Print CW/PV Name: _____

This form may not be modified

GLOBAL CONTINGENT WORKER AND PRIVILEGED VISITOR AGREEMENT - 3.15.2023

INSTRUCTIONS: READ THIS DOCUMENT CAREFULLY AND COMPLETELY BEFORE SIGNING. Every contingent worker and privileged visitor must execute this Agreement prior to being granted access to McAfee facilities. This Agreement must be re-signed annually. Nothing in this Data Privacy Notice and Consent will waive any rights you may have under applicable privacy law.

All the policies or guidelines referenced in this document may be accessed via suppliers Fieldglass.net account under Fieldglass Reference Library, the McAfee intranet, or from a McAfee Sponsor or authorized contact upon request. For purposes of this document, "McAfee" refers to McAfee, LLC, or any of its subsidiaries, affiliates, or successors.

* * * * *

As a condition of receiving access to McAfee facilities, as a contingent worker (CW) or privileged visitor (PV), CW or PV agrees to access McAfee facilities, resources (electronic or otherwise), and Confidential Information, only to the extent necessary to perform McAfee-related work and to the extent CW or PV has been authorized to do so by McAfee. Failure to comply with any applicable policies or guidelines during or after the engagement may result in denial of access to McAfee facilities, resources (electronic or otherwise), and Confidential Information. CW or PV shall comply with all applicable guidelines for doing business with McAfee including, but not limited to, those explicitly outlined in this Agreement.

For US-based personnel, by way of this agreement CW or PV have been advised CW or PV 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. CW or PV is further advised that, in the event CW or PV files a lawsuit for retaliation by McAfee for reporting a suspected violation of law, CW or PV may disclose the trade secret information to their attorney and use it in the lawsuit, if any document containing the trade secret is filed under seal; and CW or PV does not disclose the trade secret, except pursuant to court order. *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. CW or PV agrees to:

1. Not bring or use in the provision of services to McAfee or during the business engagement, any proprietary or Confidential Information belonging to a current or former employer(s) or any third party without proper and verifiable authorization.
2. Comply with all applicable McAfee *Privacy Policies* and *Information Security Policies & Procedures* to preserve and protect Confidential Information. All policies are made available via Fieldglass to your supplier to provide to provide to CW or PV.
3. Except as required for the engagement, or as specifically approved by an authorized McAfee representative, or as expressly required by law or professional requirements, not use, copy, change, destroy, remove, share, or otherwise disclose Confidential Information.
4. Upon termination of engagement immediately return to McAfee all Confidential Information in possession and securely destroy or erase any copies. Further, 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 McAfee and CW or PV or CW or PV's employer. (Note: This does not apply when there is a legal, ethical or contractual requirement to retain specific documentation or to disclose specific findings.)
5. Comply with any Legal Event Hold Notice (LEHN) directed to CW or PV and upon termination of engagement while subject to a LEHN will return to McAfee all documents, electronically stored information and other materials covered by the LEHN.
6. Provide to McAfee, personal information, including name, address, e-mail address, telephone number, birth date (month and day), contact information and other information reasonably related to the job placement from which an identity is discernible. Personal information will be stored and processed in whole or in part in the United States. Personal information may be accessible by 1) McAfee in the United States, 2) McAfee's affiliated companies in countries as necessary as part of your contract worker assignment, and 3) McAfee's trusted vendors providing contract worker management services on a worldwide basis.
7. Allow McAfee to use personal, demographic, collective or technical, for the purpose of managing the contract worker relationship with McAfee, and allow CW or PV access to McAfee premises and where applicable, McAfee data and systems.

8. Understand that the information McAfee gathers from CW or PV may be shared with CW or PV's employer, McAfee manager, McAfee Human Resources, McAfee Procurement Services, and any other McAfee function with a relevant and legal business need to know. Please see the Contingent Worker Privacy Notice, Attached as exhibit 1 to this Agreement, incorporated in its entirety.
9. Understand that other than as stated above, McAfee will not transfer personal information to third parties without CW or PV's explicit consent. McAfee will ensure that all Individuals with access rights to 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.
10. Allow McAfee to store personal information in Mcafee's global contingent worker database located in the United States.

CW or PV further agrees to:

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

SUPPLIER GUIDELINES

I agree that access to McAfee facilities is a privilege that may be granted upon request at McAfee'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 CW or Privileged PV they place at McAfee, 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.

McAfee considers the Supplier accountable for any individual misconduct that brings harm to people, assets, or McAfee'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 McAfee, and to ensure the CW/PV has the legal right to work or operate in the location and capacity they are assigned.

Supplier has all referenced policies in this Agreement made available via the suppliers secured Fieldglass Reference Library. All these policies should be made available to the CW/PV. They can be found by the supplier logging onto fieldglass.net and scrolling down the left side of the page to Reference with a subcategory of Reference Library. This Reference Library includes McAfee California Consumer Privacy Act Notice for California Contingent Workers effective 1/1/2023, McAfee Information Security Policy, McAfee Acceptable Use Policy, McAfee Code of Conduct Policy, McAfee Anti-Harassment Policy, McAfee Alcohol Drug-Free Workplace Guidelines.

Notice & Consent: By signing this document the CW or PV agrees and consents 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 McAfee conducts business, for storage or the business reasons listed below. McAfee may share this document, as deemed necessary by McAfee for business purposes, with my direct employer (or McAfee 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, McAfee may transfer this document and all related evidence to a third-party supplier for the purpose of facilitating such action on McAfee's behalf and I hereby consent to sharing of any personal information contained in the form for that purpose. McAfee 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 by CW/PV:

Signature of Contingent Worker/PV: G. Pra

Printed name of Contingent Worker/PV: PRANESH G

Date Signed (mm/dd/yyyy format): 07/01/2023

UNDERSTOOD AND AGREED BY SUPPLIER:

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

SUPPLIER NAME: Brillio LLC

SIGNED: Ykulkarni

DATE: 07/01/2023

NAME: Yogesh Kulkarni

TITLE: Project Manager