Annex 5 to the Supplementary Contractual Terms for Information Security
Rolling stock

Version dated November 1, 2026

4 Preamble

These regulations apply in addition to the Supplementary Terms and Conditions of Deutsche Bahn AG and its Affiliated Companies on Information Security Requirements (Supplementary Contractual Terms for Information Security) and regulate the following application case:

- Rolling stock
- Spare parts for rolling stock, where they do not meet the definition of functionally equivalent spare parts

For the purposes of this Annex, the term IT/OT assets refers to all products, systems, components, spare parts, software and services with digital elements that are delivered, provided or operated by the Contractor for the Client, including all operationally required components and documentation.

5 Product-specific information security requirements

5.1 General requirements

5.1.1 Availability

The following response times shall apply to the contact persons, unless the Client and Contractor have expressly agreed otherwise in the contract or service level agreement (SLA).

Response times are given in Central European Time/Central European Summer Time. Public holidays at service delivery locations of the Client and Contractor are not considered business hours. If the provisions on availability are to apply in the absence of a separate service agreement, this will be specified in the supply agreement.

	Protection requirement	
	Standard	High or very high
Normal communication		
Contractor's response time to Client request	8 hours (during business hours: Mon. - Fri., 9 am - 5 pm)	4 hours (during business hours: Mon. - Fri., 9 am - 5 pm)
Incident-related communication		
Reporting of information security incidents and vulnerabilities	Immediate	Immediate
Response time for Contractor's emergency contact person	4 hours (during business hours: Mon. - Fri., 9 am - 5 pm)	1 hour (during extended business hours: Mon. - Fri., 8 am - 8 pm)

Table 1: Response times

5.1.2 Support for information security risk management

If the Contractor supplies or operates IT and/or OT assets that are to be used in network infrastructure of the DB Group or that transmit information to such a network, it shall implement structured information security risk management and provide the necessary information from this to enable appropriate risk management on the Client side. This includes, where applicable, the provision of information on the following topics:

- Supply chain security, including security-related aspects of the relationship between the Contractor and service providers/suppliers contracted by the Contractor
- Security measures for the development, integration, operation and maintenance of IT and OT systems, including the reporting and management of vulnerabilities

The Contractor shall provide this information for the first time as part of the conclusion of the contract and shall keep it up to date throughout the provision of the contractually agreed work.

See also Section 5.7.1. "Security documentation"

5.1.3 Cybersecurity risk assessment

The Contractor shall conduct a cybersecurity risk assessment, using an established method, for the IT/OT assets covered by the contract and shall keep this assessment up to date throughout the provision of the contractually agreed work or the agreed period for which the Contractor provides support for the IT/OT asset (unless contractually agreed otherwise; whichever date is the later shall apply). For OT assets, the assessment shall be performed in accordance with IEC 62443-3-2. The use of other, demonstrably equivalent cybersecurity risk assessment methods is permitted, provided that the Client's written consent is obtained when the contract is concluded. For rail system assets, the analysis may be performed in accordance with CLC/TS 50701 or its successor standard, for example.

The cybersecurity risk assessment and any updates to it shall be provided to the Client in a digitally editable format. The Contractor shall, at no additional cost to the Client, implement any measures necessary to comply with the legal requirements applicable to the Contractor, particularly Regulation (EU) 2024/2847 (Cyber Resilience Act). With regard to any additional measures requested by the Client, the Client and Contractor shall agree on the scope of implementation and costs.

The Contractor shall have the risk assessment verified by an independent third party if requested. If the Client requests this, the Client shall bear the resulting costs.

5.2 **Asset and configuration management**

The Contractor shall provide the Client with technical documentation for all components of the deliverable. This includes the complete configuration data, software bills of materials (SBOM) in accordance with BSI TR-03183-2 in the version in force at the time of entering into the contract, hardware bills of materials (HBOM) and a detailed description of the structural dependencies. When changes or updates are made to the asset, the technical documentation must be reviewed, documented and made available as an updated version.

Configuration data refers to all data required to set up, customize and optimize software or hardware. It may include information used to set parameters and customize functions or to integrate the software or hardware into existing systems.

The SBOMs to be provided include a bill of materials listing all direct and transitive dependencies contained in the asset. This includes, among other things, a complete list of software libraries, firmware, drivers and BIOS. The same applies to the HBOMs to be supplied, provided that the information is available to the Contractor. Bills of materials are to be provided in CycloneDX format in a version that supports hardware components. The Contractor undertakes to provide the technical documentation via defined interfaces if requested by the Client.

For each version currently in use by the Client, the Contractor must be able to fully reproduce the software delivery artifacts so that changes can be made within a reasonable timeframe. The artifacts shall be provided upon request within 10 working days; recreating them shall suffice.

5.3 Authentication and identification

5.3.1 Passwords

All passwords used must meet the agreed complexity criteria and be centrally resettable. Password complexity, the ability to change the passwords and their period of validity must be technically secured, and the necessary processes for configuring and changing passwords must be documented. For IT/OT assets whose operation may be impaired by expiring authentication credentials, a procedure for timely renewal and a documented recovery process must be established to prevent the Client from being permanently locked out. Login credentials that are hard-coded in the source code, configuration files or firmware and cannot be changed by the Client are not permitted. The Contractor shall provide the Client with a complete list of default passwords. If the contract provides for the operation of IT/OT systems, the Contractor undertakes to change default passwords before the go-live.

5.3.2 Additional authentication options

For machine-to-machine authentication, a cryptographic authenticator should be used as the means of authentication.

When biometric methods are used, the authentication devices shall not allow more than five consecutive failed biometric login attempts. Once this threshold is reached, the account must be unlocked using a different means of authentication. Failed authentication attempts must be logged.

5.3.3 Storage of authentication information

Authentication information must be stored in encrypted form. This also applies to authentication information stored in configuration files, scripts, container images, program code, code repositories or log data. The associated keys must be managed separately and in accordance with the need-to-know principle. Exceptions to this rule, such as for existing products, must be defined in the contract.

5.4 Identity and privileged access management

The Contractor shall guarantee and document the management of identities for its IT/OT asset in conformity with the state of the art, unless otherwise agreed in the contract. A template may be provided, if necessary, to document the access authorization policy.

If the Contractor operates IT/OT assets on behalf of the Client, the following requirements shall apply: All natural persons and technical users shall be provided with a separate account for the duration of their work. Permissions shall be granted according to the principle of least privilege, and assigning excessive permissions to an individual user shall be avoided. Changes to permissions shall be logged. The account shall be deactivated upon termination of the work and deleted after a period to be agreed. Users created at the time of delivery must be documented. Upon request, the Contractor shall provide the Client with the identities, accounts, permissions and access methods relevant to the specific work, including their purpose, responsibility and period of validity.

Access to the IT/OT asset that bypasses identity and access management, for example through local standard accounts, (technical) shared accounts, generic service accounts, hard-coded passwords or uncontrolled remote maintenance access, must be technically prevented. If local emergency access (break-glass) is required for maintenance, troubleshooting or regulatory approval, this access must be limited to the operationally necessary minimum, documented, designed such that it is individually attributable, and approved by the Client. In the case of products purchased as a service, the Contractor shall, for the duration of the contract, maintain an identity management system that meets the requirements described here for use by the Client.

5.5 Management of information security incidents

The Contractor has established a process for handling information security incidents affecting the Client and for exchanging information with the Client via the Contractor's central contact person.

The initial assessment of an information security incident shall be carried out in the context of the notification by the Contractor within the agreed response times (see Section 5.1.1 "Availability"). The Contractor shall inform the Client of targeted cyberattacks as well as the potential impact on personal data and/or critical infrastructure-related services. Any updates to the assessment must be reported to the Client without undue delay. The Contractor shall keep the Client continuously informed of the status of the incident response.

To minimize the impact of information security incidents, the Contractor shall also take appropriate preventive and corrective measures within its area of responsibility.

The Client must be notified if the Contractor outsources the management of information security incidents to third parties.

5.6 IT/OT emergency management

Where the Contractor operates IT/OT assets, the Contractor is responsible for implementing IT/OT emergency management. Requirements in this regard, such as recovery times, are detailed in the statement of work.

5.7 Operational readiness of IT/OT assets

5.7.1 Security documentation

The Contractor shall document the security features of the IT/OT asset in such a way that the requirements of the Client can be verified. The documentation shall include information about

- Mechanisms to protect processed and stored data
- Archiving systems
- Components used (meaning the smallest exchangeable unit, including network components and third-party components) including unique serial numbers or identification features
- Data flows and the mechanisms that protect them
- Network diagrams
- Interfaces and the measures that protect them

In the event of changes to the asset, the Contractor shall keep the documentation up to date for the duration of the contract or of the period for which the Contractor has agreed to provide product support. This obligation shall apply to changes made by the Contractor or on its behalf; where changes are made by third parties, it shall apply only if the Contractor was notified of such changes and if the asset itself was unaltered in the process. The cybersecurity risk assessment is governed exclusively by the provisions of Section "5.1.3 Cybersecurity risk assessment."

5.7.2 Preparation for commissioning and hardening

If the contract provides for the delivery of an IT/OT asset, the Contractor shall guarantee that any components and functions that are not absolutely necessary for the fulfilment of the contractual tasks are deactivated or removed. A corresponding confirmation must be included with the asset handover. Installation principles, steps for hardening and protecting interfaces, configuration instructions, and tools and programs required for installation must be documented and made available to the Client.

Unneeded applications, services, accounts and functions should be deactivated on delivery and unused ports and interfaces blocked. Digital certificates needed to operate the asset and the management of these certificates shall be agreed with the Client. The use of self-signed certificates is prohibited; any exceptions shall require the Client's approval. Device identifiers assigned by the manufacturer (e.g. IEEE 802.1AR IDevID) must be disclosed.

In the case of independent commissioning and operation by the Client, the Contractor shall provide the Client, via secure means, with all administrator access credentials and the administrative documentation.

5.7.3 Safety-relevant systems/Safety

Prior to handover to the Client or the commissioning of safety-relevant systems, the Contractor shall ensure that

- The necessary validation and verification measures in accordance with EN50126 have been successfully completed
- The measures identified in the risk analysis have been completed
- Communication with the system is routed via a dedicated gateway and authorized there
- Remote access is properly configured, unauthorized control and covert remote channels are prevented, activities conducted via remote access are logged and remote access itself can be disabled, the system's safety-critical communication is segregated from other communication and protected from interference
- Workstations within the system are protected from remote access and do not endanger the system with third-party software
- Unauthorized components are excluded from use within the system
- Configuration mode must be enabled separately

5.7.4 Remote maintenance access

Remote maintenance access must be limited to the minimum operationally necessary, documented and approved by the Client.

Remote maintenance access must be encrypted, authenticated, authorized, logged and monitored. Use of the DB remote maintenance system shall be preferred; details are to be agreed between the Client and Contractor.

Remote access to OT assets relevant to safety or approval may only be enabled and used within the scope expressly permitted in the safety or approval documentation for the OT asset.

5.7.5 Protection against malware

The Contractor shall provide the Client with a solution for protecting the IT/OT asset against malware. If the Contractor operates the asset on behalf of the Client, the Contractor shall be responsible for its implementation in consultation with the Client.

Among other things, the solution shall include:

- Documentation on the installation, operation and updating of the protection solution
- Requirements for monitoring the operating status including up-to-dateness of definition files (signatures)
- Possible workarounds until an updated protection mechanism is provided
- Proof that the protection mechanism is working correctly
- Timeframe for the provision of updated definition files

5.7.6 Removable storage media in the OT

If the Contractor provides data for OT assets on removable storage media or operates an OT system on behalf of the Client, the following rules shall apply to the use of removable storage media:

- Only removable storage media approved for a defined and documented purpose may be used.
- Removable storage media must be encrypted. If encryption is not possible for operational reasons, alternative security measures to protect confidentiality and integrity must be defined, documented and implemented, such as secure transport and shipping routes.
- Removable storage devices must be scanned for malware before being connected to OT hardware.

5.7.7 IT/OT change management

If the Contractor operates an IT/OT asset, the change management process shall be coordinated with the Client and documented. The following rules shall apply:

- Changes must be planned and their impact on operations assessed and coordinated with the Client.
- All changes must be tested and approved before installation.
- In the case of changes to safety- or approval-relevant OT assets, verification of no interference is required, which must be approved by the safety officer.
- All changes to IT/OT assets must be documented and incorporated into configuration management.

5.7.8 Data backup and recovery

The Contractor shall provide the Client with a plan for data backup and recovery of the IT/OT asset. If the Contractor operates the system on behalf of the Client, the Contractor shall keep it up to date and be responsible for its implementation.

The plan shall include:

- Documentation of data backup and recovery mechanisms and procedures, including scope of backups and necessary configurations
- Proof of the correct functioning of data backup and recovery mechanisms
- Client-side requirements for the implementation of the plan
- Physical and cryptographic measures to protect the backups
- Parameters and configurations of IT/OT assets
- Schedules, including for the periodic deletion of data backups
- Framework for ensuring that data backup and regular operations do not interfere with one another
- Logging of backup and recovery activities and of the deletion of backups

5.7.9 Decommissioning

The Contractor shall provide the Client with a plan for the decommissioning of the IT/OT asset. This shall include, in particular, the necessary steps for the orderly decommissioning of the asset and for securely deleting the stored data, cryptographic material and device configurations.

5.7.10 Support with data return

In the case of application management or the provision of 'as-a-service' products by the Contractor, the Contractor shall guarantee the Client support in retrieving data and/or applications in the event that the contract is terminated. This support shall include, where requested by the Client, a suitably dimensioned technical interface to a system defined by the Client and the return of data in a portable, machine-processable format. Proprietary formats and proprietary encryption technologies are not permitted.

5.7.11 Disposal and transfer of IT/OT assets

If the Contractor disposes of IT or OT assets on behalf of the Client, the following rules shall apply:

- Storage media must be permanently erased before disposal or transfer.
- If erasure is not possible for technical reasons, the device must be physically destroyed.

5.7.12 Support for IT/OT assets over a defined time period

Manufacturer support for IT/OT assets must be ensured for at least the period specified in the description of the work or product. The Contractor shall notify the Client of end-of-service-life dates and consider replacement strategies from both a functional and technical perspective in the event of a foreseeable end of service life. It shall provide the Client with the relevant information regarding the affected assets.

5.8 **Cryptographic measures**

5.8.1 Cryptographic measures and list of materials

Information processed and stored in IT/OT assets must be protected by cryptographic methods using a risk-based approach. The Contractor shall ensure appropriate (e.g. in accordance with BSI TR) key and certificate management for all cryptographic keys, X.509 certificates and other secrets and tokens used in the IT/OT asset. Cryptographic keys and secrets shall not be stored in plain text, hard-coded or stored in unprotected form on the IT/OT asset.

The Contractor shall document the cryptographic measures in coordination with the Client. The documentation/cryptographic inventory shall include the following items:

- An architecture sketch (including existing interfaces),
- All cryptographic methods used (protocols, algorithms, parameters) for data at rest and data in transit
- The secret management used throughout the secret's lifecycle.

If available, the Contractor shall provide this information in the form of a cryptographic bill of materials (CBOM) in CycloneDX format. If the relevant IT/OT asset does not use cryptography or secrets, this must also be documented.

If cryptographic measures become insecure during the contract period (e.g. in the view of recognized expert bodies, such as the German Federal Office for Information Security), the Contractor shall notify the Client without delay and coordinate the process for replacing this measure.

5.8.2 Verification of certificate validity

IT/OT assets that use X.509 certificates must verify the validity of the certificates in accordance with RFC 5280, including updates. In particular, revocation information in the form of certificate revocation lists (CRLs) or the Online Certificate Status Protocol (OCSP) must be checked if available.

The application's behavior when revocation information is missing or certificates are revoked must be considered when designing the system and documented.

5.9 **Logging and monitoring**

5.9.1 Integration with security monitoring

For IT/OT assets located within an IT/OT network infrastructure managed by the DB Group, such as control and data transmission networks, the Contractor shall assist the Client with integration into the Client's security monitoring system/intrusion detection system. Details shall be set out in the statement of work. In addition, the Contractor shall recommend tools for security analysis and indicate any adverse effects of certain tools.

If the Contractor operates IT or OT assets within its own network on behalf of the Client, it shall guarantee logging and monitoring of such assets according to the state of the art.

5.9.2 Reference time

The Contractor's IT/OT assets shall use a generally accepted time source that is synchronized with the DB reference time source. The Contractor shall specify this in the documentation and agree it with the Client if requested.

5.10 **Network security**

5.10.1 Network architecture and operation

If the statement of work provides for the integration of the IT/OT assets supplied by the Contractor into the DB Group's network infrastructure, the necessary details shall be agreed between the contracting parties.
For IT/OT assets developed specifically for the Client, the Contractor shall guarantee that the network layout, including the use of network components with security features or equivalent mechanisms, has

been implemented in accordance with the design approved by the Client. This includes wireless networks. The network infrastructure must be documented in the form of a network diagram. Communication links between networks must be documented and approved by the Client.

Networks operated by the Contractor shall be continuously monitored according to the state of the art. The use of unauthorized device addresses must be prevented by appropriate measures. Administration networks must be technically segregated. Network administration must be conducted via an encrypted connection.

If the Contractor operates IT/OT assets on behalf of the Client in its own or third-party network environments, or other network environments for which it is responsible, it shall guarantee the use of network security measures corresponding to the state of the art and agreed with the Client.

5.10.2 Connection

If the Contractor operates IT/OT assets on behalf of the Client or provides an 'as-a-service' product, it shall guarantee that the connection between its data center/network and the DB Group's network infrastructure offers sufficient performance, redundancy and security. If there is a network interconnector or interface with the Contractor's services, the bandwidth (min/max) must be agreed with the Client in an SLA, and the technical transfer point must be named. If the connection is made via the Internet, the bandwidth of the Internet connection must be sufficient.

If a network connection is primarily wireless (e.g. mobile communications, microwave transmission), the Contractor is obliged, prior to commissioning, to agree with the Client to what extent the service can be accessed via alternative connections (e.g. wired or via alternative service providers) in the event of a loss of availability in order to maintain the Client's business processes while complying with information security requirements.

5.10.3 Web application firewall

Internet-facing web applications operated by the Contractor on behalf of the Client must be secured with a state-of-the-art web application firewall. Equivalent protective measures must be implemented for non-web-based Internet-facing interfaces.

5.10.4 Hardening and physical protection of network devices

Network devices must be configured securely. This must include at least the following aspects:

- Software/firmware version
- Access control
- Services and interfaces (especially approach to serial interfaces)

Network devices must be physically protected from unauthorized access, tampering, theft, damage and environmental threats.

5.11 **Patch and vulnerability management**

5.11.1 Provision of security patches

If the contract provides for the delivery or operation of IT/OT assets – including as part of a service – the Contractor shall guarantee, during the contractually specified period in which it provides support for the IT/OT asset, to close security vulnerabilities using patches. It must be possible to install patches without altering core functionality or compromising protection goals. The Contractor shall guarantee that any patches installed are developed, tested and released according to the state of the art, that they can be revoked in the event of production problems, and that changes are recorded and documented by the system. The patch frequency shall be based on the state of the art. When the asset is operated by the Contractor on the Client's network, the Contractor shall provide an evaluation of the patches and a timetable for their deployment.

The patch documentation shall include the necessary prerequisites and installation steps, such as version dependencies and any potential performance issues.

For patches that cannot be installed for operational reasons, the Contractor shall prepare instructions for workarounds and, if necessary, further mitigation measures in coordination with the Client. If necessary, the Client and Contractor shall coordinate immediate measures to minimize risk.

The integrity of security patches and updates must be verifiable by a cryptographic mechanism.

5.11.2 Patch management

When operating an IT/OT asset in the DB Group's network, the Contractor undertakes, during the contract period, to control and monitor all changes to hardware and software versions or configurations in coordination with the Client via the latter's patch management. Changes shall be recorded in configuration management.

Deadlines for the installation of the patches (by Client or third party, e.g. manufacturer) must be verifiably adhered to, and transparency must be maintained with respect to the installation status of all applicable patches. The system's hardened state must be restored and guaranteed after the patches have been installed.

5.11.3 Vulnerability assessment

The Contractor shall use methods corresponding to the state of the art to continuously check its IT/OT assets for vulnerabilities throughout their defined lifecycle, for example by comparing them against security advisories and using vulnerability scanners, web application scans and penetration tests.

The frequency and intensity of vulnerability assessments are determined by the Client and the Contractor when the contract is concluded. In the absence of such an agreement, these activities shall be based on the state of the art.

5.11.4 Notification of vulnerabilities

If IT/OT assets provided or operated by the Contractor are affected by vulnerabilities, the Contractor shall be obliged to report them to the Client securely and without undue delay. The results shall be classified using the latest version of the Common Vulnerability Scoring System (CVSS).

The notification should contain the following elements in particular:

- Precise description of the asset (if applicable, details regarding the design, subsystem, component, manufacturer's name, release, product and/or batch number of the software, firmware, driver, BIOS and hardware provided)
- CVSS Base Score
- Detailed description of the vulnerability, including its exploitability
- Time of initial detection, detection method
- Initial evaluation from the Contractor's point of view and recommendation of specific countermeasures for dealing with the vulnerabilities, taking into account any relevant requirements for security-related approval and release
- Number and documented installation locations (stating the technical system including room and cabinet location) of the affected assets, provided that the Contractor has this information and, particularly for 'as-a-service' products, that the information is relevant

The obligation to notify also includes follow-up notifications if a vulnerability cannot be resolved within the agreed timeframe.

5.11.5 Security advisories

If possible, security advisories should be published in a machine-readable form (in Common Security Advisory Framework (CSAF) or CycloneDX format as agreed with the Client).

5.11.6 Managing vulnerabilities

The technical vulnerabilities identified in IT assets must be addressed within the following timeframes, based on their CVSS Base Score:

- CVSS Base Score 9 or higher; timeframe: 48 hours in digital access zone 6, otherwise 14 calendar days

- CVSS Base Score 7 to <9; timeframe: 48 hours in digital access zone 6, otherwise 14 calendar days
- CVSS Base Score 4 to <7; timeframe: 30 calendar days
- CVSS Base Score >0 to <4; timeframe: 90 calendar days
- CVSS Base Score = 0; no timeframe

The technical vulnerabilities identified in OT assets must be addressed within the following timeframes, based on their CVSS Base Score (where they differ, timeframes for OT assets relevant to critical infrastructure, safety and approval are shown in brackets):

- CVSS Base Score 9 or higher
    - Digital access zone 6: timeframe: 48 hours
    - Digital access zone 5: timeframe: 14 calendar days
    - Digital access zones 1–4: timeframe: 30 calendar days (14 calendar days)
- CVSS Base Score 7 to <9
    - Digital access zone 6: timeframe: 48 hours
    - Digital access zone 5: timeframe: 14 calendar days
    - Digital access zones 1–4: timeframe: 90 calendar days (14 calendar days)
- CVSS Base Score 4 to <7
    - Digital access zones 5-6: timeframe: 30 calendar days
    - Digital access zones 1-4: timeframe: within the regular patch cycles, no longer than 6 months (30 calendar days)
- CVSS Base Score >0 to <4
    - Digital access zones 5-6: timeframe: 90 calendar days
    - Digital access zones 1-4: timeframe: within the regular patch cycles, no longer than 12 months (90 calendar days)
- CVSS Base Score = 0; no timeframe

The applicable digital access zone will be specified in the contract. When determining the vulnerability management timeframes for OT assets relevant to safety and approval, the requirements of the safety management system (e.g., absence of feedback/interference, etc.) must also be taken into account.

The deadlines for managing vulnerabilities begin upon publication as a CVE or in accordance with a comparable industry standard. At least one risk-mitigation measure must be implemented within the specified timeframe; in this case, the final remediation shall adhere to a schedule agreed with the Client.

5.12 **Conducting penetration tests**

If the Contractor operates IT/OT assets or provides 'as-a-service' products for the Client, the Contractor shall conduct penetration tests in accordance with the following criteria.

- Annually for IT/OT assets relevant to critical infrastructure or IT/OT assets requiring a very high level of protection
- On an ad hoc basis following a cyberattack or critical IS incident
- Prior to commissioning or go-live of significant changes
- After addressing vulnerabilities with a CVSS score greater than 7 in Internet-facing IT/OT assets, if requested by the Client

The Contractor and Client shall agree on the scope, timing and methodology of the tests prior to their implementation; this shall also apply to other active security analyses (e.g. network scans) of IT/OT assets on the Client's network. For OT assets related to rolling stock, the tests may be conducted using a representative test rig, laboratory setup, or reference vehicle.

The Contractor shall provide the Client with the test reports, including the corrective action plan.

The Client may require that the penetration tests be conducted by the Client itself or by a third party engaged by the Client. The Contractor may propose the same; in this case, performance of the tests by the Client shall be subject to the Client's written consent. In both cases, the Client shall bear the cost of conducting the tests.

The Contractor shall facilitate the tests by providing the necessary access credentials, accounts, test environments and documentation within a reasonable timeframe to be agreed on a case-by-case basis, and by obtaining the necessary authorizations from all third parties involved, in particular its subcontractors and service providers. The Contractor shall bear the costs associated with the cooperation required of it. If the Contractor is unable to provide the necessary permissions, the Contractor shall remain obligated to conduct the tests itself and provide the test reports.

Regardless of who conducted the tests, the Contractor shall submit a corrective action plan based on the findings. Section 5.11.6 shall apply to the management of identified vulnerabilities; the Contractor shall bear the costs of remediation.

5.13 **Public key infrastructure**

5.13.1 Documentation of public key infrastructure

If the Contractor operates a public key infrastructure (PKI) on the Client's network, this must be documented in accordance with RFC 3647. The permitted use of the certificates shall be limited to the business purposes of the Client. Only certificates from PKIs approved by the Client may be used. Publicly trusted certificate authorities and manufacturer-specific device PKIs (e.g. for IEEE 802.1AR IDevID) shall be considered to have been approved, provided they are disclosed to the Client.

5.13.2 Monitoring availability of revocation information

The validity and availability of certificate revocation lists shall be monitored, and revocation information shall be made available on an ongoing basis.

If a private key is compromised, all certificate holders and relying parties shall be notified, and the corresponding CA certificate shall be revoked immediately.

5.14 **Requirements for secure development**

5.14.1 Development and testing

If the Contractor performs development work specifically for the Client, it shall conduct development and testing within the framework of a Secure Software Development Life Cycle (SSDLC) and in consultation with the Client. The Client reserves the right to inspect the test logs.

The SSDLC must include rules on the following topics, among others:

- Use of secure development software and a source code management system
- Design principles for secure development
- Data validation at interfaces, including inputs and outputs, data flows and metadata
- Testing plan, including test procedures, protection of test data and segregation of environments
- Handling of debug code (debug code may only be used in production systems after approval and review by the Client)
- Scope of documentation, including software bill of materials (SBOM)
- Performing dependency analyses.

5.14.2 Handling third-party components

The Contractor shall ensure that all third-party components used in the IT/OT asset are checked for exploitable known vulnerabilities prior to commissioning and are secured in accordance with the state of the art. This shall apply to all libraries, modules, assemblies and binaries.

Known exploitable vulnerabilities in components from the (software) supply chain must be remediated before commissioning or addressed using mitigating measures approved by the Client. The Contractor shall also ensure that vulnerabilities in third-party components are continuously monitored, assessed and addressed even after the system goes live.

5.14.3 Secure storage of release artifacts

All release artifacts in software development must be managed and versioned consistently. This also includes third-party binary files that are a functional component of the software solution. The integrity of release artifacts should be guaranteed through appropriate cryptographic mechanisms.

5.14.4 Depositing code

If requested by the Client, the Contractor shall deposit the complete source code for each version currently in use by the Client with a recognized depository. The depository may be replaced by an equivalent procedure agreed with the Client, provided this grants the Client the same access to the source code and the associated artifacts when necessary. The costs of the chosen procedure shall be agreed between the parties.

5.14.5 No undesirable functions or components

The Contractor shall guarantee that the IT/OT assets it delivers do not have any undesirable functions that endanger the integrity, confidentiality or availability of software, hardware or data or adversely affect the confidentiality or security interests of the Client, e.g. malware, backdoors or functions for manipulating data or processing logic.

5.15 **Physical security**

The Contractor shall take reasonable precautions to ensure the physical security of its assets and/or infrastructure. This shall particularly include implementing measures for:

- Protection against loss and tampering
- Protection against fire and water
- Protection against burglary and vandalism
- Protection against or avoidance of extreme temperatures
- Adequate power supply

The Contractor shall guarantee that access to areas containing information or systems is restricted to the authorized group of persons. This includes, for example, access protection measures for data centers, including monitoring of critical areas, access logs and protection against burglary.