**Intel Information Technology**

**Information Risk and Security**

Supplier Security Requirements &

Expectations

For

**ODC *(Off-site / Off-shore Development Centre)***

Version 3.3

**Supplier Security Compliance Agreement:**

Signed by:

Company:

Responsibility:

Date:

*This addendum specifies minimum security requirements to be implemented and maintained when a 3rd Party is issued with, and manages*

*Intel High Value Physical Intellectual Property outside the controls of an Intel facility.*

Please return this signed ODC Supplier Security Requirements and Expectations document to Intel Information Security. This document will be periodically updated, based upon evolving threats and security requirements, and re-distributed to Intel Suppliers.

**VERSION 3.3 ODC SECURITY EXPECTATIONS**

**Contents**

**1.0 ODC PHYSICAL SECURITY .................................................................................................................. 4**

**1.1 PHYSICAL ACCESS CONTROL ........................................................................................................... 4**

**1.2 ACCESS CONTROLS AND RETENTION SCHEDULES....................................................................... 5**

**1.3 NETWORK SECURITY.......................................................................................................................... 5**

**2.0 ODC OPERATIONAL SECURITY EXPECTATIONS ....................................................................... 8**

**2.1 CLASSIFIED DATA ............................................................................................................................... 8**

**2.2 ADDITIONAL RULES ........................................................................................................................... 9**

**2.3 ENGINEERING SAMPLES.................................................................................................................... 9**

**3.0 UNIVERSAL SECURITY PRINCIPLES ............................................................................................ 11**

**3.1 INTEL INFRASTRUCTURE ACCESS PREREQUISITES ................................................................. 11**

**3.2 LEGAL AND REGULATORY REQUIREMENTS................................................................................. 12**

**4.0 SECURITY MANAGEMENT .................................................................................................................. 13**

**5.0 DATA PROTECTION .............................................................................................................................. 15**

**6.0 ODC GOVERNANCE & COMPLIANCE ............................................................................................. 16**

**6.1 INTEL ODC GOVERNANCE & COMPLIANCE ............................................................................... 16**

**6.2 SUPPLIER COMPLIANCE EXPECTATIONS .................................................................................... 16**

**DOCUMENT OBJECTIVES**

Provide minimum security requirements for an Intel Offsite Development Center (ODC) to deliver protection to Intel

Intellectual Property (IP) aligned to Intel’s Information Security policy.

**SCOPE**

This document is intended to define Offsite Development Center (ODC) security requirements and operational ex- pectations. Compliance to security requirements herein is required before an ODC goes live and starts work with In- tel IP. Any subsequent revision changes will require full compliance no longer than 90 days after signing.

**AUDIENCE**

Intel supplier providing: Resources; Collaboration; Product hardware, firmware or software development and/or sup- port; Validation testing: Support of Business Critical or Mission Critical applications; Solutions development or Sys- tem hosting.

**ASSUMPTIONS**

 All arrangements have been managed through Intel Procurement

 Signed Non-Disclosure Agreements (NDAs) are in place with the supplier before sharing this document

 Personal data must be classified as either Intel Confidential or Restricted Secret

 New relationships are reviewed by Intel Secure Outsourcing or Secure External Presence process

~~~~ ODC’s are subject to compliance reviews on a regular cadence, with oversight by ODC Governance. Supplier will have up to 60 days to mitigate and risks / non-compliances identified.

 IP data classifications have been identified, communicated and documented in the Statement of Work (SOW) by

Intel business and ratified by their IP Attorney

 Legal and regulatory requirements for Intellectual Property (IP)), High Value Physical Intellectual Property

(HVPIP), Data Privacy, Sarbanes-Oxley (SOx) and Controlled Technologies

 Suppliers are accountable for compliance to controls defined herein.

**USE CASES**

 Supplier is hosting directly with internet facing web sites

 Supplier provides test and validation services to Intel Product Development groups

 Supplier provides laboratory facilities to support the testing, validation and engineering services

 External supplier provides any services, personnel or facilities to support Intel systems and applications

 Supplier provides remote application engineering support to Intel development or production environments

 Supplier provides engineering services for hardware, firmware and or software for Intel product development

**DEFINITIONS**

**REQUIRED for all data types:** Specific security controls required by default regardless of the information sensitivity or classification level. The supplier must comply with these requirements and these items may be audited for com- pliance.

**REQUIRED for Top Secret classified data:** Specific security controls required by default for information classified by Intel as Top Secret. The supplier must comply with these requirements and these items may be audited for compli- ance. NOTE: Personal data classification is the responsibility of the appropriate Intel Privacy subject matter expert.

**1.0 ODC Physical Security**

Measures taken to protect ODC systems and related support infrastructure against threats.

**1.1 Physical Access Control**

|  |  |
| --- | --- |
| REQUIRED  for all Data | REQUIRED for  ITS data |
|  Egress points security controlled, and access restricted for business need only. Logs recorded and maintained for 90  days.   Where ODC has a lab and/or HVPIP, unauthorized access pre- vented (e.g. false ceilings, tailgating etc.). Must have intrusion detection 24 x 7.   All controlled area ‘emergency exit’ doors must sound an alarm when opened.   All egress points must have automatic closing devices, with an alarm activation if propped opened for longer than 30 sec- onds. Activation requires a security incident response.   Where ODC is on ground floor, all windows must be sealed or safeguarded with locks and have tamperproof sensors or alarm sensors. Alarm activation must instigate an incident re- sponse. All alterations to windows must comply with local government regulations. Contact Intel External Collaboration Group for resolution if there’s any conflict between Intel’s re- quirements and local government regulations.   The ODC should not be apparent by labelling (e.g. signs, evac- uation maps).   Where ODC is on ground floor all glass on the perimeter of  ODC is obscured.   Security alarm activation and/or unauthorised access inci- dents are documented , and made available to Intel by re- quest   |  Silicon/System on a Chip (Si/SOC) integra- tion projects classified as Intel Top Secret  (ITS) must be located in isolation from any other protects.   Unauthorized access prevented (e.g. false ceilings, tailgating etc.). Must have intru- sion detection 24 x 7.   All glass on internal perimeter of ODC is ob- scured.   Labs require physical and logical isolation from ODC office environment, and have unique access controls   Devices and data must be stored securely when not in use. Implementation of these controls including governance metrics are auditable by Intel.   Supplier must implement controls to pre- vent IP and/or HVPIP from leaving the ODC without authorization. Areas of focus in- clude but not limited to entry/exit points, windows and trash.   Access to Lab environments and HVPIP stores are restricted to those with a busi- ness need to know. |

ODC location moves, ODC extensions Change Notice Requirement

1. ODC rooms that are not an integral part of an existing approved registered ODC must be considered as a

separate ODC, which will require its own set of compliant controls. In all cases Intel External Collaboration Group

must be informed before any move to new locations occurs. The Security controls will require validation before

implementation or project support.

2. Extensions to existing ODC’s must be managed by Intel External Collaboration Group. Therefore notice to External Collaboration Group is required before any extension work starts. Interim security controls need to be proposed and approved before extension commences.

**1.2 Access Controls and retention schedules**

|  |  |
| --- | --- |
| REQUIRED  for all Data | REQUIRED for  ITS data |
|  Access granted to the granularity of every authorized person, and is based on Intel business support only.   All visitors must sign in and out of ODC area   Access logs retention period 3 month’s minimum.   Visitor policy includes a no tours policy.   Authorized access list scrubbed at least once per quarter.   Labs are subject to all Information Security Policy Security re- quirements and controls and lab access is based on business need only. |  Visitors including Janitorial staff must be escorted at all times   Access granted to authorized persons listed in RUNDA   All devices connected to Intel Global Busi- ness Network (IGBN) will have whole vol- ume encryption (PGP or McAfee) and  Enterprise Rights Management (ERM) de- ployed. |

**1.3 Network Security**

for all data (Confidential, Restricted Secret and Top Secret)

ODC networks have only 2 modes of operation and support that can be approved by Intel:

1. Intel owned and managed network and devices

2. Supplier owned and managed networks

This section defines supplier responsibility for each type of network management for setup, approvals, sustaining man- agement and compliance accountabilities.

**Intel owned and managed networks**

 Network Infrastructure isolated / segregated to enable the development and implementation of a secure inter connection tunnel back to Intel.

 If lab within the ODC has direct internet access a firewall preventing any unauthorized access to Intel’s Global Busi- ness Network must be deployed. All unused services and ports are to be disabled by default.

 Network traffic security control device (router or firewall) must logically isolate or segregate the lab network from the ODC office network.

 All telecommunications equipment must be located in a secure room with managed access control.

 All cabling must be secured or have tamperproof detection and alerting.

 All equipment must be returned to Intel when no longer required.

**Supplier owned and managed networks**

 Network Infrastructure isolated / segregated to enable the development and implementation of a secure inter- connection tunnel back to Intel.

 Before any connection to Intel is made: Work with Intel IT Network Operations to present proposed topology for approval to implement network specific controls. Details defined in section **Review** below.

 All network equipment is configured securely, implementing configuration details defined in section **Configura- tion,** below, at a minimum.

 All network equipment is continuously managed in compliance to section **Monitoring** below.

 Changes to any approved network must be reviewed by Intel Network Operations before implementation, unless change was removing security risk or vulnerability detecting. In the latter instance Intel Network Operations must be notified with updated topology diagrams within 48 hours of change.

 If lab within the ODC has direct internet access a firewall preventing any unauthorized access to Intel’s Global Busi- ness Network must be deployed. All unused services and ports are to be disabled by default.

 All telecommunications equipment must be located in a secure room with managed access control.

 All cabling must be secured or have tamperproof detection and alerting.

REQUIRED

for Supplier Provided Network Equipment for all data types

Prior to live data connection between Intel and Supplier, network device configuration must be reviewed by Intel to determine if adequate controls are in place to protect confidentiality, integrity, and availability of Intel's information assets and systems.

**Review prior to enabling data communications between supplier and Intel Corporation**

**Details Required for review:**

 Network topology diagrams illustrating device configuration and data flows. Intel to provide network to- pology templates.

o Device name, device type and purpose

o Port and protocol of proposed networking equipment

o External IP address of firewalls / routers with direct internet access

 Network equipment security specification (Intel Minimum Security Specification (MSS))

o Device type

o Operating system

o Firmware / Patch revision process and commitment of implementation

 Logical access controls protecting network hardware

o Implementation of multilevel password use

o Restriction of sources for all remote administrative access using only secure protocols (ex: Secure

Shell (SSH)/https)Configuration sufficient to protect against disruption, tampering, or eavesdrop-

ping

 Network device access

o SNMP access must be non-default settings for Read-Only or Read-Write access

o Restrict access to device to only source the necessary IP address

 Administrator access controls

o All administrative passwords must be stored securely (ex: If using local enable passwords, then use ‘secret’ passwords)

o Allow admin access from certain source IP addresses as necessary

 All accounts must use proper security: No default usernames or passwords

 Implement a change control process ensuring changes are managed, reviewed and recorded

**CONFIGURATION:**

 All networks that terminate at site-to-site VPN’s or Point-to-Point VPN’s to Intel must use IP-Sec network parameters with at least minimum **strong** security of AES encryption method or 3DES if AES not supported

o Networks **must** disable ports and protocols and services that are not actively required (eg. HTTP, HTTPS, FINGER, BOOTP, TCP/UDP small servers, etc.)

 Supplier networks **must** utilize approved network traffic routing and implement the following where sup- ported by hardware

o No IP source routing

o Service password encryption

o Logging enabled and sent to a central server for storage

o Establish ‘terminal’ (VTY) passwords (for console access)

o Auto-loading disabled (for booting device remotely)

o Timeout values present on console and remote VTY sessions

o IP directed broadcast disabled

o IP redirects disabled

o Transit encryption > = TLS 1.2 / 128-bit AES

o Proxy ARP (Address Resolution Protocol) disabled

o IP mask-replies disabled

o Utilize only authorized IP addresses

All networks installations must consider the following when configuring routing

 If network gear is routing, isolate routing functions physically or logically

o Physical - use a dedicated L3 router for Intel business only

o Logical - use a Virtual Routing Forwarding (VRF) or equivalent separation mechanism to keep Intel

business routing isolated from the non-Intel business networks

**MONITORING:**

For all sustaining network management the following is required of supplier:

 Notify Intel when significant changes are made, by updating requirements for review above. Change exam- ples include: Device upgrades, operating system upgrades, major system updates, equipment modifica-

tions or security configuration change

 Provide network device configuration / change reports compliant to “review” paragraph above

 Network excursion reporting process includes Intel Information Risk and Security Management (IRSM), In- tel Network Engineering (NE) and Threat Management as defined in section 2.1 ODC Operational Security

Expectations

 Intel reserve the ‘right to inspect’ all ODC on-site networking equipment

 All networking equipment security event logs preserved for forensic evaluation and made available to Intel

Security in the event of an incident

Remote audit capability of ODC network hardware is supported or enabled when requested by Intel

 Provision for Intel to access ODC network for evaluation of device configuration. Intel to provide scanning source IP to supplier.

 Firewall rule allowing Intel scanning services access to ODC networking equipment. Intel to provide details on device configuration.

ODC networking hardware is registered in an asset register database

 Assets must be traceable to an owner

 Asset data must be made available to Intel Network Operation for use in case of emergency

**2.0 ODC Operational Security Expectations**

**2.1 Classified data**

|  |  |
| --- | --- |
| REQUIRED  for all Data | REQUIRED for  ITS data |
| 1. ODC Physical Security Requirements are implemented in full.  2. Systems logical access managed in alignment to physical access.  3. Supplier employs continuous improvement programs for ODC con- trols where required.  4. Intel assets are not to be removed from ODC unless preapproved by  Intel and each asset must be traceable and auditable.  5. Supplier network must be separated from Intel’s distributed net- work.  6. Lab networks must be isolated or segregated from Intel’s network.  7. HVPIP, On Loan equipment and Intel IP documents must be pro- tected at all times, and must be locked up when not in use.  8. All Intel materials must be inventory managed with regular cycle counts and reporting system.  9. Incidents involving ODC management, ODC personnel, or unauthor- ized data access are to be reported to  *Report Incident to Intel*.  10. Incidents which result in loss or damage to Intel assets and/or HVPIP  must have a local police report number reported to Intel.  11. Supplier to implement compliance audit programs to measure ODC  controls success and provide results reports to Intel upon request.  12. Post ODC rules, and implement read and understand process in loca- tion seen by all ODC CW’s working on Intel projects. |  Storage devices, smartphones, cameras and camera phones are prohibited in Lab areas, Data Cen- tres and the ODC office area at all times.   All storage devices Top Secret data must have storage encryption em- ployed.   |

**2.2 Additional Rules**

These ODC Rules should be printed and posted clearly in the ODC

**ODC Rules include but are not limited to:**

REQUIRED for all data

 Treat all Intel data as confidential (as defined in the Master Services Agreement (MSA))

 Intel pre-approval required before removal of Intel assets from ODC

 Systems account sharing is prohibited

 Do not let others use your system, you are accountable

 Be aware all systems, applications and accesses are monitored and logged

 Prohibit Storage media (CD/DVD-ROM’s, Disk drives, USB flash, iPods & MP3) where Intel Top Secret projects are executed

 Photography in ODC or ODC labs is strictly prohibited without Intel Business or Security approvals

 Print on coloured paper only – to identify Intel printed materials

 Printed materials cannot be removed from ODC

 Printed materials disposal by shredding

 Do not share Intel information with others, unauthorized access is not permitted

 Do not install unauthorised or unlicensed software on Intel systems

 Intel system administration is restricted to Intel’s Technical Assistance group

 All Intel HVPIP materials, on loan equipment, printed IP documents and/or Intel devices must be protected at all times, and locked away when not in use

**2.3 Engineering Samples**

|  |  |
| --- | --- |
| Intel Products |  Engineering Samples: loose components, Boards w/Silicon, system, Form Factor Reference  Design (FFRD) and Solid State Disks (SSD’s) |
| Unit Tracking |  All Engineering Samples are to be tracked by unique identifier supplied at Intel   Supplier to maintain an up to date inventory of Intel assigned Engineering Samples   Implement secure Unit Tracking System (UTS) for location of all Engineering Samples inventory   If serial number is not readable, unit tracking can be performed at a batch level |
| Inventory Verification |  Inventory reconciliation between Intel business unit and supplier   Verification frequency and sample size to be defined by Intel business (Minimum quarterly required)   Any discrepancy must be resolved within one week. If missing a unit, report to the Intel project lead so that Intel can conduct an incident response.   Reconciliation document will be used as audit evidence during Intel compliance audit |
| Secure handling/Storage |  Inventory must be kept secured location for storage with limited user access   Use a lockable cabinet, drawer, cage or room to secure storage   CCTV for monitoring secure cabinets and cages   Samples in immediate use should be in the ODC office / lab area (i.e. Work-In-Progress  (WIP) material). When not in use, samples must be stored in a secured location. |
| Scrapping/Retention |  Defective, damaged or End of Life Samples must be returned to Intel business owner   Shipping documents to be retained until RMA process step has completed   Shipping must be via licensed carrier with tracking capability utilized and must require sig- nature on receipt |

**3.0 Universal Security Principles**

Generally accepted principles with common practices used in securing IT systems

**3.1 Intel Infrastructure Access Prerequisites**

|  |  |
| --- | --- |
| REQUIRED for all data | REQUIRED for ITS data |
| All Supplier, Partner and sub-contractor associates requiring access  to Intel sites and Intel systems as administrators must have appro- priate training and a background check/investigation (BI) complete.   **Training:** Security training is required annually for all staff.  Without completion, account access must be disabled.   Information Security Essentials for CW’s – Required for all employees   Contingent Worker Ethics/Code of Conduct – Required for all employees   Privacy Essentials - Required only when accessing Personal data   **Implement Intel Information Security Policy of:**   Minimum Access Privilege   Need-to-know access   Separation of Duties   **CW Agreement & NDA form**  Each associate will be required to complete a Contingent  Worker (CW) Agreement & NDA form at the Intel badge & Key  process  **Conflict of Interest**   Supplier must disclose if they provide similar services/support to Intel's competitors   Supplier must ensure that Intel Architecture projects are not  co-located with other Architecture projects even if both are In-  tel projects. Contact Intel Information Security for help. |  Access to ITS systems will require spe- cific approvals defined by a RUNDA,  and access will be monitored. Access approvals are temporary and authori- zation is reviewed on regular cadence.   When access is no longer required, re- newal should not be requested   **Background Checks**  *All persons requiring access to ITS data*  *must have a background investigation com- pleted. Supplier’s obligations in regard to Background Information will align with lo- cal privacy and labour legislation and/or with Intel’s local customs and practices. To check on details of Intel’s local processes in this matter Supplier should check with their procurement contact. Buyer may request to understand what background investigation checks are implemented by default.*  Supplier must retain background data, which could be auditable by Intel in the event of an incident.   **Training:** Additional Security training is required annually for all staff with access to sensitive information.   Handling Classified Infor- mation   Classifying Information  Intel must understand by current metrics:   Volume of associates with required training complete   Breakout of what training has been completed |

**3.2 Legal and Regulatory Requirements**

|  |  |
| --- | --- |
| REQUIRED for all data | REQUIRED for ITS data |
| All Supplier, Partner and sub-contractors must be knowledgeable  and at all times compliant with all regulatory and local governing laws that are applicable to Intel for support function outsourced. Examples include but not limited to: Privacy, HIPAA, SOx, U.S. Ex- port license and PCI-DSS compliance.   **Training:** Controlled Country (CC) / Controlled Technology (CT)  training is required annually for all staff that are:   Resident in a CC   Has a CC/CT support responsibility  Note: Intel is a US registered company and therefore is bound by US Dept of Commerce Export requirements. Remote access to Controlled Technology and/or High Performance Computing con- tent can be considered an import. | Note: *Intel is a US registered company and there-*  *fore is bound by US Dept of Commerce Export re- quirements. Remote access to Controlled Technology and/or High Performance Computing content can be considered an import. For details go to* [*http://www.bis.doc.gov/*](http://www.bis.doc.gov/) |

**Requirements**

Intel from Offshore / Offsite Design Center (ODC)

**ODC NETWORK CONNECTIVITY:**

 Network connections must be submitted using the ‘ODC Portal’.

 User access to data must utilize Intel approved network services.

 Additional capacity for existing projects must be reviewed prior to enabling.

**ODC CLIENT / ODC SERVER:**

 Clients / Servers used by supplier must be able to connect to Intel for updates.

 Clients / Servers resources must be registered to the owner / primary user of the device.

 Client / Server logon credentials must not be shared between team members in the ODC.

 Clients not managed by Intel must not use network connections established by Intel clients.

 Clients / Servers must have malware antivirus services that meet or exceed Intel standards.

**ODC DATA PROTECTION:**

 Data collected from Intel project services must not be transferred to non-Intel managed clients.

 Data must not be migrated to storage repositories without authorization and approval.

 Encryption must be applied to data at rest and while in transit.

 Project data must be segregated one project from another.

**ODC LOGGING / MONITORING / ALERTING:**

 Network security monitoring must be utilized on networks where Intel project work is located.

 Compute devices in the ODC must be protected from unauthorized use.

 Cyber excursions must result in notification to Intel project sponsor(s).

|  |  |
| --- | --- |
| REQUIRED for all data | REQUIRED for ITS data |
| Supplier employees must never share Intel account credentials. Suppliers will implement a process to ensure all associates are made aware of this requirement.  Remote access to Intel’s network must be via a managed secure connection solution. Exceptions must be approved by Intel business management and documented with an IS policy waiver before ac- cess is granted. Contract the Intel business sponsor for assistance.  All Intel assets and equipment must be stored and managed to en- sure there are appropriately secured and access is managed to the need to know level. Inventory validation on regular cadence is re- quired to ensure all items are accounted for. Missing items must be reported to Intel immediately.  ***Preapproval required before removal of asset/ equipment from***  ***ODC (including laptops):***   *Intel CW Sponsor must approve in writing*   *Time frame has to be defined (max. one month)*   *Reason for removal has to be clearly stated*   *Record approvals, may be audited*   *Update inventory tracking database to assure traceabil- ity*  ***Return of asset/ equipment to ODC***   *Intel owns responsibility for Intel asset and account manage- ment. When a user is being off boarded the account must be*  *terminated and assigned devices returned to Intel*   *Intel CW Sponsor must be informed as soon as the asset/*  *equipment is returned to ODC*   *Update inventory tracking database to assure traceabil- ity*   *Provide architecture layout that include CCTV, Badge*  *Readers, Hard Walled / Lab / Network Closet*  Compute devices must have data disposal completed within 10 days of CW off boarding or system no longer required for project support | All Client systems with sensitive information must have full volume encryption enabled.  All sensitive information in draft must be pro- tected by encryption. Intel’s Enterprise Rights Management (ERM) is one capability or option to implement. The Intel business owner must be in- cluded into the ERM entitlements.  All systems accessing or storing sensitive data must have encryption implemented. This applies to laptops and desktops. Intel approved capabili- ties are McAfee EEPC or embedded SSD encryp- tion. Contact Intel business rep or Intel ODC Services for assistance.  Electronic data disposal: Any sensitive infor- mation must be securely disposed of when no longer in use, even if storage encryption was used. |

**6.0 ODC Governance & Compliance**

**6.1 Intel ODC Governance & Compliance**

All ODC’s are subject to Intel governance oversight, an ODC Security Controls review will be scheduled on a cadence based on the sensitivity of the data accessed and managed.

**6.2 Supplier Compliance Expectations**

Supplier has responsibility to ensure security requirements are adhered to and remain consistent throughout the duration of the project/support. Below is a sample of a minimum compliance checklist. This can be tailored in order to fit business requirements. Completed checklists should be posted to the Intel ODC portal.

Any changes in ODC location, size, controls status or ODC additions must be communicated to Intel ODC Governance and Compliance program in advance.

|  |  |  |  |
| --- | --- | --- | --- |
| **Intel ODC Minimum Controls Compliance Checklist** | | | |
| Company: ODC Ref #: Audit Date: | | | |
| Audit item | Yes | No | Details |
| **Physical** |  |  |  |
| Entry Points have access controls to the granularity of each authorized person |  |  |  |
| Access logs retained for min of 3 months |  |  |  |
| All entry door sound alarm when propped open for > 30 seconds (tested) |  |  |  |
| All emergency door activate alarm when opened |  |  |  |
| All windows locked and include tamper proof sensors |  |  |  |
| Incidence response to alarm activation for all sensors, (doors and windows) |  |  |  |
| Unauthorized access prevention (e.g. false ceilings, wall not true floor to ceiling) |  |  |  |
| Perimeter glass obscured, includes windows if ODC is a ground floor location |  |  |  |
| ODC is not labeled or identified as Intel |  |  |  |
| CCTV monitoring ODC entry doors |  |  |  |
| Security monitoring 24 x 7 |  |  |  |
|  |  |  |  |
| **Access Management** |  |  |  |
| Visitor policy in place |  |  |  |
| No tours policy |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| ODC authorized access list scrubbed at least once per quarter |  |  |  |
| Authorized access based on need to know basis for Intel business support only |  |  |  |
|  |  |  |  |
| **Network** |  |  |  |
| Only one network distributed in the ODC |  |  |  |
| Network equipment in locked access controlled location and restricted |  |  |  |
| If Intel network is distributed in ODC – air gap isolation implemented |  |  |  |
| If Intel managed network is accessed - network enclave or segregated VLAN |  |  |  |
| Firewall documented / configured / monitored (refer to Intel’s Firewall Tech-  nical Design Review (FTDR) documentation) |  |  |  |
|  |  |  |  |
| **Operations** |  |  |  |
| ODC Rules posted inside ODC |  |  |  |
| Prohibit Storage devices (USB, Cameras, Camera phones, Smartphones in ODC) |  |  |  |
| Clean desk policy enforced (tested) |  |  |  |
| Only approved laptops and systems are taken into or removed from ODC |  |  |  |
| If Printer is mandatory then only color coded paper is used in ODC |  |  |  |
| Validate process to prevent color paper removal from ODC |  |  |  |
| Paper shredder use for all confidential waste |  |  |  |
| All Intel issued PC are returned to Intel at associate off boarding or termination |  |  |  |
| Exit interview includes NDA's ‘continue past project support’ clause |  |  |  |
| All Intel issued servers have been returned to Intel post project completion |  |  |  |
| All servers with Intel Restricted and/or Top Secret information have data secu- rity deleted - certificate of disposal required or hard disk drive sent to Intel for destruction |  |  |  |
|  |  |  |  |
| **Training & Resourcing** |  |  |  |
| All staff trained and aware of challenging Unauthorized Access if detected |  |  |  |
| All staff trained and aware of ODC operations requirements |  |  |  |
| All staff completed Intel annual training requirements |  |  |  |
| Information Security Essentials - % complete |  |  |  |
| Contingent Worker (CW) Ethics / Code of Conduct - % Complete |  |  |  |
| Privacy Essentials (Required if Personally Identifiable Information is accessed) -  % complete |  |  |  |
| Handling Classified Information (Required fir Restricted & Top Secret data ac-  cess) - % Complete |  |  |  |
| Controlled Technology (Req. if access to Controlled/HPC technology or located  in a Controlled Country) |  |  |  |
|  |  |  |  |
| **For Intel issued systems all staff aware :** |  |  |  |
| No account sharing with others and limit Intel systems for business use only |  |  |  |
| Intel Systems administration restricted to Intel TAC administrators only |  |  |  |
| Additional or non-Intel unapproved software deployment prohibited unless  fully licensed |  |  |  |
| PC systems should only be removed from the ODC on approved business need |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **For Non-Intel systems supporting Intel:** |  |  |  |
| Minimum Systems Security requirements defined checked for compliance (de- pendent on remote connection) |  |  |  |
| Servers are located in a secure managed location, outside this location servers  are prohibited |  |  |  |
|  |  |  |  |
| **Resourcing Process** |  |  |  |
| Assigned staff background checks completed |  |  |  |
| Each assigned staff member has completed CW Agreement & NDA form at Intel |  |  |  |
| All assigned staff complete own in house induction and training program |  |  |  |
| Associates supporting Intel comply with contractual cool-off period |  |  |  |
|  |  |  |  |
| **Management of Intel assigned equipment and materials** |  |  |  |
| Inventory of Intel assigned equipment is maintained |  |  |  |
| Monthly inventory check includes discrepancy check |  |  |  |
| Software user licenses for non-Intel sourced/issued software obtained |  |  |  |
| U.S. Dept. of Commerce Export License requirements have been met |  |  |  |
| Intel equipment or HVPIP products are secured when not in use |  |  |  |
|  |  |  |  |
| **IP Protection:** |  |  |  |
| Drop ship location for HVPIP delivery the same as SAP shipping designation |  |  |  |
| Tracking, handling, scrap and loss process in place for HVPIP |  |  |  |
| Is there a matching reports to Security Incident Report (SIR) |  |  |  |
| Reconciliation report for loss identified |  |  |  |
|  |  |  |  |
| **Current Projects:** |  |  |  |
| Projects in the ODC are classified and match what is in the ODC Portal? |  |  |  |
| Intel project sponsor or Intel business group is identified |  |  |  |
|  |  |  |  |
| **Contingent Workers:** |  |  |  |
| Contractors can be associated to the Intel project they are assigned to |  |  |  |
| Contractors use an approved remote access (RVPN / Citrix XenApp / MOKA ) |  |  |  |
|  |  |  |  |
| **Lab Registration / Inventory:** |  |  |  |
| ODC labs in the registered with Intel |  |  |  |
| Registered labs have completed the annual security survey |  |  |  |
|  |  |  |  |
| *Legal = Approver / Procurement = Approver / GST = Approver / ISRM = Decider* |  |  |  |
|  |  |  |  |