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

- Edition January 01, 2021 -

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:

- Hosting
- SaaS, PaaS, cloud services, data center operation
- Outsourced operation of IT systems

5 Additional information security requirements

5.1 Availability

During the contract period, the following availability and response times for the availability of contact persons shall apply, unless the Client and Contractor have expressly agreed otherwise in the contract.

	Need for protection	
	Standard	High or very high
Normal communications		
Response time of contractor to request from client	8 hours (during business hours)	4 hours (during business hours)
Emergency communications		
Incident report	Without undue delay	Without undue delay
Response time for contractor's central POC	4h within business hours (9 am - 5 pm)	1h within extended business hours pursuant to SLA
Vulnerability report	72 hours	24 hours

Table 1: Response times

5.2 Not applicable

5.3 Transfer of responsibility

If the Contractor organizes the introduction of the product, it shall submit a proposal to the Client in text form in order to unequivocally regulate the transfer of operational responsibility between the Contractor and the Client.

5.4 Safety 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 includes information about data flows and security mechanisms, among other things.

5.5 Design principles

The Contractor shall ensure that the IT/OT products which it delivers or operates for the Client do not have any undesirable functions that endanger the integrity, confidentiality and availability of software, hardware or data and are contrary to the confidentiality or security interests of the Client, e.g. backdoors or functionalities for manipulating data or flow logic.

5.6 N/A

5.7 **Connection**

If the Contractor operates IT/OT products for the Client, it shall guarantee a sufficiently high-performance, redundant and secure connection of its computer center/network to the computer center/network of DB AG and its affiliated companies. If there is a network connection, the bandwidth (min/max) in an OLA/SLA must be agreed with the Client, 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 made primarily via air interface (e.g. mobile, directional radio), prior to commissioning, the Contractor is obliged to agree with the Client to what extent the service can be called up 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 in compliance with information security requirements.

5.8 **Cryptography**

If cryptographic procedures are used, the contractor shall document them in coordination with the Client in accordance with the specifications of the service description. The Contractor guarantees that the cryptographic software used conform to the agreed state of the art.

5.9 N/A

5.10 **Patchability**

If the contract provides for the delivery of IT/OT products, the Contractor guarantees that security gaps shall be closed during their lifecycle by means of patches. The Contractor shall deliver a patchable IT/OT system so that changes can be made subsequently without changing basic functionalities. The Contractor guarantees that any patches installed are tested according to the current 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 rhythm is based on the current state of the art.

5.11 N/A

5.12 N/A

5.13 N/A

5.14 **Identity management**

If the Contractor operates IT/OT products on behalf of the Client, the Contractor shall guarantee the management of identities and access to data and interfaces in conformity to the current state of the art, unless otherwise agreed in the contract. All natural persons and technical users are provided with a separate user account. Only the rights that are absolutely necessary are granted. The Contractor shall provide the Client with intelligence from its identity and access management (IAM) system concerning the specific service upon request.

5.15 N/A

5.16 **Configuration data**

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

The Contractor undertakes to make this configuration data available to the Client upon request. If the Contractor operates assets in the Client's network, reporting configuration data to the Client's asset management is mandatory.

In the event that the Contractor provides neither maintenance nor operation, the Contractor undertakes to hand over to the Client the complete configuration of the versions/releases of the product and all components, libraries, firmware, bios as well as the hardware used at description level.

The Client can demand the transfer of ownership or deposit of the source code at a recognised depository; if the service to be rendered is a product, information about the object code and source code must be added to the hardware parts list of the product. Libraries and interfaces used must be listed in this information in particular.

5.17 N/A

5.18 **Support for data restitution**

In the event of operations management by the Contractor, the Contractor shall guarantee the Client support for 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. Proprietary formats and encryption technologies are not permitted.

5.19 **Physical security**

The Contractor must take reasonable precautions to ensure the physical security of its infrastructure.

In particular, measures for:

- Protection against fire and water,
- Protection against or avoidance of extreme temperatures,
- must be implemented with an adequate energy supply.

The Contractor guarantees that access to areas with information or systems is restricted to the authorised group of persons.
This also includes access protection measures for data centers, including monitoring critical areas, access logs, protection against burglary, etc.

5.20 **Handling security incidents**

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 security incidents (e.g. IDS, IPS, SIEM). The Contractor has established a system for handling security incidents affecting the Client and for exchanging information with the Client via the Contractor's central contact person. The initial assessment of a 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 must be modeled by an Incident Response Team at the Contractor's place of busines. If these activities are outsourced by the Contractor, the Client must be informed.

5.21 **Vulnerability assessment**

The Contractor undertakes to continuously check its products and services for vulnerabilities during the contract period in order to be able to react to new vulnerabilities as quickly as possible.
The frequency and intensity of the vulnerability assessment must be based on the Client's risk situation. For this purpose, the Client and the Contractor reach agreements on a regular basis.

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.
In addition, the Contractor shall recommend tools for safety 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 of an initial analysis should be classified according to the Common Vulnerability Scoring System or on the basis of assessments by the Federal Office for Information Security.

The notification should contain the following elements:

- 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.

5.24 **Removal of vulnerabilities**

The times 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.

❑