

# 2008

Morgan State University

## [POLICY]

[Type the abstract of the document here. The abstract is typically a short summary of the contents of the document.  
Type the abstract of the document here. The abstract is typically a short summary of the contents of the document.]

# **Desktop, Laptop & Portable Devices Security Policy**

**Effective Date:** June 30, 2008.

## **Policy Statement**

Morgan State University requires that all individuals utilizing University Electronic Information Resources abide by the desktop and laptop security standards described by this policy.

## **Reason for the Policy**

With the prevalent use of personal computing in the University, there is the risk that if computing system security vulnerabilities are left unsecured, then the information and data stored in personal computers are susceptible to theft and/or exploitation. This policy defines a number of safe computing standards to provide data protection on desktops and laptops.

## **Primary Guidance to Which This Policy Responds**

This policy is established under the provisions of Morgan State University's Information Systems Security and Policy Program.

## **Responsible University Office & Officer**

Morgan State University office of Information & Related Systems Security is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Chief Information Security Officer (CISO) is the responsible officer.

## **Revision History**

This policy was established in June 2008.

## **Who is Governed by This Policy**

This policy applies to all individuals who access, use, or control University Electronic Information Resources. The individuals required to adhere to this policy include, but are not limited to faculty, staff, students, those working on behalf of the University, guests, tenants, contractors, consultants, visitors and/or individuals authorized by affiliated institutions and organizations.

## **Who Should Know This Policy**

Anyone who accesses, uses, or controls University Electronic Information Resources should be familiar with this policy.

# Exclusions & Special Situations

None

## Policy Text

Computing technology is constantly evolving and new vulnerabilities are discovered everyday; therefore, no system is completely immune to exploitation. Applying layered security controls will better protect University computers from unauthorized and malicious access. This policy outlines Morgan State University's multi-layer security strategy for defense against unauthorized access to University desktops, laptops and portable devices data and information.

The following steps must be adhered to by the User and/or the System Administrator (SA) indicated in parenthesis following each of the items below. We will use system to refer to desktops, laptops or any portable electronic device.

1. **Implement** credible and reputable anti-virus software on your systems. Perform continuous and/or scheduled scanning, and keep anti-virus software up-to-date. An anti-virus program will protect your computer from malicious programs. (User and SA)
2. **Implement** anti-spyware software to protect private information on your system. Spyware is a class of software designed to steal personal information. (User and SA)
3. **Enable** the built-in firewall that is included in all major operating systems, and/or install a third-party firewall application. A firewall application help restrict others from connecting to your computer. (User and SA)
4. **Check** regularly for vendor security updates and apply them. When possible turn on automatic updates. Periodically, security vulnerabilities in the operating system and/or application are discovered and software vendors typically will then provide security updates to remediate such security exposures. (Users and SA)
5. **Use** strong passwords for all devices in compliance with University password policies. A password is used to provide authentication to an application and/or system. (User and SA)
6. **Log-out** from a website session once you complete your online transactions. Also log out from desktops, laptops and other applicable devices when you are not at your desk or using the device. Where applicable, utilize a password protected screen saver on all devices when they are temporarily not in use. (User and SA)
7. **Keep** your machine, especially laptops and portable devices, physically secured. (User and SA)
8. **Safeguard** all confidential and sensitive data and or information. Take appropriate measures; including disk encryption for electronic data or information, physically secure physical media; to prevent unauthorized disclosure. (User and SA)
9. **Scan** all email attachments, using anti-virus software, before opening them. Email is a method to spread malicious program via email attachments. (User)
10. **Refrain** from using the save password feature applications to avoid inadvertent access to your data by others who may have physical access to your computer. (User)
11. **Disable** accounts, which are no longer in use and always change default passwords. Some Operating Systems and applications

*come with predefined user accounts. These accounts could be active by default. (SA)*

12. **Disable** services that are not needed. Operating systems are packaged with services that are used by specific applications, such as *ftp* (for file transfer) or *SMTP* (for email). (SA)
13. **Backup** your data and files regularly. Computers are like any machinery and can fail, and may result in the data and files that are corrupted or unrecoverable. (User and SA)
14. **Be aware** and alert of information stealing methods such as: social engineering, phishing scams, and shoulder surfing to obtain personal and sensitive information about you. (User).
15. **Notify** the University Office of Information security as soon as you discover the loss of a computer or related system or devices, and or as soon as you suspect a potential data breach as a result of unauthorized access to your data or computer system. (User and SA)
16. **Sanitize** your computer before donating or disposal. (User and SA)

Examples to assist with interpretation and administration of this policy are provided in the *Appendix A “Examples of Desktop and Laptop standards and guidelines”* at the end of this document.

## Responsibilities

Implementing these security standards and guidelines provide you with added protection from malicious programs and unauthorized access. Failure to implement these security controls may result in your machine being infected or in the loss of critical and or sensitive data. If your computer is connected to Morgan State University's network and if it is infected, Morgan State University will immediately prohibit your connection until your machine has been sanitized.

## Definitions

- *Data* is a stored collection of information that may include alphanumerics, words, sounds, symbols, or images.
- *Electronic Information Resources* include data, networks, computers, and other devices that store or display data, communications devices, and software used on such devices.

## Contacts

For questions or comments:

Morgan State University  
Office of the V.P for Planning & I.T.  
Email: [security@morgan.edu](mailto:security@morgan.edu)  
Telephone: 443-885-3372

## References

Morgan State University Information Security policies, standards, guidelines and procedure. Draft version 0.7.5.1

Maryland DBM OIT IT. Security Policy & Standard. Version 1.5, January 2007.

## Examples of Desktop and Laptop standards and guidelines

### 1. *Implement anti-virus software*

An anti-virus program is necessary to protect your computer from malicious programs, such as: virus, trojan, worm, etc. Implement credible and reputable anti-virus software and keep it up-to-date.

Note that an anti-virus application cannot stop viruses that it does not know about. Therefore, it is very important to keep the definition database up-to-date by configuring automatic update of the definition list daily; but be sure not to set it to a time when the machine will be turned off.

Enable the real-time protection functionality and perform regularly scheduled full system scans because these features will identify, stop, and quarantine a virus as it attempts to execute.

### 2. *Implement anti-spyware*

Malicious software created with the intention of financial gain (e.g., with the creator being paid for every advertisement he can pop up on your desktop, going to market with your private information, or even assuming your identity to make purchases, etc.) is referred to as spyware.

Spyware is often installed on your machine via tagging along with a game or application that you want to use, or it can be installed by certain network worms. Once it is in your computer, it then begins collecting information about you and your activity, and then it sends the information to someone else.

Install an anti-spyware program, and keep the definition database up-to-date via configuring automatic update of the definition list daily; but be sure not to set it to a time when the machine will be turned off.

### 3. *Enable the built-in firewall and/or use a third party firewall program*

A firewall program is an application that limits the types of connections that the rest of the world can make to your machine. Major operating systems have a built-in firewall that is simple to implement and does not interfere with your normal use.

If you are connected to a network or the internet, install a firewall application, some are available for free, which will offer you more robust protection than the operating system's built-in firewall.

### 4. *Check for and apply vendor security updates for your operating system and applications*

Operating systems are made up of numerous components with different functions and some of these components are vulnerable to exploits. Hackers are continually probing and testing for vulnerabilities in all the major computer operating systems and are generally pretty adept at finding them. When this happens, the

company that markets and distributes the operating system rushes to develop a patch to fix the problem and makes it available at no charge to users of the operating system. The problem is many users rarely check for availability of patches and system upgrades and apply them. Major operating system vendors offer mechanisms that will allow you to regularly check for updates and apply them relatively easy.

A service pack is a collection of the critical updates and often includes major updates to the operating system. Some updates cannot be loaded until the latest service pack is installed. Periodically ensure that you are on the current service pack.

Likewise, there's often a security aspect to individual software applications (word processing, spreadsheet, database, etc.) as well. When application updates are available, implement the security updates.

#### *5. Use strong password and protect your password*

The key for complete access to your computer is your password. There are countless programs that attempt to determine passwords, both by guessing common ones and by randomly generating possibilities and trying them all, or a combination of the two.

The best defense is a strong password. This makes the password nearly impossible to guess in a reasonable amount of time.

Change your password if you think it has been compromised.

Don't share your password with anyone, and don't write it down. If you must write down passwords, keep the information secured and do not write down the corresponding ID.

For more information on passwords visit <http://msusac.morgan.edu/?p=7>

#### *6. Logout of finished sessions and lock computer when left unattended*

All major operating systems provide the ability to "lock" and password-protect the screen and system so that an unauthorized person with physical access cannot tamper with your computer. Every time you leave your computer, logout the session if you no longer need access to the system and/or enable password-protected screensaver to lock your computer.

#### *7. Physically secure your machine*

Never assume any location is completely secured, even if the location is restricted via swipe-access or locked door. There is almost always a way for someone to get to a restricted area.

Never leave an unsecured laptop computer unattended.

#### *8. Protect confidential and sensitive information*

Use encryption software to protect confidential and sensitive information/data stored in your computer.

Never send confidential and/or sensitive information via email. If you must send such information via email, encrypt the information before sending it.

USB thumb drives and external hard drives are commonly used to store information and data because of their portability factor. Also note that other mobile devices (e.g., memory cards, iPods, multimedia players, PDAs, etc.) have the capability to store data as well. If you use portable devices to store confidential and sensitive data, keep them physically secured and encrypt the confidential and sensitive information and data on them for protection against unauthorized disclosure, as well as, in the event of theft or loss of the device.

#### *9. Scan email attachments before opening them*

An effective method by which viruses, trojans, worms and backdoor programs are propagated is via e-mail attachments. If you receive an attachment that you weren't expecting or from someone you don't know, chances are that the attachment carries some variety of malware (malicious software) just waiting for you to set it loose by opening it.

When you get an email attachment, unless you feel very confident about what it is, where it came from, and why it was sent to you - **DON'T OPEN IT!**

Take precautionary measures and scan all email attached files with your anti-virus software even from people you know because their machine could have been compromised and used to propagate the spread of malware.

Be cautious about clicking on links sent to you in email - it is very easy to create a link that hides the true location of where the link goes. You should always either cut or paste the link into your browser, or manually retype it.

#### *10. Refrain from using the save password features for sensitive applications*

Various programs (e.g., email programs, web browsers, etc.) can be configured to save user name and password information. This can be convenient for you, but if you share your computer with others, they will also have access to your accounts. Additionally, if your computer is lost or stolen, then the saved account passwords are now compromised.

#### *11. Disable unused accounts*

Some operating systems have predefined user accounts (e.g., 'Guest' account, etc) that are well known and commonly exploited because the user doesn't always change their default settings, including the default password. To protect your computer, the unused accounts must be disabled and/or deleted to prevent anyone from using them to login to your computer. If you need to keep a default account, ALWAYS change the default password.

#### *12. Disable all unused services*

All major operating systems come packaged with all sorts of application and server software. These services include: ftp, telnet, SQL, SMTP (e-mail server), Apache (web server) and others. Vendors often turn these

services on by default and frequently give you very little explanation about what they do and little flexibility with regard to configuration settings. In general, the more services you have running on your computer, the more potential targets you have for hackers to exploit, not to mention slowing down your computer running things you don't need.

When considering what services should be running on your system, here's a simple rule of thumb:

- If you don't know what it is or what it does, *don't turn it on*. In most every case, if you find out later that you need it, you can go back and turn it on.
- If it's on, and you don't need it, *turn it off*.
- If it's off, and you don't need it, *don't turn it on*.

### 13. Create regular backups

There is the potential that files may be lost or corrupted due to hardware and/or software failures, and/or human errors (e.g., unintentionally deleting the file), and having another copy of your files prior to such catastrophe will alleviate the burden of recreating the lost or corrupted files to their original form.

There are numerous software solutions that will back up everything on your machine.

An effective and low cost backup alternative is simply copying the files/data on a CD and keeping it in a safe and secured location.

Perform regularly scheduled (e.g., daily and/or weekly) backup of your files/data. The backup frequency should be based on the importance of the data and the frequency of change to the data. If you use backup software, the software will typically provide you with the option to schedule the backup on a regular basis. Alternatively, if you manually create backups to CDs, perform the task on a regular cycle.


If your backups contain confidential and/or sensitive files/data, ensure that you have provided the same level of security protection (e.g., encryption) as you would for the original files/data.

### 14. Be alert and aware of information stealing techniques

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential and sensitive information, such as password, social security number, etc.

A technique in phishing scams is using either email or regular mail to obtain personal and sensitive information from you. For example, a common phishing scam is an email informing you as the winner of a 'lottery' but to collect you must supply them your banking information to initiate the transfer of funds. Another recent phishing scam is an official looking email from your bank or financial agency stating there is a problem with your account and telling you to verify your credentials via a weblink in the email or your account will be deactivated. If you click on the weblink, the website may appear to look official, some sites even forged the company's logo to make it appear legitimate, but the site is setup to steal your personal and sensitive information. If you receive emails from your bank or financial agency, always verify with the agency by contacting them directly (e.g., calling customer service) and explain to them the situation and that you would like to verify its authenticity.

Especially when using your computer in open or public areas, be alert to shoulder surfers, – people who look over your shoulder while you type in your user name and password or other sensitive information.



*16. Sanitize your computer before donating and/or disposal*

Before selling, donating, or discarding old computers, make sure that sensitive data is removed. Files that are simply deleted can be easily recovered. To sanitize your hard drives, use a program designed to overwrite the drive in a secure manner, formatting your drive does not remove the data effectively. See your system administrator for more information on acquiring a copy of the software to sanitize your hard drives.