Annex 2 to the Supplementary Contractual Terms for Information Security
SaaS, PaaS, cloud services, data center operations

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:

- Procuring 'as-a-service' products and cloud services
- Data center operations

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 – not applicable –

5.2 – not applicable –

5.3 Authentication and identification

5.3.1 – not applicable –

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 – 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 – not applicable –

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 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 – not applicable –

5.7.12 – not applicable –

5.8 – not applicable –

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 Network security

5.10.1 – not applicable –

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 – not applicable –

5.10.4 – 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.

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 – not applicable –

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 **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 – not applicable –

5.14 – not applicable –

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.