Smithsonian Institution

SMITHSONIAN DIRECTIVE 931,
November 2, 2016

USE OF COMPUTERS, TELECOMMUNICATIONS DEVICES, AND NETWORKS

I. PURPOSE

The Smithsonian Institution's (SI) computers, telecommunications devices, and networks are to be used for Smithsonian-related work or work performed by approved partners and affiliates. Users must understand the rules for using these resources appropriately, and their role in protecting these resources from unauthorized use.

II. BACKGROUND

Information technology (IT) Security is a critical element of risk management for all organizations today. As evidenced by the ever-growing list of high-profile and increasingly sophisticated security breaches profiled in the media, organizations are at high risk of attack from criminal activity, "hactivism," espionage, insider threats, terrorism, and accidental self-imposed incidents, resulting in large financial losses, reputational damage, business disruption, and other serious consequences. Protecting the Smithsonian and the resources entrusted to it requires a concerted effort and relies on the cooperation of all Smithsonian personnel who must understand how they fit into and affect the Institution's overall IT security posture.

An important aspect of IT Security is ensuring that everyone at the Smithsonian understands not only the security policies that apply to them, but also their own role in maintaining IT Security, and the consequences of non-compliance. Smithsonian personnel must have a basic understanding of the security risks in their IT environment and what they can and are expected to do to help protect the Smithsonian's resources.

III. APPLICABILITY

This directive applies to all staff, contractors, volunteers, interns, visiting researchers, and other affiliated persons who use Smithsonian computers, telephones, mobile devices, software applications, storage drives, websites, data, printers/copiers, and networks, including all hardware connected to Smithsonian computers and networks. The directive does not apply to public use of external-facing websites or use of guest WiFi networks by visitors from the general public.

IV. DEFINITIONS

A. **Affiliated Persons** — For purposes of this directive, the term Affiliated Persons is defined as the following: (i) contractors who perform work similar to Smithsonian employees, such as employees of temporary help firms; (ii) volunteers, as defined in SD 208, *Standards of Conduct Regarding Smithsonian Volunteers*; (iii) interns and Fellows; (iv) emeriti, as defined in SD 206, *Emeritus Designations*; (v) Smithsonian Early Enrichment Center (SEEC) employees; (vi) visiting researchers, including scientists, scholars, and students; (vii) research associates, as defined in SD 205, *Research Associates*; (viii) employees of federal, state, and local agencies, approved partners or affiliated organizations working with SI employees at SI facilities and property; and (ix) Regents and Advisory Board members.

B. **Computer** — Any programmable electronic device, including servers, desktop and laptop computers, tablets, smartphones, and network devices, that can be used to input, process, or store information.

C. **Mobile Device** — Any portable computer, such as a laptop, smartphone, tablet, or other portable device that can store or process data**.**

D. **Network** — A set of computers connected together for the purpose of sharing resources.

E. **Personnel** — Everyone who participates in the operation of the Smithsonian and the performance of its mission, including staff, contractors, volunteers, interns, Fellows, and other affiliated persons.

F. **Security Incident** — Any action that threatens the confidentiality, integrity, or availability of Smithsonian IT resources, whether located inside or outside of the Smithsonian, or any activity that violates Smithsonian IT Security policies. IT resources include computer

IV. DEFINITIONS (continued)

hardware and software, data, communication links, mobile devices, digitized assets, automated processes, physical computing environments, and associated personnel.

G. **Sensitive Information** — Sensitive information includes personally identifiable information (PII), Payment Card Information (PCI), system account credentials, financial account information, security information, protected intellectual property, and other information whose access by the wrong people would be detrimental to the Smithsonian or its customers and stakeholders.

H. **Software** — The programs and instructions that run a computer, as opposed to the actual physical machinery and devices that compose the hardware. Examples include operating systems, internet browsers, add-ins, business applications, productivity tools, software utilities, etc.

I. **Telecommunications Device** — Any electronic device used for communication over a network.

J. **User** — Anyone who accesses or makes use of Smithsonian computers, networks, and telecommunications devices.

V. POLICY

A. Rules for Users

Rule 1: Do Not Expect Privacy

The Smithsonian Institution's computers, telecommunications devices, and networks are Smithsonian property and are to be used for Smithsonian-related work or work performed by approved partners and affiliates. This provision applies without regard to the location of the Smithsonian computer or telecommunications device.

Emails, documents, text messages, voice mail, or other files or data created, transmitted, or received while using Smithsonian computers, telecommunications devices, or networks are the property of the Smithsonian.

Users should have no expectation of privacy in email (including private password-protected email accounts), internet usage, text messaging, voice mail, video/teleconferencing, system

V. POLICY (continued)

access, usage logs, or other files or data created, transmitted, or received while using Smithsonian computers, telecommunications devices, or networks.

The Smithsonian has the right to monitor the use of its computers, telecommunications devices, and networks, and may monitor, access, inspect, store, or disclose any emails, documents, text messages, voice mail, or other files or data created, transmitted, or received while using Smithsonian computers, telecommunications devices, or networks.

In addition, Smithsonian records are subject to the Institution's public records disclosure policy outlined in Smithsonian Directive 807, *Requests for Smithsonian Institution Information*.

Incidental and occasional personal use is permitted, provided it does not interfere with the conduct of normal Institution business, does not cause expense or security risk to the Smithsonian, and meets the requirements of the other sections of this document. Such personal use does not create a user right of privacy, as any such personal use is subject to monitoring by the Smithsonian and the other provisions of Rule 1 described above.

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 Security Awareness Training

All personnel with SI network accounts must complete the Smithsonian-approved online Computer Security Awareness Training (CSAT) annually, which includes reviewing and renewing acceptance of this directive. See IT-930-TN21, *Computer Security Awareness Training*, for more information.

All personnel without SI network accounts must complete Information Security Awareness Training (ISAT) annually. See IT-930-TN38, *Security Awareness Training for Staff without Network Accounts*, for more information.

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).

V. POLICY (continued)

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

Smithsonian 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, texts, or other communications
- access computers, mailboxes, systems, or data for which they have not been authorized
- intercept or otherwise monitor network communications without authorization
- misrepresent their 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 or transfer malicious programs such as computer viruses, except for the forwarding of suspicious emails to SpamAdmin
- participate in gambling
- perform activities involving personal profit such as:

V. POLICY (continued)

  - — operating or promoting a personal business
  - — performing paid work for another organization
  - — online brokerage trading
  - — selling personally owned items online, via email, or by phone
  - — personal fund raising
  - — performing any of the above-listed activities for a family member

- post personal opinions to a bulletin board, listserv, blog, social network, 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 or infringe upon any copyright or other intellectual property right

- disclose confidential or sensitive information without authorization

- 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) or the Office of Public Affairs (OPA), to multiple groups that include most or all Smithsonian staff. SD 112 provides guidance on Smithsonian-wide email announcements

- automatically forward Smithsonian email to a non-Smithsonian email account

- use any peer-to-peer file-sharing applications (such as Bit Torrent)

- store Smithsonian sensitive information on personal devices, a personal cloud account, or a personal email account

- set up personal accounts on internet sites or services using Smithsonian account credentials, except where approved or instructed by OCIO

V. POLICY (continued)

Rule 6: Avoid Overloading System Resources

Each user should carefully evaluate his or her use of computers, telecommunications devices, and networks and:

- 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: Comply with Software and Hardware Requirements

Users may not download, purchase, or install software unless it has been approved for use in the Technical Reference Model (TRM), IT-920-01, maintained by OCIO, and is able to operate on computer equipment specified in the TRM. 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.

Copyrighted and licensed materials may not be used on a PC, other hardware, SInet, or the internet unless legally owned by the Smithsonian or otherwise in compliance with intellectual property laws. Users must read and understand all license material included with software. Personally owned software may not be installed on Smithsonian computers and devices.

Software must be retired or replaced when the version is no longer supported by the vendor/developer or when security updates are no longer being provided for that version. When acquiring software for Smithsonian use, personnel must plan and budget for its periodic replacement.

Personnel will ensure that all laptops and Windows-based tablets that they purchase have full disk encryption enabled. Personnel must also ensure that the inventory management and theft deterrence software recommended by OCIO is installed on these devices.

V. POLICY (continued)

All Smithsonian-owned computers, servers, and mobile devices must be configured in accordance with Smithsonian standards. Personnel will ensure that any new computers and devices that they acquire are configured to these standards or are submitted to IT support personnel for configuration of these standards.

Personnel will submit any new technologies, systems, cloud services, Web applications, websites, server applications, payment card processing solutions, or other IT services (or significant changes to existing ones) to the OCIO Technical Review Board for approval prior to acquisition or implementation. See SD 920, *IT Life Cycle Management*, for more information.

Rule 8: Protect Sensitive Data (including PII)

Users must take appropriate measures and exercise due diligence to protect sensitive data from loss, misuse, modification, and unauthorized access. Examples of sensitive data include personally identifiable information (PII) (such as Social Security numbers), payment card information (such as credit card numbers), proprietary information, and system security information (such as computer security deficiencies, User IDs [usernames], passwords, network architecture information, etc.).

Everyone 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 store sensitive data on any laptop, phone, tablet, removable drive, or other mobile device unless the device is encrypted
- not share sensitive data without approval of the appropriate management official
- mark or label media containing sensitive data to control and limit its distribution
- protect sensitive data that is in paper form by storing it in a secure location and shredding it when no longer needed

V. POLICY (continued)

- follow SI published procedures for properly disposing of surplus PCs, smartphones, and other hardware to ensure that data is securely wiped from these devices before disposal

- conduct Smithsonian business via the official Smithsonian email system when using email.

Users must protect and handle PII in accordance with SD 118, *Privacy Policy*.

Users must protect any payment card data they handle in accordance with the requirements in SD 309, *Merchant Accounts, Payment Cards, and the PCI Data Security Standard*.

Rule 9: Apply Required Safeguards

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

- keeping laptops, tablets, cellular phones, and other mobile devices secure at all times, especially when traveling

- storing critical data where it will be subject to the Institution's automated backup process

- accounting for hardware loaned for at-home use in a unit's property management records. Users are responsible for completing the required OCon 204, Personal Property Assignment/Personal Property Pass Form (available at the Office of Contracting and Personal Property Management [OCon&PPM] Forms webpage), 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 (managed by OCon&PPM)

- exercising appropriate precautions to protect computing devices and data when traveling. See OCIO document "Computer Security While Traveling"

All Smithsonian computers must have anti-virus software provided by the Institution installed and active. The entire Institution's risk from the spread of malicious software is lowered when

V. POLICY (continued)

computers are properly configured to automatically update malware protection and to scan all files at the time they are received or used.

Any computers used to remotely access the Smithsonian network, including personally owned computers, must:

- have anti-virus software installed. SI-provided anti-virus licenses may be available for staff home use — contact OCIO for assistance; and
- use vendor-supported versions of operating system and internet browsers and keep them up to date with software patches (updates) from their vendors.

Users may not tamper with, disable, or intentionally bypass any IT security protections implemented by the Smithsonian.

Rule 10: Protect Access Credentials

Users are required to exercise due diligence in protecting their logon credentials by:

- having a network password with at least eight characters that includes letters, numbers, and special characters. It must not be found in a dictionary and not easily guessed. Use of pass phrases is recommended;
- not leaving any passwords in writing unless locked in a secure location;
- changing passwords every 90 days or more frequently, as appropriate;
- not re-using passwords;
- never disclosing or sharing passwords;
- not using the same password they use for Smithsonian systems on other (non-Smithsonian) systems. This includes externally hosted systems used for Smithsonian work (such as the Concur travel system);
- immediately notifying their supervisor and the OCIO Help Desk if they suspect their password has been compromised;
- immediately changing their password if it may have been compromised;
- not sharing any accounts without receiving an approved waiver from OCIO;

V. POLICY (continued)

- locking their desktop when leaving the immediate area of their computer;
- not displaying any cellular telephone, mobile device, or carrier wireless card passwords in public or attaching passwords to any devices; and
- never emailing passwords.

Rule 11: Report Security Incidents

All Smithsonian staff and affiliated personnel are required to:

- promptly report any suspected security incidents, including the loss or theft of computers and devices, to the OCIO Help Desk in accordance with IT-930-TN30, *Computer Security Incident Response Plan and Procedures*, and SD 119, *Privacy Breach Notification Policy*; and
- fully cooperate with security incident investigation and response activities.

Rule 12: Use Cellular Phones and Mobile Devices Appropriately

Users are required to comply with the following when using a Smithsonian-issued cellular telephone, mobile device, or carrier wireless card:

- Read and comply with IT-980-TN01, *Smithsonian Cellular Telephone, Mobile Device, or Carrier Wireless Card Policy;*
- Follow all local, state, and federal telecommunications laws when using these devices;
- Understand that users may be required to reimburse the Smithsonian for any unauthorized cellular telephone, mobile device, or carrier wireless card service charges and/or those deemed to be personal use that exceeds permitted usages;
- Contact the OCIO Help Desk or the unit administrative officer to have cellular telephone/mobile device/wireless service discontinued and billing stopped when no longer required. Users are responsible for all billing charges associated with the device until they have done so;
- Understand that users are only permitted to have either a cellular telephone or a mobile device, but not both, unless a waiver is granted by OCIO;

V. POLICY (continued)

- Understand that cellular telephones, mobile devices, and carrier wireless cards are not approved for transmitting sensitive information (including PII) and that users must exercise discretion when using them;

- Configure and periodically change a PIN code on the cellular phone to protect it from unauthorized use; and

- Only use Smithsonian-issued wireless cards in Smithsonian-issued computers, not personally owned computers.

B. 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.

C. Access to Files and Email

As described in Rule 1 above, staff should have no expectation of privacy when using Smithsonian IT resources. Electronic files, email, and other data 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), the General Counsel, or the OIG must first approve access

- Staff representing the Smithsonian in litigation or a legal dispute, including responding to a discovery request, law-enforcement investigation, or court order, or otherwise complying with a legal obligation

- Staff responding to a public records request pursuant to SD 807, *Requests for Smithsonian Institution Information*

V. POLICY (continued)

- 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 criminal or policy violations to the employee's supervisor, senior management, the General Counsel or the OIG. 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
  — routine monitoring for compliance with this directive and for potential security incidents
  — security incident investigation and response

- 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, but are not limited to:

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

D. 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.

VI. RESPONSIBILITIES

A. The **Chief Information Officer**:

- establishes computer security policies and standards; and

VI. RESPONSIBILITIES (continued)

- grants waivers or exceptions to these policies and standards as appropriate.

B. The **Smithsonian Director of IT Security**:

- manages the computer security awareness program;
- administers the Institution's computer security awareness training;
- periodically distributes security awareness information via email notices and other mechanisms;
- leads the Smithsonian's security incident response activities; and
- monitors compliance with IT security policies.

C. The **Director, Office of Human Resources (OHR)**, ensures that:

- computer security awareness training is included in the orientation of new employees;
- employees receive a copy of this directive and user agreement during orientation; and
- the Human Resource Management System (HRMS) includes employee training completion to ensure employee compliance.

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

- each SI network account user completes the online Computer Security Awareness Training (CSAT) annually;
- each person without an SI network account completes the Information Security Awareness Training (ISAT) annually;
- new users sign user agreements; and
- signed user agreements are provided to the Office of the Chief Information Officer (OCIO).

VI. RESPONSIBILITIES (continued)

E. **Users** ensure that they:

- read and understand the requirements in this directive before signing the user agreement;
- comply with the requirements in this directive; and
- report suspected violations of this directive to OCIO or their supervisor.

CANCELLATION: SD 931, Use of Computers, Telecommunications Devices and Networks, September 18, 2009.

INQUIRIES: Office of the Chief Information Officer (OCIO).

RETENTION: Indefinite. Subject to review for currency 36 months from date of issue.
