

SUPPLIER INFORMATION SECURITY CONTROL REQUIREMENTS

Contents

1.	Introduction.....	1
2.	Definitions	2
3.	Information Security Policies.....	2
4.	Standard of Care.....	3
5.	Personal Data Protection and Handling Requirements	4
6.	Human Resource Security	5
7.	Responsible Use of Artificial Intelligence	5
8.	System Acquisition, Development and Maintenance.....	6
9.	Asset Management.....	6
10.	Access Control.....	7
11.	Cryptography	7
12.	Physical and Environmental Security.....	8
13.	Operations Security	8
14.	Business Resiliency.....	9
15.	Information Security Incident Management	9
16.	Data Incident or Breach Notification	10
17.	Communications Security.....	10
18.	Supplier Relationships	11

1. Introduction

Micron management is committed to ensuring the security of IT Assets and Micron Data (as defined below).

Scope:

These supplier information security control requirements (“**Information Security Control Requirements**”) apply to all suppliers who handle, process, or provide IT Assets and Micron Data or provide solutions or platforms for the handling or processing of IT Assets and Micron Data.

Suppliers for Micron (hereinafter called “**Supplier**”) shall implement administrative, physical, and technical safeguards to protect any 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 shall have in place as part of Supplier's standard policies and procedures. In accordance with these requirements, Supplier shall maintain multiple control domains as discussed further below.

This document outlines the expectations and requirements for information security and risk management between Micron and its suppliers. Importantly, compliance with international standards—specifically ISO 27001 and SOC 2 Type II—serves as a practical way to meet the requirements set forth in this document. These recognized certifications and assessment frameworks demonstrate that robust security controls, risk management practices, and data protection measures are in place to safeguard Micron's data, including when third-party providers are involved. This document further details the protocols for ongoing security evaluations and emphasizes a collaborative approach to address and remediate any identified risks or deficiencies, ensuring full alignment with Micron's information security standards. In circumstances involving Micron's more sensitive information, Micron may, in its discretion, impose additional security requirements.

2. Definitions

- a) **"Incident"** means an occurrence that actually or potentially compromises the confidentiality, integrity, or availability of an information system or the Micron Data it processes, which includes any data critical to Micron operations. This includes any unauthorized access, use, disclosure, disruption, modification, or destruction of Micron Data, or any violation or imminent threat of violation of Micron's security policies, procedures, or acceptable use policies.
- b) **"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.
- c) **"Micron Data"** includes intellectual property and other confidential and proprietary data owned by Micron or entrusted to Micron by third parties.
- d) **"Personal Data"** is a subset of Micron Data, and means 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.
- e) **"Processing"** is collectively the creation, collection, possession, disposal, handling, processing, receipt, transmission, storage, retention, and disclosure of Micron Data.

3. Information Security Policies

Suppliers that possess a current ISO/IEC 27001 certification and/or SOC 2 Type II attestation may be deemed to meet certain Micron security requirements, provided the certifications:

- Are issued by a recognized and accredited body;
- Remain valid and up to date; and
- Encompass in-scope systems, processes, and controls materially relevant to Micron services or data.

Micron reserves the right, at its sole discretion, to evaluate the sufficiency of such certifications. In such cases, the Supplier may be exempt from duplicative evidence submissions under Micron's security assessment process.

In lieu of the above, Suppliers should maintain and implement documented security policies and procedures that govern the receipt, transmission, processing, storage, access, and protection of Micron Data, IT Assets, and associated services being provided by them. Supplier policies and procedures must align with NIST Cyber Security Framework, ISO 27001/27002, or any superseding industry accredited standard or framework.

These policies must address, at a minimum, the following control areas:

- Information security governance and accountability
- Information classification, labeling, and handling (including data segregation)
- Acceptable use of IT systems (restricted to agreed purposes with technical and administrative controls)
- Incident detection, response, and breach notification (including defined roles, evidence preservation, and Micron cooperation protocols)
- Network and host security (e.g., anti-malware, firewalls, IDS/IPS, system hardening)
- Authentication and access management (including periodic user access reviews)
- Logging and monitoring of systems processing Micron data (physical and logical)
- Security and privacy awareness training for employees
- Data protection through encryption (at rest, in transit, and in use)
- Physical and environmental security of facilities
- Data retention, disposal, and lifecycle policies (available upon request)

4. Standard of Care

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

Supplier shall be responsible for, and remain liable to, Micron for the actions and omissions of its users, employees, contractors and/or data processors who have access to Micron Data and must have written agreements with all parties who will have access to Micron Data or IT Assets. In recognition of the foregoing, Supplier agrees and covenants that it shall:

- 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 document, 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 chatbots, search engines, or tools that may result in unauthorized disclosures.
- e) not, directly, or indirectly, disclose Micron Data to any person other than Supplier's employees, contractors and/or data processors 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.
- f) ensure that if any employees of, or subcontractors to, Supplier are provided with access to any Micron systems or facilities, Micron Data, or IT Assets, such persons shall comply with all applicable policies and processes of Micron that Micron communicates to Supplier and shall not access or attempt to access any Micron computer system, electronic file, software, or other electronic services other than those specifically required to provide the services. If a Supplier employee or contractor is terminated or will no longer be providing services to Micron, the Supplier shall notify Micron at least twenty-four (24) hours in advance to terminate the employee's or contractor's access to Micron Data and IT Assets (e.g., badge access, login, etc.).

Supplier shall maintain a technology and cybersecurity risk management program with a minimum annual review cadence. Supplier shall 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 Personal Data.** Supplier shall maintain the confidentiality of all Personal Data collected in the process of doing business with Micron.
- b) **Data Minimization and Purpose Limitation.** Supplier shall limit the collection and use of 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 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 Personal Data on the obligation to keep Personal Data confidential and to limit its collection and use to only those processes necessary to provide Micron goods and services. Supplier shall contractually obligate all subcontractors or sub-processors handling 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 Personal Data in its records and data repositories upon the written direction of Micron, limited only by its lawful obligation to retain such 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 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 Personal Data Information. Notice of Incidents involving Personal Data Information must be sent to security@micron.com.
- f) **Proof of Compliance.** Supplier shall timely provide adequate written assurances of its compliance with this section (Personal Data Protection and Handling Requirements) upon Micron's request. These obligations to protect Personal Data must remain in effect for so long as Supplier or its agents hold Personal Data, regardless of whether Supplier is currently providing Micron goods or services.

6. Human Resource Security

Supplier shall 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 shall 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 shall require that all employees acknowledge their understanding and compliance with Supplier's information security policies.

7. Responsible Use of Artificial Intelligence

To ensure the responsible adoption and use of artificial intelligence ("AI") within Micron's business operations, Supplier shall comply with the following with respect to any of Supplier's use of AI in connection with its support to Micron:

- a) Engage in transparent use of AI, which may include implementing labeling or other clear designation for any AI-generated materials or outputs provided to Micron.
- b) Provide notice to Micron of any use of AI in processing Personal Data associated with Micron's human resources operations.
- c) Receive prior written consent from Micron for any use of Micron Data for training Supplier's or its contractors' AI models or enrichment of Supplier's or its contractors' data sets.
- d) When analyzing, processing, or developing work or services for Micron or with Micron Data, only utilize Micron approved AI tools for data processing and handling, and Supplier will not utilize unauthorized or public AI tools and/or language models for Micron confidential or non-public data. To confirm a current list of approved Micron tools, contact AI_OPS_CORE@micron.com.
- e) Provide transparency into Supplier's or its contractors' AI quality, regulatory, and compliance controls. Upon Micron's reasonable request, Supplier will provide Micron responsive information relating to Supplier's AI quality, regulatory, and compliance controls, including for example controls directed to bias testing, confirmation-bias controls, performance monitoring, and other such controls as may be necessary to comply with applicable laws, rules, or regulations.

8. System Acquisition, Development and Maintenance

Supplier shall 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 shall 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) at least on an annual basis conduct secure code review, including open-source reviews, and penetration testing or equivalent, using automated scanning tools and manual analysis. Supplier shall ensure that identified vulnerabilities are remediated in accordance with documented policies that prioritize remediation based on risk.
- e) manage source code in accordance with documented procedures that restrict access and verify the integrity of code prior to deployment.
- f) if Supplier or a Supplier subcontractor uses a website, portal, and/or other technology to provide any service, each year, Supplier will engage, at its own expense, an independent third party to perform a penetration test. Supplier shall promptly remediate any critical findings by such third party. Micron will have the right to validate that such tests were completed and any findings remediated.

9. Asset Management

Supplier shall maintain an information security program designed to educate employees on how to classify, label, handle, and dispose of information and all types of media, throughout the data lifecycle.

Supplier shall 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 shall:

- a) maintain an inventory of IT Assets and manage the associated asset lifecycle.
- b) ensure that IT Assets are used for the agreed purpose only.
- c) follow industry standards and applicable regulations when handling, processing, and storing Micron Data, including Personal Data.

- d) implement procedures to sanitize or securely destroy media in accordance with current industry standards such as ISO 27001 or CMMC Level 2, or its superseding standard.
- e) Upon conclusion or termination of Supplier's work for Micron or upon Micron's request, the Supplier shall sanitize and securely destroy (or at Micron request, return to Micron) all copies of all Micron Data, including all backup and archival copies, in any electronic or non-electronic form, and shall provide a certificate signed by an officer of Supplier that certifies such return or destruction in detail acceptable to Micron.

10. Access Control

Supplier shall maintain reasonable access policies and controls (i.e. identity and access management systems and authentication mechanisms) to ensure that only authorized employees 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 shall 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 an employee's or contractor's termination or in a commercially reasonable amount of time following internal transfer of a Supplier employee 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.
- g) implement secure and encrypted solutions for remote access to IT Assets that are restricted to only authorized individuals.

11. Cryptography

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

12. Physical and Environmental Security

Supplier shall maintain:

- a) 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,
- b) intrusion detection and alerting capabilities,
- c) appropriate access control systems, visitor management, and logs.
- d) Infrastructure and environmental controls to protect against destruction, loss or damage of IT Assets due to human error, potential environmental hazards, such as fire and water damage, or technological failures, 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.
- e) Supplier shall ensure physical assets are protected by, at minimum, active supervision, lock and key mechanism, and clear desk policies.

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 shall maintain controls no less stringent than the local regulations for operations outside of the United States of America.

13. Operations Security

Supplier shall maintain an appropriate security operations program designed to protect Micron Data and IT Assets that must be tested and continuously improved. Supplier shall 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 Supplier employee connections to the internet.
- 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.
- j) operating a secure change management process to install, configure, operate, and maintain information systems (e.g., workstations, servers, networks and applications) storing Micron Data and IT Assets.

14. Business Resiliency

Supplier shall maintain a comprehensive business continuity and disaster recovery program, which includes technology and business operational recovery. Supplier shall 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 goods or 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 shall maintain recovery plans that may be executed during or after an event and, on request, must share evidence of their existence.

15. Information Security Incident Management

Supplier shall 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 shall 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.
- d) conduct investigations in accordance with legal requirements for preserving evidence.
- e) identify lessons learned to improve overall Incident management capabilities.

16. Data Incident or Breach Notification

Supplier shall promptly notify Micron at security@micron.com and in accordance with any applicable contractual or legal requirements, of any vulnerabilities that results in Micron Data being lost, destroyed, damaged, corrupted, unusable, or is accessed (e.g., viewed, copied, altered, disclosed, or transmitted) by an unauthorized individual or entity. Supplier shall restore such Micron Data at its own expense. Supplier shall notify Micron without undue delay in accordance with any applicable laws, rules, or regulations, but in any event not later than seventy-two (72) hours after becoming aware of an 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 shall 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) 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 shall not inform any third party of any 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 shall cover all reasonable expenses associated with the performance of the obligations under this section. Supplier shall 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 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. If Supplier fails to correct or regenerate the lost or destroyed Micron Data within the time reasonably set by Micron, then Micron may obtain data reconstruction services from a third party, and Supplier shall cooperate with such third party as requested by Micron. Supplier shall prioritize this effort so that the loss of Micron Data will not have an adverse effect upon Micron's business, or the services provided by Supplier.

17. Communications Security

Supplier shall 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 shall: 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.

18. Supplier Relationships

Supplier shall 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.

Annually, upon Micron's request, Supplier shall provide assurance, in the form of an 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 shall 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 shall 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 will 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 ninety(90) days written notice. Security Assessment hours incurred by Supplier shall 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 employees. Supplier shall make available information security personnel to address Micron's reasonable questions. Micron will 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 shall promptly and mutually agree on a remediation plan, including timeframes and Supplier shall use commercially reasonable efforts to remediate any deficiencies or material risks found.

Additionally, upon request of Micron, Supplier will provide a written certification for the period between completion of any SOC 2 report (or its functional equivalent) and Micron's fiscal year end, describing the changes Supplier made during such period (if any) to the controls, procedures, and systems that were the subject of such report to allow Micron to use such report to meet its own audit and compliance needs.

In the event that Micron determines that Supplier is not in compliance with any of the requirements set forth herein, or if Supplier fails to provide any audit report or other request for verification of compliance with these terms, Micron shall have the right, without penalty and at no cost, to (i) perform a supplemental Security Assessment to confirm Supplier's compliance with these Information Security Control Requirements and/or (ii) suspend or terminate the services or, at Micron's option, withhold payment, and Supplier hereby waives any applicable termination charges or outstanding fees in connection with such suspension or termination.