SUPPLIER's SECURITY TECHNICAL AND ORGANIZATIONAL MEASURES

Last Update Date: 5 May 2026

The Supplier maintains a set of Technical and Organizational Measures (TOMs) provided below to ensure that it complies with data protection regulations and protects data responsibly. These requirements may be updated at any time without prior reference or notice to Supplier.

Security Policies
The Supplier maintains and follows information security policies and practices that are integral to its business. These security policies apply to all its employees, including contractors, interns, and part-time employees. They are reviewed annually or whenever Customer deems fit to maintain the protection of the personal data.

Privacy by Design
The Supplier incorporates Privacy by Design principles at the earliest stage of software development to proactively address privacy risks and enhance privacy protection for customers.

Security/ Privacy Training
The Supplier ensures that all employees complete security and privacy awareness training annually and certify on an annual basis that they comply with the code of conduct, security, and data privacy policies. Additional policy and process training will be provided to the employees with granted administrative access to secure components, and handling of personal data, that is specific to their role within the operation and support of the service.

User Access Management
The Supplier maintains proper controls for requesting, approving, granting, modifying, revoking, and revalidating user access to systems and applications containing Personal Data. Only employees with a business-justified requirement can access the data located on servers, within applications, databases, and the ability to download data within the Supplier's network. The Supplier limits privileged access to employees for a limited period, and usage will be monitored and logged. All the access requests are approved based on role-based access and regularly reviewed for continuous business requirements. All systems must meet corporate security standards and employ security configurations and security hygiene practices to protect them against unauthorized access to the system resources.

Physical Security
The Supplier implements the physical security of its facilities including office premises and the server room. Access to the server room and controlled areas within the data room will be limited by job role and subject to authorized approval.

Risk Management
The Supplier has an established process of identifying, assessing, and mitigating risks associated with the processing of personal data. It implemented measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction and ensured compliance with data protection regulations.

Security Hardening
The Supplier ensures that all its systems and applications are configured to comply with its security standards and hygiene practices to reduce the attack surface thereby protecting them against unauthorized access to the system resources.

System and Network Security
The Supplier employs encrypted and authenticated remote connectivity to its computing environments. It implements network security measures including firewalls, remote access via virtual private networks, network segmentation, and detection of unauthorized or malicious network activity via security logging and monitoring.

End Device Security
The Supplier implements security measures on end-user devices to prevent security incidents that can compromise the confidentiality, integrity, and availability of data stored or processed by these devices. The security measures include system passwords, screen savers, antivirus software, firewall software, and appropriate patch levels. Further applications are implemented to detect and remediate end-user device compliance deviations.

Media Handling
The Supplier implements security measures to secure storage media from damage, destruction, theft, or unauthorized copying. The personal data that are stored on the portable media is secured via encryption and securely deleted when no longer needed. Similar measures are implemented for mobile computing devices.

The Supplier securely sanitizes physical media intended for reuse before reuse and will securely destroy physical media not intended for reuse.

Threat and Vulnerability Management
The Supplier maintains security measures to identify, manage, mitigate and/or remediate vulnerabilities within the its production environments. Security measures include:

- Patch management
- Threat management
- Anti-virus / anti-malware
- Regularly vulnerability scanning (all internal systems) and
- Periodic penetration testing (Internet-facing systems)

Security Incidents
The Supplier maintains an incident response plan and follows documented incident response policies including data breach notification to customers and supervising authority without undue delay where a breach is known or reasonably suspected to affect Personal Data.

Supplier Security Management
The Supplier implements security measures to ensure that third-party vendors, suppliers, and partners implement the same security standards and requirements thereby reducing the risk of security breaches and data loss involving third-party suppliers.

Change Controls and Validation
The Supplier maintains policies and procedures to manage risks associated with the changes to the systems and applications. Before implementation, changes to systems, networks, and underlying components will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing the impact, the expected outcome, the rollback plan, and documented approval by authorized personnel.

Business Continuity/ Disaster Recovery
The Supplier has defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry-standard practices, ensuring that its products and services remain functional in the event of a disruption or disaster.