Intel Information Security Addendum
Appendix A – Cloud Security 2023ww04

Cloud Security Measures

This Appendix applies in addition to the Intel Information Security Addendum if the Supplier operates one or more Cloud Computing Services to provide contracted services to Intel.

1. Definitions

"**Cloud Computing Services**" means on-demand network access to a supply of configurable computing resources or services and any software underlying the resources or services or by which the resources or services are delivered, including without limitation, software as a service, platform as a service, infrastructure as a service, or any combination of these services.

2. Security Governance and Compliance

2.1. Supplier must maintain an AICPA SOC 2 Type II certification of the Cloud Computing Services it provides to Intel or an industry standard equivalent and:

a. Remediate audits findings as per agreed timelines listed below under section 9.3.c.

b. Provide Intel with annual audit results upon request.

2.2. Supplier must enlist a third-party company to conduct penetration testing of the Cloud Computing Services on an annual basis based on industry best practices and will:

a. Remediate findings as per agreed timelines listed below under section 9.3.c.

b. Provide Intel with testing results.

3. Worker Security

3.1. No additions.

4. Asset Management

4.1. No additions.

5. Information Handling, Processing and Protection

5.1. Supplier will encrypt Intel data with data-level encryption that uses strong, industry recognized, non-deprecated algorithms.

5.2. Supplier will manage encryption keys in a FIPS 140-2 certified solution.

6. Change Management

6.1. No additions.

7. Authentication and Access Management

7.1. Supplier will support industry standard authentication mechanisms including but not limited to federated authentication, single sign-on, and multi-factor authentication.

7.2. Supplier will protect API access using industry standard API security mechanisms.

8. Physical and Environmental Security

8.1. Supplier will ensure its data processing facilities (and those of its subcontractors) that store, or process Intel Data maintain an industry standard security certification, such as AICPA SOC 2 Type II certification, an ISO 27001 certification or industry standard equivalent. Supplier will ensure that such certifications are renewed on an annual basis or more frequently and ensure timely remediation of material findings from such renewals. Certification must be available to Intel upon request.

9. Secure Operations

9.1. Supplier will maintain a restricted network with minimal access that meets industry best practices and review the network configuration at least once quarterly.

9.2. Supplier will have a security event and incident monitoring system in place with processes to alert appropriate personnel of potential threats and security events, and Supplier will have a timeline for closing alerts that meets industry best practices.

9.3. Supplier will implement a vulnerability management plan for the Cloud Computing Services that meets or exceeds industry best practices. As part this plan, the Supplier must at minimum:

a. Audit and scan the Supplier’s entire network, systems, applications and internet or external interfaces for vulnerabilities. Supplier will scan for vulnerabilities at least once per two weeks.

b. Remediate vulnerabilities and apply security configuration patches for all components in the production and development environments in accordance with Table 1 – Remediation Timeline. The remediation timeline begins once both conditions are met: the regular audit (or other discovery mechanism) reveals a gap in compliance and a remediation solution is available.

c. Implement alternative means to mitigate the vulnerabilities until the remediation solution has been applied. Mitigations must be documented by Supplier and made available by Supplier during an audit.

Table 1 – Remediation Timeline

Rating	***CVSS (V3.0) Score Range***	***Remediation Timeline (within)***
Low	Below 4	60
Medium	4.0-6.9	28 days
High	7.0-8.9	
Critical	9.0-10.0	7 days

9.4. Supplier will provide capability to audit user access, review and export log relating to Intel service and data upon request.

9.5. Supplier will separate development, test, and operational environments to reduce the risks of unauthorized access or changes to the operational system and to prevent the introduction of production data into development or test environments.

10. Security Incident Response

10.1. No additions.

11. Business Continuity/Disaster Recovery

11.1. No additions.

12. Additional Security Capabilities

12.1. Intel may, upon written request conduct a reasonable audit of Supplier’s Security Measures. In connection with such audit rights, Supplier shall provide reasonable access to information reasonably required by Intel and will make personnel available to the extent reasonably necessary to answer questions or otherwise assist Intel in performing such reviews.

12.2. All information exchanged in connection with the audit activities described in this Cloud Security section is deemed to be the Confidential Information of the disclosing party.