Intel Information Security Addendum 2019ww41

Scope

The terms of the Addendum define information security controls that Intel's suppliers must adopt when (a) accessing Intel facilities, networks, and/or information systems, (b) handling Intel Data or (c) having custody of Intel hardware assets.

Supplier is responsible for compliance to these terms by its personnel and subcontractors. Additional security compliance requirements may be specified in Supplier's agreement, appendices or statements of work.

Contents

1. Security Governance and Compliance

1.1. Supplier must have an Intel Non-Disclosure Agreement in place and comply with requirements of that agreement.

1.2. Supplier will timely and accurately complete any questionnaires furnished by Intel assessing Supplier's cybersecurity controls and provide industry standard cybersecurity attestation. If Supplier's response to such assessments indicates the presence of moderate or high levels of risk, Intel and Supplier must promptly meet to discuss such risk in good faith, and Supplier must implement a remediation plan as mutually agreed by the parties.

a. Intel will utilize third-party cyber security ratings platforms to assess Supplier's security controls. Supplier must cooperate with Intel and third-party vendor to remediate identified vulnerabilities

1.3. Supplier must maintain an effective security management program that includes:

a. executive review, support and accountability for all security related policies and practices;
b. a written information security policy that complies with applicable laws and regulations, meets or exceeds applicable industry standards and that, at a minimum, includes defined information security roles and responsibilities, a formal and effective risk mitigation program and a supplier security management program;
c. periodic security assessments and audits of all systems processing Intel Data to measure the effectiveness of controls;
d. periodic review of security incidents, including determination of root cause and corrective action;
e. a formal controls framework based on an external audit standard, such as the AICPA SOC 2 Type II reports; and
f. a process to document non-compliance with the Security Capabilities and identify and quantify the risks and mitigation plans. The mitigation plan must be approved by the Chief Information Officer (CIO) or an authorized individual who can accept responsibility and accountability on behalf of the Supplier.

1.4. Supplier must review its Security Capabilities at least once per year to ensure that they remain effective and appropriate for protecting Intel Systems and/or Intel Data and, are conforming to industry standards, laws and regulations.

a. The Supplier must inform Intel, within 24 hours, of any material findings and actions arising from each review, and Supplier must mitigate any risks in a time frame mutually agreed by both parties.

1.5. When implementing, reviewing and updating its Security Capabilities and policies, Supplier must consider:

a. Compliance to industry standards, laws and regulations;
b. Information available from the Supplier's existing vulnerability, remediation, audits or incident related activities;
c. The changing nature of threats, exploits and actual incidents relating to compromise of information hosted on connected computing platforms;

d. The sensitive nature of the Intel systems and Intel Data and the substantial harm which would result from accidental, unauthorized or unlawful loss of the confidentiality, integrity, or availability of Intel Data or Intel Systems;
e. Available and emerging means of detecting malicious activities and rendering them less effective or ineffective, and;
f. The state of technological development and the cost of implementing such capabilities.

2. Worker Security

2.1. Supplier must implement and maintain employee and subcontractor access, screening and controls policies and practices that include, at a minimum, the following controls applied to Supplier employees, subcontractors and agents who may access Intel Systems and/or Intel Data (collectively "Supplier Representatives"):
   a. As allowed by applicable law and prior to granting a Supplier Representative access to Intel Systems and/or Intel Data, Supplier must conduct or ensure the completion of appropriate background checks on each Supplier Representative, and withhold access to Intel Systems and/or Intel Data to any Supplier Representative who has failed to pass such background investigation;
   b. Supplier must ensure that all Supplier Representatives undergo adequate training in the care, protection and handling of the Intel Systems and/or Intel Data prior to having access to Intel Systems and/or Intel Data, and comply with the Security Capabilities set out in this Agreement;
   c. Supplier must maintain a disciplinary policy and process, to be used when Supplier Representatives violate Supplier security or privacy policy or access Intel Systems and/or Intel Data without prior authorization;

2.2. Supplier Representatives who are part of Intel's contingent workforce must complete annual Intel required Information Security training.

2.3. Supplier Representatives working on-premise at Intel facilities with access to Intel Systems and/or Intel Data are additionally subject to Intel's Information Security and Corporate Security Policies and practices.

3. Asset Management

3.1. Supplier must only allow Supplier Representatives to access Intel Systems and/or Intel Data from approved Supplier or Intel managed devices, including but not limited to servers, laptops and smartphones, with technical security controls compliant to the terms of this addendum.

4. Information Handling, Processing and Protection

4.1. Supplier must implement controls to ensure that only those Supplier Representatives with a need-to-know have access to Intel Systems and/or Intel Data.

4.2. Supplier must ensure that Intel Data is cryptographically protected at rest and in transit using strong, industry recognized, non-deprecated algorithms.

4.3. Supplier must ensure that strong, industry recognized, non-deprecated cryptographic keys are used, and these keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

4.4. Cross-border Data Flow

a. The geographic location of Supplier providing infrastructure resources must be disclosed to Intel. Intel must be able to specify the geographical location(s) where Intel Data is stored and/or processed to ensure compliance with local and national laws that restrict the cross-border flow of data.

b. If the Supplier intends to change geographical location of Intel Data, Supplier must notify Intel of the proposed change at least 90 days in advance and obtain Intel's authorization before changing the location where Intel Data is stored or processed.

4.5. Data Migration and Removal

a. Supplier must allow and ensure Intel can export Intel Data at any time during service use or within 30 days of no longer using the service.

b. Supplier must implement and maintain a process ensuring secure destruction and/or deletion of all Intel Data, when directed by Intel or no more than 30 days after recovery period defined in section 4.5(a).

c. Supplier must dispose of electronic media (e.g. hard drives, flash drives, optical storage discs) which contains Intel information in an industry recognizable and secure manner (e.g. clear, purge, or destroy per the Guidelines for Media Sanitization in NIST 800-88).

d. Supplier must promptly dispose of paper and printed hard copies by cross cut shredding or other secure destruction methods.

e. Supplier must maintain a method for sanitization ("zeroing out") of storage containers, removal of ephemeral data so that Intel Data cannot be practicably read or reconstructed.

f. Supplier must provide confirmation of destruction of Intel Data to Intel upon request.

5. Change Management

5.1. Supplier must document and manage operating procedures by a change control process.

5.2. Supplier must implement and maintain written policies and procedures to review, test and approve (as appropriate) changes affecting Supplier infrastructure and systems that process Intel Data.

5.3. Supplier must establish an acceptance and validation process for new information systems, upgrades, and versions to ensure vulnerabilities are not introduced during supply chain process and must conduct suitable tests of these processes during development and prior to release.

5.4. Supplier must notify Intel in advance of any change that could impact the way Intel uses a product or service provided by Supplier.

6. Authentication and Access Management

6.1. Supplier must provide industry accepted authentication and access controls to protect Intel Systems and/or Intel Data, including authentication methods utilized to prevent unauthorized access to Intel Systems and/or Intel Data.

6.2. Supplier must ensure that the Supplier's access control methods clearly state the rules and rights for each user or group of users including applications and information sharing and that these methods must include a process for granting, modifying and removing access to all information systems and Services processing Intel Systems and/or Intel Data.

6.3. Supplier must maintain a record of all privileges allocated pursuant to the requirements herein for no less than one year or for the duration of active investigations, whichever is longer, to assist in investigations and access control monitoring.

6.4. Supplier must implement controls to ensure that access granted to all Supplier Representatives is based on least-privilege principles.

6.5. Supplier must implement controls to ensure revocation of access from Supplier Representatives no longer requiring access and, at a minimum, conduct access reviews at least quarterly to ensure that only those Supplier Representatives who need access to Intel Systems and/or Intel Data are still authorized.

6.6. Supplier must ensure that administrative or remote access to Intel Systems and/or Intel Data or Supplier systems that process Intel Data comply with industry best practices, such as multi-factor authentication and virtual-private network.

6.7. Supplier must ensure that a separation of duties process is followed to prevent a single Supplier Representative from controlling more than one key aspect of a critical transaction or business process related to Intel Systems and/or Intel Data.

7. Physical and Environmental Security

7.1. Supplier must ensure that its facilities, and those of its subcontractors, that store and/or process Intel Systems and/or Intel Data:

a. are secured in an access-controlled location;

b. are protected from unauthorized physical access, damage and interference using physical security controls, which could include keycard access, and solid wall construction for all exterior walls;

c. limit, screen and log all entries and exits employing such capabilities as on-site security guard, badge reader, electronic lock, and monitored closed circuit television (CCTV); and

d. are physically isolated from service areas that provide access points into and out of the premises housing the data processing facilities.

8. Security Operations

8.1. Supplier must regularly audit Supplier networks and systems for security configuration compliance.

8.2. Supplier must apply security configuration patches and updates, as deemed necessary by the Supplier's security management program and within a reasonable timeframe given the criticality of the vulnerability, for all components in the production and

development environments in accordance with Supplier's Security Capabilities and policies.

8.3. Supplier must regularly scan the Supplier's entire network, systems and applications for vulnerabilities.

8.4. Supplier must apply vulnerability patches and updates for all components in the production and development environments in accordance with Supplier's Security Capabilities and policies, but not to exceed 90 days from release.

8.5. Upon request, and subject to NDA, Supplier must deliver to Intel, in a mutually agreed upon format, a summary of security configuration audit results, vulnerability scan results, and security patch/vulnerability remediation status.

8.6. Supplier must ensure all extranet connectivity to Intel Systems and/or Intel Data are through connections that align with industry security best practices such as those for authorization, authentication, logging, and monitoring.

8.7. Supplier must implement minimization of services and secure configuration for the Supplier connected systems.

8.8. Supplier must have the ability to detect and prevent a potential hostile attack on their networks and hosts.

8.9. Supplier must update all detection systems and signature databases to current release at the highest frequency possible, but not to exceed 30 days after release.

8.10. Supplier must ensure that all subsequent updates to such computers and network devices maintain restrictions outlined in this Addendum.

8.11. Supplier must configure computers and network devices so that only necessary and secure protocols and services are enabled.

8.12. Supplier must implement a documented means of securing and validating system build software for computer and network devices used to provide business functionality to Intel.

8.13. Supplier must adhere to secure development and validation best practices for all code, software and applications developed on behalf of Intel and/or deployed on Intel Systems and/or systems that process Intel Data.

8.14. Supplier must limit and control access to Supplier source code to prevent unauthorized access and modification.

8.15. Supplier must maintain mechanisms that record, examine, and alert (upon detection of a security event) activity in information systems that process or access Intel Data.

8.16. Supplier must ensure that Intel System event logs are retained for no less than one year or for the duration of active investigations, whichever is longer, to assist in investigations and access control monitoring, including, but not limited to, end user access and activities, and information security events.

8.17. Supplier must ensure that log information includes without limitation the type of event, date and time of event, user/process ID that triggered the event, origination address of the event, destination address for the event, and the success/failure status of the event.

8.18. Supplier must use a trusted and reliable external time source to sync internal system clocks.

9. Security Incident Response

9.1. Supplier must notify Intel immediately once Supplier becomes aware of any Data Breach or symptoms of malicious incursion involving or potentially impacting Intel Systems and/or Intel Data.

a. Security incident notifications must include at a minimum and where possible (i) unique system identifiers, (ii) source and destination IP addresses, (iii) event logs (network, system, web) indicating unique identifiers (iv) any additional evidence including, but not limited to, packet captures, payloads, and machine images.

b. Incidents which result in loss or damage to Intel assets must have a local police report filed and must be immediately reported to Intel.

9.2. Supplier must maintain and test, at least annually, a security incident response plan, procedures and means to respond in a manner consistent with that plan.

9.3. Supplier must provide assistance to Intel to include, as applicable:

a. Providing Intel with physical access to the facilities and operations affected for locations under Supplier's control;

b. Facilitating interviews with Supplier's or subcontractors' employees and others with knowledge of the incident;

c. Making available to Intel relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise required by Intel, subject to third party confidentiality restrictions;

d. Providing any other assistance Intel may reasonably require, at Supplier's sole cost and expense; and

e. Designate a senior representative to provide incident briefings and to respond to requests by Intel pertaining to security issues.

The primary Supplier and Intel contacts for (i) Data Breach and Security Incident Investigations, (ii) business continuity and disaster recovery are listed below.

Intel Contacts: IT Emergency Hotline – (916) 356-8910

Supplier Contacts: Supplier will provide to Intel in writing

Either party may change these contacts upon written notice.

10. Business Continuity/Disaster Recovery

10.1. Supplier must implement and maintain written business continuity and disaster recovery plans, which are tested and reviewed at least every 12 months.

10.2. All Supplier systems must implement an industry standard backup and restore capability to ensure that downtime and recovery times do not exceed terms of purchase/service agreement.

11. Additional Security Capabilities

11.1. Security capabilities that become industry-accepted common practices that surpass any of the above measures should be implemented, subject to review and agreement from Supplier and Intel.

12. Definitions

"Authorized User" means any individual, entity or end-user that is authorized by Intel to access or use the products or services purchased or obtained from Supplier under an Intel account. The term "Authorized User" does not include individuals or entities when they are accessing or using the products or services under their own account, rather than an Intel account.

"Data" means information, software, sample code, libraries, APIs, command line tools, and data, including without limitation, any Personal Information or Confidential Information, hypertext markup language files, metadata, scripts, programs, recordings, sound, music, graphics, video, images, applets, or servlets.

"Data Breach" means any unauthorized or unlawful processing, loss, disclosure, destruction, theft, or damage of any of the Intel Data, including Personal Information.

"Data Subject" is the individual to which the Personal Information relates.

"Intel Architecture" refers to the specific architectures originally designed by Intel, such as IA-32 and IA-64.

"Intel Data" means Data that Intel or any Authorized User (i) runs on the products or services, (ii) causes to interface with the products or services, or (iii) uploads to the products or services under Intel's Service account or otherwise transfers, processes, uses or stores in connection with Intel's Service account. For the purposes of clarity, Intel Data includes but is not limited to Intel Employees' and Contingent Workers' authentication information, Personal Information and may include Data licensed to Intel by third parties.

"Intel Systems" means compute, network or storage systems, either owned by Intel or Supplier and/or operated by the Supplier to process, transmit, and/or store Intel Data.

"Personal Information" means any information relating to an identified or identifiable natural person or a household; an identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity of which Intel is the Data Controller and in relation to which Supplier is providing goods or services under this Agreement. But for the addition of "household," "Personal Information" is synonymous with the term "Personal Data" as used in the GDPR**.**

"Security Capabilities" means the technical, physical and process controls deployed by the Supplier to ensure the confidentiality, integrity and availability of Supplier systems used to process and/or store Intel Data.

"Supplier Representative" means all Supplier employees, subcontractors and agents who may access Intel Systems and/or Data.