Annex 6 to the Supplementary Contractual Terms for Information Security
Standard software

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:

- Standard software without DB-specific customizations

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 – not applicable –

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.

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 – not applicable –

5.6 – not applicable –

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 – not applicable –

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 – not applicable –

5.7.7 – not applicable –

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 – not applicable –

5.7.10 – not applicable –

5.7.11 – not applicable –

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 agrees to notify the Client of end-of-service-life dates.

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 – not applicable –

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 – not applicable –

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 – not applicable –

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 applicable digital access zone will be specified in the contract.

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 – not applicable –

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 – not applicable –

5.14 Requirements for secure development

5.14.1 – not applicable –

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 – not applicable –

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 – not applicable –