

The Personal Information Sweep is designed to allow an individual to perform the process largely without assistance. There are, however, instances where technical support may be required or desirable. This guideline identifies those areas. Each area is presented by reference to the applicable step of the Personal Information Sweep.

Step 4: Software Installation for Windows Clients

For users without administrative privileges, IT staff will need to assist with installation of:

- .NET 1.1 or later, if not previously installed
- Cornell Spider

Group Policy or scripts can be used to install Cornell Spider and .Net framework software to clients. Information on using Group Policy is available at the Microsoft TechNet website:

Windows Server 2003:

<http://technet2.microsoft.com/WindowsServer/en/library/b7c2efc1-207e-4089-8490-0d002daf8b6c1033.mspx?mfr=true>

Windows Server 2008:

<http://technet2.microsoft.com/windowsserver2008/en/library/1b8827d7-a603-4158-acf1-87fde16f98f11033.mspx?mfr=true>

Step 8: Email

Cornell Spider identifies email messages in an Outlook mailbox as a single, large file, not as individual files for each message. It identifies Eudora and Thunderbird folders, not individual files for each message. Textpad can be used to search these large files. Textpad is available free of charge to University faculty, staff and students at the University Site License webpage <sitelicense.arizona.edu>.

The regular expressions for Textpad are:

- SSNs: `[0-9]\{3\}[-|][0-9]\{2\}[-|][0-9]\{4\}`
- Arizona Driver License: `[A|a|B|b|D|d|Y|y][0-9]\{8\}`
- Visa/MC/Discover: `[0-9]\{4\}[-|][0-9]\{4\}[-|][0-9]\{4\}[-|][0-9]\{4\}`
- American Express: `[0-9]\{4\}[-|][0-9]\{6\}[-|][0-9]\{5\}`

Step 8: False Positives

Cornell Spider may produce false positives, particularly in relation to numbers in email headers. It may identify them as Arizona driver's license numbers.

Step 8: Accessing Files

Some users will very likely ask for assistance in accessing files listed in the Spider log.

Step 8: Encryption

IT staff should coordinate several aspects of encryption:

- selection of encryption products
- key management
- backup of encrypted files

Step 9: Compliance with Applicable Security Standards

IT staff must ensure that any computer on which personal information will be stored meets the Minimum Security for Networked Devices Standard and the Server Security Standard, as applicable.

Related Guidance

Information Security Policy (IS-100)

Information Security Terms Guideline (IS-G100)

Personal Information Sweep Procedure (IS-P301)

Minimum Security for Networked Devices Standard (IS-S701)

Server Security Standard (IS-S702)

Revision History

Initial Draft	07/14/08
Effective Date	10/01/08