SMALL BUSINESS ADMINISTRATION
STANDARD OPERATING PROCEDURE

APPROPRIATE USE OF SBA'S AUTOMATED INFORMATION SYSTEMS 90 49

INTRODUCTION

1. Purpose: To establish a Standard Operating Procedure (SOP) for employee and contractor appropriate use of the Small Business Administration's (SBA) automated information systems (AIS).

2. Personnel Concerned: All SBA employees, contractors, and other authorized users who access the AIS.

3. Originator: Office of the Chief Information Officer (OCIO)

4. Directives Cancelled: None

5. Distribution: Standard

Effective Date: June 20, 2006

Table of Contents

1. What Is the Purpose of This SOP?

The Office of the Chief Information Officer (OCIO) is responsible for developing, coordinating, and disseminating Agency policy concerning employees', contractors', and others' use of SBA's Automated Information System (AIS), and ensuring that Agency management units have implemented appropriate procedures to enforce such policy.

Information Technology (IT) used as part of SBA's AIS and that are subject to this SOP include:

a. personal computers (PC);
b. peripheral equipment and software for PCs;
c. telephones;
d. facsimile machines;
e. photocopiers;
f. e-mail;
g. Internet connectivity and access to Internet services; and
h. IT mobile devices (e.g., Blackberries, Personal Data Assistants (PDAs), and cell phones).

This policy only supplements the SBA Standard Operating Procedure (SOP) 90 47, "Automated Information Systems Security Program" and is not intended to replace it. AIS users must be familiar with the requirements in SOP 90 47.

2. To Whom Does This SOP Apply?

This SOP applies to SBA employees and contractors; where indicated, "You" refers to an SBA employee or contractor. This SOP also applies to SBA's contractors and employees of such contractors, where those contractors or employees have access to, and are authorized to use, SBA's AIS. To the extent that this SOP applies to contractors and their employees, SBA's contracts with those contractors must incorporate such SOP provisions by reference, or restate such provisions within the contracts themselves in order to make them binding on such contractors.

3. What Are the Responsibilities of Agency Managers and Contracting Officer's Technical Representatives (COTR)?

Agency managers are responsible for ensuring that their employees are informed of these policies and that employees appropriately use their time and SBA's AIS resources. Managers also are responsible for ensuring that, when necessary, these policies are stated in, or are incorporated by reference in, contracts with outside contractors so that the policies apply to such contractors and their personnel. The COTR is required to ensure that the contractor's personnel comply with these policies.

4. What Is SBA's Policy on Personal Use of SBA's AIS?

a. **Limited Personal Use**. SBA employees, contractors, and other users are permitted "limited personal use" of IT within SBA's AIS. This use must not interfere with official business, and must involve no more than minimal additional expense to the Government. Limited personal use of SBA's AIS is allowed during work hours as long as such use does not result in lost productivity or interfere with official duties. This privilege to use SBA's AIS for non-Government purposes may be revoked or limited at any time by an appropriate SBA management official.

"Minimal additional expense to the Government" means costs in areas such as:

a. Communications infrastructure costs (e.g., telephone charges, telecommunications traffic);
b. Use of consumables in limited amounts (e.g., paper, ink, toner);
c. General wear and tear on equipment;
d. Minimal data storage on storage devices; and
e. Minimal transmission impacts with moderate message sizes such as e-mails with small attachments.

Under no circumstances may employees and contractors use SBA's AIS for activities that are inappropriate or offensive to coworkers or the public, such as: the use of sexually explicit materials, or remarks that ridicule or demean others on the basis of race, creed, religion, color, sex, handicap, national origin, physical appearance, or sexual orientation.

While minimal use of SBA's AIS in moderation is acceptable, usage not conforming to this policy is strictly prohibited. Official Government business always takes precedence over the limited personal use.

b. **Proper Representation**. It is the ethical responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using SBA's AIS for non-Government purposes. If there is a reasonable expectation that such personal use will or could be interpreted to represent SBA, then the employee must use an adequate disclaimer. One acceptable disclaimer is: "*The contents of this message are mine personally and do not reflect any position of the Government or my Agency.*"

c. **Privacy Expectations**. When SBA employees, contractors, and other users access SBA's AIS for personal use, they do not have a right or an expectation, of privacy; (including when accessing the Internet or using e-mail). To the extent that employees wish that their private activities remain private, they should avoid using SBA's AIS for personal use. By using SBA's AIS for personal use, employees acknowledge that the contents of any files or information maintained or passed through SBA's AIS is not secure or anonymous, and may be monitored, recorded, and disclosed. Such transactions also may fall under the National Archives and Records Administration's Electronic Record Management Policy, Subchapter B, Records Management, Part 1234 – Electronic Records.

SBA employs monitoring tools to detect improper use of SBA's AIS. Electronic communications may be disclosed within SBA to employees who have a need to know, in order to perform their duties. SBA officials, such as system managers and supervisors, may access any electronic communications. In addition, note that the Office of Inspector General (OIG) has statutory rights of access to all SBA records includes electronic communications.

d. **Sanctions for Misuse**. Unauthorized or improper use of SBA's AIS could result in loss of use or limitations on use of the AIS, a letter of reprimand, a suspension, or, in egregious cases, removal from Federal service as outlined in SBA SOP 37 52 2, "Discipline and Adverse Actions."

5. What Are SBA's "Rules of Behavior" for Computer Usage?

You and other users are expected to conduct yourselves professionally in the workplace, and to refrain from using SBA's AIS for activities that are inappropriate. The following are SBA's "Rules of Behavior" for use of SBA's AIS which apply to all users:

a. **Equipment Use –** Except as specifically allowed elsewhere in this SOP, you must use SBA's IT (including PCs, computer software, telecommunications equipment, and IT mobile devices) for work-related purposes only.
b. **IDs and Passwords –** User IDs are assigned to individuals, and must 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.
c. **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.
d. **Unauthorized Access –**You are prohibited from accessing, or attempting to access, information systems or data 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 must 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 must not read, store, or transfer information that you are not authorized to access.
e. **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 in computer systems or other communication channels.
f. **Data or Software Modification or Destruction –**Unless officially authorized, you are not allowed to intentionally modify or delete system software, data, or programs. This prohibition does not apply to personal data, unless such data is contained with an Agency record, or to limited personal use data pertaining to you.

g. **Malicious Software –**You must not install or use malicious software such as computer viruses. Likewise, you must not download any software from the Internet to be installed on your PC, including screen savers, without assistance from an authorized representative from the OCIO.
h. **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 the OCIO Office of Information Security at (202) 205-7173 for further action. You must use care when downloading information from the Internet.
i. **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, contact your local IT specialist (or the SBA Help Desk at 202 205-6400 or helpdesk@sba.gov).
j. **Remote Access –** You may remotely access SBA's AIS only with the permission of your supervisor and authorization from the OCIO. SBA reserves the right to limit remote access to ensure the appropriate security for SBA's AIS.
k. **Unauthorized Use of Government Resources –** Unauthorized use of SBA's AIS for non-work-related activities, or any abuse of access capabilities, may result in disciplinary action.
l. **Reporting Security Violations –** You must report immediately to the OCIO Office of Information Security any suspected security violations, breaches, viruses, or other security related incidents.

6. What is SBA's Policy Concerning the Use of E-mail Service Provided by SBA?

The following policies apply to you and all contractor personnel and vendors using e-mail service provided by SBA:

a. E-mail services operated by or for the SBA are for official use, are subject to the same restrictions on their personal use, and to the same review process as any other SBA AIS provided for the use of employees.
b. Messages and files contained within SBA e-mail systems regardless of whether personal or business related are considered Agency property, and are subject to examination in connection with authorized official Agency reviews (e.g., OIG investigations, audits and inspections, administrative inquiries and reviews, etc.).
c. E-mail messages and files may be classified as official or Agency records with mandatory retention periods. The Agency Records Officer is responsible for establishing Agency policy on e-mail file and record retention.
d. E-mail messages may be considered official SBA records, which mean they may be subject to administrative review under the Freedom of Information Act (FOIA) and the Privacy Act (PA). Therefore, e-mail messages should be drafted with appropriate discretion. If printed or stored e-mail messages are deemed responsive to a request for information made pursuant to either the FOIA or the PA, those items must be reviewed for disclosure in accordance with the provisions of either Act.

e. Information about individuals in electronic form (including e-mail) should be protected to the same extent as a written record, and disclosed only when required for authorized purposes. In addition, commercial proprietary information should be protected in accordance with the conditions under which it is provided and with applicable law.

f. Unauthorized reading, disclosure, modification, or deletion of e-mail messages addressed to others is strictly prohibited. Violations of this provision will be addressed within established Agency policies and guidelines on employee conduct.

g. Employees should consult with specific subject matter SOPs (for example, FOIA, employee grievances) for additional information concerning the use of e-mail for particular activities related to those subjects.

7. What Is the SBA Internet Policy?

The following policies apply to you and all contractor personnel and vendors using Internet services provided by SBA. Internet services are available to help you perform official SBA business, such as communicating with customers, researching relevant topics, and obtaining business information. This Internet use policy is designed to help users understand SBA's expectations for the use of Internet services, and to use the services wisely. The following guidelines apply to use of SBA's Internet services:

a. Existing SBA policies that apply to employee conduct in other circumstances, also apply to employee conduct on the Internet. This includes, but is not limited to, policies on intellectual property protection, privacy, misuse of SBA assets or resources, sexual harassment, information and data security, confidentiality and inappropriate or offensive usage.

b. SBA software monitors, and records, all Internet usage. Therefore, you do not have a right, nor should you have an expectation, of privacy while using the Internet, including e-mail messages that you create, send, or retrieve over the SBA Internet for personal use.

c. SBA may inspect any files stored in the SBA network and respond to reasonable requests from law enforcement and regulatory agencies for logs, diaries, and archives regarding your Internet use. If you use the Internet as part of your official duties, you must identify yourself honestly, accurately, and completely, including your SBA affiliation and function, when requested.

d. As with all the SBA AIS, you are allowed limited personal use of SBA's Internet services. You must not use the Internet for personal use if such use results in a fee charged to SBA. If you do not follow this Internet policy, SBA may revoke your Internet privileges and remove your access rights.

e. SBA employees and contractors are also are prohibited from using SBA's internet and email access, distribute, sent, intentionally receive store, record, or edit sexually explicit materials. If you find yourself accidentally connected to a site that contains sexually explicit material, you must disconnect from the site immediately and notify your supervisor.

8. How Not to Get Hooked by a "Phishing" Scam.

"Phishing" (pronounced "fishing") is the act of sending to a user an e-mail falsely claiming to be from an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to a Web site where they are asked to update personal information, such as passwords and credit card, Social Security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus, and set up only to steal the user's information.

The Federal Trade Commission suggests the following tips to help you avoid getting hooked by a phishing scam. While many of them apply to your use of your own email and the Internet, they also apply in part to your use of SBA's AIS for limited personal use.

a. If you get an e-mail or pop-up message that asks for personal or financial information, **do not reply or click on the link in the message**. Legitimate companies don't ask for this information via e-mail. If you are concerned about your account, contact the organization in the e-mail using a telephone number you know to be genuine, or open a new Internet session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.
b. **Don't e-mail personal or financial information**. E-mail is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a Web site that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
c. **Review credit card and bank account statements** as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
d. **Use anti-virus software and keep it up to date if you telecommute.** Some phishing e-mails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Antivirus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones, that can effectively reverse the damage, and that updates automatically. A firewall helps to make you invisible on the Internet and blocks all communications from unauthorized sources. It is especially important to run a firewall if you have a broadband connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or phishers could exploit.
e. **Be cautious about opening attachments or downloading files from the e-mail you receive,** regardless of who sent it.

f. **Report suspicious phishing activity to your supervisor and the SBA Helpdesk** at (202) 205-6400 **or** helpdesk@sba.gov
g. Visit www.ftc.gov/spam to learn other ways to avoid e-mail scams and deal with deceptive spam.

9. What Is the SBA Peer-to-Peer Policy?

SBA prohibits the use of Peer-to-Peer (P2P) communications on SBA's AIS which means that a single violation of this prohibition may result in disciplinary actions in accordance with SBA's personnel policies.

P2P is a type of file sharing that refers to any software or system allowing individual Internet users to connect to each other and trade files. These systems are usually highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. While there are many appropriate uses of this technology, a number of studies show that the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggests P2P is a common avenue for spreading computer viruses within IT systems.

P2P software packages are not authorized for use on SBA equipment and represent a serious threat to SBA. Popular P2P clients such as KaZaA, Limelight, Morpheus, and Gnutella programs have been used to bypass external protection measures to spread malicious code such as Worm.P2P.Duload, W32 Efno.Worm, and W32.HLLW.Electron. These viruses rely on the accessibility of P2P. In addition to these viruses, malicious software could easily change the configurations of existing P2P clients. For example, a malicious code introduced via P2P networking could modify your directory settings so instead of C:\MyMusic being accessed, the entire hard drive could be opened for browsing and downloading. If these applications are in existence on SBA-owned equipment, notify the SBA Helpdesk immediately at (202) 205-6400 or helpdesk@sba.gov so OCIO can safely uninstall the software and examine the equipment for malicious code.

10. What Should SBA Computer Users Know About Malware, Adware, and Spyware?

Along with viruses, one of the biggest threats to SBA computer users on the Internet today is malware. It can hijack your browser, redirect your search attempts, serve up nasty pop-up ads, track what web sites you visit, and generally wreak havoc. Malware programs are usually poorly programmed and can cause your computer to become unbearably slow and unstable in addition to all the other havoc they wreak.

Adware, which typically displays ads or gathers information to be used in advertising, is the most common type of malware. Adware is generally viewed as a mere nuisance. While annoying in itself, adware also makes your computer vulnerable. If attackers can install adware on your computer, they can also install a Trojan horse containing a keystroke logger or even remote access software. These more serious forms of malware have the potential not merely to inconvenience users, but to destroy all network security.

Another form of malware is spyware. Spyware programs send information about you and your computer to somebody else. Some spyware simply relays the addresses of sites you visit or terms you search for to a server located somewhere else. Others may send back information you type into forms in Internet Explorer or the names of files you download. Still others search your hard drive and report back what programs you have installed, the contents of your e-mail client's address book (usually to be sold to spammers), or any other information about or on your computer – things such as your name, browser history, login names and passwords, credit card numbers, and your phone number and address.

Here are some tips to help prevent malware and spyware from entering SBA computer systems:

a. Adhere to the SBA Peer-to-Peer Policy.
b. Avoid using Instant Messaging on SBA computer systems – Instant Messaging can bypass regular anti-virus software and firewalls, providing a back door into SBA systems.
c. OCIO recommends scanning portable data storage devices such as CDs, floppy disks, USB keys, PDAs and portable drivers with virus scanning software before they are used on SBA computer systems; all of these devices have the potential to spread viruses and other malware to SBA computer systems.
d. If you suspect that you have malware on your computer system, immediately report it to your supervisor and the SBA Helpdesk at (202) 205-6400 or helpdesk@sba.gov.

It is very common for people to use the words adware, spyware, and malware interchangeably. Most products that call themselves spyware or adware removers will actually remove all types of malware.