NCSES Restricted-Use Data (RUD) Security Plan

Security Plan Type

Researcher: New License ◯ **Amendment** ◯

Name of Institution/Organization: _____

Restricted-Use Data User Information

Principal Investigator (PI): _____

Mailing Address: _____

Phone Number: _____

Email Address: _____

Information System Security Officer Information

As stated in the license, the Senior Official (SO), who signed the license agreement, has full and final responsibility for the secure access to restricted-use data by the PI. The Information System Security Officer (ISSO) is the person responsible for maintaining the security of information systems owned by the institution and made available to the PI team. The ISSO's assigned duties shall include the implementation, maintenance, and periodic update of this security plan to verify protection of the data while accessed on the institution's network in strict compliance with statutory and regulatory requirements. The ISSO shall not be the same person as the PI.

Information System Security Officer (ISSO): _____

Mailing Address: _____

Phone Number: _____

Email Address: _____

RESEARCHER & SYSTEM INFORMATION FORM

Complete form for EACH user requesting enclave access. Duplicate page if necessary.
See next page for SDAF System Security Guidelines.

Researcher Name: _____

Institution/Organization: _____ **Job Title:** _____

Phone Number: _____ **Email Address:** _____

Work Location: **Where will you log in from? Select all that applies.**

Home: ☐ **Address:** **Work:** ☐ **Address:**

Workstation Specifications:

Make & Model: _____ **Serial Number:** _____

Desktop ☐ **Laptop** ☐ **Other:**_____

Operating System (Include version number): _____

Workstation Login Access: **Who can log into your workstation?**

Yourself: ☐ **Other:** ☐ **If other, specify:** _____

Workstation Monitor Position:
Describe how the workstation is positioned to prevent unauthorized viewing:

Workstation Antivirus:
Describe brand and version of antivirus software installed on workstation and provide details on how often the software is updated.

I have reviewed and consent to following the security procedures as described in the SDAF System Security Guidelines.

_____

Principal Investigator Signature **Date**

I have verified that the information listed is accurate and meets the criteria listed in the SDAF System Security Guidelines.

_____

Information System Security Signature **Date**

Secure Data Access Facility (SDAF) System Security Guidelines

The following security measures are the personal responsibility of the researcher:

- SDAF access must only be made on a secure network. No public Wi-Fi.
- SDAF access must only be made from approved locations.
- SDAF must not be accessed from public places (e.g., coffee shops, libraries).
- Device used to access the SDAF may not be shared with unauthorized personnel.
- Only authorized users may be present when accessing SDAF. A privacy screen must be used in an office shared with unauthorized personnel.
- Devices containing SDAF authentication tokens may not be shared.
- Devices containing SDAF authentication tokens must be password protected. Bio-Metric Passkeys are allowed.
- Devices used to access SDAF may not be relocated outside of the United States.

The Information System Security Officer (ISSO) must ensure that the following security requirements are in place:

- SDAF computer is password protected. Minimum requirements: 8 characters. Bio-Metric Passkeys are allowed.
- Timeout settings must be within 5 minutes of inactivity and require password login.
- SDAF computer has the latest operating system security patches.
- SDAF computer has anti-virus software and automatic updates are enabled.
- Devices used to access the SDAF (laptop, phone, etc.) are locked, or otherwise secured, and restricted to only one user.
- Internal audits are conducted to ensure that only authorized personnel have access to the research computer. Users who are no longer affiliated with the listed institutions must be removed within 24 hours.

NCSES reserves the right to complete unannounced and unscheduled audits by NCSES Data Security Officials to ensure compliance with the security guidelines. In addition, the Researcher & System Information Form must be updated if the researcher's workstation and/or location changes. Access to the enclave are system and location restricted.

Review and Approval

I have reviewed the requirements of the license security procedures and the contents of this security plan, which describes the protection measures for the requested restricted-use data files. I have also instructed the collaborating researchers on the requirements of the security plan. I hereby certify that this system meets all requirements of the license security procedures and that the in-place security safeguards adequately protect the restricted-use data.

_____

Principal Investigator Signature **Date**

_____

Principal Investigator Name (type/print)

_____

Information System Security Officer Signature **Date**

_____

Information System Security Officer Name (type/print)

_____

Senior Official Signature **Date**

_____

Senior Official Name (type/print)