Annex 2 to the Supplementary Contractual Terms for Information Security
SaaS, PaaS, Cloud Services, Data Center Operations

– 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:

- 'as a Service' Products, Cloud Services
- Data Center Operations

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 applicabe -

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 **Connection**

If the Contractor operates IT/OT products for the Client or provides 'as-a-service' products, it shall guarantee a sufficiently high-performance, redundant and secure connection of its data center/network to the data center/network of DB AG and affiliated companies. If there is a network connection or interface with the Contractor's services, the bandwidth (min/max) must be agreed with the Client in an OLA/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.

5.8 **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 - not applicable -

5.11 - not applicable -

5.12 - not applicable -

5.13 - not applicable -

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 - not applicable -

5.17 - not applicable -

5.18 **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 upon termination of the contract. This support shall include, where appropriate, 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.

5.19 **Physical security**

The Contractor must take reasonable precautions to ensure the physical security of its assets and/or infrastructure.

This shall particularly include measures for:

- Protection against fire and water
- Protection against burglary and vandalism
- Protection against or avoidance of extreme temperatures
- Adequate energy 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, protection against burglary, etc.

5.20 **Handling of information security incidents**

The Contractor has established a system 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 5.1). Any follow-up activities shall be modeled by an incident response team at the Contractor's place of business. If these activities are outsourced by the Contractor, the Client shall be informed.

If the contract provides for the delivery of IT/OT products, the Contractor shall take preventive measures in its context to minimize the consequences of information security incidents. This includes, for example, ensuring that the IT/OT system is free of malware when it is put into operation.

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 **Reference time**

The Contractor's IT/OT products shall use a generally accepted time source. The Contractor shall specify this in the product documentation and agree it with the Client if requested.

5.27 **Interfaces**

Data received via data exchange and input interfaces must be automatically checked for plausibility and, if necessary, rejected. Details and, in particular, deviations from this shall be set out in the statement of work.

5.28 - not applicable -

5.29 - not applicable -

5.30 - not applicable -

5.31 - not applicable -

❑