Intel Information Security Addendum
Appendix B - Off-shore Development Center (ODC) Q1 2024

This Appendix B applies as an addition to the Intel Information Security Addendum (ISA) if the supplier operates one or more Off-shore Development Centers to provide their contracted services to Intel.

Contents

1. Definitions

1.1. **“Off-shore Development Center (ODC)”** is a dedicated physical space allocated exclusively for Intel in the supplier’s premises, where work is performed by Intel contingent workers with authorized access to Intel assets, network, and resources.

1.2. **“Authorized Personnel”** is any person authorized by Intel to have access to Intel IP, Information Assets or Physical Assets required for execution of projects in ODC.

1.3. **“Unauthorized Personnel”** is any person who is not an Authorized Personnel. This includes but is not limited to visitors, janitorial and maintenance staff, and employees of the suppliers who are not authorized to access the Intel IP, Information Assets or Physical Assets in the ODC.

1.4. **“Information Asset”** is any information generated by or used in any Intel business activity. This includes, but is not limited to, information originating from direct access to computer systems, information carried over networks, information preserved on portable electronic media, and information appearing in hard copy format.

1.5. **“Physical Asset”** is any tangible asset belonging to or under the possession of Intel. It includes but is not limited to engineering samples, devices under test, and compute, network, and storage equipment.

1.6. **“Samples”** are any physical product loaned to a supplier for development or testing. It includes product in any state, including defective, damaged and end of life products.

2. Security Governance and Compliance

2.1. Intel will evaluate each ODC against security controls as outlined in the Information Security Addendum and this Appendix B – Off-shore Development Center.

a. Intel reserves the right to inspect all ODC locations, including, but not limited to, their physical security and the security of on-site computing and network devices.

b. Suppliers must enable remote audit capability of ODC computers and network devices upon request. This includes allowing and enabling Intel to use vulnerability scanning services.

i. If applicable, suppliers must allow the IP addresses and ports provided by Intel in their firewall upon request to enable remote scanning of vulnerabilities on the devices used in Intel's project.

ii. IP address may be Intel-owned or could be of a third party on Intel's behalf to run scans.

iii. If applicable, suppliers must share firewall rules configured for Intel's projects.

2.2. Suppliers must ensure security requirements are adhered to and remain consistent throughout the duration of the project and support contract including during its termination phase.

a. Suppliers must conduct internal audits on yearly basis at minimum to ensure compliance with ODC security requirements listed in ISA and this ISA- Appendix B.

b. Upon request, suppliers must provide Intel with the internal audit report.

2.3. If ODC is not in compliance with any security requirement listed in this document or ISA, but there is a business justification for a delay in bringing it into compliance, the supplier must ensure that a formal policy exception is in place. Each exception will be evaluated and approved by Intel’s risk management team.
Suppliers must contact business sponsors/commodity manager to request an exception. The business sponsor or commodity manager is responsible for filing the requested exception in Intel’s exception management tool. Supplier is responsible for ensuring that any expired or unapproved exception solution is not implemented.

2.4. Supplier must ensure that ODC related information is updated in all relevant Intel provided information systems.

2.5. Suppliers must perform required due diligence and ensure compliance with any additional security requirements, before executing projects involving Intel end customers or 3rd party partners.

3. Worker Security

3.1. Suppliers must ensure that each worker assigned to Intel's project(s) has completed the background investigation in a manner that it meets or exceeds Intel’s requirements listed under ‘Contingent workforce- Access Eligibility’ section on Intel’s supplier website. Suppliers must immediately inform Intel project sponsor of any criminal involvement of a worker assigned to Intel projects.

3.2. Supplier must ensure that that each worker assigned to Intel's project(s) completes Intel Information Security and Privacy Awareness training courses as outlined in ISA.

3.3. When an ODC worker leaves the company, supplier must ensure that the worker’s exit interview includes a review of the employee's responsibility to maintain the non-disclosure terms outlined in signed NDAs.

3.4. Supplier must keep worker location updated in Intel provided information systems.

4. Asset Management

Security measures for assets differ according to the asset category. It is very important for suppliers to be aware of different asset categories in an ODC facility to ensure proper measures are taken to secure Intel-provided assets.

Intel-provided assets used in Intel projects are categorized in two categories:

4.1. **Primary Asset (end user devices)**

a. Primary device is an Intel IT provided end user device (such as a laptop, a desktop computer or a mobile device) used for day to-day work.
   Note: Lab devices are not considered as primary asset.
b. Suppliers must ensure that a primary asset is only removed from ODC based on a valid business justification and approval from BU Project sponsor. E.g., Work from home scenario.

4.2. **Secondary Asset (any asset other than primary asset)**

a. All secondary assets must remain in the ODC.
   Note: Secondary asset includes but not limited to networking devices, servers, lab devices, engineering samples like loose components, boards with silicon, High Value Physical Intellectual Property (HVPIP), Pre-Production Hardware (PPHW), Form Factor Reference Design (FFRD) and Solid-State Drives (SSD's)

5. Asset and Information Handling, Processing, and Protection

Suppliers and ODC employees must follow Intel's Code of Conduct, safety guidelines and information security policies, including the ISA, to protect Intel assets and IP in any form.

5.1. **Asset Inventory**

a. Suppliers must maintain proper records of all inventories in the ODC, including Intel provided assets and suppliers' assets.
b. Supplier must reconcile secondary asset inventory on quarterly basis and share it with BU project sponsor or lab manager. Evidence for reconciliation is auditable by Intel.

5.2. **Asset transfer and shipping**

This section defines requirements when an asset is moved from one location to another or returned to Intel.

a. Pre-approval from BU Project sponsor or Lab manager is required for Intel asset transfer from the ODC facility.
   Note: Pre-approval is not required if the secondary asset is moved from lab to lab in the same ODC and SOW, however, suppliers must ensure that the asset inventory is updated.
b. All Intel assets including, but not limited to, defective, damaged, or end-of-life samples must be returned to Intel.
c. Shipping must be ordered by Intel via a licensed carrier with tracking capability and requires signature upon receipt. Shipping documents shall be retained until the Return Material authorization (RMA) process step has completed.

5.3. **Reporting Lost/Stolen Asset**

Supplier must report any missing asset at https://circuit.intel.com/content/corp/infosec/home.html and in addition, report the same to the Intel BU Sponsor.

A police report must be filed within 48 hours of the incident. Supplier must provide additional documentation or investigation reports, as needed.

5.4. **Physical Asset Security and Monitoring**

a. Primary assets must be in locked screen mode when not in use or when left unattended.

b. Portable secondary assets must be stored in lockable drawers/cabinets/cages when not in use. A person authorized by the supplier must be accountable for the key management.

c. Portable secondary asset in the ODC which stores Intel IP must be encrypted per the requirements of Intel’s information security policies.

d. CCTV must be placed in such a way that it does not capture any Intel IP from whiteboards, monitors etc.

e. Intel IP must be removed from desks, work areas, collaboration areas and white boards when not in use or unattended.

5.5. **Printing and Copying**

a. Supplier must have a valid business justification and approval from Intel business sponsor for using printer inside ODC.

b. Supplier must ensure colored paper is used for printing to differentiate documents containing information about Intel assets or Intel IP.

c. Intel documents or notes containing Intel IP must not be taken out of ODC area without business justification.

d. The ODC must have a cross-cut paper shredder to securely dispose of documents or notes containing information about Intel assets or Intel IP.

5.6. **Asset Usage**

a. Supplier must ensure that contingent workers must not use Intel assets for personal activities.

6. Change Management

6.1. Suppliers must report to Intel Business sponsor/commodity manager, in writing, at least 90 days prior to performing any changes that may impact Intel, including, but not limited to change of office location, addition or removal of rooms to an ODC, change in network architecture etc.

6.2. Intel commodity manager must be informed within 48 hours about supplier primary contact change.

7. Authentication and Access Management

7.1. Suppliers must ensure that individual account sharing is not allowed.

7.2. Any type of shared password or authentication code being used in the ODC (e.g., cabinet locks, cage locks, etc.) must not be shared with anyone other than Authorized Personnel.

7.3. Password or authentication code sharing and storage must use Intel IT-approved management solutions.

8. Physical and Environmental Security

8.1. Intel ODC is a secure designated area for ODC personnel working for Intel. Therefore, no one other than Intel ODC contingent workers and security personnel dedicated for Intel ODC are allowed inside the ODC unescorted.

8.2. Anyone other than Intel ODC contingent workers and security personnel dedicated for Intel ODC should be treated as a visitor and must always be escorted while inside the ODC by an Intel ODC worker, or ODC security personnel.

8.3. Access control system must be implemented at all the entry and exit points of the ODC (Examples: RFID tag readers, Biometrics) to prevent unauthorized access to the ODC.

8.4. Janitorial, cleaning and maintenance staff cannot be granted ODC access and are required to be escorted at all times.

8.5. Supplier must maintain a list of Authorized Personnel which should be reviewed and reconciled quarterly. Reconciliation report is auditable by Intel.

8.6. Access to the ODC must be revoked within 24 hours of the Last Day Office (LDO). In case of hostile or unfriendly separation, access must be revoked immediately.

8.7. Supplier must ensure that tailgating is not permitted into the ODC.

8.8. Supplier must verify that all permitted visitors present valid government ID and a record should be maintained for entry and exit of all permitted visitors.

8.9. The visitor record must include, but not limited to, visitor name, in/out time, date, purpose, and escort name.

8.10. The visitor record must not capture SPI (Sensitive Personal Information) or any other PII (Personally Identifiable Information) beyond visitor name, and must not have the Intel name, logo, or other identifying signage on the cover.

8.11. Supplier must retain ODC office area physical access logs of Authorized Personnel and visitors for a minimum of 90 days.

8.12. During an emergency, security personnel or emergency responders may enter the ODC without an escort. However, this must be flagged as incident and trigger Incident Response procedures. Examples include natural disaster, fire alarm, employee sickness, crime etc.

8.13. Supplier must maintain a floor plan for ODC area which includes work areas (including lab, network, hub, or communication rooms), entry-exit points, emergency exits, access readers, security desks, and CCTV's.

8.14. Supplier must ensure that the ODC is not labeled or identified as Intel (e.g., signs, evacuation maps, etc.).

8.15. Suppliers will ensure that all entry points, including, but not limited to doors, windows, false ceilings, etc. must be closed and locked, or otherwise secured, to prevent entry from Unauthorized Personnel.

8.16. All entry-exit points including ODC, labs, IT infrastructure room and storage spaces must be monitored using CCTV and CCTV footage must be stored for a minimum of 90 days.

8.17. ODC entry points must be alarmed with forced entry notification, break glass, and/or motion sensors and must have automatic closing devices where possible, with an alarm activation when they are open for longer than 30 seconds.

8.18. Labs, network, server, and infrastructure room in the ODC must have 10 seconds open door alarms and there must be no signs indicating the location or content of those rooms.

8.19. Opening an emergency exit door must trigger a loud alarm.

8.20. All the alarms and sensors must be actively monitored 24/7. Any violation must trigger Incident Response procedures.

8.21. All glass walls, doors and windows must be frosted or covered to ensure the ODC operations cannot be seen from outside.

8.22. Access to lab environments and HVPIP storage area are restricted to those who have a business need. Lab must be physically and logically (network) isolated from the ODC area using a different set of security controls.

8.23. Intel network, server and infrastructure devices must be stored in a dedicated room or locked cabinets in a shared room. Access to these must be restricted to those who have a business need.

8.24. Access logs for network room and Lab environment must be retained for 1 year.

8.25. All alarms used in ODC should be audible.

9. Secure Operations

9.1. ODC network

Bridging devices connected to Intel ODC and non-Intel network at the same time is not allowed.

a. Intel managed ODC network

  i. The Intel ODC network must be isolated from the rest of the supplier's network.

  ii. Supplier must ensure that only authorized ODC devices connect to the Intel ODC network.

b. Supplier managed ODC network

  i. Supplier must have a network diagram which includes the flow of data and network device which demonstrates separation of ODC network and supplier network.

  ii. The Intel ODC network must be logically isolated from the rest of the supplier's network and configured as per industry best practices.

  iii. Supplier must ensure that only ODC systems can connect to the Intel ODC network.

  iv. If wireless network is being used, supplier must ensure that SSID broadcast is disabled, MAC address filtering, authentication and encryption are used as per industry best practices.

  v. Supplier must segregate ODC office network and Lab network.

  vi. If supplier and Intel network co-exist, copper cabling needs to use different color to separate from Intel cabling. Label needs to be clearly marked with information to avoid accidental use.

9.2. Supplier must ensure that ODC workers are using Intel-provided solution (example: VPN) for remote access.

9.3. Supplier must ensure there are no software/hardware components that could bypass security controls for the ODC and/or Intel assets.

9.4. Photography, video, and audio recordings of any kind are prohibited in all ODC areas.

9.5. Supplier must ensure that personal or non-Intel electronic storage devices are not allowed into ODC Lab areas.

9.6. Supplier must ensure that non-Intel cloud storage and applications, or public email services and social media platforms are not used to transmit Intel Information Assets or discuss Intel IP or Intel projects.

9.7. Supplier must post a summary of information security requirements in a location seen by all workers who have access to Intel Information Assets and Physical Assets. The summary must include, but is not limited to:

  a. ODC workers are responsible for protecting assets from unauthorized access.

b. All systems, applications and accesses are monitored and logged.
c. Account sharing is prohibited.
d. Tailgating is prohibited.
e. Use of personal or non-customer's removable storage media is not allowed in ODC area.
f. Installing unauthorized or unlicensed software is prohibited.
g. Portable assets must be stored in lockable drawers/cabinets/cages when not in use.
h. Customer's IP must be removed from desks, work areas, collaboration areas and white boards when not in use or unattended.
i. Computer must be in locked screen mode when not in use or when left unattended.
j. Asset transfer procedure must be followed for taking out assets from ODC area.
k. Colored paper must be used for printing to differentiate documents containing information about customer's assets or customer's IP.
l. Documents or notes containing information about customer's assets or customer's IP must not be taken out of ODC area without business justification.
m. A cross-cut paper shredder must be used to securely dispose of documents or notes containing information about customer's assets or customer's IP.
n. Usage of non-approved cloud storage and applications, or public email services and social media platforms is not allowed to transmit customer's Information Assets or discuss customer's IP or projects.
o. Photography, video, and audio recordings of any kind are prohibited in all ODC areas.

10. Security Incident Response

10.1. Suppliers must have a documented Security Incident Response Plan. Objective of the plan is to set a process to detect, respond to, and recover from security incidents. This plan must cover an emergency response plan for the safety and security of ODC workers.

10.2. The Security Incident Response Plan must include, at minimum, definitions, triggers, roles and responsibilities, methodology, incident response phases and guidelines for interaction with law enforcement.

10.3. The Security Incident Response Plan and security incident logs must cover, at minimum, the below scenarios:

a. An alarm has been activated (including, but not limited to, open door alarm and emergency door alarm).
b. Any Intel Information or Physical asset is lost or stolen.

c. Any other event occurs that reasonably threatens or may threaten the confidentiality, integrity, or availability of Intel Information or Physical assets.

10.4. The Security Incident Response plan must include notification to Intel as detailed in Intel Information Security Addendum (ISA) - Security Incident Response.

10.5. Supplier must maintain security incident logs for at least 12 months.

11. Business Continuity/Disaster Recovery (BC/DR)

11.1. Suppliers must have a documented business continuity and disaster recovery plan. The plan must have provisions for, at minimum:

a. Power outage.

b. Internet outage including work from home scenario/non-Intel location.

c. Natural Disaster/Pandemic/Military conflicts/riots.

11.2. The BC/DR plan must be reviewed and tested annually (at minimum).

11.3. The BC/DR plan, the drill logs and the annual tabletop exercise report is auditable by Intel.