Appendix J

Tender No. 42240

Timetabling & Track Possession System

Cyber

1. General

1.1 The reference scenario for a cyber attack on Israel Railways' systems as a result of a supply chain attack may materialize through highly diverse attack channels, such as infiltration into the systems of a supplier with a relatively low level of protection and from there into the company's systems; use of legitimate software updates to distribute malware, etc.

1.2 The reference scenario does not describe theoretical threats but is based on analysis relying on numerous incidents that have occurred in Israel and worldwide, whose essence was harming organizations through the exploitation of their supply chain.

1.3 The ongoing operations of Israel Railways involve many external suppliers that provide it with various services. As part of these services, such suppliers may generate and receive information from/for Israel Railways, provide infrastructures for storage and processing of the information, or obtain access to Israel Railways' network and its data.

1.4 Israel Railways' information assets are classified as public/internal/business-sensitive/personal-sensitive, and their leakage to unauthorized parties may cause a security risk or significant business, reputational, or legal harm to Israel Railways.

1.5 In order to minimize the risks of harming the confidentiality, integrity, and availability of information, the information assets must be protected, both when located on Israel Railways' network and when in the possession of suppliers or under their responsibility.

1.6 This document will specify information security guidelines and requirements for suppliers who create, process, and/or store Israel Railways' information in their computing infrastructures.

1.7 This appendix does not address the subject of remote connection to the critical systems infrastructure and control systems of Israel Railways.

1.8 Requirement details and the description of the approval process for connecting external suppliers to Israel Railways' internal systems are specified in the procedure "Remote Connection of External Contractors to Israel Railways' Systems for Support Purposes."

1.9 This document constitutes a Cyber appendix to the engagement between Israel Railways and its suppliers.

2. Definitions

2.1 "Supplier": An external body—including all its employees and subcontractors—providing Israel Railways with services (including outsourcing services) or goods of any kind.

2.2 "Cyber" ("Cyberspace"): The physical and non-physical domain created from or composed of the following (in whole or in part): computerized systems, computer and communication networks, operational technology (OT), software, computerized information, digitally transmitted content, traffic and control data, including the human-related aspect (the people using all of the above).

2.3 "Cyber Defense": All actions intended to protect Israel Railways' information assets in cyberspace.

2.4 "Cyber Attack": An attack in cyberspace that endangers cyber assets, systems, and the infrastructures they support.

2.5 "Cyber Event": An occurrence indicating a possible disruption to the proper functioning of a cyber asset, for which there is reason to believe originated from deliberate activity in cyberspace.

2.6 "Information Asset": A file, record, database, or physical copy containing information created or received as part of the company's ongoing operations and having value for the proper functioning of Israel Railways.

2.7 "Protected Information ":

Any of the following:

2.7.1 Information subject to the Privacy Protection Law of 1981.

2.7.2 Information about an organization that is not public knowledge.

2.7.3 Trade secrets under the Commercial Torts Law of 1999.

2.8 "Essential Cyber Asset": A cyber asset whose proper functioning is required to ensure the continued operation of Israel Railways as a national-essential cyber asset in the State of Israel. This definition includes: operational systems, industrial control systems (ICS), computer networks critical for Israel Railways' ongoing operation during routine and emergencies. This definition also includes any data and/or information (including correspondences) related to these systems.

2.9 "Israel Railways' Information Environment" (at the supplier): Israel Railways' information assets and all infrastructures, endpoints, and components that enable access to them, or in which they are created, stored, processed, or transmitted.

2.10 "Business Need": The need arising from an employee's role and/or the tasks assigned to them for the purpose of providing services to Israel Railways.

2.11 "Confidentiality": The requirement that access to information be limited solely to defined entities whose roles require such access and who have been granted authorization accordingly.

2.12 "Integrity": The requirement for information to be complete, reliable, and accurate throughout its life cycle.

2.13 "Availability": The requirement for information to be available to authorized users when they need it.

2.14 "Secure Channel": Establishing a secure communication path to prevent interference, unauthorized viewing, or data corruption.

2.15 "Encryption": The implementation of cryptography that converts clear text into ciphertext so that it can only be deciphered and understood by authorized entities.

2.16 "HLD": The design of a solution tailored to the client's sites/systems and feasibility testing of its architecture, cyber aspects, communication infrastructures, hardware components, equipment, devices, interfaces, software, and system configuration.

2.17 "LLD": Detailed architectural design, lists of equipment and manufacturers, detailed interface specifications, and implementation plan.

2.18 "Identifier": A tool that provides details to verify the identity of a person or system when they attempt to log in, authorizing them to perform actions within an information system.

2.19 "Remote Access": Connection by users and suppliers from outside the organization's infrastructure in order to obtain access to Israel Railways' systems/servers/endpoints, etc., and the files therein belonging to Israel Railways, for work performed by organizational users and maintenance performed by business interfaces (suppliers/contractors).

3. Information Security

3.1 Confidentiality and Privacy Protection

3.1.1 The supplier declares that it is aware that information and documents delivered to it and/or to anyone on its behalf by Israel Railways during the provision of service under this agreement are defined as "sensitive" and may not be published or used except for providing service under the agreement.

3.1.2 The supplier undertakes to keep secret and not copy, notify, transfer, or disclose to any person any information it and/or anyone on its behalf obtains, or has obtained, during or by virtue of performing the services.

3.1.3 The supplier undertakes to maintain the confidentiality of the information and documents detailed above even after the engagement period has ended, in accordance with this agreement.

3.1.4 The supplier undertakes to require its employees and those providing service on its behalf, including subcontractors, to sign a confidentiality undertaking and a declaration of absence of conflict of interest, in accordance with Israel Railways' requirements.

3.1.5 It is prohibited to copy, publish, transfer, notify, disclose, or bring to the knowledge of any other person, whether directly or indirectly, by act or omission, any item of information and/or Israel Railways' trade secrets that come into its possession, control, or knowledge, directly or indirectly, in connection with the provision of the service.

3.1.6 The supplier undertakes to maintain confidentiality regarding all know-how, work methods, equipment, devices, network configuration, and cyber defense system, as well as details and structure

related to computing equipment, including manufacturers, models, components and devices, including those that Israel Railways uses or is considering for future use.

3.1.7 The supplier undertakes to bring the provisions of this agreement and of this section to the knowledge of all persons it employs for the purpose of implementing this agreement and/or in connection with it.

3.1.8 The supplier undertakes to comply with all instructions provided by the Cyber Division, security and safety instructions provided by Israel Railways' Security and Emergency Division, and as necessary, instructions provided by any other authorized entity within Israel Railways. (For the avoidance of doubt, Israel Railways shall not bear the costs of implementing these instructions). The provisions of this section are subject to the supplier's regulatory obligations.

3.1.9 The supplier, its employees, and those providing service on its behalf undertake to participate (as required) in cyber defense training/briefing, the content of which shall be determined by Israel Railways' Cyber Division, up to once a year.

3.2 General Requirements

3.2.1 The supplier shall undertake to fully implement the following main conditions:

3.2.2 The supplier undertakes to comply with all provisions of the Computers Law of 1995, and the Privacy Protection Law of 1981, and the regulations enacted thereunder, as well as to comply with future conditions and regulations regarding the handling of computerized information systems.

3.2.3 The supplier undertakes in this document, prior to the commencement of service provision, to comply with all Cyber Division requirements and instructions specified in this appendix, including requirements under the Privacy Protection Law and its regulations, related to external service providers, holders of protected databases, and Israel Railways' obligations under national law and supervisory authority directives.

3.2.4 The supplier shall undertake to manage the required services on an ongoing and controlled basis, in a secure and compartmentalized fashion, and to prevent physical access by unauthorized persons to workstations, server rooms, and communication infrastructure used for work with Israel Railways.

3.2.5 The supplier shall appoint a Cyber Defense Trustee, who shall be instructed by Israel Railways' Cyber Division and shall serve as a Point of Contact (POC) regarding cyberspace defense.

3.2.6 The supplier shall grant the Cyber Defense Trustee all authority, tools, and means required to perform their duties, including enforcement authority over supplier employees in the field of cyber defense, subject to the regulatory provisions and instructions applicable to the supplier.

3.2.7 Israel Railways shall be entitled to define additional and/or alternative requirements vis-à-vis the supplier.

3.2.8 Pursuant to the timetable and additional instructions to be provided to the supplier by Israel Railways' representatives:

3.2.8.1. The supplier shall provide a detailed description (including a topology document) of all existing IT and IOT/

3.2.8.2. IIOT systems, data flow, and existing information security measures.

3.2.8.3. The supplier shall present an implementation solution to prevent logical access to the system and its components, infrastructures, and systems connected to it.

3.2.8.4. The supplier shall present its approach to implementing layers of physical protection on system equipment within Israel Railways' facilities, including physical compartmentalization of technician access to equipment, access to control rooms, and security and hardening measures for its facilities outside Israel Railways' premises, as well as the standard physical security and compartmentalization measures it implements in similar projects.

3.3 Protecting Critical Cyber Assets and IT and OT Infrastructure

3.3.1 Technicians and supplier representatives shall not be permitted to connect or attempt to connect directly to essential systems (critical cyber assets, as defined by Israel Railways).

3.3.2 As a rule, approval shall not be given to remotely connect to critical systems infrastructure and Israel Railways' control systems. Exceptional cases shall be reviewed individually, as needed, by Israel Railways' Cyber Unit.

3.3.3 Any procurement intended for networks, defensive measures (hardware and software), critical systems infrastructure, and industrial control systems at Israel Railways shall be subject to approval by Israel Railways' Cyber Division.

3.3.4 Software components: the need for resilience/penetration testing prior to their installation shall be examined, pursuant to binding instructions to be provided by Israel Railways' Cyber Division.

3.3.5 The supplier must undertake to immediately report in writing to Israel Railways' Cyber Monitoring Center at Tel. 08-6533065 regarding any unusual occurrence in the supplier's facilities and/or harm or attempted harm to security components, or the theft or attempted theft of components planned for installation in critical systems (critical cyber assets).

3.3.6 Computers, phones, cameras, portable memory devices (disk-on-key), or any other computing or storage means shall not be permitted to connect to critical systems and industrial control systems (ICS), including for charging cellular/other devices. If necessary, permission shall be granted for one-time use of a dedicated portable memory device and/or dedicated laptop, but only after receiving prior, specific approval from the Director of the Cyber Division at Israel Railways.

3.4 Information Security Management, Regulation, and Standards – Mandatory Requirements

3.4.1 The supplier shall define an information security policy pursuant to the timetables and any additional instructions received from Israel Railways representatives, which complies with laws, regulations, and relevant standards applicable to it, and which is consistent with accepted industry standards. The policy shall be approved by senior management and implemented among all entities with access to Israel Railways' information environment.

3.4.2 The supplier must maintain information security procedures covering at least the following:

3.4.2.1. Information security events, response management, investigation, etc.;

3.4.2.2. Information security in human resources and employee life cycle management (hiring, departure, training, etc.);

3.4.2.3. Client information assets security;

3.4.2.4. Customer applications security;

3.4.2.5. Secure development and system maintenance.

3.4.3 Where relevant, the supplier must achieve full compliance with PCI-DSS.

3.5 Information Security in Human Resources – Mandatory Requirements

3.5.1 The supplier is responsible for conducting background checks on employees authorized to access Israel Railways' information environment, subject to applicable legal restrictions (e.g., Israeli Police guidelines, police certificate, Israel Railways' internal background checks, or any other check approved by the authorities).

3.5.2 The supplier shall conduct activities to raise awareness among its employees on information security, privacy protection, and risks relevant to their roles in particular. The supplier must ensure employee proficiency in these matters, including by administering effectiveness tests and transferring the results to Israel Railways.

3.5.3 The supplier shall ensure permissions are revoked and equipment or media containing Israel Railways' information is returned upon employee departure or role change.

3.6 Transferring Sensitive/Confidential Information between the Supplier and Israel Railways – Mandatory Requirements

3.6.1 Digital information shall not be transferred over the internet or via regular email between the supplier and Israel Railways or between the supplier and subcontractors. Said digital information shall only be transferred through a secure channel, as specified at the time of transfer by the supplier's POC for Israel Railways.

3.6.2 Information on physical media (hard copy, removable media) shall be delivered directly to an Israel Railways employee or via a process defined at the time of transfer by the supplier's POC for Israel Railways.

3.6.3 Information transferred on removable media must be encrypted. The encryption key shall be delivered separately to the recipient.

3.6.4 Effective deletion of all copies of information from the subcontractor's computing infrastructure must be ensured upon its transfer to removable media.

3.7 Information Storage – Mandatory Requirements

3.7.1 As a rule, Israel Railways' information shall be stored on servers within the supplier's internal network, not on endpoints.

3.7.2 Where materials are designated as sensitive by Israel Railways, all information must be stored in encrypted form using accepted encryption standards and technologies.

3.7.3 Where there is a business need to store Israel Railways' sensitive information on a laptop, the files or the computer's hard drive must be encrypted.

3.7.4 Upon termination of engagement with Israel Railways, the supplier shall ensure transfer of all information to Israel Railways and the permanent deletion of all its copies from the supplier's servers. Deletion of information must be logged. The provisions of this section are subject to the supplier's regulatory obligations.

3.8 Backup and Recovery – Mandatory Requirements

3.8.1 The system/technological solution shall be designed for high availability (99.999%).

3.8.2 The supplier shall be responsible for backing up Israel Railways' information. Backups containing sensitive information shall be securely stored, protected from overwriting, and encrypted. Access shall only be permitted based on legitimate business need.

3.8.3 Encryption keys for backups shall be stored separately from the media.

3.8.4 The supplier shall maintain business continuity and disaster recovery plans to ensure ongoing business operations for Israel Railways' assets and systems.

3.9 Network Security – Mandatory Requirements

3.9.1 The supplier shall submit an HLD pursuant to the timetable and instructions received from Israel Railways representatives, including system configuration, a description of the work environments, information flow, protocols in use, and information security measures.

3.9.2 The supplier shall submit an LLD pursuant to the timetable and instructions received from Israel Railways representatives, including detailed architecture, lists of equipment and manufacturers, detailed interface specifications, and implementation plan.

3.9.3 Direct access to Israel Railways' information environment is only permitted via secure connection and two-factor authentication, not via Internet.

3.9.4 The supplier shall provide Israel Railways with the project equipment list, including manufacturer name, equipment model, quantities, and software version.

3.9.5 The supplier shall update and harden all project equipment, particularly by changing default security settings.

3.9.6 Israel Railways' information environment shall be protected by at least the following security mechanisms:

3.9.7 NAC-Network Access Control

3.9.8 Network Firewall – traffic allowed only for business need.

3.9.9 Gateway Anti-Malware Engines.

3.9.10 Web/Category based filtering.

3.9.11 Intrusion Prevention/Detection System (IPS/IDS).

3.9.12 Web Proxy Servers.

3.9.13 DDOS Protection.

3.9.14 Application Firewall (for internet-exposed applications).

3.9.15 Database Firewall – for database protection.

3.9.16 SIEM – central log collection with correlation capabilities.

3.9.17 File sanitization system with multi-engine antivirus file scanning and CDR capabilities, including sandboxing, when ingesting files into the system.

3.9.18 Data Loss Prevention – DLP.

3.9.19 API Gateway – interface security.

3.9.20 Sensitive data discovery and classification system.

3.9.21 Database security using a dedicated DB FW component.

3.9.22 Extended detection and recovery system (XDR).

3.9.23 Endpoints and servers with access to Israel Railways' information must be protected by endpoint protection and endpoint detection and response solutions.

3.9.24 Implementation of strong user management systems (Admin) – PSM (Privileged Session Manager), PIM (Privileged Identity Manager), as well as monitoring and screen recording of such users across Israel Railways' information environment. Screen recordings must be protected against tampering or deletion for at least 6 months and available to Israel Railways at all times.

3.9.25 WI-FI for operational needs:

3.9.25.1. The WI-FI environment must be completely segregated from unrelated work environments and on a need-to-know basis.

3.9.25.2. Default router passwords must be replaced with ones meeting the minimum password policy requirements outlined in the chapter on password policy.

3.9.25.3. Remote management of wireless routers (outside Israel Railways' network) shall not be permitted.

3.9.25.4. Service shall be permitted after receiving prior approval from the Director of the Cyber Division at Israel Railways and may be subject to additional requirements beyond those listed herein.

3.9.25.5. Strong authentication must be implemented between endpoints and access points, including encryption with a complex password.

3.9.25.6. WI-FI communication protocols and their security measures must be approved by Israel Railways' Cyber Division.

3.9.25.7. WI-FI network logging and monitoring are required.

3.10 Environment Segregation – Mandatory Requirements

3.10.1 The supplier shall create a dedicated infrastructure for Israel Railways' work environment and data, which is separated from the supplier's production infrastructure and from other customer infrastructures. The infrastructure shall be physically or logically segregated as instructed by Israel Railways' Cyber Division. For the avoidance of doubt, final configuration shall be determined following approval of the LLD submitted to Israel Railways' Cyber Division.

3.10.2 Israel Railways' databases shall be segregated using a dedicated server, not merely by logical database-level separation.

3.10.3 Compartmentalization shall be implemented between different segments by physical/logical network separation, restricting inter-network connectivity, and establishing a controlled environment using a firewall and/or software component (micro-segmentation) approved by the Cyber Division, in accordance with the system's required operations, protocols, addresses, and ACLs.

3.10.4 Any data transfer into Israel Railways' network shall require review and approval by Israel Railways' Cyber Division and, in all cases, content filtering/protocol breaks.

3.10.5 Work environments shall be segregated into production, testing, and development.

3.10.6 Subnet separation shall be implemented (e.g., application servers, databases, reporting).

3.10.7 The supplier is required to implement a secure process for data transfer between environments, including support for appropriate workflows.

3.10.8 The supplier must scramble sensitive data transferred from production to non-production environments, to ensure data does not appear "as is" in non-operational environments (test, QA, etc.).

3.11 Access Control – Mandatory Requirements

3.11.1 Access to Israel Railways' information environment shall require user identification and shall be strictly limited to those with a business need.

3.11.2 User permissions shall be assigned based on business need and based on "need to know" and "least privilege" principles. This method shall define permissions for objects in the system by user names, group names, or both. Permission changes shall only be performed by authorized personnel.

3.11.3 Strong privilege accounts (e.g., system administrators) shall be limited to the minimum number of employees required.

3.11.4 Each user with authorized access to Israel Railways' information environment shall be assigned a unique user ID. The use of group or shared accounts in Israel Railways' information environment is prohibited.

3.11.5 Accounts of employees who have left or changed roles and no longer serve Israel Railways shall be blocked or disabled.

3.11.6 Application accounts shall be defined separately from system user accounts, subject to approval by Israel Railways' Cyber Division.

3.12 Identification, Authentication, and Password Policy – Mandatory Requirements

3.12.1 The system shall implement identification and authentication mechanisms.

3.12.2 The supplier shall enforce a strong password policy:

3.12.3 User password length shall be at least 14 characters.

3.12.4 Passwords shall contain a combination of uppercase letters (min. 1), lowercase letters, numbers (min. 2), and symbols (min. 1).

3.12.5 Passwords for strong privilege accounts (admin) shall be at least 25 characters and require two-factor authentication (e.g., user password + OTP).

3.12.6 Admin passwords shall contain a combination of uppercase letters (min. 1), lowercase letters, numbers (min. 2), and symbols (min. 1).

3.12.7 Initial passwords (provided by system/network administrator) must be replaced with permanent ones immediately upon first login.

3.12.8 Passwords must be changed at least every 3 months. Users shall not be able to reuse any of their last 5 passwords.

3.12.9 Passwords shall have cryptographic protection both in storage and transmission, consistent with current industry best practices.

3.12.10 Inactive sessions (20 minutes of inactivity) shall be automatically disconnected. Reconnecting shall require user reidentification.

3.12.11 User accounts shall be locked after 5 failed login attempts. Unlocking shall only be permitted after at least 30 minutes or by the system administrator following user identity verification.

3.12.12 All remote access (remote access/teleprocessing systems) to Israel Railways' information environment must occur over an encrypted channel (e.g., HTTPS/SSL-VPN) and require two-factor authentication (e.g., user password + OTP).

3.13 **Server and Endpoint Security – Mandatory Requirements**

3.13.1 As a rule, all operating systems and software in use must be supported and updated by their publishers.

3.13.2 The supplier shall harden and configure all servers and endpoints within Israel Railways' information environment in accordance with vendor instructions or industry best practices (e.g., CIS), or specific instructions provided by the Cyber Division, if issued.

3.13.3 Applications, services, ports, modules, components, etc. that are not required for the defined business purposes shall be blocked or disabled.

3.13.4 All default accounts and passwords provided by vendors in any component within Israel Railways' information environment (OS, software components, network devices, etc.) shall be removed or blocked, and replaced with designated supplier accounts with strong passwords.

3.13.5 Critical security updates for software components and operating systems within Israel Railways' information environment shall be installed as soon as possible after release, and no later than 30 days. Non-critical updates shall be installed quarterly.

3.13.6 Automated tools for defending against malware (e.g., antivirus, EDR) shall be installed on all servers and endpoints in Israel Railways' information environment. The supplier shall ensure these tools are always up to date.

3.13.7 Application control shall be implemented to restrict and control software installation on endpoints connected to Israel Railways' information environment.

3.13.8 Auto-run functionality shall be disabled on servers and endpoints.

3.13.9 Endpoints shall have a personal firewall, configuration controls, and centrally controlled and managed features under the supplier's responsibility.

3.14 Secure Development – Mandatory Requirements

3.14.1 The supplier shall undertake that it implements secure development principles addressing the OWASP Top 10 vulnerabilities.

3.14.2 The supplier shall comply with secure development principles, such as: input validation, output validation, password management and authentication, session management, permissions and access control, data encryption, logging and error handling, data protection, secure communications, server configuration and hardening.

3.14.3 When using third-party code, a signed document (bearing company logo and CEO signature) must be obtained confirming that the company reviewed all components and found them to be free of vulnerabilities/exposures that could affect the integrity of Israel Railways' systems and networks.

3.14.4 The supplier must deliver an SBOM to Israel Railways. Components with medium or higher severity vulnerabilities shall not be approved for use.

3.14.5 Prior to go-live, an information security review and resilience test must be conducted based on accepted methodologies by a third-party company that specializes in conducting reviews and penetration tests. The content of the survey and penetration test shall be submitted for approval by Israel Railways' Cyber Division.

3.14.6 The supplier must remediate, at its own expense, all high/medium severity issues identified in the information security review and resilience test, in accordance with instructions provided by Israel Railways' Cyber Division.

3.14.7 The supplier shall undertake to have penetration tests performed by a third-party company specializing in that field every calendar year. The test results shall be submitted and must confirm that the system has no high- or medium-risk issues.

3.14.8 The final report submitted to the Cyber Division shall include:

3.14.8.1. An executive summary containing general system details (description, architecture, test scope and limitations), a summary of findings regarding security exposure and compliance with information security circulars applicable to the system, and details of the findings.

3.14.8.2. The summary of findings shall be in the following format:

Number Report Section Risk Level General Description Recommendation for Remediation

The ID in the tracking table

3.14.9 Findings must include: the tested item, test description, findings, exposure description, risk level (likelihood, potential harm), practical recommendations or compensating controls, technical details (including screenshots and/or recordings) with precise explanations on how the finding was identified so it can be reproduced. The report must indicate if the finding was already noted in a previous review.

3.14.10 The report shall serve as a guiding document for operational actions. The report shall detail findings, risk levels of each exposure based on likelihood vs. impact, and prioritized remediation recommendations.

3.14.11 The above requirements apply to both new and previously identified findings.

3.15 Use of Removable Media – Mandatory Requirements

3.15.1 Within Israel Railways' information environment, removable media may only be used after undergoing a "whitelisting" process (file scanning and filtering prior to introduction into the environment) and after receiving approval by the Cyber Division.

3.15.2 Removable media containing Israel Railways' classified information must be encrypted using industry-accepted standards.

3.16 Maintenance – Mandatory Requirements

3.16.1 Planned operations (including upgrades, expansions) must be coordinated and pursuant to Israel Railways' policies, and also subsequent to documented meetings held to discuss their implications (e.g., readiness checks, rollback procedures, obtaining approvals, communicating implications, and preventing risks to service continuity).

3.16.2 As a rule, supplier access to Israel Railways' servers for maintenance shall occur only on Israel Railways' premises. Remote access to servers or system components shall not be permitted. Any exception to this section shall be individually approved by the Director of the Cyber Division at Israel Railways.

3.16.3 Updates and changes to software/infrastructure: any system change (excluding content updates) constitutes a "new version" and must undergo testing per Israel Railways' requirements (e.g., penetration tests, code reviews).

3.16.4 The supplier shall present a solution to prevent unauthorized access to sensitive system components (as defined by Israel Railways) during maintenance activities.

3.17 Encryption – Mandatory Requirements

3.17.1 All network traffic must be encrypted independently (the minimum algorithm must be based on AES-256 or higher), regardless of network encryption.

3.17.2 All stored data must be encrypted independently (the minimum algorithm must be based on AES-256 or higher), regardless of network encryption.

3.17.3 All traffic shall be encrypted using commercial encryption protocols (e.g., IPsec, TLS/SSL, SSH, etc.).

3.17.4 The system must support FIPS 140-2 encryption.

3.17.5 Any deviation from encryption policy shall generate a record that can be transferred online automatically to the monitoring hierarchy, in a format that is familiar and compatible with the SIEM systems installed at Israel Railways and/or on the supplier's premises, subject to approval by Israel Railways' Cyber Division.

3.17.6 When procuring endpoints (desktops, laptops) for the project, the devices must be ensured to include a built-in TPM (Trusted Platform Module) that enables disk encryption.

3.18 Monitoring, Logging, and Control – Mandatory Requirements

3.18.1 All logs must be transferred to a central SIEM system dedicated for log collection and protection. The SIEM must support correlation capabilities for detecting and investigating cyber events.

3.18.2 At minimum, the following must generate event logs: server operating systems, service applications, security mechanisms (Active Directory, firewall, IPS/IDS, WAF, Web Proxy, Antivirus, EDR, PSM, PIM).

3.18.3 Every system action must generate a log record and support tracking and non-repudiation mechanisms.

3.18.4 Log files shall be accessible to Israel Railways' representatives at all times, at no additional cost/charge.

3.18.5 The supplier shall undertake to provide Israel Railways with all evidence in this regard (digital, written, or otherwise) within 48 hours of request.

3.18.6 All actions must be documented in security records. The supplier shall enable monitoring outputs and logs (relevant to the engagement) to be linked from the supplier's systems to Israel Railways' Cyber Monitoring Center through interfacing with Israel Railways' event management system (SIEM).

3.18.7 The system must support log transfer to SIEM in standard formats such as Syslog.

3.18.8 The supplier shall enable support for interfacing with Israel Railways' Cyber Monitoring Center via a one-way communication component (data diode).

3.18.9 The following control operations are mandatory for system monitoring and implementation:

3.18.9.1. Documenting all system and database access attempts, including administrator, support, audit, system, DBA accounts;

3.18.9.2. System logoffs;

3.18.9.3. Access permission and monitoring when accessing the database in the production environment shall be defined exclusively for the system administrator and personnel authorized by him/her, each using a personal and exclusive account;

3.18.9.4. Blocking and monitoring database access accounts after 5 failed login attempts;

3.18.9.5. Generating reports on unsuccessful login attempts and invalid access attempts at the OS and database levels;

3.18.9.6. Monitoring all object deletions or changes in the system;

3.18.9.7. Monitoring and blocking changes (including deletions) in software, tables, data, or database controls;

3.18.9.8. Monitoring application-level events defined as requiring control according to a specified special set of rules;

3.18.9.9. Monitoring specific operations initiated by the user that are defined as requiring control (e.g., opening a vault, sending a message, etc.);

3.18.9.10. Monitoring operations performed by privileged users;

3.18.9.11. Monitoring administrative actions (user management, system shutdown/startup, services, etc.);

3.18.9.12. Monitoring operational errors (system crashes, software error messages, etc.);

3.18.10 The following details shall be recorded for every event requiring monitoring:

3.18.10.1. Date and time;

3.18.10.2. Source of the action (e.g., IP address, domain);

3.18.10.3. Username;

3.18.10.4. Event type;

3.18.10.5. Event outcome (success/failure);

3.18.10.6. Object affected by the action (file name, etc.);

3.18.10.7. Description of the action performed (relevant content must be provided for each type of event, e.g., record update, record access attempt, user deletion, system shutdown, etc);

3.18.11 The system shall allow the logs to be "enriched" with information, including machine type, OS type, user agent, etc.

3.18.12 Log messages must be reliable, complete, and clear. Log files in the system shall be protected from unauthorized access (viewing, modification, deletion), including by administrators, with the ability to identify unauthorized access attempts.

3.18.13 The system shall alert on any access/use attempt exceeding granted permissions.

3.18.14 The system must manage a structured and orderly process for storing and deleting records.

3.18.15 Log records shall be retained for at least 6 months.

3.18.16 The system shall support sending alerts to administrators (via e-mail, SMS, SNMP, traps, etc.) about events defined as reportable.

3.18.17 The control system must be properly secured. Only authorized users shall have access to it, with strict access control over enabling/disabling monitoring functions.

3.18.18 Logged data shall comply with PCI-DSS requirements and/or Privacy Protection Authority regulations, where relevant.

3.19 Cyber and Information Security Event Handling and Readiness – Mandatory Requirements

3.19.1 The supplier shall prepare an incident response policy and procedure for cyber and information security events.

3.19.2 It shall also define a program that includes preparedness, identification, containment, mitigation, recovery (BCP) and recovery objectives from cyber security events until full functionality is restored upon return to normal operations.

3.19.3 Where required, the supplier shall present Israel Railways' Cyber Division with the principles of the incident response policy and procedure and its alignment with the risk assessment performed.

3.20 Surveys and Supply Chain – Mandatory Requirements

3.20.1 When required by the Cyber Division, the supplier shall undertake to comply with the requirements of the National Cyber Directorate's supply chain questionnaire for the relevant category (e.g., cloud computing, hosting, information security management, etc.).

3.20.2 Pursuant to this appendix, Israel Railways may conduct a risk survey, either directly or through a third party, at no additional cost.

3.20.3 The supplier undertakes to allow Israel Railways representatives to conduct audits of security systems, during standard working hours and without prior notice, at its facilities that are related to or influence the security of the systems used by Israel Railways, at no additional cost.

3.20.4 Israel Railways, or its authorized representatives, may perform security system checks, resilience testing, security vulnerability locating, and checks related to the effectiveness of the mechanisms that secure the systems used by Israel Railways, at no additional cost.

3.20.5 The supplier must conduct covert security tests from systems external to the supplier, to verify defenses against external access into Israel Railways' systems from the supplier's systems or from external systems, subject of this engagement.

3.20.6 The scope of the surveys shall be adjusted to the sensitivity of the information and the level of risk posed to Israel Railways, depending on the nature of the supplier's activities, and shall include tests designed to verify the supplier's compliance with cyber defense requirements and to identify exposures to such risks.

3.20.7 Israel Railways may demand the correction of issues identified in risk surveys, planned audits, surprise audits, or through the random or proactive discovery of security flaws in the supplier's facilities. The supplier shall be obligated to remedy such issues within a reasonable period of time (for this purpose: the amount of time professional bodies estimate is required to fix the issues) and at no additional cost.

3.20.8 If critical issues are found that affect the level of cyber defense for Israel Railways' systems, the supplier shall be required to correct such issues immediately and at no additional cost.

3.21 Control Reports – Mandatory Requirements

3.21.1 The supplier undertakes to deliver to Israel Railways, upon request or on a regular basis, control reports as required in the engagement letters, as well as additional reports at the supplier's initiative, at no additional cost.

Among the reports to be included:

3.21.1.1. Reports on the permissions system (user permissions, users in a user group, etc.)

3.21.1.2. Reports from the monitoring (auditing) system, including: the number of each type of event, failed access attempts, etc.

3.21.2 Report files shall be, as much as possible, compatible with other external software and in standard formats such as XML, DOC, TXT, etc.

3.22 Remote Access – Mandatory Requirements

3.22.1 As a rule, the supplier shall not be granted any remote access to Israel Railways' systems.

3.22.2 Notwithstanding the above subsections, a connection between the supplier's domains and components of Israel Railways' systems shall only be permitted if the following conditions are met:

3.22.2.1. The connection shall be made exclusively from end-user computers that the supplier provides to Israel Railways; these computers shall be hardened by Israel Railways.

3.22.2.2. The creation of the connection has been examined and approved by Israel Railways' Cyber Division after having evaluated its necessity/requirement, the risks involved, and the compensatory controls.

3.22.2.3. Remote access shall be strictly limited to components for which remote access is mandatory.

3.22.2.4. Remote access shall be encrypted (in accordance with the requirements specified in the "Encryption" section).

3.22.2.5. Inactive session timeouts shall be defined after which access will be disconnected (session timeout).

3.22.2.6. Remote access shall be monitored and limited to supplier employees approved in advance by Israel Railways, with each employee assigned a personal username. If a personal username cannot be configured, the group user's permissions shall be restricted to monitoring and rebooting actions only, and no software component installation or update shall be permitted via remote access.

3.23 Hardware – Mandatory Requirements

3.23.1 All procurement intended for networks, protective measures (hardware and software), critical system infrastructure, and industrial control systems at Israel Railways shall be subject to approval by Israel Railways' Cyber Division.

3.23.2 When procuring servers and endpoints (desktop or mobile) for the project, the supplier is responsible for ensuring that:

3.23.2.1. Servers and desktop endpoints shall not contain built-in wireless communication components, including:

WI-FI, Bluetooth, infrared, etc.

3.23.2.2. The product shall include a built-in TPM component that enables disk encryption.

3.23.2.3. The product's storage devices shall be internal only, with no use of removable hard disks.

3.24 Intellectual Property – Mandatory Requirements

3.24.1 All software and computer systems used by the supplier in providing services to Israel Railways are to comply with intellectual property law, have valid licenses, and the supplier has the right to use them.

3.24.2 No use shall be made of software or equipment that is no longer supported by the manufacturer and has been designated by the manufacturer as End of Life.

3.25 Cloud Computing

3.25.1 When providing a cloud-based system, the supplier shall be required to successfully pass the National Cyber Directorate's Cloud Committee. Accordingly, the supplier shall be required to complete relevant documentation in preparation for the committee and comply with required controls.

3.25.2 The supplier shall provide documentation of the mechanisms to be used in operating the cloud service – including monitoring tools, logging, computation, storage, access control, access rights management, bypassing of activation and security mechanisms, encryption (cryptography), and others.

Mandatory Requirements – Cloud Computing

3.25.3 The supplier shall deliver an HLD pursuant to the timetable and instructions received from Israel Railways representatives, including the system architecture, description of work environments (public cloud, private cloud, hybrid cloud), and which specifies the deployment model for cloud services (SaaS, IaaS, PaaS), the existence of a shared responsibility model, as well as mapping of data flows between all cloud services, Israel Railways' internal computing systems, and other clients/nodes.

3.25.4 The supplier shall submit an LLD pursuant to the timetable and instructions received from Israel Railways representatives, including detailed architecture, lists of equipment and manufacturers, detailed interface specifications, and implementation plan.

3.25.5 The supplier shall comply with all the mandatory requirements of Israel Railways' Cyber Division, as specified above from Section 3.1 to Section 3.24, when providing services in cloud infrastructures.

3.25.6 The supplier must also implement a dedicated HSM encryption security system.

3.25.7 The supplier must implement a CSPM cloud security posture management system.

3.25.8 The supplier must implement a KMS system for key and secret management.

3.25.9 The supplier must implement a CNAPP cloud-native application protection platform.

3.25.10 Cloud computing shall be carried out in cloud infrastructures that comply with leading cloud standards, such as (at least 2 of the following 4 international standards):

3.25.10.1. CSA STAR;

3.25.10.2. SOC2;

3.25.10.3. IEC 27017;

3.25.10.4. IEC 27018;

3.25.11 The supplier shall ensure the cloud service full complies with the Privacy Protection Law of 1981, and regulations enacted thereunder, including the Privacy Protection Regulations (Transfer of Data to Databases Outside the State's Borders) of 2001, concerning transfer of data to databases outside the country.

3.25.12 Where relevant, the supplier shall ensure full compliance with the Privacy Shield regulation and GDPR governing privacy in information.

3.25.13 Where relevant, the supplier shall ensure full compliance with the PCI-DSS cloud computing guidelines.

3.25.14 As a rule, the access segregation configuration for Israel Railways' information environment, both during regular operations and during failover or data recovery, shall be defined through a separate tenant serving only the company's services/resources.

3.25.15 The supplier shall use Cloud Security Access Broker (CASB) solutions to address risks in cloud services, enforce security policy, and ensure regulatory compliance, even when cloud services are external to the supplier's site and outside its direct control.

3.25.16 As a rule, Israel Railways' information environment stored in cloud services shall be encrypted using accepted encryption methods, with the encryption key stored outside the cloud services by means of a logical vault.

3.25.17 Strong authentication shall be applied for every access to cloud service management/consumption using multi-factor authentication (MFA).

3.25.18 The supplier must perform communication access control for the cloud service's management interfaces.

3.25.19 The supplier must control and prevent access by supplier administrators to Israel Railways' information environment stored in the cloud.

3.25.20 Connectivity and interfaces to Israel Railways' network shall be carried out only after review and approval by Israel Railways' Cyber Division, and only via an encrypted connection.

3.25.21 Transferring data to Israel Railways' network shall be carried out only after review and approval by Israel Railways' Cyber Division, and in any case only after content filtering/protocol breaking.

3.25.22 Conditional access shall be enforced, so that the service provided is only available from Israel Railways' addresses.

3.25.23 If a service is required for external use, the (GEP) IP address list shall be restricted to exclude enemy states or based on a list provided by the Cyber Division.

3.25.24 The supplier's cloud service work processes shall ensure monitoring, logging, and control of access to Israel Railways' information environment, while preventing and documenting any unauthorized access or attempted access to the information (including attempts to create magnetic or printed copies of the information), and alerting Israel Railways of any unauthorized access or attempt.

3.25.25 The supplier's cloud service work processes shall ensure protection for audit files and other data (including system states and actions taken in response) required for analyzing failures in general and cyber events in particular.

3.25.26 The supplier's monitoring systems must detect information security events and alert Israel Railways within effective time frames, in order to meet the required response times for handling events, swiftly and efficiently neutralizing threats as early as possible, and preventing any risk to the information or the existing cloud service.

3.25.27 Cloud monitoring systems shall enable each client to only access indications regarding its own systems. Access to Israel Railways' system indicators shall not be permitted for other parties without prior official approval from Israel Railways' Cyber Division.

3.25.28 All cyber security events in the infrastructure/any other cloud service shall be logged and stored for at least six months.

3.25.29 The supplier shall enable monitoring outputs and logs (relevant to the engagement) to be linked from the supplier's systems to Israel Railways' Cyber Monitoring Center through interfacing with Israel Railways' event management system (SIEM).

3.25.30 The supplier must define efficient and rapid processes for handling service/system malfunctions that exist in the cloud, including rapid, efficient, and continuous response to inquiries and reports regarding such malfunctions (such as an available support and service center). To ensure continuous response, the supplier must maintain mechanisms that prevent the support service center from being blocked or disabled.

3.25.31 The supplier shall ensure continued cloud system service, including resource allocation monitoring (memory, processing, communication), disaster recovery mechanisms, clock site, and reliance on processes and backups (including storage in different physical locations) that enable and ensure rapid recovery.

3.25.32 Cloud Service Termination – Mandatory Requirements

3.25.32.1. For the purpose of cloud service termination (in accordance with the engagement terms in general and upon completion of the engagement in particular), the cloud service provider must delete all Israel Railways' information existing in the cloud service, including metadata, while also removing any possibility of restoring the information.

3.25.32.2. Before deleting the information detailed in the previous section above, the cloud service provider must obtain Israel Railways' approval for the deletion, and must deliver to Israel Railways a complete backup of all information belonging to Israel Railways and the project/system.

3.26 Open Source

Mandatory Requirements for Software Suppliers

3.26.1 Not Using Malicious Open-Source Software: The supplier must provide products free of malicious code. All reasonable means must be used, such as security software and the implementation of development processes and work procedures aimed at identifying and avoiding the use of malicious open-source software in the products and services supplied to the company.

3.26.2 Monitoring and Remediation of Known Vulnerabilities in Open-Source Software: The supplier must provide products and services free from known exploitable vulnerabilities, as these may endanger Israel Railways. All necessary means must be used, including software composition analysis tools, in order to validate and monitor known vulnerabilities in the open-source software included in the products and services you provide to Israel Railways, for no less than 12 months from the date on which the products were supplied to Israel Railways, and for as long as you provide Israel Railways with support for the product or service.

3.26.3 Upon the discovery of a newly exploitable vulnerability, you must provide Israel Railways with immediate notification and make every effort to supply, along with said notification, instructions regarding the required remediation actions. If no fix is available, you must provide a temporary solution until an appropriate remediation is provided.

3.26.4 Representations Regarding Open-Source Licenses: Some open-source licenses contain mechanisms intended to preserve user freedoms in relation to the open-source software, even with regard

to changes in the software, including derivative works ("copyleft"). The supplier must review the licenses of all open-source software used within the product or service supplied to Israel Railways to ensure that the use of the product, pursuant to the agreement with Israel Railways, does not expose Israel Railways to copyleft requirements or any similar requirement.

3.26.5 Software Bill of Materials (SBOM) for Open-Source Components: It is of high importance that Israel Railways have a complete and accurate picture of all open-source software used in the products distributed to Israel Railways, both for compliance/legal purposes and for security purposes. For this reason, Israel Railways may request, and the supplier is obligated to provide, a complete SBOM of all open-source software in the products distributed to Israel Railways, in a machine-readable format. This is intended to allow Israel Railways to conduct ongoing monitoring of newly discovered vulnerabilities in the open-source components of the product. If you are requested by Israel Railways to provide such an SBOM, every product update/upgrade will be required to be accompanied by an updated SBOM. To be clear, providing such an SBOM does not diminish the supplier's obligation to monitor for newly discovered vulnerabilities in the product, notify Israel Railways of such vulnerabilities, and provide fixes for any known exploitable vulnerability.

3.26.6 If the agreement with Israel Railways allows the products to be redistributed, the supplier must also provide Israel Railways with the following:

3.26.6.1. Compliance Deliverables for Open-Source Licenses: Compliance deliverables (such as copyright notices, provision of license copies, source code, etc.) enable Israel Railways to comply with the licensing requirements of the open-source software used by the company. You must provide Israel Railways with the required compliance deliverables in order to ensure full compliance with all open-source software licenses integrated into the products distributed to Israel Railways, or required for the operation of the product (i.e., open-source software necessary for product operation that is not supplied with it). If the timeline for supplying compliance deliverables is not defined in the agreement between the parties, the deadline shall be upon product delivery to Israel Railways.

Mandatory Requirements for Software Contractors Developing in Israel Railways' Environment

3.26.7 Software development activities shall be subject to Israel Railways' open-source policy. The open-source policy regulates the main processes related to the use of open-source software, such as evaluation, modification, approval, retention, monitoring, and remediation of open-source licensing violations and known security vulnerabilities. Before commencing any work, you must ensure that all your employees developing within Israel Railways' environment are familiar with Israel Railways' open-source policies and procedures.

Mandatory Requirements for Software Contractors Developing in an Independent Environment

3.26.8 Not Using Malicious Open-Source Software: As a supplier for Israel Railways, you are responsible for providing products free of malicious code. You must use all reasonable means, such as security software and the implementation of development processes and work procedures aimed at identifying and avoiding the use of malicious open-source software in the products and services supplied to the company.

3.26.9 Monitoring and Remediation of Known Vulnerabilities in Open-Source Software: As a supplier for Israel Railways, you are responsible for providing products free from known exploitable

vulnerabilities, as these may endanger Israel Railways. You must use all necessary means, including software composition analysis tools, in order to validate and monitor known vulnerabilities in the open-source software included in the deliverables you provide to Israel Railways.

3.26.10 The supplier must analyze all known vulnerabilities and deliver to Israel Railways documentation of all known vulnerabilities in the deliverables, including a reasonable explanation (for each known vulnerability) as to why the supplier believes the vulnerability is not exploitable, preferably in a machine-readable format (e.g., CyclonDX/VEX).

3.26.11 Israel Railways may require the remediation of known vulnerabilities if the explanation is not satisfactory or does not comply with the standards applicable to software development by Israel Railways.

3.26.12 Representations Regarding Open-Source Licenses: Some open-source licenses contain mechanisms intended to preserve user freedoms in relation to the open-source software, even with regard to changes in the software, including derivative works ("copyleft").

3.26.13 The supplier is obligated to review the licenses of all open-source software used within the product you supply to Israel Railways, in order to ensure that the use of the product, pursuant to the agreement with Israel Railways, does not expose Israel Railways to copyleft requirements or any similar requirement.

3.26.14 Backup of Open-Source Components and Source Code: As a supplier for Israel Railways, you are required to back up all open-source components integrated into the supplied software ("Open-Source Archive"). As part of the deliverables, you must provide Israel Railways with the Open-Source Archive, including all accompanying source code and corresponding sources (the code required to create, install, and run the binary components, including the code required to make modifications, as well as all scripts required to perform such activities).

3.26.15 Approval of Deliverables Acceptance: Israel Railways' policy requires review as part of the acceptance of deliverables from the supplier in order to verify compliance with these requirements. This acceptance process will include, at a minimum, scanning the deliverables using appropriate scanning tools, as well as building/rebuilding the supplied software to verify the integrity of the accompanying source code.

4. System Configuration

4.1 If the system contains internal/personal-sensitive/business-sensitive information, the system shall be installed in Israel Railways' server farm (on-premise) following approval by Israel Railways' Cyber Division prior to installation.

4.2 Alternatively, and subject to instructions and approval from Israel Railways' Cyber Division, the system may be supplied in a "cloud" configuration following an individual assessment by Israel Railways' Cyber Division.

4.3 In the case of a cloud configuration, the supplier shall be required to meet all information security requirements set forth in this appendix under the Cloud Computing section above.

4.4 The system shall support all requirements under this appendix, whether the system installation is on-premise or the system and services are supplied in a cloud configuration.

4.5 The system installation configuration shall be approved by Israel Railways' Cyber Division, after review and approval of the HLD and LLD architectures submitted by the supplier.

4.6 The supplier shall install the system, configure settings according to this appendix as well as Israel Railways' instructions, and integrate it at Israel Railways' sites, based on existing communications infrastructure and systems operating at each site, until full and proper operation in the production environment.

4.7 System implementation shall include integration with Israel Railways' systems via a data export and import API, following review, approval, and in accordance with requirements and instructions from Israel Railways' Cyber Division.

5. Physical Security and Safety

5.1 The supplier shall meet all Israel Railways' requirements regarding information security, including specific requirements for physical security, computing environment security, protecting documents and equipment at its facilities, and reliability checks for its employees.

5.2 Physical access to Israel Railways' information environment shall be restricted to those with a business need. The environment shall be protected against unauthorized access through entry and access control systems.

5.3 All components and devices in which Israel Railways' information is stored and processed shall be protected against environmental damage (flood, fire, etc.).

5.4 The supplier shall commit to managing an up-to-date list of service providers with access to information or workstations within Israel Railways, including their roles and authorizations to access information, as defined by Israel Railways, and to report any changes to Israel Railways. The list of service providers shall be approved by Israel Railways prior to the employment of the workers providing the services subject of this engagement.

5.5 Where relevant, the supplier shall plan and implement a security and safety solution for the entire project, from the issuance of the initial notice-to-proceed through to project completion, delivery of the system to Israel Railways, and throughout the maintenance period.

5.6 The solution shall comply with Israel Railways' security and safety requirements, applicable standards, and relevant regulations of the State of Israel, Israel Police, Ministry of Transport, Ministry of Infrastructure, and the Ministry of Public Security.

5.7 The solution shall be designed for the entire project and implemented according to the implementation plan and project phases defined in this document, and as further defined by Israel Railways during the course of the project.

5.8 The plan shall be aligned with the existing security and safety solutions currently in place at Israel Railways and shall be approved by Israel Railways' Security and Emergency Division prior to implementation.

5.9 The supplier shall present a solution to prevent access to system components during equipment maintenance, for its protection and control.

5.10 In addition to the provisions of this document, the supplier shall incorporate into the security and safety plan all relevant project-related comments and requirements presented by Israel Railways' security entities for implementation.

5.11 The security and safety plan shall include reference to the following topics:

5.11.1 Description of the overarching concept for security and safety;

5.11.2 Analysis of the current situation and how to integrate the proposed response into it;

5.11.3 Mapping and analysis of the gaps between the current situation and what is required for project implementation following the assessments.

5.12 Contents of the Project's Security and Safety Plan:

5.12.1 Writing and submission of a "Master Plan" (in a document that includes the concept, method, tasks and instructions, required achievements, timetables, registries, plans, photographs, maps and relevant supporting material, procedures, operating sequences, etc.).

5.12.2 Writing and submission of "field files" for all project components, such as:

5.12.3 Core facilities and system centers.

5.12.4 Communication and computer rooms.

5.12.5 Infrastructure facilities (power rooms, access facilities to communication infrastructure, etc.).

5.13 The implementation component of the plan in the areas of construction, infrastructure, systems, and the equipment that comprise the security and safety components, including:

5.13.1 Permanent and temporary fences;

5.13.2 Permanent and temporary barriers and gates;

5.13.3 Alarm systems;

5.13.4 Access control systems.

5.13.5 Various sensors as part of the building systems' control system (motion/volume detectors, flood, fire, smoke, door opening, window opening, power outage).

5.13.6 Communication rooms, communication cabinets, and local communication centers required to implement the security and safety plan.

5.13.7 The total requirements listed above in Section 5 – "Physical Security and Safety" constitute the minimum implementation requirements, and the supplier must present additional measures, based on its experience, to improve physical protection beyond the detailed requirements of this document.

6. Irregular Events

6.1 The supplier shall manage reports for detecting, tracking, reporting, and handling irregularities.

6.2 The supplier, or its designated Cyber Defense Trustee (see Section 3.2.5 above), shall report any information security issue discovered in the supplier's systems, within no more than 48 hours from the time of discovery.

6.3 Significant issues that directly or indirectly relate to Israel Railways' systems and/or the systems subject to this engagement shall be reported immediately to Israel Railways' Cyber Monitoring Center at the following phone number: 08-6533065.

6.4 The supplier's obligation to cooperate in cyber events includes:

6.4.1 In any event involving one of the supplier's employees, business interfaces, or where there is suspicion of involvement with a direct or indirect impact on the level of Israel Railways' cyber defense or the security of its interests.

6.4.2 In any violation, or suspected violation, of laws, instructions from issuing bodies, regulations, or cyber defense procedures.

6.4.3 In investigations of events or suspicions of security irregularities.

7. Ownership/Rights in Materials

7.1 It is hereby declared that the supplier has no rights, nor shall it have any rights, in any material delivered to it by Israel Railways for the purpose of performing the services under this agreement, and the supplier shall only be entitled to use such material within the framework of, and for the purpose of performing, the services and in accordance with all other provisions of this agreement.

7.2 It is hereby declared that Israel Railways shall be the sole owner of all rights in any material received, collected, prepared, and processed by the supplier in the framework of providing the services under this agreement, including the reports the supplier provides to Israel Railways.

Israel Railways shall be entitled to make any use of such materials as it deems fit, subject to applicable law.

7.3 The supplier shall declare that it waives its right to claim any proprietary right from Israel Railways, including intellectual property rights.

8. Non-Compliance with the Requirements of this Appendix

8.1 Non-compliance with the requirements of this appendix shall constitute a fundamental breach of the engagement agreement between the supplier and Israel Railways, and Israel Railways shall retain all remedies available to it under law and the engagement letters. In the event of breach of the contractual provisions of this appendix, Israel Railways shall be entitled to:

8.2 Partially or completely suspend operation of the system or services subjected to this engagement, at its discretion, and demand full compensation from the supplier for damages caused as a result of such action.

8.3 In any case, the supplier shall be required to immediately remedy the issues, at its own expense, following the breach of the agreement.

8.4 In addition to the foregoing, Israel Railways shall have the right to require the supplier to bear the cost of risk assessments performed by Israel Railways due to the supplier's failure to meet its obligations, as required above.

9. Termination of Engagement

9.1 Upon termination of engagement with the supplier, the supplier must perform the following actions:

9.2 Return to Israel Railways, or any entity on its behalf, all records, media, means, equipment, and components belonging to Israel Railways that were used for its work.

9.3 The supplier undertakes to destroy any information belonging to Israel Railways in its possession and which shall not be delivered to Israel Railways, all subject to applicable regulatory directives binding upon the supplier.

9.4 The supplier shall undertake that no documents, information, or items related to critical systems remain in its possession.

9.5 The supplier shall ensure that hard drives containing Israel Railways' information are erased in accordance with FIPS SP 800-88 – Guidelines for Media Sanitation, treating all information as "sensitive information".

9.6 If the supplier is required to continue holding such items, it shall be required to sign a declaration undertaking to transfer any information or component related to critical systems only to an authorized Israel Railways official and after receiving written approval from the Director of the Cyber Division at Israel Railways (Israel Railways' appointment over Critical Cyber Infrastructure).

Sincerely,

Company _____ Date _____

First name _____ Last name _____

ID _____ Signature _____