Corporation for NATIONAL & COMMUNITY SERVICE

eGrants Rules of Behavior Acknowledgement

POLICY FOR USE OF THE eGRANTS SYSTEM

As a user of the Corporation for National & Community Services (CNCS) eGrants application, you are required to be aware of, and comply with, eGrants policy on authorized use and security of the eGrants application and data.

YOU ARE RESPONSIBLE FOR ALL ACTIONS PERFORMED WITH YOUR eGRANTS ACCOUNT.

- User IDs and passwords are for your individual use only and are not to be shared with anyone, including others within your organization.
- You must not disclose your password to anyone and you must take necessary steps to prevent anyone from gaining knowledge of your password. You should not record passwords on paper or store them on unencrypted electronic devices.
- You should employ good password management practices by creating strong passwords as outlined in eGrants help manual.

POLICY, STANDARDS, AND PROCEDURES MUST BE FOLLOWED.

- Use of the eGrants system is restricted in accordance with the express purpose of the eGrants system.
- You must be aware of, and abide by the "Computer Fraud and Abuse Act of 1986" (Public Law 99- 474), the civil and criminal penalties of the Privacy Act, the Trade Secrets Act (18 U.S.C. S905), and other Federal Regulations applying to unauthorized use of Federal computer systems, files, records, and data.
- Be aware that all use of the eGrants system is subject to periodic test, review, monitoring and auditing. Any evidence of security violations or illegal activity will be immediately turned over to CNCS Security, the CNCS Inspector General, or law enforcement for action. Penalties could include loss of access, fines and/ or imprisonment.

ACCESS TO INFORMATION MUST BE CONTROLLED.

- Access only the information for which you have been authorized, and have "need to know/access."
- Do not leave computers logged on to eGrants and unattended. Log off and close your browser at the end of each session or use access control software (i.e., Screen Save with password) during unattended use.
- Prevent the unauthorized disclosure, modification or destruction of Personal Identifiable Information (PII), such as:
  - Social Security Number
  - Date and Place of Birth
  - Educational Information
  - Employment Information

  And Sensitive Information, such as:
  - Grant Information
  - Budget Information
  - User Account Information
- Protect eGrants files, reports, and information containing sensitive data and PII by:
  - Storing electronic files in secure folders that only allows access to those with need to know
  - Storing paper files in locked file cabinets
  - Storing information on encrypted removable storage media (e.g., USB drives, portable hard drives, memory cards, etc.) and encrypted mobile devices (e.g., laptops, tablets, iPhones, etc.)
  - Encrypting email messages
- If you know or suspect that PII or sensitive information has been inappropriately disclosed, modified, or destroyed, or if a person, other than yourself has used or is using your User ID, you must report the incident immediately to your supervisor and National Service Hotline (1-800-942-2677, https://questions.nationalservice.gov/app/ask_eg)