



CIT End User Device Policy



Version 1.0

**Information Systems Security Office
Center for Information Technology
National Institutes of Health
U.S. Department of Health and Human Services**

January 4, 2011

Change History

Version Number	Release Date	Summary of Changes	Section #/ Paragraph #	Changes Made By
1.0	06/09/2010	Initial Document Release	NA	Cleo Hanlon
	10/1/2010	Insert comments/Final draft	Entire Document	Kim Eccles
	11/24/2010	Incorporated final comments	Entire Document	Dawn Gonchar
	1/4/2011	Additional comments requested by DCS		Dawn Gonchar

Table of Contents

Purpose 1

Background 1

Scope 2

Policy 2

Exceptions..... 6

Non-Compliance..... 6

Information and Assistance..... 6

Definitions..... 7

References..... 9

Effective Date 10

PURPOSE

This Center for Information Technology (CIT) policy outlines desktop requirements for personnel in possession of, or responsible for operating CIT end user devices. End user devices may include CIT approved and issued desktops/laptops, PDAs, printers, or any other information technology (IT) devices operated by an end user. Lastly, this policy addresses the implementation of IT patches to comply with the CIT patch management program, as well as the anti-virus management at the end user device level.

BACKGROUND

The Federal Information Security Management Act of 2002 (FISMA) requires that agencies establish a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.¹ FISMA also mandates that agencies follow National Institute of Standards and Technology (NIST) standards and guidelines to establish and secure that framework.

In accordance with the U.S. Department of Health and Human Services (HHS) and National Institutes of Health (NIH) patch management and anti-virus policies and guidelines; this document defines the policy that will promote secure patch and anti-virus management at the end user level. Adherence to this policy is mandatory for all end users accessing CIT information through a device connected to NIHnet. Additionally, accounts accessing CIT information must follow the dictates of existing HHS and NIH policies and procedures.

The NIH Patch Management Policy establishes the requirement that software patching be implemented and managed in an efficient and timely manner. This includes those systems owned by all other parties operated on behalf of NIH.

Likewise, the NIH Automatic Update of Anti-Virus Software Policy² requires that all desktop computers connecting to NIHnet, owned by NIH and including those systems owned by all other parties operated on behalf of NIH have automatic update software used for maintenance of anti-virus software.

CIT's Division of Customer Support (DCS) manages several desktop/patch management tools including agents that provide systems management solutions such as, hardware and software inventory, patch management, and software delivery for CIT commodity desktops and laptops.

Additionally, DCS manages an anti-virus systems management agent used to provide central management of the antivirus software on CIT commodity desktops. DCS' responsibilities are to monitor, configure, and manage the software functionality of the desktop management agent and the anti-virus systems management agent.

DCS coordinates with the CIT Property Accountable Officer (PAO) to identify computers which have reached the end of their life-cycle. The device life-cycle process occurs every three years. These computers have hardware limitations which prevent them from running current versions of the operation

¹ Public Law 107-347 [H.R. 2458], The E-Government Act, Title II — Federal Management and Promote of Electronic Government Services, and Title III — Information Security Federal Information Security Management Act (FISMA) December 17, 2002.

² NIH Automatic Update of Anti-Virus Software Policy, September 2004 outlines requirements for automatic anti-virus updates.

CIT End User Device Policy

systems, may no longer be supported by the vendor with patch updates, and therefore are a security risk and cannot continue to be used.

SCOPE

This policy applies to all CIT end user systems and devices that process NIH information or access NIHnet or NIH system networks. An end user is anyone having access to NIH IT resources including employees, contractors, students, guest researchers, visitors, and others who have an Active Directory account and need access to NIH information systems and applications.

End user devices may include CIT approved and issued desktops/laptops, PDAs, or any other IT devices operated by an end user who has encryption software, antivirus software, patch software and FDCC configurations.

CIT end user devices are defined as the following components listed below (but not limited to):

- Desktop computers
- Laptop computers
- Blackberry
- Personal Digital Assistant (PDA)
- Digital cameras
- External storage devices such as hard drives, flash drives, CD-ROM drives, DVD-ROM drives, and back-up tape drives that connect to the device using either USB connections, Firewire, Serial, Parallel, or components that use or provide wireless transmissions.
- Media that contains or exchanges information with a CIT system end user device, including but not limited to, floppy discs, CDs, DVDs, USBs and other portable devices.

The policy applies whether government-owned systems are operated by NIH, operated on behalf of NIH, or operated by a non-NIH entity using NIH services.

POLICY

End user Requirements

- Personally owned devices are prohibited from being used to process or store NIH data and shall not be used to connect to the NIHnet. All official NIH business must be conducted on Government Furnished Equipment (GFE) and approved Contractor Furnished Equipment.
- In accordance with the CIT Property Business Process, all end users are required to allow all remote computers to be evaluated every twelve months. This is accomplished by physically returning the computer to the IT staff (DCS) or by automated means if feasible (e.g., via a network or VPN connection). This action will be coordinated by a designee within the office or division. This allows CIT property staff to validate the property information and allows DCS to validate that the remote computer is up to date with the latest patches/virus definitions. After the computer has been validated by DCS staff it is eligible for a property pass.

However, the computer must be used to connect at least once a month to the NIHnet and have up to date antivirus and patches. Failure to be in compliance will be assessed by the guideline of

CIT End User Device Policy

non-compliance as listed below, which may include the suspension of the user's NIH login and/or VPN account until the computer is physically brought in and made compliant.

- Personnel in possession of an end user device requiring patches and virus definitions shall not remove or disable the patch management or anti-virus management agent from the end user device.
- Contact the CIT ISSO immediately if an end user device is affected by a vulnerability
- As stated in the CIT Desktop Policy, only Desktop Support staff is permitted to install/build any desktop or laptop computers for use in the production environment. If you need a system built, or re-built, contact the NIH IT Service Desk.
- Desktop or laptop computers should be rebooted at least weekly where practical.
- When connecting remotely through VPN, connect to NIHnet on a monthly basis in order to implement the most recent patches. When connecting to NIHnet, End user devices must remain connected to the network for at least one (1) hour. Where this requirement may affect a business process, the end user must have an approved and documented exception waiver. All remote users that have approved exception waivers are required to reboot the device on a weekly basis.
- If CIT personnel will be on leave or on travel beyond a month and will not be able to connect to their end user device to NIHnet, they must submit an exception request to their CIT division director in advance. In the event of a medical emergency, or unplanned leave, the division director must notify the CIT ISSO of an extended unplanned absence.
- Desktops will not be used to perform application testing. All application testing is to be performed in a secured test environment.
- Users must report unused computers or end of life computers to their local custodial/property officer or to the PAO.
- DCS will not maintain development computers. Users will be responsible for installing patches and virus definitions to development computers. Users must have the Altiris and McAfee agents installed in order for CIT Desktop Security to be able to include the machine in reports.
- Administrative accounts are not to be used to create local accounts with administrative privileges.
- Every end user is required to have a standard (commodity) workstation. Computers needed for anything other than email and standard work functions need to be in a development/test environment.
- For computers not managed by DCS, users must scan all software files intended for CIT use before use regardless of source.
- For computers not managed by DCS, users must scan for viruses immediately after the download process for any type of file downloaded from any external network source.

CIT Division and Office Requirements

- DCS will be responsible for maintaining a desktop/laptop loaner pool. The loaner pool will remain in DCS property but the property pass will be put in the user's name. To reserve a laptop, the user can contact the NIH IT Service Desk or submit a request via web version of Remedy.
- As stated in the CIT Property Business Process, when a person leaves a division, the computer must be:
 - sent back to the supervisor/project officer and reassigned by the custodial/property officer to supervisor/project officer thereby ensuring compliance with the CIT property procedures;
 - "wiped" and updated with the latest patches/virus definitions by DCS; and

CIT End User Device Policy

- re-assigned by the supervisor/project officer or appropriately surplus if the item has reached end of life.
- In accordance with the CIT Desktop policy, computers will be surplus when they are past their lifecycle.

Patch Management

The NIH Enterprise Information Security Plan³ requires that remote users connecting to NIHnet or accessing NIH-related information, whether through GFE or Contractor Furnished Equipment (CFE), meet the Federal Desktop Core Configuration (FDCC) security requirements⁴ through the implementation of patch updates.

DCS is responsible for ensuring that patches are applied to all end user machines in an effective and timely manner. DCS will:

- Maintain an established process for implementing patch management
- Maintain a dedicated team assigned to patch management responsibilities
- Provide the team with necessary training to perform the services
- Implement an automated patch management application that has the ability to perform patch updates on multiple systems; including the ability to implement and, if necessary, reboot the machine remotely to ensure that the patches are installed successfully. The automated process will not interfere with regular end user work requirements. The automated patch management implementation will adhere to the use of agreed assigned ports and protocols.
- Maintain an inventory of all end user machines that connect to, contain, disseminate, share, and alter CIT information. CIT will determine which end user computers are to be included in the inventory.
- Maintain a standard system configuration for end user machines that connect to a system or network within the CIT boundary protection. The implementation will maintain a regular schedule for performing end user machine updates in order to ensure consistency for end users' that may not connect to the network on a regular basis.
- Maintain an inventory consisting of end user machines that connect to NIHnet but are not part of the CIT patch management program.
- Ensure that end user computers are configured with remote rebooting capabilities.
- Run and maintain a monthly report that indicates the level of compliance for all end user computers.

³ NIH Enterprise Information Security Plan, Version 4.0, August 10, 2010.

⁴ http://irm.cit.nih.gov/security/HHS_FDCC_Windows_XP_Standard.doc

Anti-virus Management

CIT end user devices must incorporate implementation of anti-virus software as part of a critical component in the effective management of a security framework. All end user devices must be equipped with anti-virus software that encompasses the ability to provide continuous scanning of applications, data files, email, and devices attached to the end user device. The end user device will also be equipped and configured to install and apply updated anti-virus signature files as they become released by DCS.

DCS is responsible for ensuring that end user computers are updated with the most recent anti-virus definitions in an effective and timely manner. DCS will:

- Ensure end user computers implement malicious code protection that includes a capability for automatic updates.
- Ensure virus definitions are up to date daily.
- Configure automated virus-scanning software to scan end user computers at system start up and “on access”.
- Scan end user computers for spyware.
- Ensure Anti-spyware software is configured to run at start-up and on access.
- Maintain an established process for updating anti-virus definitions.
- Maintain a dedicated team assigned to anti-virus responsibilities.
- Provide the team with necessary training to perform the services.
- Implement an automated anti-virus application that has the ability to perform anti-virus updates on multiple systems. The automated process will not interfere with regular end user work requirements.
- Maintain an inventory of all end user computers that connect to, contain, disseminate, share, and alter CIT information. CIT will determine which end user computers are to be included in the inventory.
- Maintain a regular schedule for performing end user machine updates in order to ensure consistency for end users’ that may not connect to the network on a regular basis.
- Maintain an inventory consisting of end user computers that connect to NIHnet but are not part of the CIT anti-virus update program.
- Implement an alternative to protect the machine in the event an exception is granted.
- Run and maintain a monthly report that indicates the level of compliance for all end user computers.
- Educate CIT staff about the risks of malicious software, available protections against such threats, and the process of reporting suspected incidents.

EXCEPTIONS

While it is accepted that installation of updates from the desktop management agent may not be realistic for all end user devices and circumstances, the CIT Patch Management Policy requires that all end user devices be patched and that patches be installed as soon as reasonably feasible. An exception to patch management or anti-virus management must be approved for devices that for whatever reason cannot be patched.

Exceptions will be addressed on a case by case basis. An exception request should be submitted by the user to their CIT division director. The approved requests (by the division director) must be sent via e-mail to the CIT ISSO (citisso@mail.nih.gov.)

The exception request must include:

- The name of the requestor
- The device(s) that need an exception (machine name, or other identifying information)
- The purpose of the machine
- The impact of the centralized/automated patch management or antivirus software and how it prohibits or interferes with the performance of job duties
- A plan detailing how the device will receive the necessary patches or an explanation of the countermeasures that have been put in place when the patch cannot be applied.

Users must request an exception waiver if there is a circumstance requiring the Desktop Management Agent (patch or anti-virus) to be removed from the end user device. Users granted exception waivers that exclude them from automated updating by the agent(s) will be responsible for maintaining all required patch and anti-virus updates. Additionally, users granted an exception will be responsible for reporting patch/anti-virus status to CIT Desktop Support. Failure to comply may pose a serious risk to the NIH network. As a result, the device will be disconnected from NIHnet.

NON-COMPLIANCE

Non-compliance with any provision of this policy may result in suspending the user's Active Directory account until the remote computer is physically brought in and compliance is verified by DCS. Non-compliance includes but is not limited to blocking updates, not leaving the machine powered on for the automated patching process, and taking any action that prohibits the CIT patch update in any way. For those platforms not covered by the automated patch management program, non-compliance includes not keeping patches up-to-date and/or blocking access to the query system.

Non compliance with any provisions of this policy by users connecting remotely will result in suspension of the end user's VPN account, to avoid possible risk to the NIH network. The account will not be enabled until the computer has been brought to CIT's Desktop Support. Desktop Support will update the patches/virus definitions and verify that the machine is up-to-date.

The appropriate CIT Division Director will be informed prior to restricting the user's access.

INFORMATION AND ASSISTANCE

Requests for further information or other assistance should be directed to the CIT ISSO mailbox citisso@mail.nih.gov.

DEFINITIONS

The following definitions are specific to this policy.

Application – Any data entry, update, query, or report program that processes data for the user.

Availability – The security goal that generates the requirement for protection against –

- Intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data
- Unauthorized use of system resources

Boundary Protection – Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Confidentiality – The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.

Hotfix – Microsoft’s term for a security patch.

Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which:

- (i) requires the use of such equipment; or
- (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Integrity – The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an

CIT End User Device Policy

unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

Malicious Code/Malware - Any code that is intentionally included in or added to software for an unauthorized purpose.

NIHnet – NIHnet is the name used to designate the NIH backbone computer network and all sub networks attached to the NIH backbone.

Operating System – The master control program that runs a computer.

Patch – An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Patch Management – The process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization.

Risk – The probability that a particular threat will exploit a particular vulnerability.

Risk Management – The total process of identifying, controlling, and mitigating information system-related risks. It includes risk assessment; cost benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Security – Information system security is a system characteristic and a set of mechanisms that span the system both logically and physically.

Signature File – A reference file used in IT security software (e.g., anti-virus, intrusion detection system) that contains information that defines specific viruses, worms, and/or computer or network attack signatures. It is updated periodically by the vendor and loaded onto the computer either remotely or manually.

System – A set of IT assets, processes, applications, and related resources that are under the same direct management and budgetary control; have the same function or mission objective; have essentially the same security needs; and reside in the same general operating environment. When not used in this formal sense, the term is synonymous with the term “host”. The context surrounding this word should make the definition clear or else should specify which definition is being used.

System Administrator - A person who manages the technical aspects of a system.

System Owner: Individual with managerial, operational, technical, and often budgetary responsibility for all aspects of an information technology system.

Threat - The potential source of an adverse event.

Trojan Horse - An apparently useful and innocent program containing additional hidden code that allows the unauthorized collection, exploitation, falsification, or destruction of data. A Trojan horse is a program that performs some unexpected or unauthorized, usually malicious, actions, such as displaying messages, erasing files or formatting a disk. A Trojan horse doesn't infect other host files, thus cleaning is not necessary.

User – Individual or (system) process authorized to access an information system.

Virus - A program designed with malicious intent that has the ability to spread to multiple computers or programs. Most viruses have a trigger mechanism that defines the conditions under which it will spread and deliver a malicious payload of some type.

Worm - A type of malicious code particular to networked computers. It is a self-replicating program that works its way through a computer network exploiting vulnerable hosts, replicating and causing whatever damage it was programmed to do.

Vulnerability – A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

REFERENCES

- Public Law 107-347 [H.R. 2458], The E-Government Act, Title II — *Federal Management and Promote of Electronic Government Services*, and Title III — Information Security Federal Information Security Management Act (FISMA) December 17, 2002.
- NIST special publication SP800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.
- The NIST special publication SP800-23 *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.
- NIST special publication SP800-28 Version 2 *Guidelines on Active Content and Mobile Code*, March 2008.
- NIST special publication SP800-70 *Security Configuration Checklists Program for IT Products*, May 2005.
- The NIST special publication SP800-23 *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.
- NIH *Patch Management Policy*, March 2006.
- NIST special publication SP800-40v2 *Creating a Patch and Vulnerability Management Program*, November 2005.
- NIST special publication SP800-61 Rev. 1 *Computer Security Incident Handling Guide*, March 2008.
- NIST special publication SP 800-30 *Risk Management Guide for Information Technology Systems*, July 2002.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Section 8, Revised Transmittal Memorandum No.4, November 30, 2000.
- NIH *Enterprise Information Security Plan*, Version 2.0, May 21, 2008
- NIST special publication SP800-53A *Guide for Assessing the Security Controls in Federal Information Systems*, June 2007.
- NIST special publication SP800-55 *Performance Measurement Guide for Information Security*, July 2008.
- NIST special publication SP800-51 *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.

CIT End User Device Policy

- HHS Federal Desktop Core Configuration (FDCC) Standard, January 2008
- NIH FDCC Waiver Information
- NIH Patch Management Software Policy, March 2006
- NIH Patch Management Guidance, March 2006
- NIH Automatic Update of Anti-Virus Software Policy, September 14, 2004
- CIT Property Business Process, June 30, 2008

EFFECTIVE DATE

This policy is effective as of January 4, 2011.