CMSGu2011-06

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Security Guideline for Standalone and Network Computers

CERT-MU

National Computer Board
Mauritius

September 2011

Issue No. 6

Version 1.1

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

This document provides a guideline for the implementation and management of standalone and network computers. It covers preliminary guidance and focuses the attention of users on information security.

1.2 Audience

The intended audience for this technical document includes system administrators and all those who access, administer, and manage standalone and network systems and have authorised accounts on these systems.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background to understand the underlying risks with computers in general.

Section 3 offers an insight into securing a standalone computer.

Section 4 discusses how to secure a Windows computer connected to a network.

Section 5 details how to secure a computer connected to a private network.

Section 6 explains how to secure a Windows server.

Section 7 shows how to secure a Linux or Unix computer.

Section 8 details how to secure a Macintosh connected to a network.

Section 9 concludes the document.

Section 10 comprises a list of references that have been used in this document.

2.0 Understanding The Risks Associated With Computers

All organisations that make use of computers need to consider the security of information they keep. Data stored on computers may be at risk of theft, loss or corruption, either accidentally or deliberately. Organisations have to take extra care over and above the usual precautions because they are at risk of a breach of data security by people who want to harm the organisation. Such groups may target internal data to disrupt activities or to collect information on individuals, internal operations, buildings and events.

Organisations should use available computer security tools to their maximum capabilities because of the additional risks they are exposed to. Below are a few common computer security problems and basic guidance about the existing solutions.

2.1 Physical Security

Computer equipment continues to be highly vulnerable to theft. A number of simple precautions can help to protect your computers. These include restriction of access to areas where computers are kept, burglar alarms, closed circuit television monitoring and property marking.

Measures particularly applicable to computers include:

- Attach computers to permanent or heavy fixtures so they cannot be removed. It is possible to bolt computers or computer cabinets to floors, walls or heavy furniture.
- Use computer safes and cabinets that prevent computers from being removed easily but still allow the required access for usage and maintenance.
- High quality security cables can be used to attach hardware to permanent fixtures or heavy furniture.
- Install a removable hard disk. The hard disk can be removed when you close your office and locked away in a secure cabinet.

2.1.1 Control Access To Data

Consider all points of access to computer data and observe simple precautions to prevent data being accessed illegitimately. For instance, remove or lock CD/DVD drives on computers where they are not required. When setting up a computer network, make sure that all network access points are in secure areas.

2.1.2 Computers taken offsite/for repair

If computer equipment must go off-site for service or repair then you should remove sensitive data before the computers are taken away. Hard drives may be physically removed, or alternatively, data can be securely deleted by the means described below:

- **Secure Deletion/Overwriting/Wiping**

  In most operating systems (e.g. Windows, Apple Macintosh, Unix) normal deletion of files does not actually delete the data from the hard disk. Deletion only removes some of the labelling indicating where the data is on the hard drives (addressing). Easy-to-use software that allows the restoration of the original files is widely available. Fortunately, software that overwrites all the data, making it much more difficult to retrieve, is also widely available. Examples of this software are the *"Wipefile[1]"* function in Norton Utilities and the *"Wash[2]"* command in *"XtreeGold[3]"*. Using a defragmentation program (e.g. Disk Defragmenter in Windows) also overwrites some data but often leaves old files easy to retrieve.

- **Laptops, other portables and removable media**

  Staff and others using laptop and handheld computers (e.g. Palms and Psions) which carry sensitive data should keep these machines with them at all times or lock them away securely. Theft of laptops and handhelds from vehicles has become a very common issue, so do not leave them unattended in vehicles. You should take similar care over removable media (e.g. backup tapes, CDs, DVDs) containing sensitive data: do not leave them unattended and lock them away securely whenever possible. If removable media that contained sensitive data are being re-used, then their contents should be securely deleted/overwritten. A useful feature of many laptops is a removable hard disk. When travelling but not using your laptop, it is better to keep the hard drive with you, separate from your laptop. Store your hard drive (or the whole laptop) in a secure cabinet when not travelling.

[1] **WipeFile**: is a secure files and folder deletion utility, overwriting data so there is no way to recover files.

[2] **Wash command**: is a utility that deletes files permanently.

[3] **XtreeGold:** is a file manager software originally designed for use under DOS.

- **Disposal of Computers and disks**

  Before you discard, sell or pass on your old computers, overwrite all sensitive data. Similarly if you dispose of any media on which you keep data - such as, CDs, DVDs, memory sticks - overwrite them first. Alternatively, destroy them physically.

2.2 Electronic Security

2.2.1 Data Loss and Backups

Data stored on an organisation's computers is often critical to the operation of the organisation, even though computers are not totally reliable. You should regularly backup your data so that if your computer loses it you can replace it fully. Data is usually backed up on removable media (e.g. DATs, zip drives, writeable CDs) for which you may need an additional drive. Check regularly that you are backing up all the data that you need and test that you can actually restore it. Also keep a recent backup copy of your system in a secure place off-site so that if on-site backups are destroyed in an emergency you can still restore your data. Many organisations back up their systems overnight. If you do this then protect sensitive information on the backup from being removed by keeping the computer containing the backup drive in a locked cabinet.

2.2.2 Viruses

Severe data loss can be caused by computer viruses (destructive programs designed to disrupt computers). These can be propagated via CDs, USBs etc but more commonly through e-mails or downloaded files from the Internet. To avoid this all computers should have up-to-date anti-virus software installed and running. Well known anti-virus software companies include McAfee, Sophos and Norton/Symantec amongst others. If you really cannot afford to pay for anti-virus software, there are free programs available over the Internet but these may be less reliable and not updated as often. New viruses are constantly appearing so update your anti-virus software as frequently as possible. Many companies allow you to do this for free over the Internet.

Some viruses come as files attached to e-mails and sometimes the sender is unaware that they have passed on the virus. Some of these (known as Trojans) contain programs that can allow an outsider to access and take control of your computer or network over the Internet. To be absolutely sure that they do not receive viruses, some organisations do not accept files attached to e-mails. The golden rule is if you do not know the sender, do not open the attachment. If you do know the sender but have even the slightest doubt then contact them by phone or e-mail to confirm that they sent it.

2.2.3 Passwords

To protect sensitive information, you should use passwords wherever possible. You can usually set up passwords (in the BIOS) so that the computer cannot be started without the password. Passwords are also usually used to log in to networks. Individual files created in many common programs can be password protected. It is also possible to password-protect your screen to reduce access to your computer if you are away from it and have left it running.

You should keep passwords secret. If possible do not write them down. If you feel you have to write down a password then keep the written version under lock and key, away from computers that it is used with. Do not write down what the password is for in the same place as the password itself. Wherever possible change your password regularly.

Despite these precautions, in case of emergencies, more than one person should be able to access each password used. Although passwords undoubtedly make illegitimate access to sensitive data more difficult, serious hackers have many tools at their disposal to break passwords. The following precautions make a password more difficult to crack. Avoid using passwords that people will be able to work out easily. Ideally passwords should be random sequences of capitals, lower case letters numbers, and special characters. However, random passwords are difficult to remember. To avoid this difficulty, take an ordinary word (e.g. carpenter), deliberately spell it wrongly (karpenter), change some letters to capitals at random (kArpenteR) and also insert some numbers and special characters randomly (kA7rpen4teR%). Passwords should also be as long as possible.

2.2.4 Networks

- **Protected Passwords**

  Wherever possible, store all data on a network fileserver, running an operating system with built in security (e.g. Windows 2000 or Windows NT). Use encrypted passwords for all user logins.

- **Permissions**

  Control access to the different parts of your network. Restrict permission to users to access only those programs, directories and files that they need in order to be able to do their work.

- **Laptops and other portables**

  You should also consider whether and how portable computers may be connected to your system. If, for instance, you allow users to connect laptops or palmtops to your network, you will not be able to guarantee that they do not download viruses to your network and that they do not copy sensitive files from your network to the portable device.

2.2.5 Internet

- **Isolate network from the Internet**

  A major computer security weakness for many organisations is their access to the Internet. It is possible for someone with advanced computing knowledge to access the information stored on your computer and networked computers when you are connected to the Internet. If you have a broadband Internet connection (e.g. ADSL, cable modem) then your vulnerability to such an attack is increased, especially if your link to the Internet is maintained constantly or for extended periods of time.

  The most effective way to protect your network from hackers is to isolate it from the Internet. If at all possible, try to allocate a single “standalone” computer, not connected to a network, for all external contact such as Internet, e-mail and fax use. This should hold no sensitive information such as membership details and mailing lists.

  If you really are unable to have a separate machine for Internet use, consider encrypting sensitive data on your machine, and set up as many levels of password protection as possible for all your data and programs.

- **Firewalls**

  It is essential to implement Internet firewalls on both networks and standalone computers. This will help prevent attacks against computers while connected to the

Internet. Hardware and software firewalls are available. Hardware firewalls are connected between your computer and the Internet in order to stop information from your computer being transferred inadvertently to and from the Internet. Software firewalls do a similar job and, for extra security, they should be used together with hardware firewalls. On a computer network, Microsoft Internet Security and Acceleration Server (formerly known as Proxy Server) is a commonly used firewall. However, the advanced settings need to be implemented for Internet Security and Acceleration Server to be effective. For standalone computers, Zone Alarm is an excellent and easy to use product. For charitable and personal use, it can be downloaded for free from www.zonealarm.com**.**

- **Webservers**

  Most organisations have their websites hosted by an external body. If, however, you host your own website internally, i.e. on your own webserver, make sure that this is totally unconnected to your main network. Experienced hackers may be able to access your network via a webserver on your network in as little as 20-30 minutes.

- **Email/Downloading files**

  Beyond the considerations outlined above for use of the Internet, e-mail across the Internet and downloading files provide further dangers to your data and computer systems. Remember, if you have any concern about an attachment to an e-mail or a downloaded file, do not open it. You may want to enforce a policy banning the receipt of e-mail attachments and downloading files without approval by a nominated responsible person.

- **Encryption**

  Furthermore, e-mails can be intercepted and read or even changed so they should not be used for sending sensitive information. You may even want to introduce a policy forbidding sending attachments. You can use an encryption program to protect e-mail and the contents of your hard disk as well. Be sure to obtain encryption programs from a reliable distributor. A high-grade encryption program called PGP (Pretty Good Privacy) can be used (www.pgp.com).

2.3 The Human Element

The guidelines above outline some of the technical solutions to some important computer security problems. However, perhaps the most significant weakness in this field is the human element. Using technical tools and devising policies about computer security are important aspects of a computer security strategy. However, it is equally important to educate your computer users about the risks your computer systems face and to train them how to use the computer security tools you decide to employ. Once your policies, tools and training have been implemented, it is vital to monitor the behaviour of your users to ensure that security is maintained at a high level.

3.0 Securing a Standalone Computer

A standalone desktop computer is one that is not connected at all to another computer or networked device, such as a switch, hub, or router (with the possible exception of a printer), or to the Internet or a local area network (LAN). The standalone desktop computer can run Windows 2000 – Windows 7, Linux, or Mac OS X. As the standalone desktop computer is not connected to the Internet or a local or wide area network, the emphasis for securing the data is placed on physical security of the computer and controlling access to the data.

Here are the minimum steps you should take to secure data on your standalone desktop computer:

3.1 Physical Security of a Standalone Computer

- Configure the BIOS to boot the desktop computer from the hard drive only. Do not allow the standalone desktop computer to be booted from the diskette or CD-ROM drive.
- Password-protect the BIOS so changes cannot be made to the BIOS without authorisation.
- Secure the desktop computer on which data resides in a locked room, or secure the desktop computer to a table with a lock and cable (locking the case so the battery cannot be disconnected, which would disable the BIOS password).
- Remove or disable the network interface card (NIC) so it cannot be used.
- Store the data on a desktop computer only.

3.2 Controlling Access to the Data

- Restrict access to data to project personnel using the security features available via the operating system (e.g., login via user id/password and NTFS permissions in Windows 2000 – Windows 7, ACLs in Linux and OS X).
- Require strong passwords.
    1. You can run *"L0phtcrack[4]"* to look for bad passwords.
    2. You can use *"SCM[5]"* to enable password complexity.

[4] **L0phtCrack:** is a password auditing and recovery application used to test password strength and sometimes to recover lost Microsoft Windows passwords

- Password-protect screen saver and activate after three minutes of inactivity.
- Enable encryption for directories containing secure data. Windows Encrypting File System (EFS: available in Windows 2000 - Windows 7) is built into the OS and works well. Additional encryption software applications can be found here.
- Install and periodically run a secure erasure program. This program should be run monthly and after the secure data has been removed from the computer at the end of the contract period.
- Do not copy or move data out of the secured directory for any reason.

[5] **Software configuration management (SCM)**: is the task of tracking and controlling changes in the software.

4.0 Securing a Windows Computer Connected to a Network

A network refers to two or more computers and/or network devices (e.g., printer, switch, hub, router) connected to the Internet or a Local Area Network (LAN).

Below are the minimum steps you should take to secure data on a Windows computer connected to a network (for OS-specific detailed security, see these specific security guides). If only one person will be using the data stored on this computer, the external hard drive option should be considered for better security.

4.1 Physical Security of a Windows Computer on a Network

1. Configure the BIOS to boot the computer from the hard drive only. Do not allow the computer to be booted from the diskette or CD-ROM drive.
2. Password-protect the BIOS so changes cannot be made to the BIOS without authorisation.
3. Secure the computer on which data resides in a locked room, or secure the computer to a table with a lock and cable (locking the case so the battery cannot be disconnected, which would disable the BIOS password).

4.2 Controlling Access to the Data

1. Restrict access to data to project personnel using the security features available via the operating system (e.g., login via userid/password and NTFS permissions in Windows 2000 – Windows 7)
2. Require strong passwords.
    - You can run a password cracker (e.g., L0phtcrack, Cain and Abel, John the Ripper, Ophcrack) to look for bad passwords. (Be sure you have permission in writing before you do this!)
    - You can use Administrative Tools, Local Security Policy to enable password complexity (Windows 2000 – Windows 7).
    - Note vulnerabilities for accounts with no passwords or weak passwords.
3. Password protect screen saver and activate after three minutes of inactivity.

4. Install encryption software for directories containing secure data. Windows EFS encryption is free and works well. Additional encryption software applications can be found here.
5. Configure your analysis software to point temporary work files to the encrypted data directory.
6. Install and periodically run a secure erasure program. This program should be run monthly and after the secure data has been removed from the computer at the end of the contract period. (Shred 2 is inexpensive and is effective).
7. Do not copy or move data out of the secured directory for any reason.

5.0 Securing a Computer Connected to a Private Network

A private network is two or more computers and/or network devices (e.g., printer, switch, hub, router) that are not connected in any way to the Internet or a LAN (i.e., Cold Room or Secure Data Facility). The data will reside on a computer acting as a server.

Here are the minimum steps you should take to secure data on a server on a private network:

5.1 Physical Security of a Computer on a Private Network

1. Configure the BIOS to boot the computer from the hard drive only. Do not allow the computer to be booted from the diskette or CD-ROM drive.
2. Password-protect the BIOS so changes cannot be made to the BIOS without authorisation.
3. Secure the computer on which data resides in a locked room, or secure the computer to a table with a lock and cable (locking the case so the battery cannot be disconnected, which would disable the BIOS password).

5.2 Controlling Access to the Data

1. Restrict access to data to project personnel using the security features available via the operating system (e.g., login via userid/password and NTFS permissions in Windows 2000 – Windows 7, ACLs in Linux and OS X).
2. Require strong passwords.
    - You can run L0phtcrack to look for bad passwords.
    - Enable password complexity (Windows 2000 – Windows 7)
3. Password protect screen saver and activate after three minutes of inactivity.
4. Install encryption software for directories containing secure data. Windows 2000 encryption is free and works well. BitLocker Drive Encryption is also an efficient full disk encryption feature included with the Ultimate and Enterprise editions of Windows Vista and 7, as well as the Windows Server 2008 and Windows Server 2008 R2 server platforms.
5. Configure your analysis software to point temporary work files to the encrypted data directory.

6. Install and periodically run a secure erasure program. This program should be run monthly and after the secure data has been removed from the computer at the end of the contract period. (Shred 2 is inexpensive and works well).
7. Do not copy or move data out of the secured directory for any reason.

6.0 Securing a Windows Server

Following are recommended steps to be taken to secure data stored on a Windows 2000 - Windows 2008 server. Because each environment is different, your server administrator should test the following steps before implementing on a production server. Most enterprise-wide servers have highly trained professionals managing them, so some or all of the following steps may already be implemented. If your network administrator is not able or willing to implement any of the following steps, simply state the reason in the accompanying form to describe your security plan.

6.1 Physical Security of a Server on a Network

1. Secure the server on which data resides in a locked room to which only authorised users have access.

6.2 Controlling Access to the Data

1. Restrict access confidential data to personnel using the security features available via the operating system (e.g., login via userid/password and NTFS permissions).
2. Require strong passwords.
    - You can run L0phtcrack or other password recovery systems to look for bad passwords.
    - You can use Administrative Tools, Local Security Policy to enable password complexity (Windows 2000 – Windows 2008).
    - Note vulnerabilities for accounts with no passwords or weak passwords.
3. Install encryption software for directories containing secure data.
4. Configure your analysis software to point temporary work files to the encrypted data directory.
5. Install and periodically run a secure erasure program. This program should be run after the secure data has been removed from the server at the end of the contract period. (Shred 2 is inexpensive and works well.)
6. Do not copy or move data out of the secured directory for any reason.
7. Password protect workstation's screen saver and activate after three minutes of inactivity.

6.3 Protecting the Data from Unauthorised Access Across the Wire

The following are additional minimum steps you should take to secure data on a server running Windows 2000 - Windows 2008 if the server is connected to the Internet or a network.

1. Do NOT install IIS or MS SQL server on a Windows computer that will house sensitive data.
2. Turn off all unneeded services (the following list is provided as an example, and may not be a complete list for your environment. Be sure to test these items before implementing on a production server!)
    - IIS
    - Peer Web Services
    - RAS
    - Gopher
    - FTP
    - IP Forwarding
    - Simple TCP/IP Services
    - SNMP
    - Disable unneeded network protocols (e.g., IPX or NetBEUI)
3. If you operate in an IP only environment, disable NetBIOS over TCP/IP.
4. Replace the *"Everyone"* group with the Authenticated Users group for the Access this Computer from the Network user right (User Manager-->Policies-->User Rights).
5. Disable the Guest account.
6. Replace group *"Everyone"* with the appropriate group(s) on critical system folders, files, and registry keys. Share permissions to only those groups that need access (default access control on new shares is Everyone Full Control).
7. Remove, disable, or rename administrative shares (c$, d$, admin$).
8. Restrict/Prevent anonymous access and enumeration of accounts and shares.
9. Create a new userid for administrative purposes and add this userid to the Local Administrator's group. Remove the original administrator userid from the Local Administrator's group.
10. Protect the administrative password: using the resource kit, run
    - passprop /complex /adminlockout

11. Encrypt the SAM (run syskey.exe)
12. Use Windows Update or Microsoft Baseline Security Advisor to keep system patches up to date. (Consider subscribing to the Microsoft Security Notification Service.)
13. Install application (e.g., Internet Explorer) security patches.
14. Install antivirus software and keep the virus definition files updated.
15. Secure performance data.
16. Enable auditing:
    - Audit Login success and failure.
    - Audit failed attempts at exercising user privileges.
    - Audit system events such as shutdowns.
    - Move log files out of the default location and secure with NTFS permissions (%system-root%\system32\config\*.evt).
    - Restrict access to the log files to administrator only.
    - Check your logs often
17. Disable or remove Windows Scripting Host.
18. Use a corporate, hardware, or personal (software) firewall:
    - Hardware: Linksys Instant Broadband EtherFast Cable/DSL Router
    - Software personal firewall
        - ZoneAlarm or ZoneAlarm Pro
        - Tiny Personal Firewall
        - Sygate Personal Firewall

7.0 Securing a Unix or Linux Computer

Following are guidelines for securing a computer that is running a version of the Unix or Linux operating system. These rules are broad in scope; the specifics of each particular operating system preclude an authoritative guide that will cover them all. The main focus of this section is on using encrypted communications and avoiding running unneeded services.

1. Run a command like *"netstat –an"* to see which ports your computer is listening to. You should understand why your computer is listening to each port that is reported. Do not run telnet (port 23) or ftp (20 and 21), because authentication is done over the wire in clear text. (Even in a switched environment one is not immune to packet sniffing). For computers that house sensitive data, other services such as smtp (25) and http(s) (80, 8080, or 443), which have a poor security history and are prime targets for network abusers, should not be used either. Various services like chargen (19) and echo (7), which many systems activate by default, should not be on unless they serve a specific purpose. Some *"rpc"* services like *"ttdbserver"* also have a poor track record and should not be used. Hopefully if you are in a campus environment you will have other machines in place as DNS servers, so be sure to disable bind as well, because it has a poor record for security.

2. Use only encrypted authentication tools like Secure Shell version 2 (ssh2) and/or kerberos in order to protect login credentials. Very good free tools like *"openssh"* are quite robust, standards compliant, and easy to build for any Unix or Linux operating system. A good and free Windows terminal client that speaks *"ssh2"* is *"Putty"*. Secure shell version 1 is weak and should not be used. Machines running a *"ssh"* daemon should not have it configured to failover to ssh1 if the client cannot speak *"ssh2"*. If you are building *"ssh2"* be sure that you have the latest *"openssl"* version as well. Disable any r-services that may be in place by default such as *"rsh"*, *"rexec"*, *"rcp"*, and *"rlogin"*. These services are extremely vulnerable and should be replaced with similar *"ssh"* and *"scp"* commands.

3. Make use of a system logging tool like syslog and copy all of your logs to a dedicated syslog server. Running a syslog server that collects the logs from all of the other systems is a great idea. More than likely if someone is clever enough to break into your system they are clever enough to know how to purge the logs and cover their tracks. Having a syslog server allows one to at least have some confidence in knowing who has done what in the past. Syslog is the most common tool for this type of logging and comes bundled with most flavors of Unix and Linux. Review your syslog files regularly (e.g., weekly) to make sure nothing unusual is taking place.

4. Review your /etc/passwd and /etc/security/passwd files regularly to make sure all userids have a password (not null) and that only the root user has a UID of 0. Expiring passwords at least every three or four months will help ensure that old users lose access even when the sysadmin forgets to remove them. Requiring strong passwords is a necessity. Removal of default system userids like “guest” is also very important. Do not allow the use of shared accounts among users as this makes audit controls useless. One user, one account.

5. Avoid logging in as root. When logging into a system, login with a non-root userid and only su to root if absolutely necessary. Never log in to a remote host as root on a user's computer - you never know what viruses or keylogging programs may be running.

6. Log in to your systems often and see what processes are running. Using commands like “ps -ef” to list all processes can be very helpful. Anything that isn’t immediately obvious as a usual system or user process should be checked out. Reviewing who has logged into a system with “last” is also a great idea, and using system accounting commands like “sar” will help you find potential abuse as well.

7. Patch your systems. Make use of security organisations by subscribing to their mailing list so that you receive important security alerts in a timely manner. There is no substitute for keeping up with the latest exploits and fixes on the systems for

which you are responsible. Most vendors make patches available in short order once a security bug is found, so check your vendor’s Web sites often.

8. Do not copy or move data out of the secured directory or off of the secured server for any reason.

8.0 Securing a Macintosh (Mac) Connected to a Network

8.1 Physical Security of a Macintosh on a Network

1. Configure the Macintosh to boot from the hard drive only. Do not allow the Macintosh to be booted from the diskette or CD-ROM drive.
2. Secure the Macintosh on which data resides in a locked room, or secure the computer to a table with a lock and cable.

8.2 Controlling Access to the Data

1. Turn off the auto-login feature and require individual userids for anyone using the system.
2. Restrict access to data to project personnel using the security features available via the operating system (e.g., login via userid/password and ACLs permissions).
3. Require strong passwords.
4. Password protect screen saver and activate after three minutes of inactivity.

8.3 Protecting the Data from Unauthorised Access Across the Wire

1. Avoid using the root account. Use the sudo command instead.
2. Leave all unneeded services turned off, especially File and Web sharing, remote logins, and ftp sessions.
3. Maintain all OS and application security patches.
4. Install antivirus software and keep the virus definition files updated.
5. Disable any scripting capabilities in your email client (e.g., Visual Basic Script or JavaScript).
6. Enable auditing.
7. Use a corporate, hardware, or personal (software) firewall (e.g., the Macintosh comes with a built-in firewall, ipfirewall).

9.0 Conclusion

Computers, whether connected or not, need to be secured because they often contain confidential data. We are not always aware of how sensitive data on our machines is; hence do not set proper security mechanisms. It is of paramount importance that we enforce policies which are in line with internal controls so that only authorised users have access to sensitive data, preventing any breach of confidentiality, integrity and availability.

10.0 References

- Columbia Population Research Center: http://cupop.columbia.edu
- Community Security Trust: http://www.brijnet.org
- CERT-In guidelines: www.cert-in.org.in
- Wikipedia: http://en.wikipedia.org