Annex 6 to the Supplementary Contractual Terms for Information Security
Standardised Software Systems

– Version dated November 1, 2024 –

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:

- Standardised Software Systems

5 Additional information security requirements

5.1 Availability

The following availability and response times shall apply to the contact persons, unless the Client and Contractor have expressly agreed otherwise in the contract.

	Protection requirement	
	Standard	High or very high
Normal communication		
Contractor's response time to Client request	8 hours (during business hours)	4 hours (during business hours)
Emergency communication		
Reporting of information security incidents and vulnerabilities	Without undue delay	Without undue delay
Response time for Contractor's central POC	4 hours within business hours (9 am - 5 pm)	1 hour within extended business hours pursuant to SLA

Table 1: Response times

5.2 - not applicable -

5.3 - not applicable -

5.4 **Security documentation**

The Contractor shall document the security features of the IT/OT product in such a way that the requirements of the Client (e.g. due to the need for protection) can be verified. The documentation shall include information about:

- Mechanisms implemented 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 plans and interfaces
- Information on access options (including wireless, open ports) and the measures protecting them

In the event of changes to the product, the Contractor shall keep the documentation up to date.

For OT products, the Contractor shall prepare a risk analysis in accordance with IEC62443 and keep it up-to-date throughout the term of the contract or until the end of the warranty period (unless otherwise contractually agreed; whichever is the later date shall apply). If this results in the need for work on the product, the Client and Contractor shall agree on the framework and costs for this work.

The Contractor shall have the risk analysis verified by an independent third party if requested. The Client shall bear the associated costs.

5.5 **No undesirable functions**

The Contractor shall guarantee that the IT/OT products it delivers or operates for the Client 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. backdoors or functions for manipulating data or processing logic.

5.6 - not applicable -

5.7 - not applicable -

5.8 **Cryptography**

Information processed and stored in the IT/OT product, particularly access and configuration data, must be protected by cryptographic methods in consultation with the Client. The Contractor shall document these in coordination with the Client. The Contractor shall guarantee that the cryptographic methods and encryption key management measures used conform to the state of the art.

5.9 - not applicable -

5.10 **Provision of security patches**

If the contract provides for the delivery or operation of IT/OT products – including as part of a service – the Contractor guarantees that security gaps shall be closed by means of patches during the product lifecycle specified by the Contractor. The Contractor shall deliver or operate a patchable IT/OT system so that changes can be made subsequently without changing basic functionalities or jeopardizing 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 product is operated on the Client's network, the Contractor shall provide an evaluation of the patches and a timetable for their deployment. If possible, security advisories should be published in a machine-readable form (in Common Security Advisory Framework (CSAF) or Cyclone DX format as agreed with the Client).
The documentation of the patches shall include the effects of the patch on the operational risk situation as well as the requirements and steps for installation, e.g. version dependencies and possible performance impacts.
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.
The integrity of security patches and updates must be verifiable by a cryptographic mechanism.

5.11 - not applicable -

5.12 **Preparation for commissioning/hardening**

If the contract provides for the delivery of IT/OT products, the Contractor shall guarantee, prior to the rollout, that they are free of components and functions that are not absolutely necessary for the fulfilment of the contractual tasks. The product or service handover must be accompanied by a corresponding confirmation. 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.
The Contractor shall provide the Client with all administrative accesses in the event of independent commissioning and operation of the systems. The documentation for administration must also be handed over.

Unneeded applications, services, accounts and functions should be deactivated on delivery and unused ports and interfaces blocked.
Certificates needed to operate the product and the management of these certificates shall be agreed with the Client. The use of self-signed certificates is prohibited.
Before delivery, the Contractor shall check that installation data carriers and any other required data carriers are free from malware and confirm this to the Client. Data carriers used for these purposes may not be used for any other purpose.

5.13 **Passwords**

Passwords embedded in the source code are not permitted. The Contractor shall provide the Client with a complete list of default passwords. These must be randomly generated. If the contract provides for the implementation of IT/OT systems, the Contractor undertakes to change default passwords before the go-live. All passwords used must meet agreed complexity criteria and be centrally resettable. Password complexity, the ability to change the passwords and their period of validity must be technically ensured and correspond to the state of the art.

5.14 **Identity management**

The Contractor shall guarantee and document the management of identities for its IT/OT product and the access to data and interfaces from that product in conformity with the state of the art, unless otherwise agreed in the contract. Users and rights shall be managed and documented in a central, integrated database.

If the Contractor operates IT/OT products or network components on behalf of the Client, the following requirements shall apply: All natural persons and technical users shall be provided with a separate user account for the duration of their work. 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 shall be documented in the database. Only the rights that are absolutely necessary shall be granted. The Contractor shall provide the Client with intelligence from its identity and access management (IAM) system concerning the specific service upon request. Access to the IT/OT product by circumventing the IAM must be technically impossible.

For remote maintenance access, the DB remote maintenance system shall be preferred; details are to be agreed between the Client and the Contractor.
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.

5.15 -deleted-

5.16 **Asset and configuration management**

The Contractor undertakes to provide the Client with complete configuration data, including all components (meaning the smallest exchangeable unit), libraries, firmware, bios and hardware used.

Each time an asset is changed, the Contractor must check and document the configuration and provide the updated version to the Client. The Contractor must at all times be able to identify each configuration element and to obtain all the necessary data for the configuration of this element in a complete and machine-readable form down to the source code level.

If available, the Contractor shall provide this information in the form of a software bill of materials (SBOM) in SPDX or Cyclone DX format (in consultation with the Client) or in the form of a hardware bill of materials (HBOM).

The Client may demand the transfer of ownership or deposit of the source code at a recognized depository.

5.17 **End of service life**

If the contract provides for the delivery of IT/OT products, the Contractor shall, in the event of a foreseeable end of service life, consider replacement strategies in both functional and technical terms and provide the Client with appropriate information about the assets concerned.

5.18 - not applicable -

5.19 - not applicable -

5.20 - not applicable -

5.21 **Vulnerability assessment**

The Contractor undertakes to continuously check its products and services for vulnerabilities during their defined lifecycle in order to be able to react to new vulnerabilities as quickly as possible.

The frequency, intensity and methods of the vulnerability assessment must be based on the Client's risk situation. The Client and the Contractor shall consult each other on a regular basis for this purpose. In the absence of such an agreement, the activities described shall based on the state of the art.

5.22 **Integration of vulnerability management and event management**

As far as IT/OT products that are located in a DB network infrastructure or that feed information into it are concerned, the Contractor shall help the Client integrate them into the Client's vulnerability management system and the Client's event management system.

For this purpose, security-relevant events shall be logged in the system, archived for possible investigation purposes and made available in an agreed format. Details (e.g. type of notifications, quantity, robustness) shall be defined in the statement of work.

In addition, the Contractor shall recommend tools for security analysis or indicate the adverse effects of certain tools.

5.23 **Notification of vulnerabilities**

If products provided by the Contractor or IT/OT products operated by the Contractor are affected by vulnerabilities, the Contractor shall be obliged to report them to the Client securely and without undue delay. Where possible, the results should be classified according to the Common Vulnerability Scoring System or on the basis of assessments by the German Federal Office for Information Security (BSI).

The notification should contain the following elements in particular:

- Precise description of the product (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)
- Detailed description of the vulnerability, including its exploitability
- 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 products, 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 period.

5.24 **Removal of vulnerabilities**

The timeframes for neutralizing vulnerabilities (e.g. by a workaround) and for the final solution of a given vulnerability are based on the current state of the art, unless otherwise agreed in the contract.

5.25 - not applicable -

5.26 - not applicable -

5.27 - not applicable -

5.28 - not applicable -

5.29 - not applicable -

5.30 - not applicable -

5.31 - not applicable -

❑