



GLOBAL CONTINGENT WORKER AND PRIVILEGED VISITOR AGREEMENT

Please visit supplier.intel.com/forms for the most current version of this form. Prior versions may not be accepted. This form may not be modified.

INSTRUCTIONS: READ THIS DOCUMENT CAREFULLY AND COMPLETELY BEFORE SIGNING. Do not fold; this document will be scanned for retention. Every contingent worker and privileged visitor must sign and submit the current version of this document prior to being granted access to Intel and at least annually thereafter. If you or your employer requires a copy of this document for your records it is your responsibility to make and retain a copy before submitting it to Intel. For the purpose of this document, "Intel" refers to Intel Corporation, or any of its subsidiaries, affiliates, or successors.

* * * * *

I am not an Intel employee. As a condition of Intel granting access to me as a contingent worker or privileged visitor, I agree to access Intel facilities, resources (electronic or otherwise), and confidential information, only to the extent necessary to perform my Intel-related work and to the extent I have been authorized to do so by Intel. I understand that failure to comply with any applicable policies or guidelines during or after my engagement may result in denial of my access to Intel facilities, resources (electronic or otherwise), and confidential information. I agree to comply with all applicable guidelines for doing business with Intel including, but not limited to, those explicitly outlined in this document. I understand the policies or guidelines referenced in this document may be accessed via supplier.intel.com, the Intel intranet, or from my Intel Sponsor or authorized contact upon request.

Confidential Information includes, but is not limited to, proprietary information, trade secrets, information from third parties pursuant to confidentiality agreements, personal information, job titles, project code names, resource allocation to projects, and any information not generally known to others or that may confer a competitive advantage to a recipient that the recipient would not otherwise have. I understand I may be exposed to Confidential Information and agree:

1. I have not brought, nor will I bring or use in the provision of services to Intel or during my engagement, any proprietary or confidential information belonging to my current or former employer(s) or any third party without proper and verifiable authorization.
2. I will comply with all applicable Intel *Privacy Policies* and *Information Security Policies & Procedures* to preserve and protect Confidential Information in my possession, or that which comes to my attention during my engagement.
3. Except as required for my engagement, or as specifically approved by an authorized Intel representative, or as expressly required by law or professional requirements, I will not use, copy, change, destroy, remove, share, or otherwise disclose Confidential Information.
4. I will not use any non-public information regarding Intel to trade in or make investment decisions regarding Intel's stock or other securities, nor will I disclose such information to others who may buy or sell securities because of such non-public information.
5. Upon termination of my engagement I will immediately return to Intel all Confidential Information in my possession and I will securely destroy or erase any copies. Further, my obligations of confidentiality will continue indefinitely, except for information that subsequently and lawfully enters the public domain, or information that is governed by a separate non-disclosure agreement between Intel and me or my employer. (Note: This does not apply when there is a legal, ethical or contractual requirement to retain specific documentation or to disclose specific findings.)
6. During my engagement, I will comply with any Legal Event Hold Notice (LEHN) directed to me and upon termination of my engagement while subject to a LEHN will return to Intel

all documents, electronically stored information and other materials covered by the LEHN.

I agree to work safely and abide by applicable safety and security policies and guidelines, and professional standards of conduct, at all times during the provision of services to Intel. I further agree:

7. I will comply with all applicable laws and regulations governing the provision of services to Intel.
8. I will not engage in harassing or discriminating behavior whether or not that conduct is expressly prohibited by law in the country in which it occurs.
9. I will obtain information on known hazards, safety and security requirements, and emergency procedures associated with the areas and operations in which I will be involved from my Intel Sponsor or designee. I will not engage in work for which I have not first completed any and all safety training or certifications as required by Intel and/or any applicable government agency.
10. I will promptly notify Intel Security if, due to an actual or perceived threat of violence, I ever have reason to be concerned for my own safety at Intel, or the safety of others at Intel, even from an external person.
11. I will promptly notify Intel Security of any theft or loss of Intel assets, or third party assets that Intel is responsible for safeguarding, including but not limited to physical assets, intellectual property, and data governed by Intel's *Privacy Policy*.
12. I will comply with Intel's *Alcohol and Drug-Free Workplace Directive*.
13. I understand that use of Intel communication and computing resources including, but not limited to, email, internet and, computer use, are not private and are subject to monitoring or search in compliance with local laws. I will only use these resources to the extent allowed by my employer or to the extent I have been authorized by Intel to do so and I will comply with Intel's *Electronic Communications Guideline* (to the extent it applies to me as a CW or PV) at all times when using these resources.
14. I understand Intel Security has the right, subject to applicable laws and regulations, to perform reasonable cause searches (as determined necessary by Intel Security) in office areas and personal property located on Intel premises. Such searches may include, but are not limited to, personal electronic devices and data storage media, personal bags, purses, and personally-owned vehicles.
15. Except as required to carry out the provision of services to Intel, I will not remove any assets from Intel's premises or convert them to personal use. "Assets" include anything of tangible or intangible value including but not limited to "scrap", "defective material", and "trash".
16. If there is a compelling business reason to connect a Non-Intel Managed System (NIMS) to the Intel network (other than Intel's Guest Internet Access network (GIA)), I will work with my Intel Sponsor or authorized contact to achieve a secured connection or obtain a written waiver from Intel IT before connecting. I understand if I have a business need to connect a NIMS to the internet I can apply for GIA through my Intel Sponsor or authorized contact.
17. Immediately upon the end of my engagement I will return my Intel identification and all Intel assets, such as computing equipment or documents assigned to me or otherwise in my possession, to my company representative or my Intel Sponsor or authorized contact. I will also request account revocation so that my account cannot be compromised or misused after I leave.

For US-based personnel, by way of this agreement I have been advised I will not be held criminally or civilly liable under any federal or state trade secret law for disclosure of a trade secret that is made in confidence to a government official, either directly or indirectly, or to any attorney, solely for the purpose of reporting or investigating a suspected violation of law; or is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. I am further advised that, in the event I file a lawsuit for retaliation by Intel for reporting a suspected violation of law, I may disclose the trade secret information to my attorney and use it in the lawsuit,

if any document containing the trade secret is filed under seal; and I do not disclose the trade secret, except pursuant to court order.

Notice & Consent: By signing this document I agree and consent to the following: An image or copy of this document will serve as the original document. This document and the personal information contained on it may be transferred to the United States, or to any other country in which Intel conducts business, for storage or the business reasons listed below. Intel may share this document, as deemed necessary by Intel for business purposes, with my direct employer (or Intel supplier, if different), law enforcement, civil authorities, or other agencies, to enforce the terms of this agreement, including but not limited to suspected or actual violations of any portion of this agreement. If such action is necessary, Intel may transfer this document and all related evidence to a third party supplier for the purpose of facilitating such action on Intel's behalf and I hereby consent to sharing of any personal information contained in the form for that purpose. Intel will disclose this document and any and all other documents or personal information to other third parties if required to do so by law. This document, along with any other security documents you complete, will be kept for 7 years or as long as required in order to run the day-to-day business and to comply with various local, state and national laws.

UNDERSTOOD AND AGREED:

DocuSigned by:

Wayne Mitchell

6/30/2023

Signature of Contingent Worker/Privileged Visitor

wayne Mitchell

Date

Printed name of Contingent Worker/Privileged Visitor

WWID

Contingent Worker

Data Privacy Notice and Consent

PLEASE READ THIS DATA PRIVACY NOTICE AND CONSENT CAREFULLY. IF YOU HAVE ANY QUESTIONS PLEASE CONTACT YOUR INTEL SPONSOR

By signing below, you agree to the terms and conditions of this data privacy notice and consent. Intel recognizes its responsibility for complying with relevant data privacy laws, and for protecting the personal information in its possession and care. Nothing in this Data Privacy Notice and Consent will waive any rights you may have under applicable privacy law.

COLLECTION OF INFORMATION

Intel may request that you provide personal information, including your name, address, e-mail address, telephone number, birth date (month and day), Social Security or National Identification Number (used strictly for identification purposes), contact information and other information reasonably related to your job placement from which your identity is discernible. Your personal information will be stored and processed in whole or in part in the United States.

USE OF INFORMATION

Intel will use the information, whether personal, demographic, collective or technical, for the purpose of managing the contract worker relationship with Intel, and allow you access to Intel premises and where applicable, Intel data and systems.

The information Intel gathers from you, with the exception of Social Security and National Identification Number, may be shared with your employer, your Intel sponsor, Intel Human Resources, Intel Procurement Services, and any other Intel function with a relevant and legal business need to know. Other than as stated above, Intel will not transfer your personal information to third parties without your explicit consent. Intel will ensure that all Individuals with access rights to your personal information have been educated on data privacy laws and the use of personal information, and have signed Confidential Non-Disclosure Agreements holding them accountable for compliance. Locally, the HR Manager has responsibility for ensuring the protection of all personal information. On a corporate level, the Global Privacy Office has overall responsibility for data protection compliance.

Intel will store your personal information in our global contingent worker database located in the United States. In addition, your personal information may be accessible by 1) Intel in the United States, 2) Intel's affiliated companies in countries as necessary as part of your contract worker assignment, and 3) Intel's trusted vendors providing contract worker management services on a worldwide basis.

SECURITY Intel will use commercially reasonable technical and organizational measures to safeguard and secure your personal information from accidental loss and from unauthorized access, use, alteration or disclosure.

I understand and consent to this Data Privacy Notice and Consent.


F771E98A760D487...

Signature

wayne mitchell

Print Name

Mindlance Inc

Employer

6/30/2023

Date



Unescorted Access Request for
Contingent Workers & Privileged Visitors
(For all locations globally)

Please visit supplier.intel.com/forms or scan the 2D matrix for the most current revision of this and related forms. Prior revisions may not be accepted. This form may not be modified.



Minimum Access Standard: Access to Intel facilities is a privilege that may be granted upon request at Intel's sole discretion and access may be revoked at any time without notice. Each Supplier/Partner/Customer/etcetera ("Supplier") must take reasonable steps to screen every Contingent Worker (CW) or Privileged Visitor (PV) they place at Intel, and exclude any CW/PV who poses an elevated risk of harm. The following should be considered:

1. Threatening behavior, violence, harassment or stalking, inside or outside the workplace, which potentially puts other people at an elevated risk of harm.
2. Theft, dishonest, or unethical behavior, inside or outside the workplace, which potentially puts assets at risk of theft, or otherwise indicates the person is inclined to engage in unethical behavior.
3. Illicit drug use that potentially creates an elevated risk of inappropriate behavior, accidents, or theft.
4. Any other behavior(s) that put other people, assets, or a professional workplace environment, at an elevated risk.

Intel considers the Supplier accountable for any individual misconduct that brings harm to people, assets, or Intel's reputation. It is up to each individual Supplier to establish its own screening procedures and to comply with applicable laws, agency regulations, etcetera. In addition, the Supplier is responsible for verifying the identity of each CW/PV the Supplier places at Intel, and to ensure the CW/PV has the legal right to work or operate in the location and capacity they are assigned.

Request & Certification: I am an authorized manager or management representative of the Supplier. I request unescorted access for the following CW/PV:

CW/PV Name: Wayne Mitchell WWID (if known): _____

I affirm that all appropriate screening has been completed (or will be completed without delay), and should any disqualifying issue arise or become known during the Intel assignment, my company or organization will immediately end the assignment, recover his or her Intel access badge if possible, and notify Intel through proper channels to ~~disable access~~.

Supplier Manager Signature: Parth Pandya

Printed Name: Parth Pandya Date: 6/30/2023

Supplier Name: Mindlance Inc