Smithsonian Institution

SMITHSONIAN DIRECTIVE 931

September 18, 2009

USE OF COMPUTERS, TELECOMMUNICATIONS DEVICES AND NETWORKS

Introduction

The Smithsonian Institution's computers, telecommunications devices, and networks are to be used only for Smithsonian-related work or work performed by approved partners and affiliates. Incidental and occasional personal use is permitted, provided it does not interfere with the conduct of normal Institution business and meets the requirements of other sections of this document.

Applicability

This directive applies to all users of Smithsonian computers, telecommunications devices, and networks, including all hardware connected to Smithsonian computers and networks. Telecommunications devices include, among other things, Smithsonian cellular phones, desktop phones, and smartphones.

Rules for Users

The following rules apply to all users of Smithsonian computers, telecommunications devices, and networks.

Rules for Users
(continued)

Rule 1: Do Not Expect Privacy

The Smithsonian may monitor the use of computers, telecommunications devices, and networks for various purposes, including ensuring the effectiveness and integrity of the Institution's information technology (IT) resources. Users should have no expectation of privacy in email, World Wide Web logs and data, text messages, voice mail, or other files or data created, transmitted, or received while using Smithsonian computers, telecommunications devices, or networks.

When ensuring continuation of business or investigating possible misconduct, the Smithsonian may access and disclose all messages sent by its computers, telecommunications devices, and networks, as well as any data created, received, or stored on them.

Rule 2: Sign User Agreement

All users of Smithsonian computers, telecommunications devices, or networks must sign a user agreement (please see Appendix) before accessing a Smithsonian computer, telecommunications device, or network.

Rule 3: Complete Computer Security Awareness Training

All users must complete the Smithsonian-approved online computer security awareness tutorial annually.

Rule 4: Provide Encryption Keys

Because data contained on Smithsonian computers, telecommunications devices, and networks are not private, users are required to provide their encryption keys on request to their supervisors, the Institution's Director of IT Security, or the Office of the Inspector General (OIG).

Rules for Users
(continued)

Rule 5: Use Computers, Telecommunications Devices, and Networks Appropriately

Smithsonian computer, telecommunications device, and network users must not:

- harass or threaten other users or interfere with their access to Smithsonian computing or telecommunications 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
- misrepresent the user's real identity (*e.g.,* by changing the *From* line in an email); this does not include instances where an individual was granted permission to send email from another individual's account
- lobby an elected official
- promote a personal social, religious, or political cause, regardless of worthiness
- send malicious programs such as computer viruses

Rules for Users (continued)

- 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
- 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 that is not work related
- send mass mailings of a non-business nature
- send email announcements, other than those distributed by the Office of the Chief Information Officer (OCIO) or the Office of Public Affairs (OPA), to multiple groups that include most or all Smithsonian staff. SD 971 provides guidance on Smithsonian-wide email announcements.

Rule 6: Avoid Overloading System Resources

Each user should:

Rules for Users (continued)

- carefully evaluate his or her use of computers, telecommunications devices, and networks
- avoid sending large email attachments unless there is a business need
- delete email messages and files that are no longer needed in accordance with the official record retention guidance issued to his or her museum, research center, or office
- not overtax processing and storage capabilities or restrict access by others
- conserve energy by shutting down or putting computers in power-saving mode when they won't be in use for an extended period
- minimize downloading audio or video files and do not use the Internet to watch videos or listen to the radio, unless work-related.

Rule 7: Adhere to Software and Hardware Controls

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-920-01, maintained by OCIO. SD 940, *Acquisition of Information Technology Products*, provides guidance on acquiring IT products.

Users may not add hardware to a PC, modify system files or settings, or delete standard software on a PC without prior OCIO or unit IT support staff approval.

When conducting Smithsonian business via email, users must use the official Smithsonian email system, unless the system is unavailable.

Copyrighted and licensed materials should not be used on a PC, other hardware, 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.

Rules for Users
(continued)

Rule 8: Protect Sensitive Data

Users must take measures and implement controls to protect sensitive data from loss, misuse, modification, and unauthorized access. Examples of sensitive data include Social Security and credit card numbers and system vulnerability information. Detailed reports related to computer security deficiencies in internal controls are also sensitive.

Every user is responsible for protecting sensitive data and must apply appropriate safeguards. When handling sensitive data, users will:

- collect sensitive data only for a specific purpose and not retain it longer than required
- not transmit sensitive data over the intranet or Internet unless encrypted. This includes all forms of transmission, including emails, file transfers, and Web forms. Users are responsible for obtaining the appropriate encryption tools and may contact OCIO for guidance in this area
- not share sensitive data without approval of the appropriate management official
- follow Smithsonian policy regarding the disposal of media containing sensitive data. See technical note, *Disposal of Sensitive Electronic Media*, IT-960-TN15
- mark or label media containing sensitive data to control and limit its distribution

Users should also comply with Smithsonian policies for protecting sensitive information that is in hard-copy form.

Rule 9: Apply Required Safeguards

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

Rules for Users (continued)

- having a network password with at least eight characters that includes letters, numbers, and special characters. It must not be found in a dictionary, easily guessed, or left in writing in the user's office
- using passwords to secure telecommunications devices, where possible
- changing passwords every 90 days or more frequently, as appropriate
- not reusing passwords
- not disclosing passwords except to authorized staff
- never disclosing passwords over email or voice mail
- immediately notifying your supervisor and the OCIO Help Desk if you suspect your password has been compromised
- prohibiting system administrators from establishing group accounts controlled by a single password without first receiving OCIO approval
- activating a screensaver lock when leaving the immediate area of his or her computer
- deleting all sensitive data from PCs, smartphones, and other hardware when it is replaced or declared surplus in accordance with the Smithsonian policy outlined in technical note, *Disposal of Sensitive Electronic Media*, IT-960-TN15
- keeping laptops and other portable hardware in a secure environment at all times, especially when traveling. Sensitive data stored on laptops or other portable hardware must be encrypted
- storing critical data so it will be subject to the Institution's automated backup process

Rules for Users (continued)

- accounting for hardware loaned for at-home use in a unit's property management records. Users are responsible for completing the required Smithsonian form SI-4555, Personal Property Pass Authorization Form, and presenting it to the appropriate Accountable Property Officer (APO) at the time the property is assigned. Users are also responsible for returning the assigned property when it is no longer required or the user's employment with the Smithsonian ends. The APO is responsible for taking necessary actions to ensure that the assigned property is returned when required and that the location of such property is accurately recorded in the unit's property management records.

- using the Institution's centralized program for the disposal/surplus of old computers

- promptly reporting security incidents, including the loss or theft of hardware, to his or her supervisor and the OCIO Help Desk.

Rule 10: Protect Computers from Viruses and Other Malware

All Smithsonian computers must have installed and use the anti-virus software provided by the Institution. The entire Institution's risk from the spread of malicious software is lowered when computers are properly configured to automatically update malware protection and to scan all files at the time they are received or used.

Computer Security Awareness

The Institution will:

- provide an online computer security awareness tutorial

- periodically distribute email reminders of prohibited activities

Computer Security Awareness (continued)

- maintain a log-on warning screen with a reminder about appropriate use of Smithsonian computers and network security requirements.

Retention of User Agreements

Approved partners or affiliated organizations that provide user accounts on Smithsonian networks must either store their own signed user agreements or send scans of signed user agreements to OCIO.

Access to Files and Email

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

- Staff seeking to ensure efficient and proper operation of the workplace, particularly during unplanned employee absences. OCIO must first approve access, with concurrence from the IT support staff in the museum, research center, or office

- Staff searching for suspected misconduct or malfeasance. The Office of Human Resources (OHR) or the OIG must first approve access

- Staff responding to a discovery request or court order, or otherwise complying with a legal obligation

- IT system administrators and their supervisors in the legitimate performance of their normal duties. They may not reveal information obtained in this manner unless authorized by OHR, except they may report any suspected policy violations to OIG and the employee's supervisor. Duties that allow a system administrator to access the files of other users include, but are not limited to

  — maintenance or development
  — system security
  — correcting software problems

Access to Files and Email (continued)

- Staff of the Smithsonian Institution Archives (SIA) in the legitimate performance of their normal duties. Access must fall within its defined role as the Institutional Record Manager. The director in the museum, research center, or office must first approve access, with concurrence from the IT support staff for the museum, research center, or office. Duties that allow access include:

  — identification of official and historical records
  — development of unit-specific records management and retention guidance
  — transfer of selected records to the Archives

Penalties

Penalties for violations of the user rules 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 awareness program
- establishes computer security policies and standards
- grants waivers or exceptions to these policies and standards as appropriate
- ensures there are signed memoranda of understanding (MOUs) and interconnected security agreements (ISAs) with approved partners and affiliated organizations documenting any exceptions or waivers to this directive.

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

- computer security awareness training is included in the orientation of new employees

Responsibilities (continued)

- employees receive a copy of this directive and user agreement during orientation
- the Human Resource Management System (HRMS) includes employee training completion to ensure employee compliance.

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

- each user completes the online computer security awareness tutorial annually
- users who are not Smithsonian employees sign user agreements
- he or she signs MOUs and ISAs with approved partners and affiliated organizations documenting any exceptions or waivers to this directive
- he or she retains records showing OCIO approval of any group (shared) user accounts
- he or she provides signed user agreements to OCIO.

The **Smithsonian Director of IT Security**:

- administers the Institution's computer security awareness training
- monitors compliance with the password policy
- manages responses to computer security incidents
- administers the anti-virus program
- reviews MOUs and ISAs with partners and affiliated organizations.

Responsibilities (continued)

The **Smithsonian Archivist**:

- manages the official and historical records of the Institution
- develops general and unit-specific records management guidance for the Institution, including the appropriate disposition of all electronic files
- ensures that records management training is available to employees
- ensures that official and historical records are retained for the periods defined in the applicable records disposition schedules
- ensures that access to records in its custody adheres to established restrictions

CANCELLATION:	SD 931, August 5, 2002
INQUIRIES:	Office of the Chief Information Officer (OCIO)
RETENTION:	Indefinite. Subject to review for currency 24 months from date of issue.