U.S. Small Business Administration
Office of Disaster Assistance

Computer Rules of Behavior

1. **Computer Use –** Unless otherwise stated in SBA policy, agency-owned or leased computers, software, and telecommunications systems are to be used for work-related purposes only. SOP 90-47, Automated Information Systems Security Program, has additional information on limited personal use of agency Information Technology (IT) resources.

2. **ID's and Passwords** – User ID's are assigned to individuals and should not be shared with other persons or groups. You must maintain the secrecy of your password. If you suspect your password has been compromised, you must change it immediately. You are responsible for changing your password every 90 days.

3. **Accountability** – You are accountable for all actions associated with the use of your assigned User ID and may be held liable for unauthorized actions found to be intentional, malicious, or negligent.

4. **Unauthorized Access** –You are prohibited from accessing or attempting to access systems or information for which you are not authorized. You are prohibited from changing access controls to allow yourself or others to perform actions outside your authorized privileges. You may not imitate another system, impersonate another user, misuse another user's credentials (user ID, password, smart card, etc.), or intentionally cause some network component to function incorrectly. You may not read, store, or transfer information for which you are not authorized.

5. **Denial of Service Actions** –You are not allowed to initiate actions that limit or prevent other users or systems from performing authorized functions, including communications deliberately generating excessive traffic.

6. **Data or Software Modification or Destruction** –Unless otherwise authorized, you are not allowed to intentionally modify or delete system software, data or programs. This excludes personal data.

7. **Malicious Software** –You are prohibited from installing or using malicious software such as computer viruses.

8. **Use of e-mail and Internet access** – E-mail of an unknown or unexpected origin could contain a virus. If in doubt, do not open such e-mail. Contact your local Information Technology (IT) Specialist for further action. Downloading information from the Internet should be done with care.

9. **System and Workstation Security** – You are not permitted to circumvent system permissions. You are not permitted to install new software on your machine. If new software is required, please contact your local IT Specialist (or the SBA Helpdesk).

10. **Remote Access** – SBA reserves the right to limit remote access to ensure appropriate security to computer resources.

11. **Unauthorized Use of Government Resources** – Unauthorized use of SBA systems and computer resources for non-work-related activities, or any abuse of access capabilities, may result in disciplinary action.

12. **Reporting Security Violations** – Any suspected security violations, breaches, viruses, or other security related incidents must be reported to the local IT Manager immediately.