

**MEMORANDUM**

**TO:** College of Medicine Department Heads, Center Directors & Administrators

**FROM:** Steven Wormsley, PhD, Chief Information Officer

**FROM:** January 1, 2009

**RE:** **Personal Information Sweep Progress**

---

University policy clearly states that access to University data, computers and networks is a privilege conditioned on users' compliance with laws and policies. By policy, Vice Presidents, Deans, Directors, Department Heads and Center Directors have the ultimate responsibility for ensuring that computer users within their units comply with these mandates.

The Personal Information Sweep (<http://security.arizona.edu/pi>) was designed to help you meet this responsibility with respect to electronically stored Social Security numbers, credit card numbers and Arizona driver license numbers. President Shelton, in a memo to all UA Employees on September 16, 2008, asked all UA personnel who use computerized UA information to complete the Personal Information Sweep by the end of 2008.

The Personal Information Sweep is a procedure that provides strategies and tools for compliance. While many aspects of information security can be managed by IT staff, this one requires action by all of us. All College of Medicine personnel who use computerized UA information must complete the Personal Information Sweep by June 30, 2009.

Several resources are available to assist you with the completion of the Personal Information Sweep. Please refer to the Information Security Web site, <http://security.arizona.edu/pi>, or contact the Information Security Office, 621-UIISO, [iso@u.arizona.edu](mailto:iso@u.arizona.edu).

In addition, the College of Medicine Office of Information Technology Services (ITS) can also assist you or your department complete the Personal Information Sweep. For more information, please contact the ITS Helpdesk at 626-8721 or by email at [itshelp@email.arizona.edu](mailto:itshelp@email.arizona.edu)

Thank you for your assistance with this important initiative. Please don't hesitate to contact me ([wormsley@email.arizona.edu](mailto:wormsley@email.arizona.edu)) for additional information.



## Personal Information Sweep

### ▸ Biography

[President Shelton's Inauguration](#)

### ▸ Communications from the President

[Articles, Letters to the Campus Community, Memos, Public Addresses](#)

### ▸ President's Cabinet

### ▸ Campus Leadership

### ▸ About the University

[Five-Year Strategic Plan, Highlights & Rankings, Past Presidents](#)

#### MEMORANDUM

TO: UA Employees  
 FROM: Robert N. Shelton, President  
 SUBJECT: Personal Information Sweep  
 DATE: Sept. 16, 2008

Computer compromises, losses and thefts expose the University's employees, friends and associates to an increased risk of identity theft. These events negatively affect the University's reputation, generate significant departmental expense, consume hundreds of person hours, and waste other valuable University resources.

Given the traditionally open nature of our endeavors, such events will continue to be a concern. We can, however, blunt their negative impact by ensuring that we do not retain and electronically store the most sensitive, personal types of information – Social Security, credit card and driver's license numbers – unless absolutely necessary.

The national concern over privacy of personal information and identity theft is reflected in legislation and policies that mandate the protection of personal information. Whether you write letters of recommendation requiring students' Social Security numbers, process credit card transactions, retain class rosters, gradebooks or grant routing forms, or have access to student, financial, or other sensitive records, you have an obligation to protect the confidentiality of that information and to play a crucial role in the UA's efforts to ensure its protection.

University policy clearly states that access to University data, computers and networks is a privilege conditioned on users' compliance with laws and policies. By policy, Vice Presidents, Deans, Directors, Department Heads and Heads of Centers have the ultimate responsibility for ensuring that computer users in their units comply with these mandates.

The Personal Information Sweep is a procedure that provides strategies and tools for compliance. While many aspects of information security can be managed by IT staff, this one requires action by all of us. [I ask all personnel who use computerized UA information to complete the Personal Information Sweep between October 1 and December 31, 2008.](#) I understand this is an additional commitment for your already busy schedule, but it is important for all of us to make time to complete this task.

Several resources are available to assist you. Please refer to the Information Security Web site, [security.arizona.edu](http://security.arizona.edu), or contact the Information Security Office, 621-UIISO, [iso@u.arizona.edu](mailto:iso@u.arizona.edu).

# Personal Information Sweep (IS-P301)

---

If you visited the Personal Information Sweep procedure before October 1, please complete [Step 5](#) before starting to ensure that you are viewing the most recent version.

IT staff providing technical support within their units for the Personal Information Sweep are urged to review the [Technical Support Guideline](#).

- [Technical Support Guideline](#)
- [President Shelton's Communication](#)
- [Implementation Schedule](#)

The University Information Security Officer must approve exceptions to this procedure. Refer to the [Exceptions Procedure](#) and the [Exceptions Form](#) for more information.

---

This page includes important information about the Personal Information Sweep. Please read it first before proceeding to Step 1. You can navigate to the next step by clicking on the link at the bottom of each page (or section) or by clicking on the steps in the column on the left.

We strongly recommend viewing the information overview before beginning. It contains additional information about the Personal Information Sweep. Viewing requires a UA NetID.

- [For the computer user - Flash version](#) (12 minutes)
  - [For the computer user - PowerPoint version](#) (click **View** > **Notes Page** for notes)
  - [For IT staff - Flash version](#) (7 minutes)
  - [For IT staff - PowerPoint version](#) (with notes)
- 

Protection of personal information is of utmost importance at The University of Arizona. The Personal Information Sweep is a program designed to assist people who store UA information electronically.

## Why Secure Personal Information?

Personal information on a lost, stolen or hacked computer can be harvested and used to steal identities. When the security of personal information is believed to be breached, hundreds of hours of staff time and considerable financial and reputational cost can be involved in investigating and repairing the breach and in notifying those affected.

Concerns about identity theft have spurred several industry and legislative responses that address the security of the types of personal information used and stored at UA. In addition, UA employees are required to retain and dispose of records that may contain personal information in accordance with legal requirements. Failure to meet these requirements can result in [costly penalties for your department](#).

The Information Security Policy and the Policy on Acceptable Use of Computers and Networks make it clear that access to UA data, computers and networks is a privilege conditioned on users' compliance with laws and UA policy. To achieve compliance, a computer user must protect personal information while it is still in use and securely delete it when it is no longer needed. While the requirement seems simple, many computer users do not know whether their computers contain personal information. Even if they do know that they have personal information, they may not know where it is located.

## **What is Personal Information?**

Personal information includes first name or initial and last name accompanied by:

- Social Security Number (including a Student ID number not beginning with an “S” or “889”)
- Arizona driver’s license number
- Arizona non-operating identification license number (State ID card)
- credit card, debit card or bank account number with any required security code or password

This information can be used to uniquely identify a single person and is generally kept private.

## **Who is Responsible for Securing Personal Information?**

UA personnel are responsible for the security of UA information stored, sent or displayed using computing and communications resources, whether or not those resources are owned by the University. If you work with personal information, you must be aware of and comply with applicable legal requirements and policies.

Vice Presidents, Deans, Directors, Department Heads and Heads of Centers have ultimate responsibility for computing resources, including personal information, and for their units' compliance with legal requirements and policies.

The Personal Information Sweep provides tools and guidance for compliance. Complete the Personal Information Sweep on *each* computer or storage device you use to store UA information.

## **Why Can't IT Staff Do This for Me?**

You may or may not be assisted by your unit's IT staff in the technical aspects of this process, such as installing software and helping you with the clean up process. However, you yourself must ultimately decide, given your own duties and needs, which files to delete or retain. In addition, the scanning tool may find sensitive information that you should keep private even from IT staff. That means that all decisions about what to do with personal information should be made by you. The assurance that sensitive personal information is secured is **your** responsibility.

For assistance with the technical aspects of the process, contact:

- your local IT staff
- the 24/7 IT Support Center (626-TECH)
- the Information Security Office (621-UIISO or [iso@u.arizona.edu](mailto:iso@u.arizona.edu))

Non-technical questions should be directed to the Information Security Office (621-UIISO or [iso@u.arizona.edu](mailto:iso@u.arizona.edu)).

### **Which Information is Affected?**

This procedure applies to UA information stored in -

- all systems used by UA personnel, other than those centrally housing UIS, IIW, SPINS, FRS, PSOS, SIS and Matrix.
- personally owned computers and external media with UA information on them.

Note that accessing your UA computer desktop through a remote desktop program does not transfer personal information stored there to your off-campus computer.

While not within the scope of the Personal Information Sweep, paper documents with personal information should also be secured.

Additional requirements outside the scope of the Personal Information Sweep may apply if you -

- process [payment card data](#) or
- engage in certain electronic transactions involving [protected health information](#).

### **How Do I Secure Personal Information?**

The Personal Information Sweep is a program designed to assist UA personnel in addressing requirements and policies. This process will guide you through the steps you need to take:

- [LOCATE](#) personal information
- [DELETE](#) unneeded files
- [SECURE](#) personal information
- [INSTALL](#) Cornell Spider
- [DELETE](#) temporary files
- [RUN](#) Cornell Spider
- [FIND](#) the log file
- [DELETE or SECURE](#) personal information
- [COMPLY](#) with applicable standards
- [REGISTER](#) your computer
- [CERTIFY](#) completion
- [SUBMIT](#) the Certification

At their most basic, these 12 steps involve removing or securing any personal information you store on a computing device. You first do that for personal information you already know about or can readily find. Then, you use a computer program to search for personal information you missed.

Print a [checklist](#) to help you track your progress.



## Step 1 – Locate personal information

Authorities:

- [Arizona Revised Statutes Section 15-1823](#) (Identification numbers; social security numbers)
- [Arizona Revised Statutes Section 44-7501](#) (Notification of breach of security system)
- [Arizona Revised Statutes Section 41-1351](#) (Determination of value; disposition)
- [Payment Card Industry Data Security Standard](#)
- [Arizona Board of Regents Policies 9-201 \(General Policy\) & 9-202 \(University Responsibilities\)](#)
- [Information Security Policy \(IS-100\)](#)
- [Information Security Terms Guideline \(IS-G100\)](#)
- [SSN Usage \(IS-S301\)](#)
- [Data Classification \(IS-S302\)](#)
- [Encryption Guideline \(IS-G301\)](#)
- [University Network Operational Standard \(IS-S602\)](#)
- [File Deletion Guideline \(IS-G603\)](#)
- [Minimum Security for Networked Devices Standard \(IS-S701\)](#)
- [Server Security Standard \(IS-S702\)](#)
- [Acceptable Use of Computers and Networks at the University of Arizona](#)
- [Computer and Network Access Agreement](#)

Initial Draft: 2/13/08

Effective Date: 10/1/08

[Information Security Office](#)

Email: [iso@u.arizona.edu](mailto:iso@u.arizona.edu)

(520) 621-UIISO(8476)

# Personal Information Sweep Checklist

- \_\_\_ STEP 1. LOCATE personal information
- \_\_\_ STEP 2. DELETE unneeded files
- \_\_\_ STEP 3. SECURE personal information
  - Transfer files with personal information to a CD, DVD or flash drive and physically secure them, OR
  - Separate the number from the associated name, OR
  - Truncate the number to the last four digits, OR
  - Replace all but the last four digits of the number with filler X's, OR
  - Encrypt personal information
- \_\_\_ STEP 4. INSTALL Cornell Spider
- \_\_\_ STEP 5. DELETE temporary files
- \_\_\_ STEP 6. RUN Cornell Spider
- \_\_\_ STEP 7. FIND the log file
- \_\_\_ STEP 8. DELETE or SECURE personal information
  - Transfer files with personal information to a CD, DVD or flash drive and physically secure them, OR
  - Separate the number from the associated name, OR
  - Truncate the number to the last four digits, OR
  - Replace all but the last four digits of the number with filler X's, OR
  - Encrypt personal information
- \_\_\_ STEP 9. COMPLY with applicable standards
- \_\_\_ STEP 10. REGISTER your computer
- \_\_\_ STEP 11. CERTIFY completion
- \_\_\_ STEP 12. SUBMIT the Certification

## University of Arizona Personal Information Sweep Certification

I certify that:

1. I understand that I am responsible for securing access to personal information (as defined in the Personal Information Sweep Procedure) under my control.
2. I have performed on the computer(s) identified below all steps of the Personal Information Sweep Procedure, to the extent applicable:
  - LOCATE personal information
  - DELETE unneeded files
  - SECURE personal information
  - INSTALL Cornell Spider
  - DELETE temporary files
  - RUN Cornell Spider
  - FIND the log file
  - DELETE or SECURE personal information
  - COMPLY with applicable standards
  - REGISTER your computer
  - CERTIFY completion
  - SUBMIT the Certification

NOTE: This statement is not satisfied by completion of procedures other than those found on the Information Security website at <http://www.security.arizona.edu/pi>.

Computer MAC Address	Building and Room Number of Computer Location
Computer MAC Address	Building and Room Number of Computer Location
Computer MAC Address	Building and Room Number of Computer Location

3. I have applied for exceptions where appropriate.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Unit Name

\_\_\_\_\_  
Date