INTEL'S SUPPLIER COMPLIANCE HANDBOOK

The Supplier Compliance Handbook is a resource for Intel suppliers to access Intel policies and supplier expectations. Intel reserves the right to update the Supplier Compliance Handbook from time to time.

Contents

© 2021 Intel Corporation

1. DEFINITIONS

1.1 For purposes of this Intel's Supplier Compliance Handbook only, the following definitions apply:

(A) "**Agreement**" means collectively: (a) the agreement between Supplier and Intel that incorporates this Intel's Supplier Compliance Handbook by reference; and (b) this Intel's Supplier Compliance Handbook as incorporated.

(B) "**Supplier**" means the party or parties with whom Intel is contracting under the Agreement.

2. PRIVACY & DATA SECURITY

2.1 Compliance with Applicable Privacy Laws & Regulations. Supplier and Intel agree to fully comply with all applicable laws and regulations governing the privacy, security, storage, transfer and use of Intel Data.

2.2 No Information Selling. Supplier agrees that you do not receive any Intel Data as consideration for any services or other items that Supplier provides to Intel. Supplier shall not have, derive or exercise any rights or benefits regarding Intel Data. Supplier must not sell any Intel Data, as the term "sell" is defined in the California Consumer Privacy Act of 2018 ("**CCPA**"), and agrees to refrain from taking any action that would cause any transfers of Intel Data to or from Supplier to qualify as "selling personal information" under the CCPA. Supplier must not collect, retain, share, disclose, or use any Intel Data: (i) for any purpose other than for the specific purpose of performing services or selling goods to Intel pursuant to written agreements with Intel; or (ii) outside the direct business relationship between Supplier and Intel.

2.3 Control and Ownership. Supplier must not access, collect, store, retain, transfer, use or otherwise process in any manner any Intel Data, except: (i) in the interest and on behalf of Intel; and (ii) as directed by authorized personnel of Intel in writing. Without limiting the generality of the foregoing, Supplier may not make Intel Data accessible to any subcontractors or relocate Intel Data to new locations, except as set forth in written agreements with, or written instructions from Intel. Supplier must return or delete any Intel Data when Intel requests it, except to the extent that to do so would violate applicable law.

2.4 Comply with Data Security Policies. Supplier must keep Intel Data secure from unauthorized access by using your best efforts and state-of-the art organizational and technical safeguards.

A. Supplier must comply with Intel's Information Security Policy as set forth in the Intel Security Addendum (ISA) available at: https://www.intel.com/content/www/us/en/supplier/resources/misc/documents/intel-security-addendum.html.

B. If Supplier operates one or more cloud computing services to provide contracted services to Intel, Supplier will also comply with the ISA Appendix A – Cloud Security available at:

© 2021 Intel Corporation

https://www.intel.com/content/www/us/en/supplier/resources/misc/documents/isa-appendix-a-cloud.html.

C. If Supplier operates one or more Outsourced Development Centers to provide contracted services to Intel, Supplier will also comply with the ISA Appendix B – Outsourced Development Center Security available at: https://www.intel.com/content/www/us/en/supplier/resources/misc/documents/isa-appendix-b-outsourced-dev-center.html. If Supplier will handle personal card holder data (CHD), then Supplier's handling of such data is subject to the Payment Card Industry (PCI) data security standard available at: https://www.intel.com/content/www/us/en/supplier/resources/misc/documents/isa-pci-addendum.html.

2.5 Cooperate with Compliance Obligations. At Intel's reasonable request, Supplier must: (i) contractually agree to comply with laws. regulations or industry standards designed to protect Intel Data, including, without limitation, the Standard Contractual Clauses approved by the European Commission for data transfers to processors, the Payment Card Industry Data Security Standard, Health Insurance Portability and Accountability Act requirements for business associates, the CCPA, as well as similar and other frameworks, if and to the extent such frameworks apply to any Intel Data that Supplier comes into contact with; or else (ii) allow Intel to terminate certain or all contracts with Supplier. Such termination will be subject to (a) a proportionate refund of any prepaid fees, (b) provide transition or migration assistance as reasonably required, and (c) do so without applying any early termination charges or other extra charges.

2.6 Submit to Audits. Supplier must submit to reasonable data security and privacy compliance audits by regulators, Intel and/or, at Intel's request, by an independent third party, or customers of Intel, to verify compliance with this terms, applicable law, and any other applicable contractual undertakings.

2.7 Notify Breaches. In the event of any act or omission by Supplier that compromises the security, confidentiality or integrity of Intel Data or the safeguards put in place by Supplier to protect Intel Data (collectively, a "**Security Incident**"), Supplier will, at your own expense: (i) notify us without undue delay but no later than forty-eight (48) hours after Supplier becomes aware of the Security Incident or suspects that it has taken place; (ii) consult and cooperate with us in connection with any investigations, proceedings and efforts to discharge any requirements under applicable laws relating to the Security Incident; (iii) immediately commence a forensic investigation of the Security Incident and take appropriate remedial steps to minimize the harm to us; and (iv) provide any information reasonably requested by us. To the fullest extent permitted by applicable law, Supplier shall not inform any third party of any Security Incident without first obtaining our prior written consent from Intel.

© 2021 Intel Corporation

Specific terms related to Security Incidents is set forth in the Intel Security Addendum referenced in Section 5.

2.8 EEA Personal Data. With respect to any Intel Data that is subject to the EU General Data Protection Regulation ("**GDPR"**) or similar laws of other countries as "personal data," Supplier accepts the following obligations as a data importer, processor or subprocessor, as the case may be, and agrees that it:

a. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; also, the processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR, national data protection laws in the EU or other applicable law;

b. ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c. takes all measures required pursuant to Article 32 of the GDPR (security of processing);

d. respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor;

e. taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, including, without limitation, right to access, rectification, erasure and portability of the data subject's personal data; (for the avoidance of doubt, processor shall only assist and enable controller to meet controller's obligations to satisfy data subjects' rights, but processor shall not respond directly to data subjects)

f. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (Security of personal data) taking into account the nature of processing and the information available to the processor;

g. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

© 2021 Intel Corporation

2.9 Employees and Contractors. These terms also apply to Supplier employees in the course of perform their duties and Supplier's contractors, and Supplier shall use your best efforts to ensure that they comply with these terms.

2.10 Intel Contacts. Notwithstanding any contact information in governing agreements, for the purpose of Section 7 Security Incident Notifications, contact: Intel IT Emergency Hotline- (916) 356-8910 or InfoSecRM2@intel.com Privacy questions should be directed to *privacy.feedback@intel.com*.

3. ADDITIONAL COMPLIANCE WITH LAWS AND RULES

3.1 Anti-Corruption Laws

(A) Supplier represents and warrants that, in the course of performing work for Intel, neither it, nor anyone acting on its behalf, has violated or will violate the US Foreign Corrupt Practices Act; the UK Bribery Act; or any other applicable anti-corruption law (the "**Anti-Corruption Laws**"). Supplier represents and warrants that it has not and will not directly, or indirectly through any other person or entity, offer, promise, authorize, solicit, pay, or give anything of value to any Government Official for the purpose of:

(1) Influencing an act or decision of the Government Official in his or her official capacity,

(2) Inducing the Government Official to do or omit to do any act in violation of the lawful duty of such official,

(3) Securing an improper advantage, or

(4) Inducing the Government Official to use his or her influence to affect or influence any act or decision of a government or instrumentality, in each case in order to assist Intel or any of its affiliates in obtaining or retaining business.

"**Government Official**" means any officer, employee, or person acting in an official capacity for any government department, agency, or instrumentality, including any state-owned or -controlled company and any public international organization, as well as any political party, political party official, or candidate for political office, and includes any agent or intermediary of any of the foregoing.

(B) Supplier represents and warrants that, unless previously disclosed to Intel in writing, none of its employees, directors, owners, officers, or principals, or any immediate family member of a director, owner, officer, or principal, is a Government Official with influence over the work being performed for Intel. Supplier will notify Intel within five business days if at any time any of Supplier's employees, directors, owners, officers or principals is named, appointed, or otherwise becomes a Government Official with influence over the work being performed for Intel. If, in Intel's opinion, that change increases its

© 2021 Intel Corporation

compliance risks, the parties will work together to reach an acceptable solution. If no acceptable solution can be found, the change will constitute grounds for Intel to terminate its relationship with Supplier.

(C) Supplier certifies that it will ensure that subcontractors, subagents, vendors, or any other third parties performing services in connection with Supplier's relationship with Intel and acting under Supplier's authority or control are aware of and do not violate the Anti-Corruption Laws.

(D) If Supplier learns of or suspects any payment or transfer of value (or any offer or promise to pay or transfer) in connection with the work being performed for Intel that would violate or likely violate the Anti-Corruption Laws, it will immediately disclose the violation or potential violation in writing to Intel.

3.2 **Federal Contract Requirements**

(A) Intel is an equal opportunity employer and federal contractor or subcontractor. Consequently, the parties agree that, as applicable, they will abide by the requirements of 41 CFR 60-1.4(a), 41 CFR 60-300.5(a) and 41 CFR 60-741.5(a) and that these laws are incorporated herein by reference. These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities and prohibit discrimination against all individuals based on their race, color, religion, sex, sexual orientation, gender identity or national origin. These regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, protected veteran status or disability. The parties also agree that, as applicable, they will abide by the requirements of Executive Order 13496 (29 CFR Part 471, Appendix A to Subpart A), relating to the notice of employee rights under federal labor law.

(B) Section 889, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

1. Supplier represents that it will not: (i) deliver or provide to Intel Corporation any "covered telecommunication equipment or services" as defined in 48 CFR 52.204-25(a); (ii) deliver or provide any equipment or system that uses any "covered telecommunications equipment or services" as defined in 48 CFR 52.204-25(a); nor (iii) use any "covered telecommunications equipment or services" as defined in 48 CFR 52.204-25(a) in delivering any services to Intel Corporation.

© 2021 Intel Corporation

2. Section 889 questions should be directed to securitycompliance@intel.com.

3.3 International Trade Compliance

(A) Export Compliance: Supplier will comply with all applicable U.S. export control laws and regulations, including but not limited to those in the Export Administration Regulations (§15 CFR 730 et seq) and International Traffic In Arms Regulations (§ 22 CFR 120 et seq) in relation to its obligations. Supplier acknowledges that Intel products and technology are subject to United States export regulations, which apply extra-territorially, and that U.S. export control laws and regulations may apply to any shipment, transmission, transfer, or release to any foreign person (defined in 15 CFR 734.2 and 22 CFR 120.16) of technology (technical data, information, or assistance) and software (commercial or custom), regardless of where (inside or outside the United States) or how it may occur. Supplier agrees to obtain any required export license for its employees or contractors for work on any Intel site where Intel export-controlled technology will be released.

(B) Classification, Origin and Marking: Supplier will ensure that commercial invoices reflect the correct export and harmonized tariff schedule (HTS) classifications and country of origin designation. Supplier will comply with marking requirements such that physical deliverables are marked with the country of origin in accordance with applicable laws and regulations. Supplier will maintain (and provide to Intel upon request) supporting documentation sufficient to: (i) satisfy an audit of origin determination by Intel or by any government entity; and (ii) enable Intel to apply for and obtain any export, re-export, import, supply or use authorization for the deliverables.

(C) Security-Related Programs. Supplier will comply with all applicable requirements of security-related programs established under or in relation to the World Customs Organization (WCO) Framework of Standards to Secure & Facilitate Global Trade, including but not limited to the United States Customs – Trade Partnership Against Terrorism (CTPAT) and Authorized Economic Operator (AEO) programs, and will meet applicable criteria set forth in such programs established in applicable jurisdictions. Upon request, Supplier will certify in writing and provide documentary evidence of such compliance.

3.4 Whistleblower Rights. Nothing in this Agreement shall prevent a party from lawfully communicating to government authorities possible violations of federal, state, or local law or other information that is protected under the whistleblower provisions of federal, state, or local law.

© 2021 Intel Corporation

3.5 Counterfeit Items

(A) The following definitions apply to this clause:

1. "**Counterfeit Item**" means an Item that is or contains an unlawful reproduction, substitution, or alteration or that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified Item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes, but is not limited to, 1) used Electronic Parts represented as new, or 2) false identification of grade, serial number, lot number, date code, or performance characteristics.

2. "**Electronic Part**" means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, adhesive, substrate, or diode), or a circuit assembly comprising or contained in any Item, including any embedded software or firmware.

(B) Supplier agrees and shall ensure that no Items provided to Buyer are Counterfeit Items or contain Counterfeit Items. Supplier shall establish and maintain a process for trained personnel to inspect and test Items, including Electronic Parts, including criteria for acceptance and rejection, methodologies to identify suspect Counterfeit Items and a means to rapidly determine if a suspect Counterfeit Item is, in fact, a Counterfeit Item. Supplier shall monitor industry trends related to counterfeiting, including detection and avoidance techniques contained in appropriate industry standards.

(C) Supplier shall establish a process to prevent the proliferation of Counterfeit Items. In the event Counterfeit Items are delivered to Buyer the Supplier shall, at its expense, promptly replace such Counterfeit Items with genuine Items conforming to the requirements of this Agreement. Any Counterfeit Items that Buyer discovers and returns to Supplier (e.g. for testing or verification) shall be destroyed by Supplier.

(D) Supplier shall maintain, implement, and utilize a process that enables tracking of Items and components incorporated in Items from the original manufacturer to product acceptance by the Buyer. Supplier shall provide authenticity and traceability records to Buyer upon request.

(E) To protect Buyer from procuring Counterfeit Items, Supplier shall be original equipment manufacturer (OEM), the original software

© 2021 Intel Corporation

developer, or an OEM authorized distributor or reseller for an original source.

(F) Supplier shall notify Buyer when Supplier becomes aware or suspects that it has furnished a Counterfeit Item(s) and shall quarantine any Counterfeit Items.

(G) Supplier shall include this clause or equivalent provisions in lower tier subcontracts for the delivery of any materials that will be included in or furnished as Items to Buyer. In all cases, Supplier will be primarily liable to Buyer for any and all Counterfeit Items delivered to Buyer.

4. RETENTION AND AUDITS

4.1 Supplier will maintain complete and accurate records of all work associated with the performance of the Agreement, including but not limited to, the items tendered, services performed, work conducted, processes used, personnel involved, and deliverables performed under the Agreement, until the latest of: (a) seven years after the completion of such services, delivery or performance of items; or (b) the period required by applicable laws; or (c) the expiration of the Agreement.

4.2 To ensure compliance with the terms of the Agreement, minimize supply chain risk, ensure quality, secure supply, or ensure safety of items purchased from or offered for sale by Supplier, Supplier will fully cooperate with Intel, or a third party designated by Intel, who may at any time use reasonable means to inspect Supplier's work, documents, property, assets, records, and communications. Inspections may be made at Intel's written request for any reason in good faith, conducted in accordance with the terms of the Agreement, and not unreasonably interfere with Supplier's normal business activities or operations. Within two weeks of receipt of Intel's written request for such an inspection, Supplier will employ commercially reasonable efforts to disclose, make available, or obtain and provide any necessary consent for Intel, third party, or authorized government authority to conduct their inspection. Furthermore, should any third-party inspection find that Supplier is not in compliance with the terms of the Agreement Supplier will reimburse Intel for all costs associated with such inspection.

5. ELECTRONIC SYSTEMS

5.1 For the purposes of this Electronic Systems section only, the following definition applies:

(A) "**Electronic Ordering System**" means any web-based ordering system, electronic purchase order system, electronic order acknowledgement, form of electronic order acceptance, or any software-based ordering system. Electronic Ordering Systems do not include any systems

designed for the negotiation, signature, offer, or acceptance of purchase specifications or configuration specifications.

5.2 Supplier is hereby given notice and agrees that the persons responsible for using any Electronic Ordering Systems originating from Supplier on behalf of Intel do not have any actual or apparent authority to create legally binding obligations which are different from the terms and conditions contained in the Agreement.

5.3 The parties agree that any different or additional terms and conditions offered by Supplier through an Electronic Ordering System will not be legally binding on Intel, and that any of Supplier's "click to accept" arrangements or Electronic Ordering Systems will not be legally binding on Intel.

5.4 The parties agree to accept electronic records and electronic signatures (as such terms are defined in the U.S. Electronic Signatures in Global and National Commerce Act) relating to transactions contemplated by the Agreement.

5.5 Supplier represents and warrants to Intel that any of Supplier's personnel using electronic signatures, electronic approvals, or "click to accept" type arrangements originating from Intel, to accept purchase specifications, configuration specifications, or purchase orders, have the authority to accept to such specifications or purchase orders.

5.6 If a party has adopted an electronic identifier such as a digital signature, or electronic approval for a specification, the other party is entitled to rely on the authenticity of documents signed by, approved, or associated with that electronic identifier unless that party had previously received written notification stating otherwise from the party using the electronic identifier.

6. FINANCIAL DATA

6.1 If Intel is unable to access Supplier's audited annual and quarterly financial statements made in accordance with Generally Accepted Accounting Principles (GAAP), Supplier will, upon request, provide Intel with copies of such statements within three months of the period closing date. Supplier has an option to either complete the Intel provided excel base template or provide full financial statements accepted by GAAP. If GAAP is applicable to Supplier, then these statements must include either independent auditors' opinion or a signed management letter, which states that the financial statements provided to Intel are in conformity with GAAP.

7. ACCESSIBILITY

7.1 If Supplier's primary products or service is a software application with a user interface, the following provisions apply: Supplier hereby represents and warrants that products and services, as well as the information, documentation

and support for the products and services, are compliant with all applicable federal, state and local accessibility laws and standards, including the Twenty-First Century Communications and Video Accessibility Act of 2010, Sections 504 and 508 of the Rehabilitation Act of 1973, and the Americans with Disabilities Act. Supplier also represents and warrants that products and services (including any user interfaces) conform to the Web Content Accessibility Guidelines, Levels A and AA, and the requirements set forth in 36 CFR Part 1194 (Electronic and Information Technology Accessibility Standards), as amended from time to time. Supplier agrees to promptly respond to and resolve any complaint regarding accessibility of the products and services which is brought to its attention and to remediate accessibility defects to comply with the above referenced laws and regulations and to retain a third party accessibility expert to evaluate the products and services, information, documentation and support if necessary for remediation.

8. INTEL'S GIFTS, MEALS, ENTERTAINMENT, & TRAVEL POLICY FOR THIRD PARTIES

8.1 Code of Conduct: Intel's Code of Conduct reflects our commitment to conduct business with uncompromising integrity and in compliance with all applicable laws. We expect all companies or persons who provide services or act on behalf of Intel ("Third Parties") to comply with our Code of Conduct, including our anti-corruption policy, regardless of local business practices or social customs.

8.2 Giving and Receiving Gifts, Meals, Entertainment and Travel ("GMET"): The exchange or provision of GMET may create a real or perceived conflict of interest or a situation where those types of expenses could be viewed as a bribe under applicable laws and international standards. Intel expects its Third Parties to comply with the following principles when giving or receiving GMET:

(A) Compliance with Applicable Law: Supplier must comply with anti-corruption laws, including the U.S. Foreign Corrupt Practices Act, the UK Bribery Act, and applicable local laws, when giving or receiving GMET in connection with Intel business.

(B) Business Purpose: The GMET must be for a legitimate purpose, such as to promote, demonstrate, or explain an Intel product, position, or service.

(C) No Improper Influence: The GMET must not place the recipient under any obligation. You must never offer, promise, or give anything of value with the intent to improperly influence any act or decision of the recipient in Intel's or your company's favor, or with the intent of compromising the recipient's objectivity in making business decisions.

© 2021 Intel Corporation

(D) Made Openly: The GMET must be given or received in an open and transparent manner.

(E) Reasonable in Value: The GMET must be reasonable in value and neither lavish nor excessive.

(F) Appropriate: The nature of the GMET must be appropriate to the business relationship and local customs, and not cause embarrassment by its disclosure.

(G) Accurately Recorded: Supplier must accurately record all GMET provided on Intel's behalf. You must be able to produce receipts or proper documentation for all GMET expenses.

(H) Government GMET: Supplier may not give GMET on Intel's behalf to a government official (including employees of government agencies, public institutions and state-owned enterprises) without prior approval from Intel. Approval will be provided only in limited circumstances and, in some cases, will require the approval of Intel Legal. All GMET provided on Intel's behalf to a government official must be properly recorded, with appropriate receipts or proper documentation.

8.3 GMET Involving Intel Employees: Intel employees must comply with Code of Conduct and internal policy requirements and restrictions, including pre-approval requirements, when giving or receiving GMET to or from a Third Party. We discourage Intel suppliers and vendors from giving any gifts to our employees and appreciate your support on this request.

8.4 How to Raise Questions or Concerns: If you have questions or concerns, you have numerous avenues to report them to Intel. Click here to find more information: https://secure.ethicspoint.com/domain/media/en/gui/31244/index.html

9. INTEL'S CONTINGENT WORKFORCE POLICY

9.1 Intel uses contingent workers consistent with relevant laws associated by geography. Intel requires that Supplier complies with all applicable country laws when providing contingent workers and performing services.

9.2 Intel takes meaningful steps to maintain a distinction between its own employees and contingent workers.

(A) Contingent workers are employees of Intel's Suppliers.

(B) Supplier is solely responsible for providing the management of their employees.

© 2021 Intel Corporation

(C) When under contract by Intel, contingent workers are expected to follow all applicable Intel policies, including but not limited to, safety and ethics polices.

(D) Supplier must comply with Intel's expectations and requirements regarding the contingent workforce program, and Intel reserves the right to audit Supplier's compliance at any time.

(E) If a contingent worker is being requested to perform work beyond his or her statement of work stated in the applicable contract or PO, Supplier is required to escalate to its purchasing representative.

(F) Access to Intel Facilities – All suppliers and their employees are required to complete the worker access forms associated with their region and submit them to the Contingent Worker Outsourced System (Fieldglass) prior to having access to Intel facilities. All Privileged Visitors (PV) are required to complete the PV worker access forms associated with their region and submit them to an Intel Badge Office prior to having access to Intel facilities.

9.3 Intel reserves the right to deny contingent workers Intel access or remove contingent workers from Intel's premises at any time. Any decision by Intel to deny access is solely at Intel's discretion. Any Intel access denial is not intended in any way to dictate suppliers' employment decisions and should not be construed as such. All of the contingent workforce guidelines that have been established support this philosophy.

9.4 WORKPLACE SAFETY AND SECURITY

(A) Suppliers will mitigate workplace safety and security risks when terminating their employees. Specifically, they will:

i. Not terminate their employees on an Intel property;

ii. Create and implement a response plan addressing a case of any terminated employee exhibiting threatening behaviors or makes threats;

iii. Contact their local Intel Security representative (https://sharepoint.amr.ith.intel.com/sites/CS-SiteSecurity/SitePages/Home.aspx) to:

a) Disable the employee’s badge;

b) Notify Intel Security of any threats made or weapons that could potentially be used; and

c) Activate the Workplace Response Team (WRT) if necessary https://sharepoint.amr.ith.intel.com/sites/cs-corporate-security/Programs/WVP/SitePages/Home.aspx

iv. Otherwise terminate their employees in a commercially reasonable way that does not impact Intel’s workplace safety and security.

© 2021 Intel Corporation

(B) Suppliers and their Contingent Workers will make every reasonable effort to provide a safe workplace through the prevention of workplace violence, including without limitation preventing their employees from:

i. Making threats of any kind, whether explicit or implicit;
ii. Exhibiting threatening behavior;
iii. Stalking; and
iv. Acts of violence

(C) These obligations apply whether on Intel property, at work-related events, or using Intel resources to engage in threatening or stalking behavior. These obligations also apply to off-duty conduct that negatively impacts Intel's work environment, such as threatening a coworker off site.

(D) Failure to comply with the terms of the Workplace Safety and Security Section may result in the immediate denial of access to Intel property.

9.5 The Contractor will remind its employees not to attend work if they have a communicable illness (e.g., flu, pink eye).

9.6 If you have any questions, contact your Intel purchasing representative or send an email to purchasing.service.desk@intel.com

10. SUPPLIER DIVERSITY POLICY

10.1 Supplier acknowledges that Buyer has a Supplier Diversity Program (defined below) which, among other initiatives, encourages the participation of women and minorities, including lesbian, gay, bisexual or transgender, disabled and veteran-owned businesses, as suppliers and subcontractors in substantive maters to the fullest extent possible. Supplier should use reasonable efforts consistent with efficient execution of this Agreement to assist Buyer in complying with Buyer Supplier Diversity Program, at no additional charge to Buyer.

(A) Classifications for diverse suppliers or subcontractors ("**Supplier Diversity Classifications**") are provided on https://supplier.intel.com/static/supplierdiversity/ and are incorporated into this section for reference. Suppliers that have met any of these classifications and are certified by a third-party agency acceptable to Buyer are deemed "**Diverse Suppliers**."

(B) Supplier will notify Buyer if it meets any of the Supplier Diversity Classifications and will provide Buyer, upon request, its certification information. If Supplier meets any of these classifications, but has not sought certification, Supplier will promptly seek certification from an agency acceptable to Buyer in accordance with local law where applicable.

© 2021 Intel Corporation

(C) Supplier will not discriminate against Diverse Suppliers and will treat them as Supplier treats its other supplier or subcontractors and Supplier will act in a transparent way regarding business awards without discrimination on the basis of race, color, religion, gender, national origin, ancestry, disability, veteran status, gender expression, gender identity, sexual orientation, or any other characteristic protected by federal, state, or local law, regulation, or ordinance.

10.2 Supplier agrees to fairly consider Diverse Suppliers for participation under this Agreement. Supplier will use reasonable efforts to:

(A) Assist Diverse Suppliers by enabling contracting opportunities and facilitate participation of Diverse Suppliers in regard to quantities, and delivery schedules where practically feasible.

(B) Provide adequate and timely consideration of the potentialities of Diverse Suppliers in "make-or-buy" decisions.

10.3 During the Term of this Agreement, at no additional charge to Buyer consistent with efficient execution of this Agreement Supplier will use reasonable efforts to contract with Diverse Suppliers, in a quantity of goods and services that is equal to or greater in dollar amount to ten percent (10%) of Buyers total dollar amount of purchases under this Agreement ("**Diverse Spending Objective**"). If Buyer is unable to meet the Diverse Spending Objective, , then Supplier will use reasonable efforts to provide Buyer with market data evidencing the lack of Diverse Suppliers and Supplier's inability to meet the Diverse Spending Objective y. Buyer maintains discretion to adjust required Diverse Spending Objective annually with Supplier.

10.4 Buyer requires that Supplier provide Buyer, in a format acceptable to Buyer, four (4) reports per calendar year which specify the total amounts directly invoiced by and paid collectively to Diverse Suppliers for the previous calendar quarter for which the Supplier remitted invoices under this Agreement ("**Diverse Spend Data**"). Buyer requires Supplier to report on a regular schedule. Quarterly deadlines for reporting are found at https://supplier.intel.com/static/supplierdiversity/. Buyer may change the reporting schedule by providing notice to Supplier 30 days before the end of the current calendar year.

11. BUSINESS CONTINUITY POLICY

11.1 Intel's Supplier Business Continuity Policy (the "**Business Continuity Plan**" or "**BCP**") is as follows:

(A) Supplier will ensure their senior management support of Supplier's resources to: (i) identify, assess and prioritize risks, and (ii) develop a coordinated plan to manage and mitigate such supply chain risks.

© 2021 Intel Corporation

(B) The BCP will:

(1) Embrace best known risk management practices that include preparedness, protection, monitoring, containment, response, reporting and recovery

(2) Encompass considerations for short- or long-term business interruptions that may be the result of internal, external, man-made, cyber-attacks or natural disasters.

(3) Be inclusive of its employees; end-to-end supply chain for critical business functions; local infrastructure, facilities, transportation, equipment and information technology systems.

(4) Comply with the guidelines set forth at https://supplier.intel.com.

(C) Suppliers will ensure that the key elements of their BCPs are documented, current, actionable and available to key personnel and Intel when required or requested.

12. OWNERSHIP AND BAILMENT

12.1 All specifications, drawings, schematics, technical information, data, tools, dies, patterns, masks, gauges, test equipment, and other materials that are either: (A) furnished to Supplier by Intel; or (B) paid for by Intel; will: (i) remain or become Intel's property; (ii) be used by Supplier exclusively for Intel's benefit; (iii) be clearly marked as Intel's property; (iv) be segregated from the property of others, (v) be kept in good working condition at Supplier's expense, and (vi) be shipped to Intel promptly on Intel's demand or upon termination or expiration of this Agreement, whichever occurs first. Supplier will treat any such property as confidential information in accordance with the Confidentiality and Publicity section of this Agreement or the CNDA.

12.2 Except for ordinary wear and tear, Supplier will be liable for any loss of or damage to Intel's property while in the possession or control of Supplier or any third party to whom Supplier permits access.

12.3 The terms of this Ownership and Bailment section will survive the termination or expiration of this Agreement.

© 2021 Intel Corporation