Supplementary Contract Terms and Conditions of Deutsche Bahn AG (DB AG) and its Affiliated Companies on Information Security Requirements (Supplementary Contract Terms for Information Security)

– Version dated November 1, 2024 –

1. Preamble

1.1 The Contractor supplies the Client with services supported by information technology and IT (information technology) or OT (operational technology) products that are specified in more detail in the contract.

1.2 These supplementary contractual terms additionally regulate information security requirements that must be met by the Contractor.

1.3 The information and applications covered by the contract are subject to a defined security requirement (normal, high, very high), and, where applicable, special legal requirements (e.g., legislation on critical infrastructures), on which the specific form of the information security measures is based. The protection category itself, as well as details regarding measures, are described in the statement of work.

1.4 Insofar as an audit (pursuant to Item 3.2, Audits) cannot be demonstrably carried out as planned by the Client for reasons relating to professional law, the Contractor shall inform the Client of these reasons in a timely manner. The parties shall then agree on a modified audit plan. Both the professional law applicable to the Contractor and the interests of the Client shall be taken into account in the process.

1.5 Unless expressly agreed otherwise, any expenses incurred by the Contractor as a result of the implementation of the following requirements shall be covered by the agreed remuneration.

1.6 If the Contractor violates the obligations under Items 2.2a), 2.5, 2.9 and 3.1 of these Supplementary Contract Terms, it shall, for each violation, pay a contractual penalty to the Client amounting to 2% of remuneration owed under the respective (individual) contract, unless the Contractor is not responsible for such violation. This contractual penalty shall not affect the rights of the Client to claim damages for such breach of duty. However, in this case, the contractual penalty shall be offset against any such claims for damages.

Any contractual penalties incurred on the basis of these Supplementary Contract Terms for Information Security shall amount to no more than 5% of the remuneration owed under the respective (individual) contract.

2. Information security requirements

2.1 Information security management

The Contractor has established suitable processes in its company to guarantee information security within the scope of the provision of services and shall maintain this system throughout the entire term of the contract. For example, this shall be done in the form of an appropriate information security management system (ISMS) or equivalent, suitable processes for guaranteeing information security in the context of service provision. The Contractor's information security processes shall, at a minimum, meet the information security requirements stipulated below and shall be based on DIN EN ISO/IEC 27001/27002 or an equivalent requirement in the respective valid version.

2.2 Roles and contacts

a) Information security coordinator

When signing the contract, the Contractor must provide the Client with the name of a competent contact person for all aspects relating to information security (e.g., information security officer, IT security manager or chief information security officer (CISO)), who is able and authorized to provide the Client with information on all matters relating to the management of information security.

b) Contact person for regular communication

The Client may require the Contractor to designate further contact persons or role managers in all matters relevant to information security in the context of the commissioned service (e.g., functional, technical, or operational managers) and to clarify unambiguously the distribution of tasks and transfer of responsibility. The Contractor shall notify the Client of any changes without undue delay.

c) Contact person for emergency coordination

The Contractor shall designate a central contact person (SPOC, single point of contact) for emergency communications, who shall be available to the Client for the periods specified in the contract. In case of an emergency, the SPOC has access to all necessary data of the Contractor (e.g., product monitoring, identity access management (IAM) and configuration data) and provides it to the Client and its emergency team on request and in a suitable format (readable and processable).

2.3 Security verification

The Client reserves the right to demand that the Contractor carry out a security verification in accordance with the provisions of the Federal Office for Information Security on the specification of requirements on measures in accordance with Section 8a (1) of the German IT Security Act (BSIG) ("*Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen*") for employees or other persons deployed by the Contractor (including subcontractors' staff) as part of its service provision who come into contact with information or systems in critical infrastructure categorized as particularly sensitive within the meaning of the Ordinance on the Determination of Critical Infrastructures pursuant to the German decree on the Federal Office for Information Security (BSI-KritisV). The Contractor shall confirm to the Client in writing that the security review has been successfully carried out.

2.4 Status report

The Contractor shall provide the Client with a status report on the information security of the purchased service upon request. The report shall contain details such as: information on deviations from agreed information security requirements and the associated corrective measures, historical statistics on information security incidents and security patches, status of vulnerability management and audit results, availability of security controls, efforts to remedy incidents and invoicing if security measures have been agreed separately. The Client and Contractor shall bindingly agree in writing on the form, content and frequency within eight weeks after signing of the contract and, in any case, no later than the start of operations, or delivery of the product and shall be guided by DIN EN ISO/IEC 27001 in doing so. A sample report can be provided upon request.

2.5 Qualified staff

The Contractor shall ensure that the personnel it employs has the necessary qualifications and awareness of the requirements for information security and shall prove this to the Client on request.

2.6 Obligation of subcontractors

The Contractor shall warrant that its subcontractors and their subcontractors employed in relation to this contractual relationship shall comply with the requirements of this contract, with ISO27001 or with those of a comparable standard. The Contractor shall provide appropriate evidence if the Client requests this.

2.7 Data processing

Should the Contractor process or store data belonging to the Client or its affiliated companies ("Affiliated Enterprises") pursuant to Sections 15 et seq. of the German Stock Corporation Act (AktG), the Contractor undertakes to observe and comply with both regulatory and legal requirements (valid in the legal area of the Client) as well as the requirements of the statement of work, specifically the provisions on backing up data.

2.8 Encryption

The Contractor guarantees that data categorized as "DB confidential" or "DB strictly confidential" shall be encrypted for transmission and storage in conformity with the state of the art. Should cryptographic measures become insecure during the contract period, they shall be replaced as agreed between the contracting parties. The Contractor and the Client shall come to a mutual agreement regarding the assumption of costs for this.

2.9 Jurisdictions for hosting and storage

The Contractor agrees to name all the countries in which the Client's data is hosted or stored or in which application systems are operated and to confirm existing requirements listed in the statement of work (e.g., as part of the bid). Should data be stored outside of the Client's systems, the Contractor shall be informed separately of this fact.
The Contractor gives its assurance that the data shall not leave the named storage locations. Relocations within the EU are excepted from this but must be communicated to the Client in writing without undue delay.

2.10 Deletion of data

The Contractor guarantees that it shall delete and destroy all data relating to the contractual relationship at all locations of the Contractor and its subcontractors in a permanent manner without undue delay upon termination of the contract such that this data cannot be restored. Exceptions shall exist only for data only to the extent and for the period in which (a) the Contractor is legally obliged to store this data or (b) where necessary for the administrative processing of the contract, or (c) where such storage has been contractually regulated. The Contractor shall provide evidence of this at the request of the Client. The Contractor shall have no right of retention of the data.

2.11 Mobile devices

If the Contractor uses its own terminal devices to provide the agreed service, the Contractor undertakes to comply with the following specifications of the Client. For the purposes of this provision, "mobile device" shall mean any asset of the Contractor that is connected to the Client's IT/OT applications or IT/OT infrastructure (wired or wireless) or is used for processing the Client's data.

- Only mobile devices that are actively managed by the Contractor may be used.
- Efforts shall be made to secure the devices using multifactor authentication should this not be bindingly specified in the statement of work.
- The mobile devices must be protected according to the state of the art. Upon request, the Contractor shall provide evidence of such security measures and shall update these as needed.
- The Contractor shall report the loss of a mobile device to the responsible managers on the Client's side without undue delay and to deactivate and block it without undue delay.
- The use of hacking tools, sniffer software, etc. is prohibited unless expressly permitted.
- The Contractor is responsible for ensuring that the data networks of the Client and its Affiliated Enterprises are not connected to other data networks.

Any deviations to this due to technical requirements shall be coordinated with the Client in writing.

2.12 Reporting information security incidents

The Contractor undertakes to inform the Client of all information security incidents or breaches of data protection pursuant to Art. 33 GDPR that occur in the environment of the Contractor or one of its subcontractors and that impact its direct or indirect provision of services. If an information security incident is relevant for the data and systems of the Client and its Affiliated Enterprises, the notification shall be made without undue delay

At minimum, notifications must include the following content:

- Time at which the incident occurred and when it was detected,
- components affected,
- measures taken,
- an initial assessment of the severity/criticality/legal relevance.

The content of the notification specified in the contract shall be agreed in writing by mutual consent within eight weeks after signing of the contract.

Notifications shall be sent to the contacts specified in the contract, or alternatively to the following e-mail addresses:

- DB InfraGO Fahrweg: soc-dbn@deutschebahn.com
- DB InfraGO Personenbahnhöfe: infosec.db.personenbahnhoefe@deutschebahn.com
- DB Energie: DB.Energie.SOC@deutschebahn.com
- DB AG, other business units: security-issues@deutschebahn.com

Information security incidents that do not affect the Client's data or systems or those of its Affiliated Enterprises may be voluntarily disclosed to the Client as part of the regular status report.

2.13 Restoring a secure state

In the event of an information security incident of relevance to the Client and its Affiliated Enterprises, the Contractor shall, in addition to informing the Client, take all necessary measures to restore the necessary security without undue delay. If a concerted procedure with the Client is necessary for this, the Contractor shall contact the Client with a detailed catalog of measures and coordinate with the Client. Where the assistance of the Client's Affiliated Enterprises and/or third parties is necessary for processing measures, the Contractor shall grant them access to all necessary information, systems and business premises.

2.14 Access

Direct or covert access to the information systems (operational systems, networks, programs, datasets) of the Client and its Affiliated Enterprises shall be permitted to the Contractor only if it has received express access authorization from the Client and this authorization has been documented; such access authorization shall be restricted to the expressly approved and deployed employees of the Contractor or its subcontractors. Transfer of access authorization to third parties is forbidden. Any access authorization granted may be used only in the context of the contractually assumed services.

2.15 Operational safety

The Client reserves the right to monitor or block the Contractor's network access to the infrastructure of the Client and its Affiliated Enterprises due to government agency orders or in line with the conditions of use agreed with the Client. Also, it must be possible to suspend such access at any time if the devices of the Contractor that are connected to the network affect in any way the operating security or the operating behavior of the network or of other devices or software connected to the network. The above applies subject to differing provisions on the handling of personal data in the contractual relationship.

3. Assessment of the information security maturity level at the Contractor's site

3.1 Assessment of the security organization

The Contractor shall disclose to the Client intelligence from its security organization and, upon request, provide suitable evidence, on the basis of which the Client can perform an evaluation of the level of maturity of information security. This information may include, for example, a management summary of the security organization in the scope of application of the service, reports from an existing information security management system, a DIN EN ISO/IEC 27001 certificate including a detailed description of the scope and the Statement of Applicability (SoA) and the ISO/IEC 27001 assessment report or equivalent evidence, and current audit results in the scope of application of the service.

3.2 Audits

The Contractor agrees that the Client or another third party commissioned by the Client may audit the Contractor during the term of the contract with regard to its information security and compliance with data protection regulations. Information security audits are based on ISO27001 and the applicable current state of the art. The audits check the appropriate implementation of the agreed information security requirements and the effectiveness of the information security organization in relation to the order. Privacy audits are based on the GDPR and the German Federal Data Protection Act (BDSG).

a) Routine audits

Generally, at least two years shall elapse between routine audits. Audits shall be carried out during normal business hours. The duration of the on-site portion of the audit depends on the evidence provided and is estimated to be at least two working days. The Client shall provide at least six weeks' notice of routine audits.

The Contractor shall provide the necessary documents such as management reports, operational documents (configuration and authorization data), reports from the ISMS, etc. in a timely manner (generally three weeks or more before the date of the audit) and shall comply with its duties to cooperate for the purposes of the audit, e.g., granting the necessary access rights, providing documentation and access. The Client shall provide the Contractor with the results of the audit in the form of a report.

The Contractor undertakes to adapt the audit results marked as critical in improvement projects and to report on its progress in regular communications. The Client and the Contractor shall mutually agree on the scope of and schedule for these improvement projects. The Client reserves the right to check the progress of the improvement measures on site. The aforementioned time frame for audits shall apply to the preparation of these checks.

b) Issue-based audits

Issue based audits shall be possible at short notice, depending on the severity of the issue triggering the audit or the urgency.

Furthermore, the Contractor agrees that the Client may conduct audits of the Contractor's information security and compliance with data privacy provisions on an ad hoc basis in the event of a serious information security incident. This provision is valid for the duration of the contract. The audit can be performed by the Client itself or by a third party tasked by it. The scope of issue-based audits includes implementation of the current state of the art by the Contractor. In the event of an audit by an external third party, the Client shall be entitled to all audit results relating to the contractually arranged service.

If an issue-based audit reveals instances of non-compliance with contractually arranged information security requirements and data privacy provisions on the part of the Contractor, these shall be promptly addressed in the Contractor's improvement projects in order to ensure future compliance.

The Client reserves the right to have the progress of the improvement measures checked on site.

c) Calculated required time and costs

The Client shall, as a rule, conduct information security audits on a standardized basis and largely as remote audits. The average required time for preparation and implementation of the audit by the Contractor is roughly two days. The Client will require an average of five days of the Contractor's time for on-site audits. This amount does not include the time required for the provision of the ISMS documentation to be examined.

No general indications can be given with regard to the time required for non-standardized audits (e.g., issue-based audits).

The costs incurred by the Client for a routine audit shall be borne by the Client. The costs incurred by the Client for an issue-based audit shall be borne by the Contractor.

K Services in the context of important and especially important entities/critical infrastructure

The following requirements apply to contracts from which call orders can be made by the following Group companies or which are concluded directly with such Group companies:

Important and especially important entities

- Deutsche Bahn AG
- DB Bahnbau Gruppe GmbH
- DB Dialog GmbH
- DB Fahrwegdienste GmbH
- DB Fahrzeuginstandhaltung GmbH
- DB Kommunikationstechnik GmbH
- DB RegioNetz Infrastruktur GmbH
- DB RegioNetz Verkehrs GmbH
- Deutsche Umschlaggesellschaft Schiene - Straße (DUSS) mbH
- MegaHub Lehrte Betreibergesellschaft mbH
- Mitteldeutsche Eisenbahn GmbH
- RBH Logistics GmbH
- Regionalverkehre Start Deutschland GmbH
- UBB Usedomer Bäderbahn GmbH

Operators of critical facilities

- DB Cargo AG
- DB Energie GmbH
- DB Fernverkehr AG
- DB InfraGO AG
- DB Regio AG
- DB Systel GmbH
- DB Vertrieb GmbH
- S-Bahn Hamburg GmbH
- S-Bahn Berlin GmbH

K.1 Systems to detect attacks

The Client shall support the Contractor in carrying out integration into the Contractor's system to detect attacks for IT and OT product in the network infrastructure of DB Group companies classified as critical infrastructure or which transmits information into such infrastructure. This includes the provision of necessary information to implement logging, detection and response as well as evidence collection.

Specific implementation and, if applicable, distribution of tasks in cases in which the IT/OT product is operated by the Contractor, are described in the statement of work or are detailed in the context of the conclusion of the contract.

K.2 Audits

In deviation from Item 3.2c), audits in relation to critical infrastructure are usually carried on site. Should services not be provided solely be the Contractor, the audit may extend to include the entire supply chain. The Contractor must include in its contracts provisions to ensure the proper conditions for such an audit. More time may be required for audits in relation to critical infrastructure because the content of such audits is set by legal and official requirements. The provisions regarding costs set out in Item 3.2.c) remains unaffected by this.

K.3 Reporting and processing of security incidents

In addition to the provisions in Item 2.12, in the event of a major security incident, an initial report must be made to the Client without undue delay, but no later than 24 hours after the security incident is detected, and a detailed report including an impact analysis must be made within 72 hours at the latest.

If subcontractors and/or service providers are used, the Contractor shall ensure that it can nevertheless comply with the reporting deadlines specified.

As part of the handling of the security incident, the Contractor must ensure that staff members are suitably available to be contacted.

A major security incident is defined as follows: A security incident that causes or is likely to cause either serious operational disruption of services or financial loss to the DB company concerned or affects or may affect others by causing significant material or immaterial damage.

K.4 Support for risk management

If the Contractor supplies IT and OT products that are in DB Group network infrastructure or transmit information there, the Contractor shall support the Client in carrying out appropriate risk management. This includes, where applicable, the provision of information on the following topics:

- Concepts relating to risk analysis and security in information technology,
- Handling security incidents,
- Supply chain security, including security-related aspects of the relationship between the Contractor and service providers/suppliers contracted by the Contractor,
- Security measures in the development and maintenance of IT and OT systems, components and processes, including management and disclosure of vulnerabilities,
- Concepts and procedures for the use of cryptography and encryption,
- Use of multifactor authentication or continuous authentication solutions.

If the Contractor operates the IT or OT system on behalf of the Client, it shall also provide the Contractor with information on the following areas:

- Use of secured voice, video and text communications and, where applicable, secured emergency communication systems within the Contractor's entity,
- Concepts and procedures for assessing the effectiveness of risk management measures in the area of information technology security,
- Basic procedures in the area of cybersecurity hygiene and training in information technology security,
- Staff safety, approaches to access control and asset management.

The Contractor shall provide this information for the first time as part of the conclusion of the contract and shall keep it up to date during the term of the contract.

K.5 **Data backup/recovery**

The Contractor shall provide the Client with a plan for data backup and recovery (also in the event of a crisis) of the IT/OT system. If the Contractor operates the system on behalf of the Client, the Contractor shall be responsible for its implementation.

Among other things, the plan shall include:

- Documentation of data backup and recovery mechanisms and procedures, including necessary configurations,
- Proof of the correct functioning of data backup and recovery mechanisms,
- Contractor requirements for the implementation of the plan,
- Handling of removable media and cryptographic material (keys, hash values, ...),
- Parameters and configurations of IT/OT devices,
- Verification of data backup and recovery procedures,
- Timelines,
- Independence of data backup from normal operations,
- Logging of backup and recovery activities.

❑