Cybersecurity and Data Protection Requirements for Contractors

Status: June 2025

The following requirements apply to the Suppliers/Service Providers and their Subcontractors (in the following "Contractor"):

I. Requirements for the Contractor's organization, as well for the services of SMA systems and property:

- ISO 27001 certification (with scope of all relevant areas)
- If ISO 27001 certification is not met, the following requirements must be fulfilled:

1. Data Protection and Confidentiality

1.1. The Contractor shall implement and maintain appropriate technical and organizational measures to protect Confidential Information and Customer Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure.

1.2. The Contractor shall ensure that all personnel who have access to Customer Data:

- Have undergone appropriate security screening
- Are bound by written confidentiality obligations
- Have completed information security awareness training at least annually

2. Security Standards and Compliance

2.1. The Contractor shall maintain:

- ISO 27001 certification or equivalent security management framework
- Compliance with relevant industry standards including IEC 62443 for industrial control systems
- Regular third-party security assessments and penetration testing
- SOC 2 Type II reports (where applicable)

2.2. The Contractor shall provide evidence of compliance upon request and notify SMA of any lapse in certification status within 48 hours.

3. Security Incident Management

3.1. The Contractor shall:

- Maintain a documented security incident response plan
- Notify SMA within 24 hours of discovering any security incident that affects or may affect Customer Data or systems
- Provide detailed incident reports within 72 hours of discovery
- Cooperate fully with any investigation initiated by SMA

3.2. The Contractor shall maintain capabilities to:

- Detect and respond to security events 24/7/365
- Preserve forensic evidence
- Implement immediate containment measures

4. Access Control and Identity Management

The Contractor shall:

- Implement role-based access control (RBAC)
- Use multi-factor authentication for all privileged access
- Review access rights quarterly
- Maintain logs of all access to SMA systems and data
- Revoke access within 24 hours of employee termination

5. Supply Chain Security

The Contractor shall:

- Maintain an inventory of all sub-suppliers who may access or process Customer Data
- Ensure sub-suppliers are contractually bound by equivalent security requirements
- Perform security assessments of sub-suppliers at least annually

6. Secure Development and Operations

For any software or firmware:

- Implement secure development lifecycle (SDLC) practices

- Conduct security testing before each release
- Provide timely security patches and updates
- Maintain secure code signing processes
- Document all third-party components and dependencies
- The privacy by design approach and the security by default approach are mandatory

7. Business Continuity and Disaster Recovery

The Contractor shall:

- Maintain documented business continuity and disaster recovery plans
- Test these plans at least annually
- Ensure recovery time objectives (RTO) align with SMA requirements
- Back up all Customer Data according to adequate schedules

8. Audit and Assessment Rights

SMA reserves the right to:

- Conduct security assessments with 5 business days' notice
- Request evidence of security controls and their effectiveness
- Require remediation of identified security issues within agreed timeframes
- Terminate the Contract for major security violations

9. Data Return and Destruction

Upon contract termination, the Contractor shall:

- Return all Customer Data in an agreed format
- Securely destroy all copies of Customer Data
- Provide written certification of destruction
- Maintain no copies except as required by law

10. Security Enhancement and Evolution

The Contractor shall:

- Continuously monitor and evaluate security threats
- Enhance security controls as threats evolve
- Implement security improvements as recommended by SMA
- Participate in SMA security reviews quarterly

11. Compliance with Security Laws and Regulations

The Contractor shall comply with:

- If applicable Critical infrastructure protection requirements

II. Requirements for the products (concerns components / inbound devices and "white label" devices):

1. At SMA, cybersecurity and data protection are integral to our solutions and products, particularly in light of increasing connectivity, system integration, and evolving mandatory regulatory requirements and standards.
2. Secure operation of energy systems, protection against cyberattacks and trust in secure data management are crucial for a future energy supply in the age of digitalization and artificial intelligence. The vision of our organization is to make the energy supply of the future invulnerable by providing cybersecure products, solutions and services without restricting their functionality and usability and keep the data protected.
3. In the context of inbound projects and inbound products, SMA relies on the contractor's cooperation to fulfill the conformity for specific requirements and Contractor ensures SMA for such fulfillment. These requirements have been established as part of a comprehensive risk assessment for the inbound projects and inbound products provided by the Contractor and are detailed below.

III. Cybersecurity requirements for contractors of inbound devices and components

1. The Contractor affirms that all functions within the provided inbound devices and components align with the agreed intended use. This refers in particular to the absence of functions designed to intentionally damage other components or systems through malfunction and faulty operation.

2. The Contractor confirms adherence to international standards in cybersecurity and data protection in particular those applicable in Germany, EU and US, throughout product development and production, and agrees to provide evidence of compliance immediately and unsolicited. In particular, the contractor confirms compliance with ISO 27001:2022 (Information security, cybersecurity and privacy protection – Information security management systems – Requirements).

3. The Contractor commits to providing regular cybersecurity and privacy training for personnel in relevant areas to enhance awareness of potential threats.

4. Access to the inbound products is restricted to authorized personnel involved in hardware and software development and production.

5. All components and data provided by SMA may only be used for the purposes explicitly agreed upon in the contract. Reverse engineering and disclosure of data to any third party without SMA's prior written consent are strictly prohibited. In case of violation of such restriction, the Contractor shall remain liable for any damages that could be caused to SMA to the extent permitted by the applicable law.

6. The Contractor agrees to conduct regular and at any time if requested by SMA, risk assessments to identify potential cybersecurity vulnerabilities, implement appropriate risk mitigation strategies and provide this information to SMA immediately and unsolicited.

7. The Contractor will document all events related to cybersecurity and data protection and to the extent permitted by law, forward the documentation immediately and unsolicited to SMA.

8. The Contractor declares that there are no known vulnerabilities in the provided inbound devices and components at the time of delivery to SMA and agrees to substantiate this claim, for example, through a Software Bill of Materials (SBOM).

9. The Contractor commits to notifying SMA of any newly identified vulnerabilities in the provided inbound devices and components within 36 hours of discovery.

10. The Contractor agrees to provide software and firmware updates for the provided inbound devices and components free of charge during the agreed support period, which will be based on the expected service life of the provided inbound devices and components, addressing publicly known exploitable vulnerabilities.

11. The Contractor will deliver security updates for the provided inbound devices and components to SMA within the agreed support period, no later than 45 days after a vulnerability is disclosed.

12. The Contractor affirms that there are no backdoors or default passwords present in the provided inbound devices and components.

13. The Contractor declares that there is no unauthorized incoming or outgoing data communication from the provided inbound devices and components to other components or systems, aside from the SMA communication module (e.g., SMA-COM). Otherwise, if unavoidable, any data communication to external systems via non-SMA components requires prior written approval from SMA.

14. The Contractor confirms that all debug and test interfaces have been removed or lasting disabled in the production version of the provided inbound devices and components, including but not limited to any JTAG[1] interfaces on the control processor.

15. The Contractor asserts that no closed-source software (software binaries, compiled software stacks) is required for the integration of the provided inbound devices and components into SMA components. If closed-source software is necessary for technical reasons, the Contractor must provide documented source code including compilation details, checksums for validation and ensure that the closed-source

[1] JTAG is a manufacturer-independent programming and debugging interface for integrated circuits. This allows you to load new programs on these circuits and then test them ("debug"). From development to the final test, this interface makes perfect sense - in a delivered product, however, this interface can also serve as a vector for attacking the device due to its function. An attacker could use it to influence the program code and thus the function of the device. Therefore, the interface must be removed or at least deactivated in the final product.

software is able to operate in a sandbox environment[2] to prevent unauthorized data communication.

16. The Contractor guarantees that all provided inbound devices and components can be updated using SMA's supported update mechanisms. Updates via non-SMA mechanisms are not permitted.

17. The Contractor grants SMA the right to conduct audits of the production process concerning cybersecurity, particularly in areas where SMA firmware or data is utilized.

18. For the purpose of compliance and adjustment with changes that could be done to national and international standards and laws, SMA reserves the right to modify or expand its cybersecurity requirements at any time and such changes shall be binding for the Parties.

[2] A sandbox is a secure runtime environment for software programs. The sandbox regulates what the program is allowed to do beyond the limits of the sandbox, e.g. a limitation of CPU performance or memory size, or which interfaces of the component may be used by the program. This allows programs whose source code you do not own or can view and analyze ("closed source"). Such option allows SMA to mitigate or at least limit the potential damage caused by malicious code that may have been injected into the program by an attacker.