Rules of the Road
for Users of
Smithsonian Computers and Networks

Introduction

Smithsonian systems, networks and other computer resources are shared among Smithsonian employees, interns, visiting scholars, contractors, and volunteers. SInet provides access to Smithsonian application systems that operate on the Smithsonian information technology infrastructure, and provides access to the external resources via the Internet.

The *Rules of the Road* are intended to help you use the Smithsonian's computing and network facilities responsibly, safely, and efficiently, thereby maximizing the availability of these facilities to all authorized users. The *Rules of the Road* are derived from Smithsonian Directive 931, *Use of Computers and Networks*, and Smithsonian Institution Archives Publication, *Treating E-Mail as Records.*

Complying with these rules will help maximize access to these facilities, and help assure that your use of them is responsible, legal, and respectful of privacy. You must follow the *Rules of the Road* when using Smithsonian automation resources.

The *Rules of the Road* are grouped into three categories as follows:

- ***Assuring Proper Use of Smithsonian Computers and Networks***
- ***Assuring the Security of Smithsonian Computers and Networks***
- ***Understanding Privacy Limitations of Smithsonian Computers and Networks***

Assuring Proper Use of Smithsonian Computers and Networks

It is important that you understand the purpose of Smithsonian computer systems and networks so that your use is in compliance with that purpose. The purpose of Smithsonian computer systems and networks is to conduct the business of the Smithsonian in fulfillment of our mission for the increase and diffusion of knowledge. As a Smithsonian employee, contractor, intern or volunteer you have an obligation to conduct your system activities in keeping with the Smithsonian's mission, goals and objectives.

RULE 1:

Don't Conduct Unauthorized Business on Smithsonian Systems or Networks

The Smithsonian allows personal use of its computers on an occasional and incidental basis, unless prohibited by an employee's supervisor. However, some personal uses are

Arts & Industries Building Suite 2310
900 Jefferson Drive SW
Washington, DC 20560-0433
202.343.1052 Telephone
202.312.2884 Fax

not permitted. The Smithsonian prohibits the use of any means of electronic communication to:

- Harass or threaten other users or interfere with their access to SI computing facilities.
- Send, forward or request racially, sexually, or ethnically offensive messages.
- Search for or use websites that involve hate groups or racially offensive or sexually explicit material.
- Seek, store, or transmit sexually explicit, violent or racist images or text.
- Send material that is slanderous or libelous or that involves defamation of character.
- Plagiarize.
- Send fraudulent e-mail.
- Break into another computer or mailbox.
- Intercept or otherwise monitor network communications without authorization.
- Misrepresent your real identity (e.g. by changing the "From" line in an e-mail).
- Lobby an elected official.
- Promote a political candidate.
- Promote a personal, social, religious, or political cause regardless of worthiness.
- Gamble.
- Send malicious programs such as computer viruses.
- Promote ventures involving personal profit such as on-line brokering.
- Subscribe or post to external news groups, bulletin boards or other public forums except when job related.
- Post personal opinions to a bulletin board, listserv, mailing list, or other external system using a Smithsonian userid except as part of official duties (inclusion of a disclaimer that such statements are not those of the Smithsonian does not make this activity permissible).
- Participate in activities that promote computer crime or misuse, including, but not limited to, posting or disclosing passwords, credit card and other account numbers, and system vulnerabilities.
- Violate any software licensing agreement (for example using software that hasn't been purchased, or distributing unlicensed software).
- Infringe on any copyright or other intellectual property right.
- Participate in chain letters.
- Disclose confidential business information.
- Create or maintain a personal web site.
- Send mass mailings of a non-business nature.
- Send e-mail announcements other than those distributed by the Office of the Chief Information Officer, to multiple groups that include most or all Smithsonian staff. SD 971 provides guidance on Smithsonian-wide e-mail announcements.

RULE 2:

Treat E-mail as Records

The Smithsonian Institution's policy on records is "to create and keep complete and accurate records of its activities; maintain the integrity of those records; and preserve

records of enduring evidential or historical value." (Smithsonian Directive 501).

The easiest rule of thumb is that a record is anything worth saving because SI will need it later to carry on the Institution's business. Some things are worth saving for short periods of time such as weeks or months; some for years, and some in perpetuity.

You should treat e-mail messages the same way that you treat paper correspondence. An e-mail message is a record if it documents the SI mission or provides evidence of an SI business transaction and if you or anyone else would need to retrieve the message to find out what had been done or to use it in other official actions.

There are special requirements for retaining e-mail messages as records. You should make sure that the e-mail record includes transmission data that identifies the sender and the recipients and the date and time the message was sent and/or received.

If an e-mail message qualifies as part of the record, you need to make sure that related items that provide context for the message are maintained as well. This includes attachments. You would keep them under the same conditions that you would if they were paper attachments to a paper memo or incoming letter.

You should store e-mail records in an approved record keeping system. This system may be either paper or electronic. In either case the record keeping system must:

- Logically relate or group records in accordance with your office's file plan
- Ensure the records are accessible to authorized persons throughout the records life
- Support retention of the records for as long as they are required
- Facilitate destruction of records on schedule
- Enable transfer of those records which will not be destroyed to Smithsonian Institution Archives

For information about office file plans and approved recordkeeping systems, ask the administrative assistant in your office. If that person does not know, contact Smithsonian Institution Archives at 202-357-1420 or osiaref@osia.si.edu.

RULE 3:

Don't Overload System Resources

Each user of the system should carefully evaluate his/her use of this resource and not overtax processing and storage capabilities or restrict access by others. In particular:

- Avoid sending an e-mail attachments larger than 5 megabytes. This is a document of approximately 150 pages if it is only text; however, a single graphic could be this large or larger.
- Minimize downloading audio or video files from the Internet.
- Do not use the Internet to watch videos, listen to the radio, or make telephone calls.

- Archive e-mail messages you need to keep after you have read them. Delete those you no longer need.
- Do not send broadcast messages.
- Do not overtax processing and storage capabilities
- Do not attempt to extend system-processing time by overriding established system time limits.

RULE 4:

Don't Use Unapproved Software or Hardware

Do not download software from the Internet, or purchase and install it, unless it is specified in the Technical Reference Model maintained by the OCIO. Do not add hardware to a PC without the approval of the OCIO. Do not modify system files or settings, or delete software, on your PC without prior approval.

Copyright and licensed materials, including software, should not be used on your PC, on SINET, or the Internet in any fashion unless legally owned or otherwise in compliance with intellectual property laws.

OCIO purchases site and limited licenses for certain products, such as anti-virus software. Do not copy software to use on your home computer unless the license allows it.

Remote access through programs that allow dial-up to an individual's PC must be password protected and must be approved by the OCIO.

Assuring the Security of Smithsonian Computers and Networks

The Smithsonian has invested considerable time and money to establish an automation environment that provides timely access to the computing resources and information that you need. In order to protect these assets and to ensure that you and other authorized users continue to receive the service you require, you must take certain actions to protect Smithsonian automation assets.

RULE 5:

Protect your Hardware and Data.

The following safeguards are required for all PC users:

- Use a password with at least eight alphabetic, numeric, and special characters. It must not be found in a dictionary, easily guessed, or left in writing in the user's office. See note below for hints on creating passwords).
- Change passwords every 90 days.
- Do not reuse any of your last 12 passwords.
- Do not disclose passwords except to authorized staff.
- Immediately notify the system administrator when a password has been compromised.
- Do use group accounts controlled by a single password.

- Activate a screensaver lock when leaving the immediate area of your PC. Instructions for a no-cost screensaver are on PRISM.
- Logoff and power off PCs at the end of the workday.
- Delete all sensitive data when a PC is replaced or declared surplus.
- Keep laptops in a secure environment at all times, especially when traveling. Sensitive data stored on laptops must be encrypted.
- Back up data and store critical backed-up data off-site.
- Account for hardware loaned for at-home use in a unit's property management records. Form SI-4153, *Off-Site Property Utilization Authorization*, available at http://ocon.si.edu, must be completed. The property manager is responsible for ensuring the return of such property when it is no longer needed or when the user's employment ends.
- Get approval to access remote programs that allow dial-up to individual PCs from OCIO.
- Promptly report security incidents to the Smithsonian's Computer Security Manager.

Note regarding creating good passwords: Think of a favorite song or poem and use the first letter of the first seven words, then add a number somewhere - preferably in the middle, but at the beginning or end is almost as good. Also substitute a special character in place of one of the letters with the same shape (e.g. "$" in place of "S").

If someone needs to look at your mail while you are on vacation assign that person "proxy" rights to your e-mail (beforehand). You shouldn't have to give them your password.

RULE 6:

Use Anti-Virus Software and be sure it's up-to-date.

Our standard anti-virus software for desktop systems is McAfee's VirusScan for Windows and Virex for Macintosh. Check with the Information Technology people in your office to find out where to get anti-virus software. Virus signature files can be updated automatically - be sure your program is configured to do this. Laptop updates can be done through the Internet.

Also: don't spread warnings about computer viruses - most such warnings are hoaxes. And don't open e-mail attachments unless you expect them - attachments are the most common means for transmitting a virus. Even e-mail from trusted sources can contain a virus; sometimes the e-mail itself is sent without that person's knowledge.

RULE 7:

Protect your Hardware.

When you leave your PC (to go to a meeting, lunch, or just for a drink of water) invoke your password protected screensaver. The easiest way to do this is to place an icon on your desktop that allows you to invoke the Windows screensaver with a double click of

the mouse button. Complete instructions (not nearly as complicated as they may look) for creating this icon can be found at:
http://prism2.si.edu/security/screensaverinstr.html

Log off and power off the PC at the end of the workday.

Laptops must be kept in a secure environment at all times, especially when traveling. If sensitive data is stored on laptops it must be stored in encrypted form.

Hardware lent for use at home must be accounted for in the unit's property management records (Form SI-4153 Off-Site property Utilization Authorization, which is available at http://ocon.si.edu must be completed); the property manager is responsible for ensuring the return of such property when it is no longer needed or at the termination of employment of the employee.

RULE 8:

Back up your Data.

Hard drives crash; viruses destroy data; laptops get stolen. If you keep your files on a server, the server administrator has the responsibility to back up your data, otherwise you need to save it yourself.

Understanding Privacy Limitations of Smithsonian Computer and Networks

Although we refer to your desktop computer as a *Personal* Computer you should understand that it is the property of the Smithsonian Institution, as is all the data contained on it. Furthermore, even though you must enter a password to access your e-mail and files, you should not conclude that this password implies that these files and e-mails are your private correspondence. All Smithsonian computing resources are the property of the Smithsonian, even when used as permitted under the occasional and incidental personal use policy.

RULE 9:

Don't assume your e-mail (etc.) is confidential.

E-mail, World Wide Web data and logs, and any other files on you PC or server, or created or received while using Smithsonian computers or networks is not confidential. Neither is data that is transmitted over our networks. The Smithsonian monitors networks for a variety of reasons including checking for performance problems and abuses. Your use of a password, although an important safeguard, should not be interpreted to grant you confidentiality.

Sensitive information must not be transmitted over the Internet unless encryption is used. This includes all forms of transmission (e.g., e-mail, file transfers, Web forms). Sensitive information includes but is not limited to social security numbers, credit card numbers, contracting information prior to award, details involving personnel and union issues.