# Table of Contents

**INTRODUCTION**

**LOGGING IN TO YOUR DESKTOP**

- Desktop Login Overview
- Why is Desktop Security So Important?
- Novell Login
  - Novell Password Rules
- Windows Workstation Login
  - Changing Passwords
- What is Active Directory?

**AUXILIARY SERVICES CENTRAL SYSTEMS OVERVIEW**

- Novell Netware
  - Network Drives
- AS/400
  - AS/400 Password Rules
- JD Edwards
- Kronos
- CUFS Document Interface (CDI)
- CUFS Document Reconciliation
- Lotus Notes Mail & Calendaring
  - Lotus Notes Password Rules
  - Changing Your Lotus Notes Password
  - Email Attachment Etiquette
Removing Email Attachments.......................................................................................... 19

WHY IS SECURITY IMPORTANT?------------------------------------------------------------21
  Common Attack Types.................................................................................................. 21
  What Can I Do to Make my Computer Secure?.............................................................. 24
    Anti-Virus Software.................................................................................................. 24
    Protect Your System Access..................................................................................... 25
  What Is the Internet?..................................................................................................... 28
  How Do I Use The Internet Securely?........................................................................... 28
  What Are Cookies?....................................................................................................... 30
  How Do I Clear My Internet Cache, Internet History And Cookies?......................... 30

AUXILIARY SERVICES I.S. POLICIES--------------------------------------------------------33
Introduction

To carry out your job responsibilities as an employee of Auxiliary Services, you will need to access systems or use technology that resides on or is accessed through your computer desktop. All employees are required to use these resources in an effective, efficient, and responsible manner. The computer at your desk is the property of the University of Minnesota. A good rule of thumb for storing files on your work Computer is: *Don't store anything on your computer that you wouldn't be comfortable leaving face up on your desk.*

The purpose of this Training Guide is to:

- Provide users with a better understanding of the systems that are supported by Auxiliary Services I.S.
- Protect and better utilize information resources within Auxiliary Services.
- Raise awareness of U of M security policies and procedures.
- Help users understand the difference between departmental systems and central systems.

Auxiliary Services is the parent department of a diverse group of thirteen internal service, auxiliary service and central organizations.

Addressing & Mailing Services

Campus Mail

Concerts & Lectures

Fleet Services

Housing & Residential Life

Office Equipment Services

Parking & Transportation Services
Printing Services

U Card

University Bindery

University Bookstores

University Dining Services

University Stores
Logging In to Your Desktop

DESKTOP LOGIN OVERVIEW

Each time you login to your desktop there is a series of verifications that take place that check your identity and what network resources you have access to. This process is referred to as Authentication.

Yes, You are able to use this machine.....

Your home drive is H: on Server A
Make S: your shared drive on Server A
Make P: your projects drive on Server A
Synchronize time with the University Timeclock
Check and occasionally update/patch applications
Check and audit software and hardware configuration

Training Guide

Last Updated on 8/3/04
WHY IS DESKTOP SECURITY SO IMPORTANT?

The desktop is the primary entry point to the organizations information resources. Even if you do not have anything of value on your computer, once compromised, an attacker could use your computer to gain access to other things such as passwords to other computers or other personal information. The security of U of M data is everyone’s responsibility.

NOVELL LOGIN

You must log in to Novell each work day in order to access files and network applications.

1. In the Username field, type your University Internet ID.
2. In the Password field, type in your Novell password.

NOVELL PASSWORD RULES

- Password length cannot be less than 7 characters.
- Any alphanumeric character is allowed including spaces.
- Passwords cannot be the same as the previous 32 passwords (you can only re-use a password on the 33rd time).
• Because of Windows, Novell passwords are case sensitive (there is a difference between lower case and uppercase letters).

• Current recommendations from OIT suggest using a phrase instead of a password. Phrases are inherently complex and have capital letters and punctuation (for example, I Love Baseball! could be a pass phrase). Spaces are acceptable.

• You will be locked out after 3 unsuccessful login attempts. If you are locked out you will be automatically re-enabled after 30 minutes. Contact the Auxiliary Services Help Line @ 4-1442 or HDS Help Line (5-8001) if you need your password reset.

• Novell passwords expire after 60 days.

WINDOWS WORKSTATION LOGIN

Microsoft Windows 2000 or XP is the standard operating system within Auxiliary Services. Windows 2000/XP requires a User Name and Password. This identifies the user profile (list of rules and access rights). Typically, this will be synchronized with Novell. However, they can get out of synch. When you are prompted to change your Novell password you are also asked to synch your Novell and Windows password. The end result is a single login to the network and to the operating system. If you are prompted for a Windows password after signing in to Novell, contact the Auxiliary Services Help Line at 4-1442 or the HDS Help Line at 5-8001.

Refer to the Changing Passwords section for more information.
CHANGING PASSWORDS

Novell will prompt you after you login to change your password before it is set to expire. It is recommended that you change your password when you get this message.

1. Click Yes.

2. Type in your new password.

3. Retype your new password.

4. Click OK.

Your new Novell password will automatically synch to your Windows workstation password. If you have any problems changing your password, contact the Auxiliary Services Help Desk (4-1442) or HDS Help Desk (5-8001).
WHAT IS ACTIVE DIRECTORY?

Active Directory (AD) is part of Windows 2000. Active Directory lets organizations efficiently share and manage information about network resources and users. In addition, Active Directory acts as the central authority for network security, letting the operating system readily verify a user’s identity and control his or her access to network resources. Users are automatically joined to AD when they log in to Novell.
Auxiliary Services Central Systems Overview

Auxiliary Services I.S. supports the following core systems:

- Novell Netware (Connect to our servers)
- JD Edwards (Financial)
- Kronos (Timekeeping)
- CUFS Document Interface (CDI) (Financial)
- CUFS Document Reconciliation (Financial)
- Lotus Notes (E-mail and Calendaring)

NOVELL NETWARE

Novell Netware is networking software that is used for printing and file sharing. Files you work with are stored on shared network drives. Administrators in Auxiliary Services I.S manage our Novell network. All files on shared space are backed up nightly and the tapes are stored off site. Monthly server maintenance is performed on the 2nd Saturday of the month. E-Mail reminder notifications are sent out to all Novell users prior to each scheduled downtime.
**NETWORK DRIVES**

1. Click on **My Computer** to verify you are signed in to the network.

![My Computer Window]

- **FDD (A):** Floppy Disk
- **C:** Local Disk
- **GHOST:** Local Disk
- **Apps on Server (G):** Network Drive
- **Aux_fileshare (H):** Network Drive
- **Comm on Aux_server/Projects (P):** Network Drive
- **Aux administration/Aux_server/Shared (S):** Network Drive
- **Sys on Aux_server (V):** Network Drive
- **Compact Disc (C):** Compact Disc
- **Control Panel:** System Folder
<table>
<thead>
<tr>
<th>Drive Letter</th>
<th>Description</th>
<th>Backed Up Nightly?</th>
</tr>
</thead>
<tbody>
<tr>
<td>C Drive</td>
<td>This is the drive in the computer on your desktop. Do not store any files on the C:\ drive that you cannot afford to lose. Talk to your departmental technical support person if you have any questions about your default setups for where documents are stored (e.g. Word documents can default to be stored in My Documents which is located on the C drive).</td>
<td>No</td>
</tr>
<tr>
<td>H Drive</td>
<td>Your H:\ drive cannot be shared with other users. You should never store files critical to your department on your H: drive because other people in your department cannot access it. Your manager will determine what to do with any remaining files on your H: drive when you leave the department.</td>
<td>Yes</td>
</tr>
<tr>
<td>S Drive</td>
<td>This is a shared drive for your department. Typically, all department users have rights to this directory.</td>
<td>Yes</td>
</tr>
<tr>
<td>Drive Letter</td>
<td>Description</td>
<td>Backed Up Nightly?</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>P Drive</td>
<td>This is a shared drive for specific projects. All project team members would have rights to this directory. The Novell Administrator in Auxiliary Services assigns these rights.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
AS/400

The AS/400 processes both financial and departmental transactions. The AS/400 also hosts Lotus Notes and web based programs. Auxiliary Services has two AS/400’s.

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUX_400</td>
<td>Hosts Lotus Notes and web based programs.</td>
</tr>
<tr>
<td>SSO</td>
<td>Hosts JD Edwards and financial interfaces.</td>
</tr>
</tbody>
</table>

Users log in to the AS/400 to access the following applications:

JD Edwards
Kronos
CUFS Document Interface (CDI)
CUFS Document Reconciliation

AS/400 PASSWORD RULES

Password length can be between 8 and 10 characters.

The first character cannot be a number.

A number is required in all passwords.

Characters cannot be repeated consecutively.

The position of characters can be the same for each new password (e.g., Flower01 can be followed Flower02). However, this is not a secure password and this should not be done.
Passwords cannot be the same as the previous 32 (i.e. you can reuse a password on the 33rd time).

Passwords are not case sensitive (both lower and upper case letters can be used).

User profile is disabled after 5 consecutive failed sign-on attempts. Contact the Auxiliary Services I.S. Help Line @ 4-1442 or HDS Help Line @ 5-8001 to re-enable.

Login is disabled after 30 days with no activity. Contact the Auxiliary Services I.S. Help Line at 4-1442 or HDS Help Line @ 5-8001 to re-enable.

**JD Edwards**

Our departments use JD Edwards (JDE) for financials and for billing. JD Edwards is a fully integrated system. Information flows between one sub-system to another. When a transaction is entered in Accounts Receivable, a transaction will automatically be made in the General Ledger. JD Edwards refers to each group of its software programs as a system. For example, Accounts Receivable and Accounts Payable are separate systems. Typically several systems are used to achieve a comprehensive business solution. JD Edwards user group meetings are held on an as-needed basis. Following is a list of systems that Auxiliary Services is currently using:

- Address Book
- Accounts Receivable
- Accounts Payable
- General Ledger
- Fixed Assets
- Budget
- Sales Order

**Kronos**

Kronos is used for timekeeping and attendance. Kronos is also interfaced to PeopleSoft for payroll. An interface to JD Edwards is planned for the future.
CUFS DOCUMENT INTERFACE (CDI)

An interface is an electronic connection between two computer systems that replaces the need for paper documents. Our CUFS document interface (CDI) is used to electronically transmit CUFS documents to the CUFS Financial System. This interface allows more efficient entry of a large volume of documents into CUFS. Specific billing applications can also be programmed to feed CDI. Documents entered either manually or through an automated interface can be transferred to JDE to minimize the need for duplicate entry.

CUFS DOCUMENT RECONCILIATION

CUFS Document Reconciliation is used to reconcile JD Edwards to CUFS. A monthly download of transactions that have cleared CUFS in the accounting period is compared to the activity recorded in JD Edwards. The reconciliation is by
document, amount & reconciling unit (Area/Org or defined Area/Org combination). Matching and open item reports are run for each reconciling unit to facilitate data entry, identification of timing differences and to insure all activity is identified.

LOTUS NOTES MAIL & CALENDARING

Lotus Notes is the only e-mail and calendaring package that is supported by Auxiliary Services. Lotus Notes is a Groupware product for enterprise communications. Groupware allows you to share information with other people by putting the information you create in a centralized and shared location. Auxiliary Services I.S. offers Lotus Notes training classes for new and current users.

LOTUS NOTES PASSWORD RULES

Any alphanumeric character is allowed including spaces.

A password is required for Notes but you are not required to change it. Change your password if you believe it has been compromised.

Passwords are stored locally in your Notes ID file. This means it is not easily re-set by the Notes Administrator.

CHANGING YOUR LOTUS NOTES PASSWORD

Following are instructions for changing your Lotus Notes password if you believe it has been compromised.

1. Select the File Menu.

3. Type in your current password and click OK.

4. Click the Change Password button.
5. Type in your current password again and click **OK**.

6. Type in your new password twice and click **OK**.
EMAIL ATTACHMENT ETIQUETTE

Not only does email allow us to communicate with people all over the world, but it also lets us share documents via email attachments. Email attachments are files sent along with an email message. An attachment can be any kind of file at all; including formatted word-processed documents, spreadsheets, databases, graphics, and even software.

File attachments add to the time it takes for a mail message to open and also increases the amount of disk space the memo takes up. It is important to understand when and where to use attachments in email messages. Following are some “Do’s and Don’ts” for email attachments.

DO

Send an attachment if the recipient does not have access to our network and the file cannot easily be copied into the text of the email.

Copy the text of the attachment into the email if this can be done easily.

Reduce the size of your mail file by removing attachments from your messages. Refer to the Removing Email Attachments section of this document for more information.

DON’T

Send an attachment to a large mailing list. The email, including the attachment, is copied multiple times and if many of the recipients are hosted on the same mail server, the message can put a significant strain on the system.

Attach the file if the recipient can easily access that file on a network server.

Open or save an email attachment if you do not know the sender. Attachments can contain computer viruses.

Use your U of M email account to send out jokes, chain letters, etc.
**REMOVING EMAIL ATTACHMENTS**

You can reduce the size of your mail by removing attachments from your messages. The following table describes how to easily remove attachments from your mail.

<table>
<thead>
<tr>
<th>When you...</th>
<th>Do this....</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reply to a message</td>
<td>Click <strong>Reply/Reply to All</strong> and select <strong>Reply without Attachment(s)</strong>.</td>
</tr>
<tr>
<td>Forward a message</td>
<td>Click <strong>Forward</strong> and select <strong>Forward without Attachment(s)</strong></td>
</tr>
</tbody>
</table>

![Attachment Removal Table](image-url)
<table>
<thead>
<tr>
<th>When you...</th>
<th>Do this....</th>
</tr>
</thead>
</table>
| Remove large attachments from the All Document View | 1. Open the **All Documents** View  
2. Click the **Size** sorting triangle. This will sort your view by size of the document (the largest files should be at the top).  
3. Open the message that has an attachment you want to remove.  
4. Select the attachment and press the **Delete** key (or right-click on the attachment and select Delete).  
   ![Lotus Notes](lotus_notes.png)  
   **Lotus Notes**  
   This operation cannot be undone. Do you wish to proceed?  
   ![Yes No buttons](yes_no_buttons.png)  
   **Yes**  
   5. Click **Yes**.  
   6. Close the e-mail message.  
   7. Click **Save Only**.  
   The e-mail will be saved with the attachment name only. |

[attachment "Advanced Topics.doc" deleted by Diene KleinmenJunn]
Why is Security Important?

The security of financial data and systems is everyone’s responsibility. Colleges and universities continue to be prime targets for attacks because they have vast computer networks that tend to be more “open” because research and academic data are shared. It is critical that all users of University of Minnesota systems are aware of security policies, procedures and standards.

COMMON ATTACK TYPES

We live in the age of computer viruses. It is vitally important that you take precautions to prevent catching or spreading computer viruses. The consequences of attacks can range from the mildly inconvenient to the completely debilitating. Important data can be lost, privacy can be violated and your computer can even be used by an outside attacker to attack other computers.

In our enterprise mail system (Lotus Notes) all incoming and outgoing mail is scanned for known viruses, as are the servers and your desktop. When a new virus appears the scanning software is usually updated within a few hours or days.

You should still be very careful when opening attachments you may receive. If you are not expecting someone to send you a file, don’t open the attachment until you have confirmed that it is legitimate. You should always be very suspicious of any attachment that ends with .exe or .vbs. These are not documents (such as something made in Word or Excel) they are programs that are activated by opening them.

It is important that you report anything suspicious to your technical coordinator or the Auxiliary Services Help Line @ 4-1442 or HDS Help Line @ 5-8001.
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Service</td>
<td>This is the most frequent type of attack. These attacks prevent access to all or part of a computer system. This is usually achieved by sending large amounts of jumbled or other unmanageable data to a machine that is connected to the Internet, blocking legitimate traffic from getting through. Even more malicious is a Distributed Denial of Service attack which the attacker compromises multiple machines or hosts.</td>
</tr>
<tr>
<td>Virus</td>
<td>A Virus is a small computer program that hides itself in another program. You can have a virus on your computer without ever knowing about it. A computer can be infected with a virus from an outside source such as an e-mail attachment or a file downloaded from the internet. Although less common viruses can be passed between computers via removable media such as CD’s and floppy disks. At some time the virus will trigger, doing damage such as erasing your hard drive, sending mail to people in your address book, or corrupting files.</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Trojan Horse</td>
<td>A Trojan horse is similar to a virus except it is used to install a program that can grant access to your desktop. Trojans are often disguised as a game, a funny greeting card, or a useful utility. Trojans are most common in e-mail messages.</td>
</tr>
<tr>
<td>Worm</td>
<td>A worm is similar to a virus except that it exploits security bugs in Operating Systems or spreads itself to other systems frequently without user intervention. For instance, when an e-mail recipient clicks on an attachment the worm installs itself on their computer and then sends itself to everyone in that persons address book.</td>
</tr>
<tr>
<td>Targeted Attacks</td>
<td>These attacks are launched against a single computer or defined group of computers with the intent to gain access for a specific purpose such as stealing secure data (e.g., credit cards).</td>
</tr>
</tbody>
</table>
WHAT CAN I DO TO MAKE MY COMPUTER SECURE?

It is critical that you do everything that you can to secure your computer. You should ensure your virus protection software is updating properly in order to protect your computer from viruses and also take steps to guard your system access. Passwords are the key to many systems and applications. Your password helps to prove who you are and protects the data that you have access to.

ANTI-VIRUS SOFTWARE

Our desktop virus software automatically updates new virus definitions once a week (at a minimum). If the Symantec AntiVirus icon (yellow shield in the lower right hand corner of your desktop) has an exclamation point then your virus protection software may not be updating virus definitions properly. Click on the shield and check the date. If the virus update is more than one week old, contact the Auxiliary Services I.S. Help Desk @ 4-1442 or the HRL Help Desk @ 5-8001.
PROTECT YOUR SYSTEM ACCESS

Log off completely at the end of the day.

Log-out if you are leaving your desk for more than a few minutes (e.g., lunch, meetings, etc.).

Lock your screen by pressing Ctrl/Alt/Delete/Enter. This will resume your session where you left it.

Use a password protected screen saver. This will automatically lock your workstation after 5-15 minutes of inactivity. You will need to reenter your password for access.

Do not share your password with anyone under any circumstances.

Keep password lists in a locked location, not taped on your computer.

Make sure that only technical personnel in your department or Auxiliary Services I.S do any technical work on your desktop.

Make sure your desktop is physically secured if it is located in a public place (e.g., locked to the desk). You may also consider disabling the floppy/cd drives in Bios and applying a Bios password to prevent someone from booting your computer from removable media and altering/accessing the computer files.

Call the Auxiliary Services I.S. Help Line @ 4-1442 or HDS Help Line @ 5-8001 if you believe your password has been compromised.
OIT SYSTEMS AND SECURITY GUIDELINES FOR CHOOSING A PASSWORD

Passwords are the key to many systems and applications. Your password helps to prove who you are, and to ensure your privacy and help protect the privacy of data you may have access to.

Compromised passwords are one of the means by which unauthorized people gain access to a system. Someone logging on under your name has access not only to your computer files, but also can get access to your co-workers files through your file server, and can impersonate you to send malicious e-mail.

Many times you are requested to choose and maintain a password for various purposes (e.g., sign on to a file server, access your e-mail, use a password protected screen saver). At the University of Minnesota, there are two widely used passwords, the Internet and Enterprise. These passwords allow access to important central (e.g., central e-mail, WebCT, Tech Mart, some department web pages) or Enterprise systems (e.g., PeopleSoft, Financial FormsNirvana, Electronic Grants Management System, Enterprise Document Management System) at the University.

It's important to choose a good password and protect it, since there are many password-cracking programs readily available on the Internet and passwords are the key to access many computer systems or applications. Each system or application may have different password restrictions or requirements.

General Guidelines for Choosing a Password

Current recommendations from OIT suggest using a phrase instead of a password. Phrases are inherently complex and have capital letters and punctuation (for example, I Love Baseball! could be a pass phrase). Spaces are acceptable.

Do Choose...

Something obscure. For instance, you might deliberately misspell a term or use an odd character in an otherwise familiar term (e.g., pHnEbon). Or use a combination of two
unrelated words and a combination of letters and numbers (e.g., MutT37Yu)

A combination of letters and numbers, or a phrase like "many colors" and then use only the consonants, "mnYc0l0Rz".

The first letter from each word or phrase (e.g., TaYrrTooT, represents a line in the song "Tie a Yellow Ribbon Round That Old Oak Tree")

To alternate between one consonant and one or two vowels, to create nonsense word. This provides nonsense words that are usually pronounceable, and thus, easily remembered. (e.g., rouTBoo or QuaDPop).

A combination of letters, numbers and special characters in a word (wR1t#rS, represents writers)

(Note: U of M Internet & Enterprise passwords must be 6-8 characters, with a mix of numbers and letters. See Internet and Enterprise Passwords for more information.)

**Other Tips**

Use a MINIMUM of 7 or more characters (system permitting).

Use mixed case wherever possible. Use uppercase on more than the first letter.

Include at least two digits or special characters (#, >, $).

The idea is to make it harder for the automated password cracking programs to figure out the password.

**These examples should NOT be used as they are now published widely!**

**Don’t Choose…**

Simple words that are easy to remember, such as common or famous names of people or places.

Words that can be easily associated with you, such as your birth date, your name, spouse or child’s name, pet’s name, street.
Hello, password, welcome, etc.

Common words from English, foreign language or technical dictionaries

Keyboard patterns (e.g., qwerty) or duplicate characters (e.g., aabbccdd).

A new password by simply changing one character in your existing password. (E.g., Kathy5)

The same password on important and trivial systems (e.g., production and test systems).

**WHAT IS THE INTERNET?**

The Internet began in the 1960’s as a computer network for the U.S. military. The Internet has now grown into a global communication tool of many thousands of computer networks that can exchange information with each other. To accomplish this all the computers on the Internet have to use a common set of rules for communication. Those rules are called protocols, and the Internet uses a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol). Many people equate the World Wide Web with the Internet. In fact, the Internet is like the highway, and the World Wide Web is like a truck that uses that highway to get from place to place.

All web browsers have their own mail clients. Only Lotus Notes is supported by Auxiliary Services I.S. A typical desktop should not have any other mail clients running besides Lotus Notes.

**HOW DO I USE THE INTERNET SECURELY?**

Don't believe everything you read. Be skeptical. Check it out before acting on any information. Treat web sites and every new person you encounter on the Internet as a stranger. Just because a product or service is presented on a professional-looking web site doesn't necessarily mean the claims are true.
If you use the Internet to access an application, clear your cache between using applications and before logging off your system.

Disconnect your computer from the Internet when you are no longer using it. This will lessen the chance that someone will be able to use your computer. Close all web browsers when you are done.

When using any computer (your U of M desktop, kiosk or public lab), completely log out and quit the application before you leave.

Do not download attachments from any personal web based mail accounts to your U of M desktop. This is because of the risk of viruses from mail that is not scanned by our virus protection software.

Don’t download any software unless authorized by I.S. staff.

**WHAT IS A WEB BROWSER?**

A Web Browser is a program that allows you to view web pages. Always use the most recent browser version unless told by technical staff not to.

- Microsoft Internet Explorer (6.0.2 or above)
- Netscape (7.1 or above)
- Mozilla (1.4)

No other browsers are supported

Talk to your Technical Coordinator if none of these browsers meet your requirements.
**WHAT ARE COOKIES?**

A Cookie is a coded piece of information that is stored on a user's computer by a Web site so preferences are remembered on future requests. Cookies are passed from a Web server through a Web browser to the user's hard drive. This information is essential for many of the features taken for granted on the Web, such as shopping carts and personalized portals.

Privacy advocates have raised concerns over the role of cookies in online advertisements. They fear that large companies could piece together information that could be used against individuals, especially if offline information is merged with online information.

Cookies are not universally used. Estimates vary, but some percentage of the Web population browses with cookies turned off. Cookies can be blocked completely via the browser, or selectively via a cookie manager.

**HOW DO I CLEAR MY INTERNET CACHE, INTERNET HISTORY AND COOKIES?**

Go to [www.umn.edu/oit/security/](http://www.umn.edu/oit/security/) site and show guidelines

Following are instructions for clearing temporary Internet files (Cache), History and Cookies using the Internet Explorer. If you use a different browser (i.e., Netscape) the process will be different.

1. Open Internet Explorer.
2. Select the **Tools** Menu and select **Internet Options**.

3. Click the **Delete Cookies** button to delete any cookies that have been stored on your hard drive.

4. Click the **Delete Files** button to clear any temporary Internet files (cache).
5. Select Delete all offline content and click OK.

6. Click the **Clear History** button to clear the history of the web sites you have accessed.

7. Click **Yes** to delete history of visited web sites.

8. Click **OK** to return to Internet Explorer.
Auxiliary Services I.S. Policies

All Auxiliary Services I.S. policies are available at
www.auxs.umn.edu

Acceptable Use of Technology Policy

Hardware Disposal Policy

Technology Use Employee Separation Policy (in development)