Agreement. In this same agreement, SIG also states our standards for incident management, awareness training, recruitment and screening, audit and review and supply chain security.

When a supplier relationship ends, suppliers are required to return to SIG and/or delete all copies of data in their possession. As well, where appropriate based on the services provided and associated risk, an off-boarding plan is developed that describes how SIG data is to be removed from the supplier's environment. The plan is reviewed and approved by SIG management.

4.9 IT compliance and audit

4.9.1 Relevance

Audits are relevant measures that can help ensure that the SIG information security management system is up to industry standards and meets any relevant regulations. Compliance by SIG personnel to SIG information security policies, protocols, directives, and instructions are essential to not undo the effectiveness of the information security management system put in place.

4.9.2 Overarching commitment

We are committed to establishing a framework that complies with the regulations applicable to SIG Global IT and SIG businesses through conducting periodic audit reviews of SIG's information infrastructure. We do not tolerate violations of information security policies, standards, or procedures.

4.9.3 Targets

SIG's goals for IT compliance and audit are:

- Percentage of security risk addressed in SIG Enterprise Risk Management: 100%.
- Percentage of severe and high IT security risk closed on time: 100%.
- Percentage of policy exceptions registered with countermeasure defined: 100%.
- Percentage of non-conformity finding from IT security audit completed on-time: 100%.

4.9.4 Implementation approach

A comprehensive framework governs the control activities within the SIG IT and OT applications and infrastructure. Applicable controls are evaluated against the environment for effectiveness and compliance with regulations applicable to SIG businesses. Changes to the framework itself are maintained by the SIG Enterprise Risk and Compliance team and, where applicable, new, or updated controls are implemented and/or evaluated against the processes supporting the SIG IT applications and infrastructure.

SIG is certified according to the ISO/IEC 27001:2013 standard. The scope of the certification covers the provision of ICT infrastructure, the associated application data centres and production operations in Germany, Romania, and China.

SIG performs periodic audits and reviews of its applications and infrastructure. SIG personnel who violate information security polices, standards or procedures are subject to disciplinary action up to and including loss of computer network access, dismissal from SIG and/or legal action. Other users who violate service offerings policies, standards or procedures are subject to actions that include loss of computer access, termination of contracts, and/or legal action.

4.10 Information security – system secure mobility

4.10.1 Relevance

Working remotely and the associated flexibility is increasingly more relevant for workers, including SIG employees. As remote information access methods improve, employees can work remotely in more efficient ways. However, as the capability improves, so do the risks. These risks may include loss or theft of devices, compromised classified information through observation by public environments and introduction of viruses and malware to the network.

4.10.2 Overarching commitment

We are committed to setting out a remote work policy that enables SIG employees to work as securely as possible remotely/from home, while keeping work efficiency stable. SIG is committed to maintaining a cohesive contingency plan for remote work and fosters business continuity with secure mobility, IT governance, and access management.

4.10.3 Target

SIG's goal for information security – system secure mobility is:

- Percentage of compliant managed mobile devices (iOS & Android): 100%.
- Percentage of user protected with multi factor authentication: 100%.

4.10.4 Implementation approach

Overall, SIG provides employees with appropriate devices which will be configured to comply with the organisation's policies. In some exceptional cases, employees may use devices not provided by SIG, to control and take correct security measures, which is specifically authorised via a set approval process.

Where relevant, all mobile devices will be managed via our mobile device management to secure employees are using specific remote security solutions so that all data is encrypted, and passwords protected. Where applicable, virus protection will be installed on the device by SIG.

When working remotely, users are to adhere to the following information security procedures:

- The user must ensure the device is transported in a protective case and not exposed to situations where it can be damaged.
- The user must not remove any identification marks from the device, such as its serial number.
- The user must ensure the device is locked away when being stored.
- The user must ensure that the device is configured to lock its screen after a short period of not being used. A strong access code or password must be used to lock the devices.
- Devices may be asked to be returned to the IT Service Desk for inspection at any time.
- The user should not install any unauthorised software or change the configuration without consulting the IT Service Desk.
- The user must not disable any encryption configuration on devices.
- The user should schedule some time to back up files on the device on a regular basis. The user must be careful to not take their own unencrypted back-ups of any classified information.
- The user must ensure that the device is connected to the internet on a regular basis to allow the virus signatures to be updated. The user must not disable the virus protection.
- When in public places, the user must ensure to place the device such that the screen cannot be viewed by unauthorised persons.

- In the event of the device being lost or stolen, the owner must inform the IT Service Desk as soon as possible, giving details of the circumstances of the loss and the sensitivity of the business information stored on it. SIG IT reserves the right to remote wipe the device where possible as a security precaution.

A common practice of working from home is web conferencing. To ensure information security during web conferencing, employees are advised to:

- Use organisation approved web conferencing platform, as non-approved platforms may have security problems.
- Double-check, cover, or blur backgrounds to hide personal information.
- Refrain from share invite links, even to trusted co-workers. Employees should tell the conference organiser to give this individual access to the conference.
- Review the people attending the conference and ask unrecognised persons to confirm their identity. Remove any persons suspected of unauthorised attendance.
- Inform attendees when recording conferences.
- Refrain from taking screenshots, as sensitive SIG specific information could be shared accidentally.

5 Changes to this Policy

The Cybersecurity and Information Privacy Protection Policy will be regularly reviewed by the respective Policy owner. Any changes or updates will be communicated. This policy was last updated on July 23, 2024.