Non-Employee Acceptable Use Agreement

This Non-Employee Acceptable Use Agreement sets forth minimum requirements for the acceptable use and protection of SAIC's information assets and systems accessed by non-employees.

DEFINITIONS

Information Systems

Information systems include, but are not limited to, SAIC owned, SAIC-operated, or third-party equipment such as mobile devices, computers, networks, external drives and applications that enable the use, processing, transmission, and storing of SAIC and Controlled Unclassified Information (CUI).

Information Assets

Information assets consist of sensitive data, including but not limited to CUI, personally identifiable information, protected health information and other SAIC or government-designated sensitive data. Information assets can also include the physical devices provided by SAIC or non-employee to process transmit and store sensitive data.

Non-employee account

Non-employee accounts include contractors and vendors with varying levels of access and network resource needs, and are categorized as:

- ✓ **Customer –** a legal entity that has established a contract with SAIC for SAIC to provide some form of goods and services.
- ✓ **Supplier –** a legal entity that SAIC has established a contract with for the supplier to provide some form of goods and services.
- ✓ **Employee –** personnel that have entered into an employment agreement with SAIC.
- ✓ **SAIC Sponsored Temporary Personnel –** personnel that are self-employed and are being provided to SAIC on a temporary basis by a staffing agency.
- ✓ **Supplier Personnel –** Personnel that have entered into an employment agreement with the Supplier and are working on behalf of the supplier per a defined contract with SAIC.
- ✓ **Customer Personnel –** personnel that have entered into an employment agreement with the Customer and are working on behalf of the Customer per a defined contract with SAIC.

Company POC

Point of contact at the non-employee's legal entity that can verify the non-employee's work and location status.

Requestor

Individual that requests an account for access to SAIC systems.

SAIC Account Sponsor

Responsible for certifying, recertifying, and closing the account. Furthermore the sponsor will keep non-employee data current in Cornerstone. Account sponsors must also transfer account ownership upon termination of project or corporate responsibilities.

ACCOUNT SPONSORSHIP

Non-Employee accounts must be sponsored by an SAIC employee. The SAIC sponsoring employees may request the non-employee account.

All sponsors are required to validate non-employee's affiliation status with the company. Any change in non-employee status with affiliated company must be updated immediately.

ACCOUNT RECERTIFICATION

SAIC account sponsors must recertify the non-employee's access needs every 90 days. Recertification entails contacting the non-employee's company POC for confirmation of access needs and validation of employment.

NO RIGHT TO OR EXPECTATION OF PRIVACY AND CONSENT TO MONITORING

All non-employees have no expectation of privacy while on SAIC property or using or accessing SAIC electronic assets and are subject to monitoring. SAIC reserves the right to review, audit, or monitor any information technology and information asset accessed by non-employees. Non-employees who place personal information on SAIC's information systems and assets waive any right to privacy and do so at their own risk.

PROPER USE AND PROTECTION OF SAIC INFORMATION SYSTEMS AND ASSETS

Access to and use of SAIC's information systems and assets shall be consistent with applicable laws and regulations as well as the terms and conditions outlined in this document. The non-employee or company POC acknowledges and agrees to the following as a condition of use:

- ✓ Use only accounts authorized by sponsoring employee within SAIC.
- ✓ Access only those resources for which they are specifically authorized.
- ✓ Use multi-factor authentication to authenticate to SAIC systems.
- ✓ Safeguard their SAIC issued account and log-on information, including not sharing, or otherwise disclosing it to unauthorized personnel.
- ✓ Use SAIC-issued information systems and assets, including email, only in a professional and respectful manner consistent with applicable laws and regulations as well as the terms and conditions outlined in this document.
- ✓ Safeguard, in accordance with applicable laws, regulations, and contractual obligations, information that is not publically available, such as government CUI **[Note 1]**, proprietary information, export-controlled information, personally identifiable information, and Health Insurance Portability and Accountability Act information.
- ✓ Exercise extreme caution when opening e-mail and attachments from unknown senders. Every authorized user has an obligation to report phishing attempts or the existence of malware. Report any suspected phishing and malware by calling 833-YO-CYBER and follow instructions provided by the Cybersecurity team.
- ✓ Permit SAIC to access, audit, or destroy SAIC information systems or assets or take other appropriate measures necessary to adhere to cybersecurity and privacy requirements and otherwise comply with applicable law, regulations and contractual obligations.
- ✓ Report any suspected compromise, misuse or classified spill involving SAIC information systems or information assets and the ITO Cybersecurity Team by calling 833-YO-CYBER.
- ✓ Protect SAIC information systems and assets from theft, loss or damage, and immediately report stolen, lost or damaged SAIC information systems or assets the ITO Cybersecurity Team by calling 833-YO-CYBER and notify your sponsor immediately.
- ✓ Use virtual desktop services (VDS) to access SAIC information systems and assets when deemed appropriate by SAIC Cybersecurity or sponsoring employee.

- ✓ Store CUI only on SAIC-approved devices, where attestation to DFARS clause 252.204-7012 compliance has been documented.
- ✓ Sign a non-disclosure agreement if provided and comply with additional cybersecurity-related contractual and customer-dependent requirements that may be applicable.
- ✓ Company POCs must notify SAIC sponsor if non-employee ceased affiliation with company.
- ✓ Company POCs must re-certify non-employee's company affiliation in accordance with recertification period by notifying SAIC sponsor.

All non-employees have an individual responsibility that if you see, observe, or suspect non-compliance with this policy by others to report it to the ITO Cybersecurity Team by calling 833-YO-CYBER immediately.

Note 1: National Archives: Controlled Unclassified Information (CUI).

PROHIBITIONS CONCERNING SAIC INFORMATION SYSTEMS AND ASSETS

Certain uses of SAIC information systems and assets are strictly prohibited. Non-employees that use SAIC's information systems and assets acknowledge and agree to NOT:

- ✓ Allow improper or unauthorized access to SAIC information systems and assets (e.g., by sharing passwords, leaving passwords unprotected, and leaving SAIC devices unlocked and/or unattended in non-secured locations)
- ✓ Perform any unauthorized changes to any SAIC information system, including changing desktop configurations as well as removing or disabling required security features.
- ✓ Use SAIC information systems and assets to engage in any form of offensive cyber operations, including "hacking back" or the unauthorized installation of honeypots or similar technology.
- ✓ Store data on unapproved devices (as defined in *"Proper use and protection of SAIC information systems and assets"*) or connect any unauthorized device to SAIC information systems [Note 2].
- ✓ Export technical data, software or other export-controlled information or items without appropriate authorization from SAIC contracting technical officer and Cybersecurity.
- ✓ Travel outside of the United States with any assigned SAIC information assets unless approved in writing by the ITO Cybersecurity Directorate. Contact the SAIC project or program representative for more information..
- ✓ Use SAIC information systems to upload/download unapproved software or to view, transmit, or store inappropriate material, including material that is contrary to law or regulation, contrary to this acceptable use agreement, or that is considered offensive, disruptive, defamatory, and disparaging.
- ✓ Store CUI data on unencrypted removable media devices.

Note 2: Any removable media that is required for business operations to be used in connection with SAIC information systems or to store SAIC information assets must be approved in advance by Cybersecurity. Contact the SAIC project or program representative for more information.

TRAINING AND AWARENESS

All non-employees with access to SAIC's information systems and information assets are required to acknowledge and sign this Non-employee Acceptable Use Agreement.

REPORTING IMPROPER USE

The users of SAIC's information systems and assets are the first line of defense against the misuse of these systems and assets. All non-employees are required to immediately report suspected cybersecurity incidents, misuse of SAIC information systems and assets, or use of questionable IT security practices to the SAIC's ITO Cybersecurity Team (available on the Cybersecurity Home page of ISSAIC or by calling 833-YO-CYBER) and your local security representative.

COMPLIANCE AND INDIVIDUAL ACCOUNTABILITY

Individual actions have broad-reaching enterprise impact, and all users of SAIC systems and assets are required to comply with this agreement. Any non-employee who fails to comply with the terms and conditions outlined in this agreement may be subject to loss of access.

NON-EMPLOYEE ACKNOWLEDGEMENT

I have read and electronically acknowledged this Acceptable Use Agreement. I understand that this access is designed for specific business use only and to be used as outlined in this document. I have provided all required documentation to expedite my request for access and certify to the best of my knowledge that all information is accurate.