Global Information Assurance Certification Paper

INTRODUCTION

If you need to electronically communicate with others, whether it be for business or other purposes, your computer has to be networked. This exposes your computer to various attacks. Typically a user would like to ensure the following when connected to a network:

- **Availability** which will ensure that information; resources and services are there for the business as and when required.
- **Integrity** which ensures that data residing on a user's machine has not been tampered with and that it is correct.
- **Access control** to protect critical resources by limiting access to only authorised and authenticated users, principals, programs or processes.
- **Confidentiality** which protects sensitive information from disclosure.
- **Compliance (Auditability)** to ensure protected and reliable records of system activity with security significance (e.g., logins, logouts, file accesses, security violations) must be available.

This document attempts to touch on a few of standards that can assist in ensuring that the above objectives are met when using a Windows 2000 operating system.

Continuity and availability

1.	**Appropriate measures should be implemented to offer protection against physical access and tampering.**
Requirement	To protect system against unauthorised physical access and tampering. Without these restrictions other system controls may be compromised.
How	Locate system in physically secure areas that implement restrictive access control. Restrictions may include locked doors or access cards to computer labs. Where possible, BIOS level tamper detection options should be enabled. Removable hard disks and essential peripherals should be locked down if possible to protect against their removal by unauthorised personnel.
Additional Notes	Theft of easily removable systems such as laptops and devices such as printers may be reduced with the use of cable locks.

2.	**Create a copy of the data on the hard disk.**
Requirement	The Backup utility helps you create a copy of the data on your hard disk. In the event that the original data on your hard disk is accidentally erased or overwritten, or becomes inaccessible because of a hard disk malfunction, you can use the copy to restore your lost or damaged data.
How	Click **Start**, point to **Programs**, point to **Accessories**, point to **System Tools**, and then click the appropriate icon. You can also use the **Backup** utility to create an Emergency Repair Disk (ERD), which will help you recover or repair your system. A full system back-up to off-line storage media, should be performed at least once a week. A copy of the backup should be kept on site in secure storage while a second copy of this backup should be sent to an off-site secure storage warehouse.
Additional Notes	Ensure that the Automatically reboot option in the **Startup/Shutdown** tab of the System applet in the **Control Panel** is disabled. This will prevent damage to databases caused by repeated reboots of the operating system due to failures.

User accounts - Guest

3.	**Ensure that you have disabled the guest account.**
Requirement	The guest account may allow anonymous access to the machine.
How	This can be done by pointing to **Control** Panel, click **Administrative Tools**, **Computer Management** , **Local Users and Groups**. Double click on the **Guest** and check the **Account is disabled** box.
Additional Notes	

Password Policies

4.	**Passwords should be carefully selected.**
Requirement	Passwords are the primary method of authenticating users who require access to a system. A poor password selection may be compromised to gain unauthorised access to the system.
How	Ensure that passwords are suitably complex with an appropriate character mix being employed. The character mix should include at least two of each of the following character types: Upper case, lower case, numeric and non alpha numeric. Your password should also not be: i) Dictionary words; ii) Directly related to you (name, girlfriend's name or password); iii) Blank iv) Your birthdate
Additional Notes	

Shared resources

5.	**Limit access and minimise the number of network shares.**
Requirement	Network share directories are the primary mechanism for sharing files between computers in an Windows 2000 compliant network and should be appropriately set up to ensure that access to sensitive data is limited to trusted groups and users and that the integrity of all shared data can be maintained.
How	Open Windows Explorer, and then locate the shared folder or drive on which you want to set permissions. Right-click the shared folder or drive, and then click **Sharing**. On the **Sharing** tab, click **Permissions**. To set shared folder permissions, click **Add**. Type the name of the group or user you want to set permissions for, and then click **OK** to close the dialog box. To remove permissions, select the group or user in **Name**, and then click **Remove**. In **Permissions**, click **Allow** or **Deny** for each permission, if necessary.
Additional Notes	

Auditing

6.	**Ensure that Auditing is enabled for sensitive files and folders.**
Requirement	Audit logs may further may provide evidence of wrongdoing in the event of an intrusion.

How	Open Windows Explorer, click **Start**, point to **Programs**, point to **Accessories**, and then click **Windows Explorer**. Open Windows Explorer, and then locate the file or folder you want to audit Right-click the file or folder, click **Properties**, and then click the **Security** tab. Click **Advanced**, and then click the **Auditing** tab. Do one of the following: To view or change auditing for an existing group or user, click the name, and then click **View/Edit**. To remove auditing for an existing group or user, click the name, and then click **Remove**. If necessary, in the **Auditing Entry** dialog box, select where you want auditing to take place in the **Apply onto** list. The **Apply onto** list is available only for folders. Under **Access**, click **Successful**, **Failed**, or both for each access you want to audit. If you want to prevent files and subfolders within the tree from inheriting these audit entries, check the **Apply these auditing entries** box.
Additional Notes	You can set file and folder auditing only on drives formatted to use NTFS. Since the security log is limited in size, you should select the files and folders to be audited carefully. You should also consider the amount of disk space you are willing to devote to the security log.

7.	**Set up an independent audit group of which you are the only member**
Requirement	It is essential to partially segregate administrative functions from audit functions. An audit group should thus be created, granting and ensuring that only this group has access to the audit logs for sensitive files and folders.
How	Open Windows Explorer, and then locate the file or folder you want to audit Right-click the file or folder, click **Properties**, and then click the **Security** tab. Click **Advanced**, and then click the **Auditing** tab. To set up auditing for a new group or user, click **Add**. In **Name**, type the name of the user you want, and then click **OK** to automatically open the **Auditing Entry** dialog box.
Additional Notes	

Access Controls

8.	**Access to sensitive files and folders should be restricted.**
Requirement	Any user can gain access to your computer over a network or the Internet if the user knows your computer name, and the user name and password of a user who is a member of the Administrators, Backup Operators, or Server Operators group. A user who gains access to your drive over the network or Internet can view all folders and files on that drive, even those that are protected using NTFS permissions, provided the NTFS permissions allow access to members of the Administrators, Backup Operators, or Server Operators group.
How	Open Windows Explorer, click **Start**, point to **Programs**, point to **Accessories**, and then click **Windows Explorer** Open Windows Explorer, and then locate the file or folder for which you want to set permissions Right-click the file or folder, click **Properties**, and then click the **Security** tab. Do the following: To set up permissions for a new group or user, click **Add**. Type the name of the group or user you want to set permissions for using the format *domainname\name*, and then click **OK** to close the dialog box. To change or remove permissions from an existing group or user, click the name of the group or user. In **Permissions**, click **Allow** or **Deny** for each permission you want to allow or deny, if necessary. Or, to remove the group or user from the permissions list, click **Remove**.
Additional Notes	You can set file and folder permissions only on drives formatted to use NTFS.

9.	**Screen saver locking mechanisms should be employed**
Requirement	This would facilitate the automatic locking of an unattended computer, which would add to the security of the system.

How	Open the Control Panel item, click **Start**, point to **Settings**, click **Control Panel**. **Open Display**. Under **Screen Saver**, choose a screen saver from the drop down list. Select the **Password protected** check box.
Additional Notes	

Configuration of new systems

10.	**Disks should be partitioned into at least two partitions.**
Requirement	Careful structuring and partitioning of disks will produce a more secure and robust operating platform. Failure to do so could result in an insecure system and one that is difficult to recover following a disaster.
How	Structure at least two partitions using any disk manager prior to installation, ensuring that the first partition is at least 2MB in size and that all valid drive letters are allocated to remaining partitions. Set the first partition to be the active partition. Ensure that the Windows 2000 operating system is installed to the active partition and that applications and data are installed on the remaining partitions. This may allow for the restoration of the operating system without effecting the data and vice versa.
Additional Notes	Re-partitioning or formatting a disk after installation will result in the loss of all data on the disk.

11.	**The NT File System format should be applied on all disks and partitions.**
Requirement	The NT File System (NTFS) supports Access Control Lists (ACL's) which afford a higher level of protection to the operating system and it's data. NTFS also allows for the auditing of access to files and folders contained by the file system.
How	A partition can be converted after Setup by using Convert.exe. For more information about Convert.exe, after completing Setup, click **Start**, click **Run**, type **cmd** and then press ENTER. In the command window, type **help convert** and press ENTER.
Additional Notes	

12.	**The latest Microsoft released service packs and hot fixes should be installed.**
Requirement	Service packs and hot fixes provide security and performance enhancements to Windows 2000, which may better manage the exposure of the server.
How	Install the latest service pack released by Microsoft as soon as operational circumstances allow it. Identify W2K security patches released after the installed service pack, and ensure that only those relevant to the installed service pack are applied.
Additional Notes	Always evaluate changes made after the installation of a new service packs or hot fix by ensuring that the system is stable and that all applications still function as expected. Check all file permissions after installation of a service pack or hot fix as these may be changed. Visit http://windowsupdate.microsoft.com/default.htm to identify the latest security patches released by Microsoft.

Securing registry keys

13.	**Editing of the registry by non administrative users should be denied.**
Requirement	The registry is a sensitive part of the operating system and if tampered with may result in complete failure of the operating system. Editing of the registry should thus be restricted to skilled administrative users only.
How	Click the key to which you want to assign or revoke Special Access. On the **Security** menu, click **Permissions**. Click **Advanced**, and then double-click the user or group to whom you want to assign Special Access. Under **Permissions**, select the **Allow** or **Deny** check box for each permission you want to allow or deny.
Additional Notes	

14.	**Activities on the registry key should be audited**
Requirement	Successful and failed attempts to access the registry keys should be audited on critical machines.

How	lick the key you want to audit. On the **Security** menu, click **Permissions**. Click **Advanced**, and then click the **Auditing** tab. Double-click the name of a group or user. Under **Access**, select or clear the **Successful** and **Failed** check boxes for the activities that you want to audit or to stop auditing: **Select : Query Value** **To audit::** Any attempts to read a value entry from a registry key. **Select : Set Value** **To audit::** Any attempts to set value entries in a registry key. **Select : Create Subkey** **To audit::** Any attempts to create subkeys on a selected registry key. **Select : Enumerate Subkeys** **To audit::** Any attempts to identify the subkeys of a registry key. **Select : Notify** **To audit::** Any notification events from a key in the registry. **Select : Create Link** **To audit::** Any attempts to create a symbolic link in a particular key. **Select : Delete** **To audit::** Any attempts to delete a registry object. **Select : Write DAC** **To audit::** Any attempts to write a discretionary access control list on the key. **Select : Write Owner** **To audit::** Any attempts to change the owner of the selected key. **Select : Read Control** **To audit::** Any attempts to open the discretionary access control list on a key.

Additional Notes	

Network security

15.	**Ensure that unnecessary networking services are disabled.**
Requirement	Network services that allow client connections to the system but which are not serving services valid to the business function of the system should be disabled as these services may offer potential exploit paths to unauthorised users.
How	Network services deemed to be unnecessary for the day to day running of the system should be disabled. Standard services including FTP and HTTP should not be installed or enabled **without valid justification** for their business use. One way of achieving this is through typing **netstat –a** at the command line.
Additional Notes	To check which services are associated with certain ports visit one of the following sites: http://advice.networkice.com/Advice/Exploits/Ports/default.htm http://www.snort.org/

CONCLUSION:

The secure installation, configuration and maintenance of a networked machine is of utmost importance. Users of Windows 2000 should be aware of specific threats when ensuring the confidentiality, integrity and availability of the data and system configuration of their computers. The standards outlined above are the first steps to ensuring a more secure system.

NOTE: There are many other standards that can be used to secure your system. These are dependent on the user's need and operating environment.

REFERENCES:

White Paper: "Default Access Control Settings in Windows 2000" Last Update March 15, 2001; URL
http://www.microsoft.com/technet/win2000/win2ksrv/technote/secdefs.asp

Sethos Jeremy. "Securing Windows 2000: First Steps": URL
http://www.arstechnica.com/tweak/win2k/security/begin-2.html#passwd

Sutton, Steve. "Windows NT/2000 Security" Last Update Feb 19, 2001; URL
http://www.isaserver.org/pages/wp/windows%202000%20security.htm

bernie@labmice.net "Windows 2000 Installation Security Checklist" Last Update March 30, 2001; URL
http://www.labmice.net/articles/securingwin2000.htm

Project Team: Clement, Miles; Creasey, Jason - Information Security Forum (ISF) – Windows 2000 Security Version 1 (March 2000)[1]

[1] Many other individuals were involved in the compilation of the document, however these are too many to mention. A work group, project team, review and quality assurance team and production person was involved in the project.

Last Updated: May 29th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event