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

1. Definitions
2. Privacy & Data Security
3. Additional Compliance with Laws and Rules
4. Retention and Audits
5. Financial Data
6. Accessibility
7. Intel's Gifts, Meals, Entertainment, & Travel Policy for Third Parties
8. Human Rights Principles and Code of Conduct
9. Intel's Contingent Workforce Policy
10. Business Continuity Plan Expectations
11. Ownership and Bailment

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 Personal Data, including without limitation, where applicable, the General Data Protection Regulation EU 2016/679 ("**GDPR**"), Standard Contractual Clauses set out in the Annex to European Commission Implementing Decision (EU) 2021/914 for data transfers to processors ("**SCCs**"), the United Kingdom Data Protection Act of 2018 ("**UK GDPR**"), the UK's Information Commissioner Office's International Data Transfer Addendum to the SCCs as set forth in Section 2.12 below ("**ICO Addendum**"), the Swiss Federal Act on Data Protection ("**Swiss FADP**"), the EU-U.S. Data Privacy Framework Principles, including the Supplemental Principles and Annex I of the Principles ("**DPF**") and the Swiss DPF and UK extension, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act and any subsequent amendments ("**CCPA**"), the Brazilian Data Protection Law ("**LGPD**"), the Chinese Personal Information Protection Law ("**PIPL**"), the Israeli Protection of Privacy Law 5741-1981 ("**PPL**"), the Japanese Act on the Protection of Personal Information ("**APPI**"), the Payment Card Industry ("**PCI**") Data Security Standard, Health Insurance Portability and Accountability Act ("**HIPAA**") requirements for business associates, as well as similar frameworks (collectively, the "**Data Privacy Laws**"). For Personal Data subject to a Data Privacy Law, if a provision of this Section 2 conflicts with the relevant, Data Privacy Law, the Data Privacy Law will prevail. "**Personal Data**" and "**Personal Information**" are defined by the applicable, Data Privacy Law and are used synonymously in this document unless otherwise specified.

2.2 No Information Selling or Sharing for Cross-Context Behavioral Advertising. Supplier will not receive or disclose any Personal Data as consideration for any payments, services, or other items of value. Supplier will not sell, share, or engage in any targeted advertising with any Personal Data, as the terms "sell", "share", and "targeted advertising" are defined in the CCPA. Supplier will not retain, use, or disclose Personal Data: (i) outside the direct business relationship with Intel or (ii) for cross-context behavioral advertising, (iii) except

for the business purposes specified in the written contract with Intel. Supplier must not combine Personal Data with other data if and to the extent such combination would be inconsistent with limitations on service providers under the CCPA.

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

2.4 Comply with Information Security Policies. Supplier must keep Personal Data secure from unauthorized access by using Supplier's 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 Information 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:
C. https://www.intel.com/content/www/us/en/supplier/resources/misc/documents/isa-appendix-a-cloud.html.
D. 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.
E. 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. Supplier must cooperate with Intel to comply with Data Protection Laws designed to protect Personal Data. Upon Intel's reasonable, written request and to the extent required under Data Protection Laws, Supplier will provide Intel reasonable cooperation and assistance needed to fulfill Intel's obligations to carry out data-protection and/or transfer-impact assessments and to consult with supervisory authorities related to Intel's use of the Services. Supplier will immediately inform Intel if, in

Supplier's opinion, Supplier: (i) can no longer meet its obligations under the Data Protection Laws or (ii) receives an instruction from Intel that infringes a Data Protection Law. In either situation, Intel may take reasonable and appropriate steps to stop and remediate any unauthorized Processing of the Personal Data by Supplier, including but not limited to terminating the Agreement or any sub-portion thereof, e.g., Statement of Work or having Supplier cease Processing by an unauthorized Sub-processor.

2.6 Submit to Audits. As permitted by Data Protection Laws, Intel may take reasonable and appropriate steps to exercise its obligations and rights to ensure Supplier is using the Personal Data in compliance with Data Protection Laws, including Intel's right to request Supplier provide all information necessary to demonstrate such compliance, e.g., third party-audit reports, or mandate inspections conducted by Intel or a third-party auditor appointed by Intel.

2.7 Notify Breaches. In the event that any actual or suspected incident in which Personal Data are subject to accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access ("**Security Incident**"), Supplier will, at its own expense: (i) notify Intel without undue delay but no later than forty-eight (**48**) hours after Supplier becomes aware of the Security Incident or suspects a Security Incident has occurred; (ii) consult and cooperate with Intel 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 Intel; and (iv) provide Intel any information reasonably requested by Intel. To the fullest extent permitted by applicable law, Supplier will not inform any third party of any Security Incident without first obtaining Intel's prior, written consent.

2.8 Sub-processors. If Supplier engages a third party to Process the Personal Data to help provide the Services (**Sub-processor**), Supplier will: (i) provide Intel thirty (**30**) days' notice before engaging new Sub-processor and allow Intel the right to object to such Sub-processor, (ii) ensure Sub-processor is bound by a contract with the same terms as this Section 2.8, (iii) comply with relevant Data Protection Law provisions relating to transfers of Personal Data to Sub-processor, and (iv) remain liable for the acts and omissions of Sub-processor.

2.9 Data-Subject Requests. "**Data Subject**" or its equivalent is defined by the applicable, Data Protection Law. In the event Intel or Supplier receives a request from a Data Subject seeking to exercise a Data-Subject Right under Data Protection Laws, including without limitation right to access, rectification, erasure, and portability of the Data Subject's Personal Data, Supplier will: (i) take into account the nature of the Processing, (ii) assist Intel by appropriate technical and organizational measures, to the extent possible, for the fulfilment of Intel's obligation to respond to such requests, and (iii), for the avoidance of

doubt, Supplier will assist and enable Intel to meet Intel's obligations to satisfy Data-Subjects Rights, but Supplier will not respond directly to Data Subjects.

2.10 Third-Party Disclosures. If Supplier receives a request for Personal Data from a third party other than a Data Subject (including a government agency, court, or law enforcement), Supplier will only disclose the Personal Data with Intel's written consent, save where first notifying Intel before such disclosure is strictly prohibited by law or valid, legal process (e.g., subpoena, warrant, or court order). If Supplier receives such a request, Supplier will: (i) refuse such request, (ii) instruct the third party to request the Personal Data directly from Intel, and (iii) provide the third-party Intel's contact information listed in Section 2.15. If compelled to disclose Personal Data to a law-enforcement agency or third party, Supplier will give Intel reasonable notice of the request prior to disclosure to allow Intel to seek a protective order or other appropriate remedy. If notice is legally prohibited, Supplier will: (i) take reasonable measures to protect the Personal Data from undue disclosure as if such Personal Data were Supplier's own confidential information being requested, (ii) only provide the minimal amount of Personal Data needed to meet the request, and (iii) inform Intel as soon as possible when such legal prohibition ceases to apply. Where the Personal Data become subject to confiscation by third parties during bankruptcy or insolvency proceedings or similar measures while being Processed by Supplier, Supplier will inform Intel in writing without undue delay.

2.11 Transfers of Personal Data outside the EEA under SCC Module Two. Where Supplier is located outside the European Economic Area ("**EEA**") in a country that is not deemed to have an adequate level of protection by the European Commission or is in the United States but not self-certified under the DPF, the parties agree to incorporate by reference the SCCs for the transfer of Personal Data that are subject to the GDPR from a data controller in the EEA to a data processor established outside the EEA, in the form set out in Module Two to the Annex to European Commission Implementing Decision (EU) 2021/914, and the SCCs are deemed to be executed by the parties. A copy of the SCCs can be accessed here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en. For the purpose of the SCCs: (i) Intel is the data exporter, Supplier is the data importer, and the contact details of each party are deemed to be included in Annex I.A; (ii) optional Clause 7 (Docking clause) is excluded; (iii) for Clause 9(a), Option 2 is selected and thirty (**30**) days' prior, written notice before a change of sub-processor is required; (iv) for Clause 11(a), the optional paragraph is deleted relating to an independent, dispute-resolution body; (v) for Clause 13(a), the first option is selected and the competent supervisory authority will be the Irish Data Protection Commission; (vi) for Clause 17, Option 1 is selected and the SCCs will be governed by the law of the country indicated in the governing law provision of the Agreement, unless such country is not an EU Member State, in which case the laws of Ireland; and (vii) for Clause 18(b), the parties agree

to the courts of the country indicated in the jurisdiction provision of the Agreement, unless such country is not an EU Member State, in which case the courts of Ireland will have jurisdiction for any disputes relating to the SCCs. The parties acknowledge and agree that Supplier can meet its obligations under the SCCs, having considered the sundry factors specified in Clause 14, including but not limited to the laws of the receiving country or countries, the volume and categories of Personal Data, and (to Supplier's knowledge) Supplier's history and similar organizations' likelihood of receiving government-information requests or surreptitious surveillance. On this basis, additional, no supplemental measures for the transfers envisaged under the SCCs are required beyond the contractual safeguards contained herein and the security measures employed by Supplier reflected in Section 2.4 above. If there is any conflict between the SCCs and the Supplier Compliance Handbook, the SCCs will prevail.

2.12 UK Personal Data Transfers. For transfers of or remote access to Personal Data subject to the UK GDPR, the ICO Addendum will apply where the Intel Affiliate is established in the UK and Supplier is located outside the UK in a country that is not the subject of an adequacy decision from the UK or is in the United States but not self-certified under the UK extension of the DPF. A copy of the ICO Addendum can be accessed here: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf. For the purposes of the ICO Addendum: (i) the Start Date is the Effective Date of the Agreement; (ii) Intel is the Exporter, Supplier is the Importer, and the contact details of each party are deemed to be included in Table 1; (iii) for Table 2, the parties select to append the ICO Addendum to the version of the Approved EU SCCs described in Section 2.11 above; (iv) for Table 3, the parties agree to input the corresponding information included in the Approved EU SCCs described in Section 2.11 above; and (v) for Table 4, "Exporter" is selected.

2.13 Swiss Personal Data Transfers. For transfers of or remote access to Personal Data subject to the Swiss FDPA, the SCCs cited and related language included in Section 2.11 above will apply where Intel is established in Switzerland and Supplier is located outside Switzerland in a country that is not the subject of an adequacy decision by the Swiss Federal Data Protection and Information Commissioner ("**Swiss FDPIC**") or is in the United States but not self-certified under the Swiss DPF. In addition, when applying such SCCs to such Personal Data, (i) for Clause 13(a), the Swiss FDPIC is the competent supervisory authority; (ii) for Clause 17, the laws of Switzerland govern; (iii) for Clause 18(c), Swiss Data Subjects may bring legal proceedings in their place of habitual residence (Switzerland); and (iv) generally, references to the GDPR include reference to equivalent provisions of the Swiss FADP.

2.14 Employees and Contractors. These terms also apply to Supplier employees in the course of performing their duties and Supplier's contractors, and Supplier

will ensure that Supplier's employees and contractors (i) are subject to an obligation of confidentiality, (ii) only process Personal Data as instructed by Intel, and (iii) otherwise comply with these terms.

2.15 Intel Contacts. Notwithstanding any contact information in governing agreements, for the purpose of Section 2.7 (Notify Breaches), contact Intel's IT Emergency Hotline: +1 (916) 356-8910 or it.cloud.sec@intel.com. Privacy questions should be directed to Chief.Privacy.Officer@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

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.

3.3 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.

3.4 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 Electrical, Electronic, or Electromechanical ("**EEE**") part, 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 Items, including any embedded software or firmware.

(B) In the event the Supplier provide an Electronic Part, as defined above, to Intel, Supplier agrees, and its lower tiers as required, to comply with the latest version of SAE International Standard AS5553, Counterfeit Electronic Parts, Avoidance, Detection, Mitigation, and Disposition.

(C) Supplier agrees and shall ensure that no Items provided to Intel 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.

(D) To protect Intel from procuring Counterfeit Items, Supplier shall be the original equipment manufacturer (OEM), the original software developer, or an OEM authorized distributor or reseller for an original source.

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

4. RETENTION AND AUDITS

4.1 Retention. Supplier will maintain complete and accurate documentation associated with Supplier's compliance with the Agreement. Unless otherwise stated in the Agreement, Supplier will retain such documentation until four years after the expiration date of the Agreement.

4.2 Inspection and Audit. Intel, or a third party designated by Intel, may access Supplier's premises and all documentation associated with Supplier's compliance with the Agreement for the purpose of conducting an inspection or audit. Supplier will promptly and fully cooperate with Intel, or a third party designated by Intel, upon receipt of Intel's reasonable written request for such an inspection or audit. If an inspection or audit finds that Supplier is not in compliance with the Agreement, then, in addition to any other rights or remedies available to Intel, Supplier will reimburse Intel for all costs associated with such inspection or audit.

5. FINANCIAL DATA

5.1 Within 30 days of Intel's request, Supplier will provide to Intel Supplier's most recent audited annual and quarterly financial information. At Intel's discretion, Supplier will provide such information to Intel electronically or via secure on-line system. Supplier will provide either an independent auditors' opinion or a letter signed by Supplier's executive management to verify that the financial information conforms to applicable accounting principles and standards.

6. ACCESSIBILITY

6.1 Any product, service, solution, or deliverable developed or provided by Supplier must conform with applicable Level A and Level AA Success Criteria of the latest published version of the Web Content Accessibility Guidelines ("WCAG"), available at https://www.w3.org/. Supplier agrees to i) promptly respond to and resolve any complaint regarding the accessibility of its products and services and ii) retain a third-party accessibility expert to evaluate the products and services, information, documentation, and support if necessary for remediation.

6.2 In addition to the requirements in Section 6.1, Supplier must comply with all local accessibility laws, standards, and requirements, including but not limited to:

(A) 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, and
(B) The requirements in 36 CFR Part 1194 (Electronic and Information Technology Accessibility Standards), as amended from time to time.

6.3 Supplier facilities with publicly accessible areas must comply with the local accessibility laws and meet the latest International Code Council (ICC) A117.1 Standard for Accessible and Usable Buildings and Facilities or equivalent standard, whichever is more stringent. If meeting the ICC A117.1 accessibility standards is not technically feasible, supplier must provide reasonable accommodations to enable equal access to its facility.

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

7.1 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.

7.2 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.

(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.

7.3 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.

7.4 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

8. HUMAN RIGHTS PRINCIPLES AND CODE OF CODUCT

8.1 Supplier will comply with Intel's Global Human Rights Principles available at supplier.intel.com.

8.2 For clarity, Supplier will: (i) comply with the Responsible Business Alliance ("RBA") Code of Conduct including without limitation the Responsible Labour Initiative ("RLI") and the Responsible Mineral Initiative ("RMI"); and (ii) ensure their suppliers, agents (including recruiting agents), and subcontractors comply with the RBA Code of Conduct. At Intel's request, Supplier will participate in periodic training provided by Intel in connection with the RBA Code of Conduct.

8.3 Supplier will develop, maintain, and utilize a process to annually assess Supplier's conformance to Intel's Global Human Rights Principles and the RBA Code of Conduct. Such process will include assessment of conformance of all operations and all sites of: (i) Supplier; and (ii) Supplier's suppliers, agents (including recruiting agents), and subcontractors.

8.4 At Intel's request, Supplier will promptly (but no later than the required deadline as provided by Intel) complete and provide to Intel completed surveys, audit results, and other information necessary for Intel to conduct: (i) supply chain risk assessments; and (ii) due diligence in connection with current and changing laws, statutes, regulations, rules, ordinances, and codes.

8.5 Suppliers who engage the use of any private or public security forces will ensure that: (i) such security forces comply with the RBA Code of Conduct, Intel Global Human Rights Principles, and all applicable laws, regulations, standards, and

codes in relation to human rights and (ii) such security personnel receive appropriate level of training and /or guidance to comply with this section.

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 Intel's own employees and contingent workers.

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

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

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

(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 Supplier's purchasing representative.

(F) Access to Intel Facilities – Supplier and Supplier's employees are required to complete the worker access forms associated with the 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 the 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 Supplier employees. Specifically, Supplier will:

i. Not terminate Supplier's employees on Intel property;
ii. Create and implement a response plan addressing a case of any terminated employee exhibiting threatening behaviors or making threats;
iii. Contact the local Intel Security representative 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
iv. Otherwise terminate Supplier employees in a commercially reasonable way that does not impact Intel's workplace safety and security.

(B) Supplier will make every reasonable effort to provide a safe workplace through the prevention of workplace violence, including without limitation preventing Supplier 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 Supplier will remind its employees not to attend work if they have a communicable illness (e.g., flu, pink eye).

9.6 For any questions, contact the Intel purchasing representative.

10. BUSINESS CONTINUITY PLAN EXPECTATIONS

10.1 Intel's Supplier Business Continuity Planning

(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.

(B) The Business Continuity Plan ("**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) Include a detailed section within it that addresses the company's recovery plan for cybersecurity related excursions, including drilling timeline and alerting customers.

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

(5) Utilize the guidelines as set forth at https://supplier.intel.com.

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

11. OWNERSHIP AND BAILMENT

11.1 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.

11.2 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.

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