



**Annex 1 to the Supplementary Contractual Terms for Information Security
“Software Procurement
and
Software Development Services”**

- 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:

- Software procurement
- Software development services

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		
Notification of security incidents	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 Contact person after production rollout

In the case of custom developed IT/OT products that are managed by the Client at the company, the agreed availability and response times of the contact persons must be upheld for at least 3 months after the rollout, unless the contract stipulates otherwise. Appropriate availability and response times must be guaranteed for the remainder of the expected lifecycle.

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 **Network architecture and operation**
The Contractor guarantees that the physical network layout used by the IT/OT product specifically developed for the Client, including the use of network components with IT security properties or equivalent mechanisms, has been implemented in accordance with the design approved by the Client. Networks operated by the Client are to be continuously monitored according to the current state of the art.
- 5.7 N/A
- 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 **Development and test**
If the Contractor carries out development services for the client, it shall plan development and tests in coordination with the Client and according to the current state of the art. For DB-specific developments, the Client reserves the right to inspect the test protocols.
- 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 **Patch management**
When operating an IT/OT product in DB's network, during the contract period, the Contractor undertakes to control and monitor all changes to hardware and software inventories or configurations in coordination with the Client via the latter's patch management and to record changes in configuration management and accesses to patching in identity and access management.
- 5.12 **Preparation for commissioning**
If the contract provides for the delivery of IT/OT products, prior to the rollout, the Contractor shall guarantee 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. The installation principles must be documented and transmitted 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.
- 5.13 **Standard passwords**
Passwords embedded deep in the source code are not permitted. The Contractor shall provide the Client with a complete list of standard passwords. If the contract provides for the implementation of IT/OT systems, the Contractor undertakes to change standard passwords before going live.
- 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 **Configuration management**

In the case of DB-specific developments, the Contractor shall coordinate configuration management with the architecture specifications from the Client's service description, define the necessary configuration standards in agreement with the Client in the project initiation phase and provide the Client with the necessary information for its asset management. The Client and Contractor shall agree on the necessary format together.

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 **End of service life**

If the contract provides for the delivery of IT/OT products, the Contractor undertakes to consider replacement strategies in the event of a foreseeable end of service life already during product creation and development, both professionally and technically, and to provide the Client with appropriate information about the assets concerned.

5.18 N/A

5.19 N/A

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. This includes, for example, ensuring that the IT/OT system is free of malware when it is put into operation. In addition, 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 5.2). Any follow-up activities must be modeled by an Incident Response Team at the Contractor's place of business. 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 these products 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.

