

ABB Cyber Security Requirements for Suppliers

This document outlines minimum cyber security requirements applicable to ABB Suppliers that:

- i. process, access, interact with, or store ABB Information, Personally Identifiable Information (PII), or
- ii. have access to ABB Information Systems, or
- iii. supply software-related products¹ and/or services to ABB

pursuant to the respective contract referencing this document.

The Supplier is responsible to take all the necessary measures and steps to comply with the requirements listed in this document.

ABB reserves the right to ask for documentation and evidence, as well as to perform or order a compliance audit, to determine whether the listed requirements are fulfilled.

The Supplier shall ensure that all sub-suppliers or sub-contracting relationships or external dependencies that provide services or supply software-related products¹ that are part of supplied products to ABB or provide services related to the development of supplied products to ABB (e.g., code implementation or testing) comply with the requirements listed in this document or with equivalent requirements to the ones listed in this document.

Notwithstanding the foregoing, the Supplier shall be fully responsible for all acts and omissions of its sub-suppliers or sub-contracting relationships or external dependencies as if they were Supplier's acts or omissions.

ABB reserves the right to update this document from time to time and any such modification or amendment will be applicable from the date of the respective modification or amendment as indicated in the new release of this document which shall, however, not be earlier than the actual release date.

This document contains the terms “including,” “include,” “in particular,” “such as,” or similar expressions. They shall be construed as illustrative and shall not limit the sense of the words preceding those terms. The term ‘Third-Party’ used in this document refers to any entity that is providing goods or services or products¹ to ABB pursuant to the contract referencing this document or any contractor, agent or third-party who provides hardware, software, goods, or services to any member of the Customer (ABB) Group.

¹ A software-related product is defined as a product or system, including all versions and updates, that (i) uses any type of software, (ii) is partly based on any type of software, or (iii) is in itself a type of software. Here, software shall be considered in its broadest sense and includes for instance firmware, drivers, applications, etc.

1. IT Security Requirements

1.1. Cyber security & Privacy Governance

To comply with ABB's cyber security and privacy policies and standards, the Supplier shall implement and maintain a comprehensive cyber security and privacy program. The Supplier shall define roles and responsibilities by assigning qualified individuals and resources to manage and coordinate the program. The Supplier shall have measures to monitor and report on the program's effectiveness and provide ongoing education and training to align with industry best practices in cyber security and privacy.

1.2. Risk Management

The Supplier shall implement and maintain a risk management process to identify, assess, and manage information security risks. This process shall include regular risk assessments and the prioritization of resources to address identified risks. The Supplier shall maintain a risk register to document key risk factors, including organizational risk tolerance. Additionally, the Supplier shall have a program to manage risks associated with third-party software, artificial intelligence, and autonomous technologies.

1.3. Third-Party Management

The Supplier shall implement and maintain a third-party risk management process to effectively oversee and manage risks associated with third-party providers. This process shall ensure the identification, assessment, and mitigation of risks, as well as the regular review and adjustment of third-party relationships to align with organizational security requirements.

1.4. Information Assurance

The Supplier shall implement and maintain processes for assessing cyber security and privacy controls in systems, applications, and services. The Supplier shall conduct regular assessments, including third-party evaluations, to ensure that the controls are implemented effectively. For Suppliers hosting ABB data, SOC 2 Type II certification or an equivalent attestation is required to demonstrate compliance and security assurance.

1.5. Incident Response

The Supplier shall implement and maintain a documented cyber security incident management program to ensure an organization-wide capability for handling cyber security and privacy related incidents. This program shall cover preparation, automated detection, reporting, analysis, containment, eradication, and recovery. The incident response plan shall be made available to the Customer and shall be regularly reviewed and modified to incorporate lessons learned, business process changes, and industry developments, as necessary. Processes shall exist to monitor and report incidents both internally to the organization and externally to regulatory authorities, Customers, and affected parties, as necessary. An integrated team of cyber security, IT, & business function representatives capable of addressing incident response shall be established.

Incident Response controls shall cover, but not be limited to, the following areas:

- Training personnel in their incident response roles and responsibilities
- Evaluate incident response capabilities to determine their operational effectiveness.
- Performing forensics and preserving the integrity of chain of custody in line with applicable laws and regulations

- Providing incident information to the product/service providers and other supply chain partners
- Implementing and governing an insider threat response capability
- Responding to sensitive information spills and formally assigning roles and responsibilities for managing such incidents
- Incorporating lessons learned by analyzing incidents to reduce future impact.

The Supplier shall notify the Customer (business/engagement manager and ABB CSIRT at cert@abb.com) promptly, in accordance with any applicable law or regulation and in any event within 72 hours after discovery of any security incidents or threats relating to the Services and/or Customer Material, data, or information. Identified remedial actions following an incident shall be documented in a remediation plan, including action items, ownership, and delivery dates, and shall be shared with the Customer. Remedial action shall be executed in a timely manner.

1.6. Asset Management

The Supplier shall implement and maintain an asset management program to oversee and control organizational assets. This program shall ensure accurate tracking and accountability for assets throughout their lifecycle, maintaining documentation and regular review. It shall also include measures to secure and manage asset information and ensure compliance with organizational standards and audit requirements.

Cyber security and privacy controls must be applied to all assets by identifying, assigning, and documenting asset scope, categorization, and control applicability boundaries. Assets shall be securely disposed of, destroyed, or repurposed to prevent information recovery. All organizational assets must be returned upon termination of employment or contract. Regular inspections of critical assets shall be conducted to detect and prevent tampering. Asset inventories must be reviewed regularly and be available for audit by designated officials.

1.7. Data Classification

The Supplier shall implement and maintain a data classification and handling process to ensure that systems, applications, and services are classified according to the highest level of data sensitivity that is stored, transmitted, and/or processed. Physical and logical controls shall be implemented to securely store digital and non-digital data and/or media using Supplier-defined security measures until they are destroyed or sanitized. Data handling requirements shall guide the management, processing, storage, transmission, and protection of data to ensure its confidentiality, integrity, and availability.

Data classification controls shall cover, but not be limited to, the following areas:

- Identifying and documenting the location of information and its residing system
- Protecting and controlling media during transport
- Securely disposing media when it is no longer required, using formal procedures
- Sanitizing media according to data sensitivity before disposal
- Data flow diagrams to capture data flows for applications, infrastructure, and third-party sharing.
- Guidance for securely sharing information between systems.
- Data retention shall comply with regulatory and contractual obligations.

1.8. Human Resources Security

The Supplier shall implement and maintain a comprehensive human resources security program to protect organizational assets and data. This program shall cover cyber security responsibilities, conduct screening (as permitted by regional regulations), and establish clear guidelines for acceptable technology use, including consequences for violations. Employees shall receive role-based training to maintain compliance with security standards, and third-party personnel security shall be managed through regular reviews and monitoring of their cyber security and privacy roles and responsibilities. Internal and third-party users shall sign appropriate access agreements, such as Non-Disclosure Agreements (NDAs), before being granted access.

1.9. Security Awareness & Training

The Supplier shall provide cyber security and privacy awareness training to all employees and contractors relevant to their job functions. This training shall occur before authorizing system access, during system changes, and annually thereafter. All training activities shall be documented, maintained, and regularly updated.

1.10. Change Management

The Supplier shall implement a change management process to oversee and control modifications to organizational assets. This process shall ensure that changes are authorized, reviewed by relevant stakeholders, and communicated to all affected parties, with the aim of minimizing risk and maintaining system integrity.

1.11. Security Operations

The Supplier shall ensure continuous protection of systems, applications, and data to maintain the organization's security posture. A security operations center or an equivalent continuous monitoring shall be established to maintain vigilance over the organization's networks, systems, and applications thereby ensuring a proactive defense posture against cyber threats.

1.12. Threat Management

The Supplier shall implement and maintain a threat intelligence program with cross-organization information-sharing capability to influence development of security architectures and selection of security solutions. Utilizing threat intelligence feeds to stay aware of evolving threats, the Supplier shall leverage attacker tactics and procedures for implementation of preventative controls. An insider threat program shall be established to report potential threats and promote awareness. Cyber threat hunting using indicators of compromise shall be conducted to detect and disrupt advanced threats. The Supplier shall implement measures to detect and trace data exfiltration activities, ensuring the identification of unauthorized access or individuals involved.

1.13. Vulnerability & Patch Management

The Supplier shall implement and maintain a vulnerability management program to identify, analyze, prioritize, and address security vulnerabilities. This program shall ensure continuous detection, monitoring, timely response to identified vulnerabilities, and effective mitigation strategies.

Vulnerability management controls shall cover, but not be limited to, the following areas:

- Patching for all operating systems, applications, end-user software, middleware, network devices, firmware etc.
- Centrally manage and track remediation of vulnerabilities based on defined timelines.
- Compare the results of vulnerability assessment reports over time to determine trends in system vulnerabilities.

1.14. Network Security

The Supplier shall implement measures to ensure the integrity and confidentiality of network communications or information transmitted across network interfaces by monitoring and controlling communications at boundaries, restricting untrusted connections, and protecting data flows.

Measures shall exist to uniquely identify and authenticate source and destination points for information transfer. Data protection measures shall be implemented to protect sensitive the Customer information.

Techniques such as network segmentation, intrusion/detection systems, and secure transmission channels shall be employed to minimize risks. The Supplier shall protect data over open networks, define secure remote access methods, and control third-party access. Secure wireless access and continuous monitoring shall be implemented to prevent unauthorized connections.

1.15. Continuous Monitoring

The Supplier shall ensure continuous oversight of security events and effective incident response through comprehensive enterprise-wide monitoring. Enhanced activity monitoring shall be implemented for high-risk individuals. The Supplier shall utilize tools to support the centralized collection and correlation of security-related event logs across the enterprise. Measures shall exist to integrate the analysis of event logs with other sources to enhance the ability to identify inappropriate or unusual activity. Measures shall provide event log report generation capabilities to aid in detecting and assessing anomalous activities. Trend analysis and reporting shall aid in refining security controls. The Supplier shall utilize non-repudiation measures to ensure the origin, authenticity, and integrity of information. Cross-organizational log sharing and monitoring third-party activities shall be established to help identify and mitigate potential security incidents effectively.

1.16. Configuration Management

The Supplier shall implement and maintain secure baseline configurations for technology platforms, aligned with industry standards. This process shall require that systems be configured to minimize security risks, provide only essential functionality, and are regularly reviewed and updated to prevent unauthorized modifications. Governance and reporting measures for baseline configuration management shall exist including a method to determine deviations from defined baselines. Controls shall be implemented to prevent information leakage, prevent unauthorized software installations, and enforce software restrictions to comply with applicable contracts, copyright laws, and the secure use of open-source software.

1.17. Security Engineering & Architecture

The Supplier shall develop an enterprise architecture, aligned with industry standards or leading practices, with consideration for cyber security and privacy principles that addresses risk to organizational operations, assets, individuals, other organizations. Industry recognized cyber security and privacy practices shall be implemented in the specification, design, development, implementation, and modification of systems and services. Safeguards shall be in place to prevent unauthorized and unintended information transfer via shared system resources. A diverse set of technologies shall be utilized to mitigate the impact of vulnerabilities from the same original equipment manufacturer (OEM). The Supplier shall consider the adoption of deception security controls. Time synchronization technology shall be utilized to synchronize time across all systems. Additionally, the Supplier shall develop and maintain a network architecture diagram to illustrate the network architecture, including configuration, interconnections, and security controls, ensuring it is kept up-to-date and reflective of the current state.

1.18. Endpoint Security

The Supplier shall protect the confidentiality, integrity, and availability of endpoint devices by ensuring they are secure from unauthorized access and potential threats. Controls shall prohibit software installations without explicitly assigned privileges. The Supplier shall maintain system stability and consistently apply security measures across all endpoint devices. Anti-malware technologies shall be used and regularly updated, with central management to combat evolving threats. Protections against phishing and spam shall also be centrally managed to detect and minimize risks from malicious code.

1.19. Cryptographic Protections

The Supplier shall implement and maintain cryptographic measures to protect data at rest and during transmission to ensure confidentiality and integrity. Secure authentication and encryption techniques shall be used for wireless access.

1.20. Identification & Authentication

The Supplier shall implement and maintain identification and access management controls to uniquely identify, authenticate, and audit users, devices, and services. Access rights shall be reviewed based on defined frequency and revoked promptly upon termination of employment. Measures shall be in place to proactively govern account management of individual, group, system, service, application, guest, and temporary accounts. Multi-factor authentication shall be required for critical systems and remote access. Vendor supplied default credentials shall be changed during installation. Measures shall exist to federate credentials to allow cross-organization authentication of individuals and devices.

1.21. Mobile Device Management

The Supplier shall implement and maintain mobile device management (MDM) controls. Measures shall be implemented to protect mobile devices from tampering and capability to remotely wipe devices shall be enabled to prevent unauthorized access to organizational data.

1.22. Physical and Environmental Security

The Supplier shall implement and maintain physical access controls to authorize access to facilities based on individual roles and responsibilities. The Supplier shall identify, authorize, and monitor visitors before allowing access to the facility. Asset location and movement within organization defined controlled areas shall be tracked and monitored. Additionally, the Supplier shall designate secure areas to safeguard sensitive information and assets and implement measures to detect and respond to physical security incidents. Power and telecommunications cabling carrying data or supporting information services shall

remain protected always from interception, interference, or damage. Technical, operational, and management controls shall be implemented at alternate work sites (e.g., disaster recovery sites, business continuity locations etc.).

1.23. Privacy

The Supplier shall implement and maintain a comprehensive privacy program to protect personal data (PD). A Privacy Officer (PO) or similar position being responsible for privacy compliance shall be appointed to oversee privacy practices. Information about privacy-related activities shall be accessible to the public and privacy notices shall be clear and readily available. The scope of personal data processing activities, including geographic locations and third-party recipients that process personal data, shall be defined. Personal data shall be retained only as long as necessary (or for the duration of the agreement with the Customer, whichever is earlier) and securely disposed. The use of personal data for internal purposes shall be minimized and authorized. Individuals shall have access to a defined process for appealing adverse decisions and correcting incorrect information to ensure fairness and accuracy. Personal data shall be shared with third parties only for specified purposes and with the general written authorization of the customer consent. Privacy testing, training, and monitoring activities shall be conducted regularly. The quality and integrity of personal data shall be ensured, and records of data disclosures shall be maintained and made available upon request to the Customer.

1.24. Artificial & Autonomous Technologies

The Supplier shall maintain an inventory of all artificial intelligence (AI) and autonomous technologies (AAT) including third-party components. The Supplier shall assess and map the risks and benefits of these technologies to manage potential impacts. Additionally, the Supplier shall identify data sources for AI and AAT to prevent third-party intellectual property (IP) rights infringement and ensure compliance.

1.25. Business Continuity & Disaster Recovery

The Supplier shall implement and maintain a business continuity and disaster recovery program to ensure service resilience through coordination with internal and external parties. Critical systems and applications supporting essential missions and business functions shall be clearly identified. Measures shall be in place to adequately train contingency personnel and stakeholders in their roles and responsibilities. Contingency plans shall be regularly evaluated, updated, and informed by root cause analysis and lessons learned. Procedures shall ensure the availability and integrity of data to meet recovery time and point objectives (RTO/RPO). Recovery operations at alternate sites shall align with these objectives. Telecommunication service providers shall be required to have contingency plans to avoid single points of failure.

1.26. Maintenance

The Supplier shall implement and maintain processes to perform controlled maintenance activities throughout the lifecycle of a system, application, or service. Processes shall be defined to ensure maintenance support for systems meet the defined recovery time objective. Checks shall be in place to validate if media containing diagnostic and test programs are verified for malicious content before usage. Measures exist to review remote maintenance/diagnostic sessions and to validate if systems performing remote maintenance/diagnostics have a security capability like the system being serviced. A current list of authorized maintenance personnel shall be maintained and reviewed as per defined timelines. Physical security of technology assets awaiting service or repair shall be maintained.

1.27. Compliance

The Supplier shall ensure compliance with relevant statutory, regulatory, and contractual requirements. Instances of non-compliance with relevant statutory, regulatory, or contractual requirements incidents shall be documented and addressed. Oversight of cyber security and privacy controls shall be reported to executive leadership. An internal audit function shall exist to provide insights around the effectiveness of the organization's technology and information governance processes. Audits shall be planned with minimal impact on business operations. Legal assessments shall determine the validity of government data requests and notify the Customer of investigation requests when permissible. Access for investigations shall be restricted to the least privileges necessary.

1.28. Capacity & Performance Planning

The Supplier shall implement measures to manage resource utilization of systems and to ensure sufficient capacity for information processing and support during contingency operations.

1.29. Technology Development & Acquisition

The Supplier shall integrate security into all phases of software development, aligning with industry standards. Development, testing, and production environments shall be kept separate to reduce risks of unauthorized access or changes or impact to production environments. Unsupported or end-of-life systems shall be replaced, or their continued use shall be justified and documented.

2. Product Security Requirements

This section states additional minimum cyber security requirements that shall be fulfilled for any software-related product² that is supplied to ABB pursuant to the respective contract referencing this document (hereinafter referred to as “Product”).

2.1. Secure Development Lifecycle

The Supplier shall establish, document, and implement initiatives in line with commonly accepted industry standards and practices to build security into the software development process of the Product. Such initiatives shall build security within all phases of the development lifecycle, e.g., training, requirement, design, implementation, verification, release, and response.

2.2. Security Quality

The Supplier shall take measures to improve the security quality of the Product. These measures shall follow commonly accepted industry standards and practices and shall include, where technically feasible:

- Robustness testing, including fuzzing and flooding.
- Vulnerability scanning for known vulnerabilities and exploits.
- Security testing, including static code analysis or binary code analysis.

2.3. Backdoor Accounts and Hardcoded Credentials

The Product shall not have any accounts, passwords, or private/secret keys that cannot be changed, disabled, or removed by the authorized end user of the Product. The Product shall not have any accounts (individual, shared, debug, etc.,) that are not documented (this does not imply that the associated access credentials must be disclosed).

2.4. Cryptographic Tools and Security Functionalities

Any cryptographic tool and security functionality implemented or used in the Product shall follow commonly accepted security industry recommendations and guidelines (e.g., as recommended by NIST or defined in international standards). This includes, for example:

- Cryptographic algorithms to hash, encrypt, or sign data for storage or transmission.
- Protocols and procedures to support cryptographic algorithms (e.g., to exchange certificates, to establish keys, or to generate random numbers).
- Functionality to authenticate end users or for access control.

Any cryptographic tool or security functionality implemented or used in the Product that does not follow commonly accepted security industry recommendations and guidelines shall be documented and communicated to ABB. Such documentation shall include, at least, its origin (e.g., proprietary tool), its reference documentation (e.g., academic publication), its functionality (e.g., encryption), its main security-related features, characteristics, and parameters (e.g., used ECC curve), as well as in which context or part of the Product it is used (e.g., user authentication).

² A software-related product is defined as a product or system, including all versions and updates, that (i) uses any type of software, (ii) is partly based on any type of software, or (iii) is in itself a type of software. Here, software shall be considered in its broadest sense and includes for instance firmware, drivers, applications, etc.

2.5. Protection from Malware Propagation

The Supplier shall proactively take measures to prevent malware from being propagated. These measures shall follow commonly accepted industry standards and practices and shall include successfully scanning software deliverables (including their storage media, e.g., CDs, hard disks, or flash cards) with different suitable and up-to-date antivirus solutions before delivery.

2.6. Handling of Digital Certificates

If digital certificates are used in the development of the Product (e.g., to sign code or as a root to derive product-specific certificates), they shall be protected and handled according to commonly accepted industry standards and practices.

2.7. Product Documentation

The documentation provided with the Product shall include:

- All user and system accounts in the Product with a recommendation to change at least the access credentials.
- Description of all ports, services, and software needed to support any functionality in the Product, as well as how these ports, services, and software can be configured and, when applicable, how these can be disabled, blocked, or uninstalled.
- Information on proper configuration and usage of cyber security related functionalities in the Product.
- Specific instructions on how to configure the security controls provided by the Product (e.g., RBAC, security logging, or secure communication), as well as security controls provided in addition to the Product (e.g., antivirus, whitelisting, or security monitoring).
- A recommendation for at least one malware prevention solution to be used during the operation of the Product, if such a solution exists. The recommendation shall include the specific version of the malware prevention solution, as well as a description of the performed testing and validation by the Supplier.

2.8. Vulnerability Handling

The Supplier shall establish, document, and implement a process to react to vulnerabilities and security issues associated with the Product. The process shall follow commonly accepted industry standards and practices and shall include procedures and interfaces to:

1. Enable ABB to submit vulnerability reports.
 - The Supplier shall provide ABB with all necessary information on how ABB can report found vulnerabilities.
2. Acknowledge the receipt of a vulnerability report submitted by ABB within two business days or such shorter term as reasonably requested by ABB from the report submission.
3. For vulnerabilities where ABB is the original finder, submit information to ABB on the result of the vulnerability verification within seven business days or such shorter term as reasonably requested by ABB from the acknowledgment of a vulnerability submission by ABB.
 - The Supplier shall provide information on the vulnerability validity and severity, the list of potentially affected Products and their versions, as available at that time, and whenever possible, information on how to verify the existence of the vulnerability in its Products.
 - The Supplier shall also provide an estimate regarding the timeframe for the remediation release, as well as possible workarounds while the remediation solution is defined and implemented.

4. Share vulnerability remediation and advisory reports.
 - The Supplier shall provide ABB with information on how vulnerability remediation and advisory reports related to any submitted vulnerability by ABB or any other entity are shared with ABB.
 - The advisory report shall include the description of the vulnerability, information about the remediation and workarounds, the list of affected systems and products, the vulnerability impact (threats, exploits, and severity rating), and related references (e.g., to related vulnerabilities).
 - If the Product is included in the build or installation package of any ABB product (e.g., such as libraries or an embedded OS), the Supplier shall have a means to release the vulnerability remediation and the advisory report to ABB prior to public disclosure.

In addition, the Supplier shall take all actions as reasonably requested by ABB in case of a vulnerability or other security issue associated with the Product.

2.9. Patch Management

The Supplier shall establish, document, and implement a strategy and process to deal with third-party software security updates and patches relevant to the Product.

Relevant third-party software shall at least include:

- A. Any third-party software that is included in the build or installation package of the Product (e.g., third-party libraries or embedded OS).
- B. Any third-party software on which the Product depends or that is typically used in the deployment of the Product without being an integrated part of it (e.g., MS Windows, MS Office, Java Runtime Environment, or Acrobat Reader).

The strategy and process for third-party software of type A (as specified above) shall at least include:

- Monitoring for security updates and patches to all relevant third-party software.
- Execution of the vulnerability handling process (as defined in requirement 2.8) for security updates and patches deemed applicable and where the patch or update addresses vulnerabilities or security issues.

The strategy and process for third-party software of type B (as specified above) shall at least include:

- Maintaining a list of all relevant third-party software dependencies.
- Recommended general approach for application of security updates and patches for each of the listed third-party software dependencies.
- As reasonably requested by ABB, for security updates and patches deemed applicable:
 - Validation of third-party software updates and patches.
 - Communication to ABB of the validation results and the taken/planned actions to resolve validation issues.
 - At ABB's discretion, ABB can perform the validation of the Product's third-party software updates and patches. In such circumstances, the Supplier shall first inform ABB of any Product's third-party software update or patch and then support ABB during the validation and to resolve validation issues.

2.10. Software Integrity and Authenticity

The Supplier shall provide ABB with the capability to verify the integrity and authenticity, e.g., through digital signatures, of software deliverables associated with the Product, at least, by packaging any software delivered to ABB in a way to allow ABB to verify the integrity and authenticity of such package. Where technically feasible, all relevant files of the software deliverable shall be digitally signed.

2.11. Data Collection

While the Supplier's rights, if any, with regard to collection, processing, and use of data are covered in separate documents, the Supplier shall in any case document, and make available to ABB such documentation, any data collection activity performed by the Product, detailing which data are collected and the related functionality and/or purpose, as well as if, where, and how these data are stored, used, processed, and transmitted.

2.12. Vulnerability Assessment

ABB reserves the right to perform an assessment on the security of the Product to identify potential vulnerabilities.