CfA

Mobile Devices

1 message

McGlasson, Van <vmcglasson@cfa.harvard.edu> Thu, Apr 10, 2014 at 9:02 AM
To: sao-all@cfa.harvard.edu

To: SAO-Affiliated Staff (SAO employees, contractors, post-docs, pre-docs, interns, and visiting scientists)

Many of us are increasingly using mobile devices (laptops, tablets, and smart phones) in our work and so it is timely to review the computing policies and procedures that we operate under as part of the Smithsonian. For full background please review the three attached documents: Rules of the Road, SD-931 and a description of "sensitive data". Of particular note are the following items:

(a) Storing sensitive information. Do not store sensitive information (information which, if breached, could damage the reputation of SAO or possibly jeopardized future funding opportunities, see attached) or personally identifiable information (information which, if breached, could be used to conduct financial transactions on someone else's behalf, i.e., identity theft) on any mobile computing device.

(b) Traveling with sensitive information. If you should need to take sensitive information when you travel please either store the data in your CfA Google Drive space for remote access, or store the data on a hardware-encrypted device such as an Iron-Key USB stick, available from the CF.

(c) Export Controlled projects. If you are involved in a project that is subject to U.S. Export Control Laws, i.e., ITAR, you are subject to the additional requirements found at http://www.cfa.harvard.edu/spp/cg/ecc/index.html. Please pay particular attention to the Mobile Device Travel Policy.

Please let me know if you have any questions.

Best,

Van

--
You received this message because you are subscribed to the Google Groups "sao-all" group.
Visit this group at http://groups.google.com/a/cfa.harvard.edu/group/sao-all/.

3 attachments

RulesOfTheRoad.pdf
55K

SD931.pdf
142K

Sensitive Data.pdf
78K

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 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 202-633-5870 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://prism.si.edu/ocfo/ocon/ocon_forms.htm, 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

Right click on the screen.
Select Properties
Select tab: Screen Saver
Set preferences for TIME (e.g. 10 minutes of inactivity).
Click On Resume pw protect
Click Apply
Click OK.

Alternately: press CTRL ALT DEL and Lock the Computer.

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://prism.si.edu/ocfo/ocon/ocon_forms.htm 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.

Examples of Sensitive Information

TSG-930-02 *Security Control Manual*

Institutional / Business Usage

- Institutional Financial Bank account numbers
- Copyright Restrictions
- Trademark Restrictions
- Patent Restrictions
- Commercial Use / License Restrictions

Collection Usage

- Protected Species Data
- Cultural / Native American Repatriation Data
- Moral Sensitivity
- Cultural Rights
- Publicity Rights
- Artifact Donor Request to remain Anonymous
- Physical Artifact - Storage Location Protections

Contract Usage

- Contract Data Prior to Award
- Vendor Labor Rates – Restricted Use
- Intellectual Property Rights
- Protected Labor / Union Information Restrictions

Computer Usage

- Account Pins / Passwords
- Internal IP addresses
- Computer Security Vulnerabilities (Systems, Applications, Databases)
- Firewall Rules / Network Routing Tables
- Logical Intrusion Information

Member of Public / Donor / Employee / Staff / Academic Appointment Usage:

Personally Identifiable Information (PII)

- Genealogical Data
- Social Security Numbers (SSN)
- Payment Card / Credit Card (CC) Numbers
- Financial Donor Requests to remain anonymous
- Financial Donor Background / Family Information
- Medical / health information
- Resumes or Curriculum Vitae (CV) / Detailed Employment / Salary History / Professional References
- Performance Reviews
- Results of Background / Suitability Investigation
- Photographs
- Fingerprints
- Individual Unpublished Research
- Human Research Data / DNA

Security Usage

- Physical Access Protections
- Physical Access Control Lists
- Keys / Lock
- Physical Intrusion Protection & Monitoring
- Security Force Protections Capabilities
- Cryptographic key Management Information

Smithsonian
Institution

SMITHSONIAN DIRECTIVE 931,

September 18, 2009,
Date Last Declared Current: January 30, 2013

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.