

August 5, 2002

USE OF COMPUTERS & NETWORKS

Introduction	1
Applicability	1
No Expectation of Privacy	1
User Agreement	2
Computer Security Awareness	2
Access to Files & Email	2
Encryption Keys	3
Misuse of Computers & Networks	3
Overloading System Resources	5
PC Software & Hardware Controls	5
Transmitting Sensitive Information	5
Required Safeguards	6
Computer Viruses	7
Penalties	7
Responsibilities	7
Relationship to Other Computer Security Policies	8
Appendix: User Agreement	

Introduction The Institution's computers and networks are to be used only for Smithsonian-related work. Incidental and occasional personal use is permitted, provided that such use does not interfere with the conduct of normal Institutional business and meets the requirements of other sections of this document.

Applicability This directive applies to all users of Smithsonian computers and networks.

No Expectation of Privacy In the course of operation and maintenance activities, use of computers and networks may be monitored to ensure the continuing effectiveness and integrity of Institutional IT resources. Email, World Wide Web logs and data, and other files created or received while using Smithsonian

No Expectation of Privacy
(Continued)

computers and networks are neither private nor confidential.

The Smithsonian Institution reserves, for cause, the right to access and disclose all messages sent by its computers and networks, as well as any data created, received, or stored on them.

User Agreement

All users of Smithsonian computers and networks must sign a user agreement (please see Appendix) before access to a Smithsonian computer or network is permitted.

Computer Security Awareness

The Institution will

- provide an online computer security awareness tutorial and require users to complete the tutorial annually
 - periodically distribute email reminders of prohibited activities
 - maintain a log-on warning screen with a reminder about appropriate use of Smithsonian computers and network security requirements.
-

Access to Files & Email

Although the Smithsonian intends to convey no expectation of privacy, its business communications must be protected from unauthorized access. Electronic files and email may be accessed by

- authorized staff seeking to ensure efficient and proper operation of the workplace or searching for suspected misconduct or misfeasance. Only the Secretary; an under secretary; a director of a museum, research institute, or office; the Institution's Computer Security Manager; and staff of the Office of Inspector General may authorize access to and disclosure of electronic files and only in fulfillment of their responsibilities.

Access to Files & Email
(Continued)

- system administrators and their supervisors in the legitimate performance of their normal duties. They may not, however, reveal information obtained in this manner unless authorized by one of the officials named above. Duties that allow a system administrator to access the files of other users include, but are not limited to,
 - system maintenance or development
 - system security
 - correcting software problems.

The Smithsonian may disclose electronic files and email pursuant to a discovery request, court order, or applicable law.

Encryption Keys

Because data contained on Smithsonian computers and networks are not private, employees, contractors, volunteers, and interns are required to provide their encryption keys on request to their supervisors, the Institution's Computer Security Manager, or staff of the Office of Inspector General.

Misuse of Computers and Networks

The Smithsonian prohibits use of computers and networks to

- harass or threaten other users or interfere with their access to Smithsonian 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 email
- break into another computer or mailbox
- intercept or otherwise monitor network communications without authorization

**Misuse of
Computers and
Networks**
(Continued)

- misrepresent the user's real identity (e.g., by changing the *From* line in an email)
 - lobby an elected official
 - promote a personal social, religious, or political cause regardless of worthiness
 - send malicious programs such as computer viruses
 - gamble
 - promote ventures involving personal profit such as online 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 user ID except as part of official duties (including a disclaimer that such statements are not those of the Institution 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
 - infringe upon any copyright or other intellectual property right
 - participate in chain letters
 - disclose confidential or sensitive information
 - create or maintain a personal website
 - send mass mailings of a non-business nature
 - send email announcements, other than those distributed by the Office of the Chief Information Officer (OCIO), to multiple groups that include most or all Smithsonian staff. SD 971 provides guidance on Smithsonian-wide email announcements.
-

Overloading System Resources	<p>Each user should</p> <ul style="list-style-type: none">• carefully evaluate his or her use of computers and networks• avoid sending email attachments larger than five megabytes, a document of approximately 150 pages if text only. A single graphic could be as large as that or larger.• minimize downloading audio or video files• archive required email messages; delete others• not overtax processing and storage capabilities or restrict access by others• not use the Internet to watch videos, listen to the radio, or make telephone calls unless work related• not send broadcast messages• not attempt to extend system-processing time by overriding established system time limits.
-------------------------------------	---

PC Software and Hardware Controls	<p>Users may not download, purchase, or install software unless it is able to operate on computer equipment specified in the Technical Reference Model (TRM) (IT-920-1) maintained by OCIO. SD 940 provides guidance on acquiring IT products.</p> <p>Users may not add hardware to a PC, modify system files or settings, or delete standard software on a PC without prior approval of OCIO.</p> <p>Copyrighted and licensed materials should not be used on a PC, SInet, or the Internet unless legally owned or otherwise in compliance with intellectual property laws. Users must read and understand all license material included with software.</p>
--	--

Transmitting Sensitive Information	<p>Sensitive information must not be transmitted over the Internet unless encryption is used. This includes all forms of transmission such as email, file transfers, and Web forms. Sensitive information includes, but is not limited to, social security numbers, credit card numbers, contracting information prior to award, and personnel issues.</p>
---	--

**Required
Safeguards**

To protect Smithsonian equipment and data, users are required to use safeguards that include

- having 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.
 - changing passwords every 90 days
 - not reusing passwords
 - not disclosing passwords except to authorized staff
 - immediately notifying the system administrator when a password has been compromised
 - prohibiting system administrators from establishing group accounts controlled by a single password
 - activating a screensaver lock when leaving the immediate area of his or her PC. Instructions for a no-cost screensaver are on PRISM under *IT at SI*.
 - logging off and powering off PCs at the end of a workday
 - deleting all sensitive data when a PC is replaced or declared surplus
 - keeping laptops in a secure environment at all times, especially when traveling. Sensitive data stored on laptops must be encrypted.
 - backing up data and storing critical backed-up data off-site
 - accounting 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.
 - accessing remote programs that allow dial-up to individual PCs with protected passwords approved by OCIO.
 - promptly reporting security incidents to the Smithsonian's Computer Security Manager.
-

Computer Viruses All PCs must be set up to use and have installed the anti-virus software provided by the Institution. When PCs are properly configured to update automatically virus signature files and to scan all files at the time they are used, the entire Institution is protected from the spread of malicious software.

Penalties Penalties for violations of these provisions may include disciplinary action up to and including suspension without pay and termination of employment administered in accordance with Smithsonian personnel policies and procedures. Illegal activities will be reported to law enforcement authorities for prosecution and punishment as provided by law.

Responsibilities

The **Chief Information Officer**

- manages the computer security program
- establishes computer security policies and standards
- grants exceptions to these policies and standards as appropriate.

The **Director, Office of Human Resources**, ensures that

- computer security awareness training is included in orientation of new employees
- employees sign user agreements during orientation
- signed user agreements are retained in the official personnel files of all employees.

The **director of each museum, research institute, and office** ensures that

- each user annually completes the online computer security awareness tutorial
- users who are not Smithsonian employees sign user agreements
- signed user agreements are retained in unit files.

Responsibilities
(Continued)

The **Director, Smithsonian Center for Education & Museum Studies** ensures that computer security awareness training is included in orientation of interns.

The **Smithsonian Computer Security Manager**

- administers the Institution's computer security awareness training
- monitors compliance with the password policy
- manages response to computer security incidents
- administers the anti-virus program.

Relationship to Other Computer Security Policies

These provisions supersede corresponding ones in SD 506, *Computer Security Manual*.

CANCELLATION:
INQUIRIES:
RETENTION:

Announcement 97-11, December 17, 1997

Office of the Chief Information Officer

Indefinite. Subject to review for currency 24 months from date of issue

USER AGREEMENT

Smithsonian Institution computers and networks are to be used for purposes that benefit the Institution and assist in fulfilling its mission. Incidental and occasional personal use is permitted if such use is consistent with Smithsonian Directive 931, *Use of Computers & Networks*, which is available under *Policies* on PRISM.

You are expected to comply with the provisions of SD 931, to act in a responsible manner, and to respect the security of all systems to which you have access. You must maintain the security of the system for which you are responsible so that it does not provide a means of unauthorized entry to other parts of the Smithsonian network.

Please refer any questions to the Smithsonian Institution Computer Security Manager at 202-633-9035.

☐ ☐ ☐

I have read Smithsonian Directive 931, *Use of Computers & Networks*, and understand that I am required to observe the policies and procedures stated in it.

Print User's Name Unit

User's Signature Date