Annex 7 to the Supplementary Contractual Terms for Information Security
Functionally equivalent spare parts

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:

- Functionally equivalent spare parts (form, fit, function)

For the purposes of this Annex, a spare part is an IT/OT asset that replaces (form, fit, function) an IT/OT asset currently in operation with the Client in the same installation configuration, without expanding its purpose or functionality and without adversely altering its information security-related characteristics.

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 – not applicable –

5.2 – not applicable –

5.3 – not applicable –

5.4 – not applicable –

5.5 – not applicable –

5.6 – not applicable –

5.7 Operational readiness of IT/OT assets

5.7.1 Security documentation

The Contractor shall provide the Client with the security documentation for the IT/OT asset where available. 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.

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 – not applicable –

5.7.4 – not applicable –

5.7.5 – not applicable –

5.7.6 – not applicable –

5.7.7 – not applicable –

5.7.8 – not applicable –

5.7.9 – not applicable –

5.7.10 – not applicable –

5.7.11 – not applicable –

5.7.12 – not applicable –

5.8 – not applicable –

5.9 – not applicable –

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 – not applicable –

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 – not applicable –

5.11.6 Managing vulnerabilities

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 – not applicable –

5.13 – not applicable –

5.14 **Requirements for secure development**

5.14.1 – not applicable –

5.14.2 – not applicable –

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 – not applicable –

5.15 – not applicable –