

The header features a dark blue background with a silhouette of a group of people in a meeting. On the left, there is a large, stylized blue arrow pointing to the right. The title 'SUPPLIER INFORMATION SECURITY REQUIREMENTS' is written in white, bold, uppercase letters across the center.

SUPPLIER INFORMATION SECURITY REQUIREMENTS

Jabil delivers comprehensive design, manufacturing, supply chain and product management services for a wide array of industries. Aspiring to be the most technologically advanced and most trusted in our field, minimizing potential risks and protecting our information technology (IT) systems from compromise is a top priority for the Company. For this reason, Jabil understands that information security is an essential function of the business and has the same expectations of our Suppliers.

Suppliers who are engaged in providing products or services to Jabil Inc. and/or any of its affiliate entities (collectively, "Jabil"), who will have access to Jabil data and Jabil Systems are expected to abide by the following information security requirements as applicable to the Suppliers' business engagement with Jabil. These requirements set forth a minimum baseline of information security measures that Jabil expects of its Suppliers. As warranted to account for specific risks associated with the scope of services, additional information security requirements will be addressed in the Suppliers' Agreement with Jabil. The requirements outlined herein serve as a supplement to and do not supersede any information security related provisions set forth in the Agreement.



1. Definitions

Agreement: the governing contracts, purchase orders or other documented agreements between the Supplier and Jabil that set forth the scope of products and/or services being provided.

Confidential Information: has the meaning set forth in the Agreement for confidential information relating to Jabil, howsoever defined.

Customer Data: includes any information provided to Jabil by its' customers in the course of business.

Data Protection Laws: means all applicable laws, regulations and other legal requirements of any jurisdiction relating to privacy, data security, communications secrecy, Security Breach notification, or the processing of Personal Data.

In-Scope Data and Systems: Jabil Data, Jabil Systems, and/or Supplier Systems, as applicable.

Jabil Data: includes Personal Data, Customer Data, Confidential Information, and any other communications or business records that Supplier receives from Jabil, has access to, or otherwise processes for or on behalf of Jabil, in connection with the Agreement.

Jabil System: any hardware, software, media, network or other information technology ("IT") resource, whether physical or virtual, owned, licensed or operated by or on behalf of Jabil, whether on Jabil's premises or connected to or accessible from its network, other than any that are owned by Supplier or its Sub-processors.

Personal Data: any information relating to an identified or identifiable individual.

Security Breach: any breach of security leading to the accidental or unlawful access, destruction, loss, alteration, or unauthorized disclosure of Jabil Data and/or Jabil System(s).

Sub-processor: any service provider, affiliate or sub-contractor engaged by Supplier for purposes of fulfilling services in connection with the Agreement.

Supplier Personnel: Supplier's employees, contractors, officers, agents, and service providers.

Supplier Systems: Supplier operating systems, applications, hardware, software, media, or devices, whether physical or virtual, that are used to conduct business and facilitate communications with Jabil, that may store, process, or transmit Jabil Data, or are used to access Jabil Systems or Jabil Data, whether on Supplier's (or its affiliates') premises, connected to or accessible from Supplier's (or its affiliates') network(s), or hosted in the cloud.



2. Use Restrictions.

Supplier shall only access and use Jabil Data and Jabil Systems to fulfill its obligations under the Agreement or as v explicitly directed by Jabil, and for no other purposes.

3. Compliance with Data Protection Laws.

Supplier shall comply with all applicable Data Protection Laws in its performance of services for Jabil.

4. Information and System Security.

Supplier shall establish and maintain an information and system security program to protect Data and Systems from unauthorized access, loss, alteration, misuse, and other unintended activities or malicious threats (“Information Security Program”). Jabil reserves the right to terminate access to Jabil Data and Systems for any Supplier that (i) fails to implement an Information Security Program with adequate security measures, and/or (ii) where Supplier Personnel is suspected of negligence or misuse of Jabil Data or Systems. Access termination upon Jabil’s decision shall not mean a waiver for Supplier from its obligations of performance under the Agreement and shall not give rise to any additional claims from Supplier against Jabil.

4.1 Information Security Policy. Supplier shall have documented information security policies in place to ensure the confidentiality, integrity, and availability of all Data and Systems.

4.2 Access Management. In order to ensure proper management of access to In-Scope Data and Systems, Suppliers shall implement the following access controls:

- a. Appropriately restrict access (consistent with the principles of least privilege, need-to-know and separation of duties) to only those Supplier Personnel that require such access to In-Scope Data and Systems to perform the services described in the Agreement;
- b. Perform commercially reasonable background checks in compliance with applicable law on Supplier Personnel who will have access to In-Scope Data and Systems, ensuring that any such Supplier Personnel do not possess a criminal history that should reasonably disqualify them from having such access;
- c. Assign unique access/authentication credentials to each Supplier Personnel with authorized access to In-Scope Data and Systems;
- d. Prohibit sharing of assigned access/authentication credentials;
- e. Protect all access/authentication credentials in accordance with security best practices when stored for Supplier Systems and/or when stored for applications developed, provided or maintained by Supplier for Jabil to prevent unauthorized account access;
- f. Implement password security best practices, including but not limited to complex password requirements, account lockout controls, enforcing periodic password reset, and changing all default passwords on Supplier Systems before deploying any new hardware or software asset;
- g. In cases where remote access is authorized, ensure access to In-Scope Data and Systems requires multi-factor authentication (at least 2 factor) and session encryption;



- h. Promptly disable access privileges to In-Scope Data and Systems for any Supplier Personnel who are terminated or otherwise no longer need such access;
 - i. Conduct periodic reviews of access lists to In-Scope Data and Systems to ensure that access privileges have been appropriately provisioned and disabled;
 - j. Prohibit access to Jabil Data and Jabil Systems from unauthorized devices;
 - k. Where the services include the storage of Jabil Data in a multi-tenant service (e.g., SaaS, PaaS, IaaS), implement technical measures, including but not limited to hypervisor segmentation and database-level authentication and authorization controls, to ensure that third parties are unable to view, access, or acquire Jabil Data without authorization.
- 4.3 Encryption. Supplier shall encrypt all Jabil Data in transit or at rest using industry-standard encryption algorithms and secure key management protocols.
- 4.4 Removable Media. External removable media should not be used to view, store or transfer Jabil Data, unless there is a legitimate business need supporting the use of such devices. In such cases, Supplier shall restrict write function to and from external removable media, and ensure that all such removable media is encrypted at all times.
- 4.5 Secure Data Handling and Transmission. Where Supplier services involve accessing, storing and/or processing Jabil Data, Supplier shall implement secure data handling best practices, including but not limited to: need-to-know and limited privilege access restrictions, technical safeguards such as encryption, locked files and cabinets, and other electronic and physical security controls designed to prevent unauthorized access, misuse, loss or theft of Jabil Data.
- 4.6 Network Security. Supplier shall maintain appropriate network security measures, including but not limited to: firewalls to segregate Supplier's internal networks from the internet, risk-based network segmentation, and intrusion prevention or detection systems to alert Supplier to suspicious network activity.
- 4.7 Malicious Code Prevention. Supplier shall install anti-virus and malware protection software with up-to-date definitions and signatures on all Supplier Systems. Such software must be properly configured to protect against all known threats, including, but not limited to: viruses, worms, Trojans, rootkits, spyware and keystroke loggers.
- 4.8 Vulnerability Assessments. Supplier shall perform regular, periodic vulnerability scans and assessments on all Supplier Systems used to conduct business and/or communicate with Jabil, store, process or transmit Jabil Data, or connect to Jabil Systems, to identify all potential vulnerabilities on such systems. The vulnerability assessment process shall include steps to risk-prioritize and remediate identified security issues in a timely manner, including timely implementation of all manufacturer and developer-recommended security updates, maintenance of current operating system and application software versions and patches to operating systems and third-party software.
- 4.9 Configuration Management. Supplier shall maintain documented, secure baseline security configuration standards for Supplier Systems consistent with the concept of least functionality and monitoring for unauthorized changes or deviations from these baselines in deployed devices.



4.10 Logging and Security Monitoring. Supplier shall ensure that local logging has been enabled on all applicable systems and networking devices to capture detailed information necessary for security investigations. Supplier shall ensure that logs are analyzed for anomalous and suspicious activity to assist in the identification of potential Security Breaches.

4.11 Security in Development. Where applicable to the services provided, Supplier shall perform security testing on applications or application code provided to or developed on behalf of Jabil to ensure that the application or application code is secure.

4.12 Training and Awareness. Supplier shall provide ongoing training and awareness on the Information Security Program to all Supplier Personnel who have access to In-Scope Data and Systems.

5. Physical Security.

Access to applicable Supplier information processing facilities, such as server rooms, shall be restricted to Supplier Personnel with authorized access. Such restricted areas of Supplier facilities shall be subject to risk-appropriate access controls, such as requiring key cards and/or PINs for entry. Supplier shall maintain access control logs for all visitors entering such restricted areas and ensure that visitors to these areas are escorted by Supplier Personnel at all times. Supplier shall periodically review audit trails of access to these restricted areas.

6. Subcontracting.

If for any reason sub-contractors are engaged, Jabil requirements for sub-contracting must be fulfilled including assurance that all sub-contractors implement and maintain appropriate security measures in accordance to Jabil's information security requirements.

7. Compliance Monitoring.

Supplier shall regularly test and monitor the effectiveness of the security practices and procedures of their Information Security Program, and will evaluate and adjust its Information Security Program and information security safeguards in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that Supplier knows or reasonably should know may have a material effect on its Information Security Program and information security safeguards.

8. Incident Response.

Supplier shall have in place a security incident response plan for identifying, reporting and appropriately responding to known or suspected security incidents impacting In-Scope Data and Systems. In the event of a Security Breach, Supplier shall notify Jabil within 48 hours of discovery. Supplier shall maintain and periodically test its incident response plan outlining the steps to be taken in the event of a Security Breach, including notification to Jabil and coordination of investigation and remediation activities with Jabil. Supplier shall cooperate with Jabil in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required.



9. Disaster Recovery Planning.

Where the services rendered involve the on-going processing and maintenance of Jabil Data and/or Jabil Systems, Supplier shall maintain and periodically test disaster recovery plans to ensure the ongoing availability of such services. Disaster recovery plans should at a minimum, be based on industry standards and best practices as defined by the Disaster Recovery Institute or the Business Continuity Institute.

10. Data Retention and Destruction.

If Supplier is required by law to retain archival copies of Jabil Data for regulatory purposes this data backup must be stored in a physically secured facility and must be stored in an encrypted format. Encryption keys must not be stored on the system storing the backup. At Jabil's direction, at any time, and in any event upon termination or expiration of business agreements, except to the extent required by law, Supplier shall immediately (or consistent with another time frame set forth by Jabil) return to Jabil or, if so directed by Jabil, destroy and certify the destruction of any and all Jabil Data consistent with NIST Special Publication 800-88.

11. Cyber Insurance.

Supplier shall procure and maintain, at its own expense, Cyber Risk insurance in such monies and with such limits and deductibles customary for its business and industry. At a minimum, Supplier agrees to carry full Cyber Risk insurance coverage for all activities reasonably connected with the Agreement. Upon Jabil's request, Supplier shall supply to Jabil certificates of cybersecurity insurance evidencing such insurance coverage.

12. Right of Audit by Jabil.

Without limiting any other audit rights of Jabil, Jabil shall have the right to review Supplier's data privacy and information security program prior to the commencement of Services and from time to time during the term of the Agreement. During the providing of the Services, on an ongoing basis from time to time and without notice, Jabil, at its own expense, shall be entitled to perform, or to have performed, an on-site audit of Supplier's data privacy and information security program. In lieu of an on-site audit, upon request by Jabil, Supplier agrees to complete, within thirty (30) days of receipt, an audit questionnaire provided by Jabil regarding Supplier's data privacy and information security program.

13. Audit Findings.

Supplier shall implement any required safeguards as identified by Jabil or by any audit of Supplier's data privacy and information security program.