

# **Security Policy**

## **System Access Control, Data Protection and Recovery**

This document describes the security policy for system access control, data protection and recovery in the for the Controller's Office and Treasury Services at Miami University. The security policy sets forth guidelines to prevent unauthorized access to University systems and data, and loss or compromise of data through mishap, mischief or mayhem. The goal of this policy is to educate employees and encourage acceptance and adherence to these guidelines.

Each category (system access control, data protection and data recovery) can be divided into two subcategories. System access control is comprised of physical access to systems through hands-on interaction, and logical access to systems through logins and passwords. Data protection refers to maintaining data in first tier electronic storage (i.e. hard drives of personal computers (PC) and local area network (LAN) servers) and virus protection. Data recovery refers to the disposal of unneeded data and recovery of data from catastrophic loss such as accidental deletion, file corruption or hardware failure.

### **System Access Control**

1. Physical Access: Although this may seem like the most obvious area to secure, it is by far the most exploited. Physical access is the ability of an unauthorized intruder to physically access a computer. A person can do this in one of two ways without criminal trespass (i.e. breaking and entering). They can either walk up to an unattended system or open an unlocked door and access an unattended system.

#### Security Measures:

- a. *Use the "lock workstation" feature of Windows 2000/Novell.* Anytime, you anticipate leaving your desk for an extended period, press the control, alt and delete key simultaneously and select the Lock Workstation option. Your computer will be locked until you enter your password. The drawback with this method is you have to consciously lock your workstation.
- b. *Use the password protect feature of your screen saver.* Access Start/Settings/Control Panel/Display/Screen Saver. Place a checkmark in the Password Protect box, set the time interval and click OK. Windows 2000/Novell will automatically lock your workstation when you have not pressed a key in the defined time interval. The drawback with this method is setting a time interval that works for you.
- c. *Be alert to anyone you don't know trying to access a computer in your area.* Ask them what they are doing or report the activity to a supervisor immediately.

Summary: While physical access is the most common security breach, it is also the most preventable. *This policy recommends using option b above and setting the time interval to 15 minutes.* If you choose to use option a, it is recommended that you lock your workstation anytime you will be out of sight of it for more than 10 minutes.

# Security Policy

## System Access Control, Data Protection and Recovery

2. Logical Access and Passwords: Logical access is logging onto a PC, LAN or specific software package with a user id and password. Your uniqueid and associated password provide access to PO (email), Novell (MU network), myMiami, MInE, BannerWeb and Oracle (Toad). Separate IDs and passwords of your choice are used for regular Banner, LISTSERV, UNIXGen and MeetingMaker. In some cases, the ID may be the same as your uniqueid, but your password is not linked to your uniqueid password.

### Security Measures:

- a. Change your password regularly. Although MCIS sets no formal time interval for password change, industry standard is typically 90 days. However, there is a trade-off between frequency of change and effort to maintain. *This policy recommends changing your password every six months, in January and July.* These months are the beginning of the calendar and fiscal years and should be easy to remember.
- b. Select your password carefully.
  - use *six to eight digits in a random combination of numbers and letters* (include both)
  - make it easy to remember and difficult to guess with no words from the dictionary
  - commit it to memory and *do not write it down*
  - *do not inform anyone* of your password (with the exception of your supervisor in case of extended absence)
  - *use a different password than you use for any non-Miami system* (don't kill two birds with one stone!)
- c. *Make all your primary Miami system passwords the same.* It is significantly more secure to have separate passwords for all systems. When all passwords are the same, if one is compromised, all the systems you access are compromised. However, when you are required to juggle four or more passwords, there is a greater probability that you will forget a password or record them to remember. This also creates security risks. So to aid you, this is the policy. When used, it must be balanced with a high sense of security for your one password.

Summary: Passwords are the keys that unlock system security. Over time, they become duplicated through communication and observation so they need to be refreshed at regular intervals. *This policy recommends changing your password twice a year, in January and July; using the same password for all Miami systems; not using your Miami password for any outside systems; and following the above recommendations for selecting a password.*

### **NOTES:**

1. To ensure password changes are effectively propagated, MUnet/NDS passwords should only be changed at <http://www.miami.muohio.edu/passwordchange>. This common password will be in effect for Novell network logins, Eudora, MInE and a host of other systems. Banner passwords must be changed within Banner.
2. If you forget your MUnet/NDS password, you are required to take a picture ID to MCIS to have it reset.
3. At some point, MCIS may set more stringent standards for changing passwords. We will be required to follow those standards.

# Security Policy

## System Access Control, Data Protection and Recovery

### Data Protection

1. Data Maintenance: Each day, nearly every computer user is creating data in some form. Every file you create (Word document, Excel spreadsheet, email message, data query and etc.) is a data object. Each of these objects has the potential to contain data that is critical to your individual work, departmental and/or university-wide activity. It is an individual responsibility to store data such that; it can be located on demand, the correct version can be identified, it is protected against viruses and backed up on a regular basis.

#### Security Measures:

- a. Create a logical storage structure. The Windows 2000 “My Documents” directory (C:\Documents and Settings\...) is difficult to access. *Create your own subdirectory structure off of the root (C:\). Name it “mydocs” or “data”.* Create whatever subdirectory structure you require below this to store your data. Maintain all data objects you create in this directory structure. *Point your Office applications to this directory as their default data directory.*
- b. Determine the proper location for files and directories. *Any file or directory that has departmental or broader impact should be stored on the departmental server (G drive).*
- c. *Establish adequate versioning methods for each critical file/subdirectory you have.* If you require versions of files or if you store a “production” copy on the server and make modifications at your local PC, *develop a plan for versioning.*

*The library method works well.* The production copy is stored on the server. When changes are required, create (check out) a copy of the server file to your workstation. Make the required modifications on your PC. Copy (check in) it back to the server when complete. Remove the working copy from the PC. Before copying the updated version back to the server, ensure no one else has made changes while you had the file “checked out”.

- d. *Establish clear ownership for shared server directories.* The owner will have responsibility for maintaining, updating and deleting files.

Summary: Data maintenance is critical to data and system security. If data is not owned and maintained adequately it is vulnerable to accidents, loss and integrity issues. Create a storage structure that is easy to access and logical in naming convention. Store all data files in this directory structure. Files with departmental and higher applicability should be stored on the departmental server and an appropriate versioning methodology should be instituted. Server based files and directories should have one clearly defined owner who is responsible for them.

## Security Policy

### System Access Control, Data Protection and Recovery

2. Virus Protection: Both malicious and mischievous viruses are being created daily by computer hackers. The most common entry point for viruses is through email and specifically email attachments. When you click on or open a file (or attachment) containing a virus, that action allows the virus program to execute and begin its activity. Miami University deploys virus protection software on PCs and email servers to identify virus carrying data objects (files) and to remove or cleanse the virus before it can be opened. While very effective, these methods are not foolproof.

#### Security Measures:

- a. Ensure PC virus protection software is in place and operational. McAfee virus software is installed on each PC at Miami. It should be operational at all times. *In the lower right icon tray, there should always be a shield with a "V" in the middle.* This is the McAfee logo. Each day, your computer is scheduled for two virus events; update from McAfee and virus scan. Both events take place during the night. *You should check the results weekly by clicking Start/Programs/Network Associates/VirusScan Console.* There will be five items listed. The last run column for "Auto Update" and "Scan Drive C" should have today or yesterday's date and the next time column should have today or tomorrow's date.
- b. Use common sense when opening unidentified email messages and attachments. While Miami's email server virus scrubbers are effective and reducing viruses significantly, there is always the possibility that a new virus will get through before the scrubbers have the appropriate solution. *Therefore, you must be alert regarding your email. Remember that email containing viruses can come from people you know (friends and family). Viruses come in attachments to email.* Once opened, the virus will usually attempt to look in your local address book and resend itself to everyone in that book while simultaneously wrecking havoc on your PC. *Do not open any email attachment unless you are absolutely certain of its contents. Call the sender if you need to verify it.*

Summary: Virus protection is a key element of system security. Among computing issues, viruses cause the greatest amount of lost time and money for businesses. With effective software, regular updates and scans and appropriately cautious employees, viruses can be controlled and virtually eliminated. *Weekly, verify that your desktop virus protection software is operating correctly. Use appropriate caution when handling suspicious email. Do not open any email attachment unless you are absolutely certain of its contents. Call the sender if you need to verify it.*

# Security Policy

## System Access Control, Data Protection and Recovery

### Data Recovery

1. Data Removal: Just as it is important to maintain your data in a logical manner. It is equally important to remove your data systematically. With the large amount of data that is created daily, it is easy for containers (folders and directories) to become cluttered and confusing, and data objects (files) lost or forgotten. When this happens, the likelihood of losing valuable data while organizing or deleting files and folders increases.

#### Security Measures:

- a. *Clean out (purge) your containers, folders and files on a regular schedule. Fall and spring cleaning days are logical times to do this.*
- b. *Delete unneeded data files and folders in a methodical manner, not casually or rushed.*
- c. *Maintain (purge as needed) all data on the departmental server that you create and/or own.*

Summary: The first step to recovering lost data is to prevent it from becoming lost. Store data in a logical data structure; maintain your data weekly and purge unneeded data; delete files carefully; and maintain all data for which you have responsibility.

2. Data Recovery: If a file is inadvertently deleted or lost to a hardware failure, network outage or file corruption, there must be a way to recover the data to a previous point in time. Our method for doing this is through tape backup and restore. Both servers and desktop systems are backed up nightly with ADSM storage manager.

Our server, admserver2, is on a five-cycle backup with a 400 day deleted file save. That means ADSM stores the five most recent changes to each file. Changes beyond that are lost as the space is recycled. Deleted files are saved for 400 days and then purged. Our desktop systems are on a two-cycle backup with a 60 day deleted file save. That means ADSM stores the two most recent changes to each file. Changes beyond that are lost as the space is recycled. Deleted files are saved for 60 days and then purged.

#### Security Measures:

- a. Store your data in a logical, easy-to-remember directory structure.
- b. Ensure the Tivoli Storage Manager Scheduler is in your minimized tray at the bottom of your Windows desktop.
- c. *Verify your backup on a regular basis (monthly) by retrieving a file or directory.*
  - 1) *One time only - Create a folder on your C: drive to do your test restore.*
    - a) Double click "My Computer" icon on your desktop.
    - b) Double click "Local Disk C:".
    - c) Single click your right mouse button (left button for left-handed mouse setup).
    - d) Select "New".
    - e) Select "Folder".
    - f) Name the new folder "RestoreTest" (without quotes).

## Security Policy

### System Access Control, Data Protection and Recovery

- 2) *Monthly – perform a test restore from ADSM to your RestoreTest directory.*
- a) Double click “TSM Backup Client” icon on your desktop.
  - b) Single click “Restore” button.
  - c) Single click the “+” box beside “File Level”.
  - d) Single click the “+” box beside your current C: drive name. There will usually be only one selection. If there are two, after you single click, you should be able to find the directory “RestoreTest”. Also, continue to single click and check your “mydocs” or “data” subdirectory for current data. If you are still unsure, contact your TSR.
  - e) Single click the “+” beside your “mydocs” or “data” subdirectory.
  - f) Continue to traverse your subdirectories by single clicking the “+” sign. When you reach the lowest level subdirectory, there will not be a “+” sign beside it. At this point, single click on the directory name and a list of files in the directory will appear on the right side of the window.
  - g) Select (single click) the file you want to restore for the test.
  - h) In the icon tray near the top of the screen above the “Restore” heading, select (single click) the yellow box with a red checkmark inside it.
  - i) You should now see a yellow box with a red checkmark inside it beside the file you selected. If you do not, try this again from the beginning or contact your TSR.

**NOTE: Use caution and follow the instructions in steps j) through m) exactly. Errors can result in overwriting a newer file on the local hard drive (C:) with an older backup version.**

- j) Click the “Restore” gray button on the upper left of the ADSM window.
- k) In the “Restore to” box, click “Following Location”.
- l) In the “Select destination directory” input box, type your restore path – “C:\RestoreText” (without quotes).
- m) Click the “Do not preserve directory structure” button also in the “Select Destination Directory” box.
- n) Click the gray “Restore” button in the lower left corner of the ADSM window.
- o) You will see a “Task List” box with “Preparing ...” in the bottom center of the window. This will remain for one to three minutes depending on server and network activity.
- p) Once it is completed, you will see a “Detailed Restore Status” box with a message that the restore is completed. Click “OK” in the message box. If you get any other message, contact your TSR.
- q) Close the ADSM window.
- r) Open the document you restored with the appropriate application (Word, Excel, etc.) and verify its content. After verifying the content, delete your restored document to avoid confusion.

## **Security Policy**

### **System Access Control, Data Protection and Recovery**

Summary: Data recovery is the glue for data protection. It includes not only recovery of lost data, but systematic purging of unneeded data. Data should be evaluated and purged on a regular basis (monthly). Store your data in meaningful directory structures and use logical versioning schemes to identify production versions of data files. Clean as you go by deleting temporary and unneeded files when you are finished with them.

The ADSM storage manager is an effective tool for backing up both desktop and server data. It is your responsibility to test and verify the accuracy of your desktop backup. This should be done monthly with a random, but important, file. Follow the instructions carefully so you do not accidentally overwrite newer data.