INFORMATION SECURITY CONTROL REQUIREMENTS

1. Introduction

Micron management is committed to ensuring the security of Micron Data.

Scope:
These Information Security Control Requirements apply to all suppliers who handle, process, or provide Micron Data.

Suppliers for Micron (hereinafter called "**Supplier**") must implement administrative, physical, and technical safeguards to protect any tangible or intangible Micron-owned or supplied item that Supplier has access to, is provided with, or stores for Micron ("**IT Assets and Micron Data**") from unauthorized access, acquisition, disclosure, destruction, alteration, accidental loss, misuse, or damage, using best known methods that are no less rigorous than industry practices, including information security environment and governance approaches, aligned to the International Organization for Standardization (ISO) 27001 "Information security, cybersecurity and privacy protection – Information security management systems – Requirements" standard, or its successor.

These Information Security Control Requirements are not intended to replace Supplier's standard policies and procedures but are intended to address the minimum controls that Supplier must have in place as part of Supplier's standard policies and procedures. In accordance with these requirements, Supplier must maintain multiple control domains as discussed further below.

2. Definitions

"**IT Assets**" include without limitation; computer equipment (e.g., laptops and desktops), mobile devices (e.g., mobile/smartphones, tablets), hardware, software, operating systems, storage media, network resources, identities (e.g., providing access to electronic mail, online browsing, file transfer protocols, and other IT services), and computing environments (e.g., development, test, stage, production, and backup application environments) made available by Micron to its directors, officers, team members, contractors, and other third parties for the purpose of conducting Micron's business;

"**Micron Data**" includes intellectual property and other confidential and proprietary data owned by Micron or entrusted to Micron by third parties; and

"**Personal Data**" is a subset of Micron Data, and must mean any information relating to an identified or identifiable natural person; meaning one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural, or social identity; and as defined by applicable data protection laws.

"**Micron Incident**" An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information (Micron data) the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

"**Processing**" is collectively the creation, collection, possession, disposal, handling, processing, receipt, transmission, storage, retention, and disclosure of Micron Data.

3. Information Security Policies

Suppliers must manage and sustain a documented set of security policies and procedures that govern the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of Micron information, assets, and associated services.

Supplier must maintain comprehensive protection and clear accountability for IT Assets through an information security policy framework that aligns with NIST Cyber Security Framework, ISO27001/27002, or any superseding industry accredited standard or framework.

Supplier's information security policies and procedures must cover, at a minimum:

a) Supplier's commitment to information security.

b) Information classification, labeling, and handling, including segregating Micron Data from information of Supplier or its other clients.

c) Acceptable use of IT Assets (such as using it only for agreed purpose with controls enabled), including computing systems, networks, and messaging.

d) Information security incident management, including breach notification and cooperation and procedures for collecting evidence.

e) Host and network-based security controls, including anti-virus, Intrusion Detection System /Intrusion Prevention System (IDS/IPS), firewalls, and systems hardening requirements.

f) Authentication requirements for end users, administrators, and systems.

g) Access controls, including remote access and periodic reviews of access rights.

h) Logging and monitoring of Supplier's production environment, including physical and logical access to IT Assets that process or store Personal Data.

i) Providing appropriate privacy and information security training to employees.

j) Endpoint security, cryptographic techniques used to secure data at rest, in transit and in use.

k) Physical security and environmental security controls to protect physical assets.

l) Data lifecycle management, records retention and provide such policies and documentation for practices to Micron upon request.

Upon reasonable notice to Supplier, Micron may request, review, and inspect such information security policies and procedures and request reasonable changes to such plan.

4. Standard of Care

Supplier acknowledges and agrees that during its engagement by Micron, Supplier may create, receive, or have access to Micron Data including Personal Data. Supplier must comply with the terms and conditions set forth in this Standard Processing Micron Data and be responsible for any unauthorized or unlawful Processing by Supplier or a third party of Micron Data under its control.

Supplier must be responsible for, and remain liable to, Micron for the actions and omissions of its users and contractors or data processors who have access to Micron Data and must treat the Micron assets in at least as protective of a manner as Supplier protects its own data. In recognition of the foregoing, Supplier agrees and covenants that it must:

a) keep and maintain all Micron Data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure.

b) not create, collect, receive, access, or use Micron Data in violation of law.

c) use and disclose Micron Data solely and exclusively for the purposes for which the Micron Data or access to it, is provided pursuant to the terms and conditions of this standard, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Micron Data for Supplier's own purposes or for the benefit of anyone other than Micron, in each case, without Micron's prior written consent.

d) restrict use of Micron Data in AI chatbot, search engines, or tools that may result in unauthorized disclosure.

e) not, directly, or indirectly, disclose Micron Data to any person other than Supplier without Micron's prior written consent; and require, in writing, all Supplier's contractors or data processors who handle Micron Data to comply with the obligations in this document.

Supplier must maintain a technology and cybersecurity risk management program with a minimum annual review cadence. Supplier must maintain risk management processes to regularly identify, assess, and manage risks to Micron Data and IT Assets.

5. Personal Data Protection and Handling Requirements

a) **Confidentiality of Micron Personal Data.** Supplier shall maintain the confidentiality of all personal data collected in the process of doing business with Micron. "**Personal Data**" is information that alone, or in combination with other information, is reasonably capable of identifying a specific person (for example, name, contact information, work location, purchase history, description, preferences, photograph, voice recording, etc.). Such information collected is "**Micron Personal Data**."

b) **Data Minimization and Purpose Limitation.** Supplier shall limit the collection and use of Micron Personal Data to only those legitimate business purposes reasonably necessary to perform its rights and obligations related to Supplier's role in providing Micron goods or services. No other use of Micron Personal Data is allowed without prior written permission from Micron.

c) **Pass Down Privacy Obligations.** Supplier shall regularly instruct its employees, contractors or other third parties handling Micron Personal Data on the obligation to keep Micron Personal Data confidential and to limit its collection and use to only those processes necessary to provide Micron goods and services. Supplier must contractually obligate all subcontractors or sub-processors handling Micron Personal Data to these same data protection obligations.

d) **Privacy.** Supplier shall cooperate with Micron in complying with lawful data subject privacy rights requests in a timely and transparent manner. Supplier shall provide a copy of, correct, or delete Micron Personal Data in its records and data repositories upon the written direction of Micron, limited only by its lawful obligation to retain such Micron Personal Data in its original form, and if so retained, only for so long as the legal requirement persists, and thereafter it shall be deleted. Supplier shall not share or sell any Micron Personal Data without Micron's prior written authorization.

e) **Privacy Incident Notice and Cooperation.** Supplier shall timely notify and cooperate with Micron's investigation of any unauthorized access, collection, use, alteration, sharing, duplication, or destruction of Micron Personal Data Information. Notice of incidents involving Micron Personal Data Information must be sent to security@micron.com.

f) **Proof of Compliance.** Supplier must timely provide adequate written assurances of its compliance with these Personal Data Protection and Handling Requirements upon Micron's request. These obligations to protect Micron Personal Data must remain in effect for so long as Supplier or its agents hold Micron Personal Data, regardless of whether Supplier is currently providing Micron goods or services.

6. Human Resource Security

Supplier must maintain a multi-layer human resources security program. Employees are required to have a unique form of identification (e.g., badge), to sign a non-disclosure agreement, and to annually review

and acknowledge a Supplier's Code of Ethics or equivalent. Employees are also required to complete a comprehensive background check that may include fingerprinting, criminal record, credit history, drug screening, and reference background checks, as permitted by law.

Supplier must require that all employees complete annual information security training regarding the appropriate use and handling of confidential information and customer data and must maintain a record of employees who completed such training. Supplier must require that all employees acknowledge their understanding and compliance with Supplier's information security policies.

7. System Acquisition, Development and Maintenance

Supplier must maintain a secure development methodology that incorporates security throughout the development lifecycle, including application development policies, security training of application developers, and secure code reviews and penetration tests of externally facing web applications.
Supplier must do the following as part of its system acquisition, development, and maintenance processes:

a) develop and configure applications and databases in a manner which is designed to protect the confidentiality, integrity, and availability of Micron Data.

b) develop web applications in accordance with security best practices (e.g., Open Worldwide Application Security Project [OWASP] Top Ten), and reasonable steps to verify that web applications are configured to protect against the OWASP Top Ten vulnerabilities.

c) implement separate environments for production, development, and test.

d) on at least an annual basis conduct secure code review, including open-source reviews, and penetration testing or equivalent, using automated scanning tools and manual analysis. Supplier must ensure that identified vulnerabilities are remediated in accordance with documented policies that prioritize remediation based on risk; and

e) manage source code in accordance with documented procedures that restrict access and verify the integrity of code prior to deployment.

8. Asset Management

Supplier must maintain an information security program designed to educate employees on how to classify, label, handle, and dispose of information and all types of media, from creation through processing, storage, and disposal.

Supplier must instruct its employees on the appropriate methods of handling information, such as distribution, discussion, mailing, copying, faxing, and storage, for each type of information.

Supplier must:

a) maintain an inventory of IT Assets and manage the associated asset lifecycle. Ensure that Assets are used for the agreed purpose only.

b) follow industry standards and applicable regulations when handling, processing, and storing Micron Data, including Personal Data.

c) implement procedures to sanitize or securely destroy media in accordance with current industry standards such as Department of Defense, NIST 800-88 or equivalent, or its superseding standard.

d) Upon conclusion or termination of Supplier's work for Micron or upon Micron's request, the Supplier must sanitize and securely destroy (or at Micron request, return to Micron) all copies of all Micron information, including all backup and archival copies, in any electronic or non-electronic form, and must

provide a certificate signed by an officer of Supplier that certifies such return or destruction in detail acceptable to Micron.

9. Access Control

Supplier must maintain reasonable access policies and controls (i.e. identity and access management systems and authentication mechanisms) to ensure that only authorized personnel are granted access to Micron Data. Access requests must be tracked and authorized through a formal access management system. Access must be granted based on the concepts of least privilege and separation of duties and must be limited to those with a business need.

Supplier must do the following as part of its access controls:

a) identifiers must be utilized to logically restrict access such that other Supplier clients cannot view or access Micron Data.

b) revoke access promptly following termination or in a commercially reasonable amount of time following internal transfer to a position where such access is no longer needed.

c) review user accounts and their privileges on a regular basis, to verify that access is appropriate to job role, and remove access that is no longer required.

d) restrict the use of privileged accounts to authorized employees performing system administration or security administration activities.

e) collect, monitor, and retain logs so that access to Micron Data can be traced.

f) only use system accounts for system-to-system communication and configure them to prevent interactive logins from users; and

g) implement secure and encrypted solutions for remote access to IT Assets that are restricted to only authorized individuals.

h) collect, monitor, and retain logs so that access to Micron Data can be traced.

10. Cryptography

Supplier must maintain a cryptography policy that aligns to the current revision of Federal Information Processing Standard (FIPS) 140 and applies to all cryptographic techniques used to protect Micron Data and IT Assets. This includes industry standard algorithms and key lengths, requirements for key lifecycle management, and requirements for key and certificate verification.

Supplier must maintain policies, processes, and technologies to encrypt Micron Data in transit and at rest. This includes tapes, removable media devices, laptops, network file transfers, and web transactions. Encryption must be provided through commercial grade, industry-standard cryptographic algorithms, protocols, and key strengths.

Supplier must work with Micron to implement reliable and secure electronic data transfer methods that satisfy Micron’s requirements.

11. Physical and Environmental Security

Supplier must maintain physical security measures to control and restrict physical access to IT Assets and include full-time, professional security personnel, cameras covering access points into the secure and restricted/critical spaces dedicated to the processing and storage of Micron data, and parking areas, intrusion detection and alerting capabilities, appropriate access control systems, visitor management and logs. Infrastructure and environmental controls which may include but not limited to, power, temperature

and humidity monitoring, fire suppression systems, Universal Power Supply (UPS), emergency or back-up systems consistent with local laws and industry standards.

All data centers used to store Micron Data must only reside in data centers in Micron approved geographies. Notwithstanding any other provision in the agreement signed between Supplier and Micron, technology support services, including but not limited to; software development, back-office operations, quality assurance, and production support, may be performed from outside of North America. Supplier must maintain controls no less stringent than the local regulations for operations outside of the United States of America.

12. Operations Security

Supplier must maintain an appropriate security operations program designed to protect Micron Data and IT Assets that must be tested and continuously improved. Supplier must maintain the following security controls as part of this program:

a) protection against data loss, malware, malicious intrusions, or malicious downloads.

b) update anti-malware and antivirus signatures in a timely manner.

c) an intrusion detection and prevention system (IDS/IPS).

d) monitoring for unauthorized access, connections, devices, and software.

e) a security vulnerability program that includes regular network vulnerability scans, patch management, and remediation of identified security vulnerabilities prioritized based on risk.

f) collection and correlation of security events from IT Assets and sensors to detect and address security events (e.g., Security Incident and Event Management [SIEM]).

g) implementation of systems and devices using standardized, hardened builds.

h) monitoring and control of employee connections to the internet; and

i) backing up Micron Data as required to meet Supplier's continuity requirements and recovery time objectives in accordance with tested backup and restoration procedures, and protection of backups from loss, damage, and unauthorized access.

13. Business Resiliency

Supplier must maintain a comprehensive business continuity and disaster recovery program, which includes technology and business operational recovery. Supplier must focus both on preventing outages through redundancy of telecommunications, systems, and business operations, and on recovery strategies in the event of loss. The business continuity and disaster recovery program must adhere to legal and regulatory requirements as applicable to Supplier as a provider of the Services.

Disaster recovery process must include training, planning, and testing critical technology and business operational recovery at least annually. Business impact analysis must be performed, and recovery strategies developed for different threat scenarios to include loss of premises, people, technology, or supply chain. Supplier must maintain recovery plans that may be executed during or after an event and, on request, must share those plans with Micron to prove systems affected by continuity events can be restored. As an outcome of the Supplier's business continuity and disaster recovery program, the Supplier's Recovery Time Objective ("**RTO**") and Recovery Point Objective ("**RPO**") should align with Micron's RTO/RPO and function as the basis for a service level agreement between parties.

14. Information Security Incident Management

Supplier must maintain and regularly test its documented, comprehensive cyber incident response plan that is designed to identify potential threats, assess any risk exposure, report risks to management, and protect business operations. Supplier must do the following as part of its information security incident management plan:

a) assess security events and suspected incidents.

b) responds by containing and mitigating incidents.

c) identify actions to minimize the risk of similar incidents from reoccurring; and

d) conduct investigations in accordance with legal requirements for preserving evidence.

e) identify lessons learned to improve overall incident management capabilities.

15. Data Incident or Breach Notification

Supplier must promptly notify Micron at security@micron.com and in accordance with any applicable contractual or legal requirements, vulnerabilities if any such that Micron Data is lost, destroyed, becomes damaged, corrupted, unusable, or is accessed (e.g., viewed, copied, altered, disclosed, or transmitted) by an unauthorized individual or entity. Supplier must restore such Micron Data at its own expense. Supplier must notify Micron without undue delay in accordance with any applicable laws, rules, or regulations, but in any event not later than 72 hours after becoming aware of a security incident, unauthorized, or unlawful Processing of Micron Data. Immediately following any unauthorized or unlawful Micron Data Processing, the parties must cooperate with each other to investigate the matter. Supplier must cooperate with Micron in Micron's handling of the matter, including:

a) assisting with any investigation.

b) providing Micron with logical, physical, and remote access to any facilities and operations affected as appropriate.

c) facilitating interviews with the Supplier's employees, former employees, contractors, sub-processors, and others involved in the matter; and

d) making available all relevant records, logs, files, data reporting, and other materials required to comply with all privacy and data protection requirements or as otherwise reasonably required by Micron.

Supplier must not inform any third party of any security incident without first obtaining Micron's prior written consent, except where law or regulation requires otherwise. Additionally, Supplier agrees that Micron has the sole right to determine whether to provide notice of the incident to any affected individuals, regulators, law enforcement agencies, or others, as required by law or regulation or in Micron's discretion, including the contents and delivery method of the notice; and whether to offer any type of remedy to individuals affected by the incident, including the nature and extent of such remedy.

Supplier must cover all reasonable expenses associated with the performance of the obligations under this section. Supplier must also reimburse Micron for reasonable expenses Micron incurs when responding to and mitigating damages, to the extent Supplier caused, through action or inaction, the incident, including all costs of notice and any remedy as set out in this section. Supplier agrees to maintain and preserve all documents, records, and other data related to any security incident. Additionally, Supplier agrees to fully cooperate at its own expense with Micron in any litigation, investigation, or other action deemed necessary by Micron to protect Micron's rights relating to the use, disclosure, protection, and maintenance of Micron Data.

16. Communications Security

Supplier must maintain reasonably appropriate network security and information transfer controls that are designed to safeguard the confidentiality and integrity of data passing over public or wireless networks, ensure the protection of IT Assets, including firewalls, intrusion detection and prevention systems, anti-malware, proxy servers, and secure file transfer technologies.

Supplier must: use multi-factor authentication for remote virtual private network (VPN) access and administration of specific core infrastructure components based upon risk; design all networks to protect network integrity and separate network zones with a firewall or equivalent to restrict traffic to only authorized business traffic; and review firewall policies annually.

17. Supplier Relationships

Supplier must maintain a third-party risk management program that includes regular reviews of Supplier's suppliers that process Micron Data, including Personal Data, using a comprehensive risk assessment derived from Supplier security policies, ISO 27001, and other industry standard practices.

Micron acknowledges Supplier may leverage cloud service providers in connection with the services provided under the agreement signed between Supplier and Micron. Supplier is responsible for the services performed by such suppliers that process or store Micron Data to the same extent as if Supplier had performed the service itself and must have written agreements with suppliers that process or store Micron Data that are consistent with Supplier's information security obligations as applicable to the services performed by such suppliers.

18. Security Assurances and Assessments

Annually, upon Micron's request, Supplier must provide assurance, in the form ISO 27001 certificate, SOC 2 Type II report or any superseding or comparable standard report, demonstrating appropriate information security safeguards and controls are in place.

Upon Micron's written request, to confirm compliance with this standard, as well as any applicable laws and industry standards, Supplier must promptly and accurately complete an information security questionnaire provided by Micron, or a third party on Micron's behalf, regarding Supplier's business practices and information technology environment in relation to all Micron Data being handled and/or services being provided by Supplier to Micron pursuant to this standard. Supplier must fully cooperate with such inquiries. Micron shall treat the information provided by Supplier in the security questionnaire as Supplier's confidential information.

Should Micron conduct an on-site or remote security assessment (a "**Security Assessment**") of Supplier's sites, facilities, systems (including infrastructure, software, people, procedures, and data) and system components through or from which the Services are provided, including those of all of Supplier's suppliers, subcontractors and subservice organizations, Micron must conduct the Security Assessment with minimum inconvenience and disruption to Supplier's operations, during normal business hours, no more frequently than annually, and with at least 90 days written notice. Security Assessment hours and audit hours incurred by Supplier must be provided at no charge to Micron. Micron may not review; data or information of Supplier's other customers or clients, any of Supplier's proprietary data (information that could compromise the controls used to safeguard both Supplier and Supplier's clients' data), or any other confidential information that is not relevant for the purposes of the Security Assessment. Additionally, Micron may not re-perform or observe control testing or execution.

Security Assessments must be of reasonable length and mutually agreed on scope and Micron shall first look to the existing SOC 2 Type II Service Auditor's Reports, ISO 27001 certificate or any superseding or comparable standard report, demonstrating appropriate information security safeguards and controls are in place to gain reasonable assurance over the controls used to safeguard Micron Data. Micron must not have logical access to Supplier's networks and systems, nor unrestricted physical access to Supplier's

facilities and personnel. Supplier must make available security personnel to address Micron's reasonable questions. Micron must not use any Supplier competitors (or any significant subcontractor of Supplier under the agreement signed between Supplier and Micron), nor Supplier's third-party service auditor or ISO 27001 auditor, to conduct such assessments. Any third-party representatives of Micron must execute confidentiality and non-disclosure agreements and comply with Supplier's security and confidentiality requirements. Micron shall maintain safeguards against the improper disclosure of security information received from Supplier, using at a minimum, the same precautions Micron uses in maintaining its own information, data, and records. Micron shall not disclose any security information received from Supplier to any third party without Supplier's prior written approval, unless required by law (in such cases, Micron shall notify Supplier in writing of the request). If Micron identifies a material risk or deficiency during a Security Assessment and the parties agree that such risk requires remediation, Micron and Supplier must promptly and mutually agree on a remediation plan and Supplier must use commercially reasonable efforts to remediate any deficiencies or material risks found.