



Workstation Security Good Practice Guide

August 2009



contents

<u>1</u>	<u>Introduction to Good Practice Guides</u>	<u>3</u>
<u>2</u>	<u>Workstation Security Overview</u>	<u>3</u>
<u>3</u>	<u>Workstation Security Good Practice Guidelines</u>	<u>3</u>
3.1	Workstation Use	3
3.2	Workstation Configuration	5
<u>4</u>	<u>Appendix A: Definitions</u>	<u>6</u>
<u>5</u>	<u>Appendix B: Checklists</u>	<u>7</u>
5.1	Good Practice Checklist	7
<u>6</u>	<u>Document Control</u>	<u>9</u>

1 INTRODUCTION TO GOOD PRACTICE GUIDES

This document is a good practice guide concerning workstation security within the various international agricultural research centers that are supported by the Consultative Group for International Agricultural Research (CGIAR). This guide forms part of the CGIAR-wide baseline ICT Security good practice set. The target audience for the good practice guides are all centers affiliated with CGIAR, and in particular, the IT teams within each center.

The good practice set does not contain mandatory requirements that centers are required to implement. Instead, it outlines a number of good practices with respect to enterprise ICT security. The prudence of implementing specific good practices identified in this guide will depend on the risk profile associated with the ICT environment in each center. A set of checklists is provided at the end of this guide to assist with the process of determining those good practices which will be relevant depending on the risk profile of each center for each area of ICT security.

The initial ICT Security and Acceptable Use good practice set has been prepared in consultation with the CGIAR center IT community under a process jointly managed by the CGIAR ICTKM Program and the CGIAR Internal Auditing Unit (IAU). This guide draws on the results of work undertaken in the CGIAR Enterprise Security and Business Continuity Project; additional inputs from the IT community, internal auditors, and from SIFT Pty Ltd, an information security and risk management services firm which assisted in the preparation of these guides. The ICTKM and IAU units will coordinate future updates in consultation with the CGIAR center IT community.

2 WORKSTATION SECURITY OVERVIEW

Engaging in good practices with respect to the use of workstations in CGIAR centers (whether these are in the form of desktop computers or laptops) is crucial. While these devices are highly powerful business tools used for processing and exchanging business information that are capable of enhancing work productivity, if they are deployed insecurely they can provide a point through which the ICT infrastructure of CGIAR centers can be compromised.

Risks that are relevant to workstations include physical theft of or damage to CGIAR workstations or data assets, infection by viruses or other malware, and unauthorised access and use of confidential information (such as non-public research data or payroll details). This document identifies a number of good practices to facilitate the secure deployment and management of workstations within CGIAR centers.

3 WORKSTATION SECURITY GOOD PRACTICE GUIDELINES

3.1 Workstation Use

Encryption of Sensitive Data on Workstations

- 3.1.1 It is recommended that CGIAR centers maintain a policy that any sensitive CGIAR data stored on laptops should be protected with encryption to minimise the possibility of it being accessed by unauthorised parties. It may in some instances be considered prudent to also use encryption to encrypt sensitive data on desktop machines. The decision as to what constitutes 'sensitive data' in the context of a particular CGIAR center should be defined by center. Examples of encryption algorithms that can be used for this purpose are provided below:

Algorithm	Minimum Strength	Notes
3DES	3 x 56 bit keys	3DES should not be used in Electronic Code Book (ECB) mode.
AES	128 bits	AES should not be used in Electronic Code Book (ECB) mode

Clear Screen Requirements

It is recommended that CGIAR centers maintain a policy which contains the following clear screen requirements:

- 3.1.2 When not working at their computer, it is recommended that staff of CGIAR centers 'lock' their computer, thereby ensuring a password is required to access the workstation again.
- 3.1.3 It is recommended that all CGIAR workstations are configured to automatically lock the computer and run a screensaver application after ten (10) minutes of inactivity. When users have finished using a CGIAR workstation, they should either log off or shut down the computer.

Secure Data Deletion

It is recommended that CGIAR centers maintain a policy which contains the following secure data deletion requirements:

- 3.1.4 Workstations storing CGIAR data should be subjected to a low-level format when they are:
 - Transferred between individuals and the workstation stored sensitive data
 - Decommissioned and the hardware is to be used by another department or for a different business purpose
 - Decommissioned and the hardware is to be disposed of

In all cases a secure wipe of the hard disk drive should also be carried out with appropriate utility software (an example of a secure wipe tool Active@Killdisk). This is to ensure that no confidential data is compromised and no data remaining on the computer system exposes the recipient to charges of inappropriate usage.

- 3.1.5 Removable media such as USB storage devices should be securely erased and/or formatted (as specified in 3.1.4) where those devices store CGIAR data that is no longer required for business purposes.

Secure Disposal

- 3.1.6 It is recommended that CGIAR centers maintain a policy that, when disposing of media such as Floppy disks, CD-ROMs, USB drives or similar that contain sensitive CGIAR data, if such media cannot be reused or recycled, these should be destroyed by breaking the media to prevent further use. If possible the media should be erased before breakage to ensure the data has been removed.

Malicious Software Protection

It is recommended that CGIAR centers maintain a policy which contains the following malicious software protection requirements:

- 3.1.7 CGIAR center staff members should not intentionally install, run, copy, store, distribute or develop any form of malicious software code. Malicious software includes any software that is intended to conduct actions without authorisation, including stealing, modifying or destroying data, bypassing access restrictions or hijacking system resources.
- 3.1.8 All workstations connected to CGIAR networks – either directly or via remote access – should have effective and up-to-date virus protection measures in place.
- 3.1.9 All CGIAR workstations should have the latest operating system and application security patches and updates applied (either by the person who predominantly uses each workstation, or the IT team) prior to being connected to center networks, and when subsequent patches become available.
- 3.1.10 Staff of CGIAR research centers should not disable or otherwise modify the behaviour of installed anti-virus software used on workstations.
- 3.1.11 All anti-virus software installed on workstations in CGIAR centers should be actively managed to ensure that the latest software updates and virus signatures are installed. The anti-virus library definitions should be updated at least once per day.
- 3.1.12 All removable media, including floppy discs, CDs, and DVDs, and also USB-based devices such as “thumb drives” and mp3 players should be scanned by virus scanning software prior to accessing any files stored on these media using CGIAR workstations.

3.2 Workstation Configuration

Configuration Requirements

It is recommended that CGIAR centers maintain a policy which contains the following workstation configuration requirements:

- 3.2.1 Workstations (whether desktops or laptops) and associated operating system within CGIAR centers should incorporate the following settings where relevant:
 - Configure BIOS to boot from the local hard drive, and, in the case of desktops, prevent booting from CD or other devices
 - Set a BIOS password to protect BIOS information
 - Install personal firewall software on workstations that have Internet access and where center-level controls such as web proxy and firewalls are either not in place or not considered sufficient. The circumstances in which this firewall should be enabled for use or disabled may vary between CGIAR centers; staff should ensure they are aware of the usage policy implemented by their center.
 - Disable unused system utilities, local services and processes in the operating system
 - Users must terminate their active sessions when they are finished using a workstation at that particular instance
 - Enable a logon banner containing a warning of possible consequences from misuse of workstations within CGIAR centers
- 3.2.2 Users of CGIAR workstations should not be permitted to change the network configuration details of a workstation (this includes IP address, names and workgroup/domain assignment) without first seeking permission from the center IT manager. Where users are travelling away from their primary center/office, and such changes are required for functionality purposes, these changes are permitted.
- 3.2.3 CGIAR staff should ensure that their workstation is kept up to date through the installation of the latest service packs, operating system patches and hotfixes. Depending on the center's IT support

structure, such updates may be the responsibility of either individual staff, or the IT team. If the responsibility of individual staff, awareness training and support should be provided.

- 3.2.4 All non-center ICT maintenance personnel should sign a non-disclosure agreement (NDA) before being permitted access to workstations. Alternatively, an NDA entered into with the company employing the maintenance personnel (if relevant) that also applies to its employees would be considered sufficient. Any non-Center ICT maintenance personnel should be escorted and closely monitored while they are in Center's facility.
- 3.2.5 Workstations should, where possible, be secured by being attached to a fixed point via a metallic cable, often known as a 'Kensington Cable', or another appropriate anti-theft mechanism.
- 3.2.6 All workstations within CGIAR centers should only be used by the authorized user of that workstation unless that user, or the user's supervisor or team leader, gives permission for another party to use the workstation.
- 3.2.7 Proper notification through email or memo to a center's IT manager should be made before any physical transfer of a desktop is made from one location to another within a center.
- 3.2.8 Users, including outsourced personnel, contractors, and consultants should not install any software or hardware that could potentially be used to compromise the security of workstations, unless there is a legitimate business purpose for this. These might include password hacking tools, network discovery or packet capture tools, and the like.

Standard Operating Environment (SOE)

It is recommended that CGIAR centers maintain a policy which contains the following standard operating environment requirements:

- 3.2.9 It is recommended that all workstations within CGIAR centers have an associated common SOE build. Any deviations to the SOE for a particular workstation should first be approved by the IT manager.
- 3.2.10 After an SOE build is installed on a CGIAR workstation, all necessary operating system patches and service packs should be installed prior to the workstation being deployed
- 3.2.11 Installation of additional software on workstations in CGIAR centers should only occur after it is first verified that the software has been obtained from a reputable source and the software installation files are scanned for viruses.

4 APPENDIX A: DEFINITIONS

BIOS: The Basic Input Output System refers to software code that is designed to always run when a computer is first switched on. It typically tests and initializes system devices so that other software such as the operating system can commence running.

Format: A format involves preparing a storage medium such as a hard disk drive for reading and writing of data. Often, these occur in the form of a 'high-level' format which does not erase any data on the storage medium but simply tests the disk to make sure all sectors are reliable, marks bad sectors and creates new internal address tables that it later uses when new information is written to or access from the disk. A low-level format, conversely, involves the entire storage medium being written with binary zeros which results in the removal of all partitions, clusters, boot sectors and data.

Personal Firewall: Refers to a software application, which, like a dedicated hardware firewall device, inspects network traffic passing through it, and denies or permits passage based on a set of rules (for example, based on the software application that is trying to send the traffic from a workstation).

Screensaver: An animated image that is activated on a PC Workstation/Notebook that displays when no user activity has been sensed for a certain time.

Sensitive Information: Information assets classified as restricted, confidential or for internal use.

Standard Operating Environment (SOE): Refers to a standard implementation within an organisation of an operating system and an associated set of software applications. SOEs are typically implemented using a standard hard disk image that can be deployed across several workstations in an organisation.

System Utility: A specialized program designed for more technical users as a tool, or set of tools for checking the system, housekeeping, monitoring system health status or repairing files.

Viruses: An unauthorized program that replicates itself, attaches itself to other programs and spreads onto various data storage media or across the network. The symptoms of virus infection include much slower computer response time, inexplicable loss of files, changed modification data for files, increased file sizes, and a possible total failure of the infected computer.

Workstation: A personal computer that includes both desktop and laptop/notebook computers used to store information or access information systems of a center.

5 APPENDIX B: CHECKLISTS

The following checklists are designed to assist CGIAR centers that wish to adopt any or all of the good practices listed in this document. The checklists should be used by a center when attempting to assess their level of current adherence with the guidelines listed in this document. This will allow any gaps with good practices to be identified, after which centers can assess whether addressing those gaps will be feasible.

5.1 Good Practice Checklist

Guideline Number	Guideline	Tick if center currently adhere to this guideline
Section 3.1 – Workstation Use		
Encryption of Sensitive Data on Workstations		
3.1.1	▪ Sensitive data stored on laptops is encrypted	<input type="checkbox"/>
Clear Screen Requirements		
3.1.2	▪ Staff lock workstations when not working at computer	<input type="checkbox"/>
3.1.3	▪ Workstations configured to automatically lock screen after 10 minutes inactivity, and users log off or shut down computers after finishing use.	<input type="checkbox"/>
Secure Data Deletion		
3.1.4	▪ Workstations storing CGIAR data are subjected to low-level format and secure wipe in situations identified in 3.1.4	<input type="checkbox"/>
3.1.5	▪ Removable media securely erased / formatted where they store CGIAR data no longer required for business	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adhere to this guideline
	purposes	
Secure Disposal		
3.1.6	<ul style="list-style-type: none"> Removable media containing CGIAR data that are disposed of should be destroyed by breaking media to prevent use. 	<input type="checkbox"/>
Malicious Software Protection		
3.1.7	<ul style="list-style-type: none"> Staff do not intentionally install/run/copy/store/distribute/develop malicious software code using CGIAR workstations 	<input type="checkbox"/>
3.1.8	<ul style="list-style-type: none"> Workstations connected to CGIAR networks have effective and updated anti-virus software installed 	<input type="checkbox"/>
3.1.9	<ul style="list-style-type: none"> CGIAR workstations have the latest patches and updates applied prior to being connected to center networks 	<input type="checkbox"/>
3.1.10	<ul style="list-style-type: none"> Staff do not disable/modify the behaviour of installed anti-virus software 	<input type="checkbox"/>
3.1.11	<ul style="list-style-type: none"> Anti-virus software on CGIAR workstations managed to ensure latest updates/signatures installed (library definitions updated daily) 	<input type="checkbox"/>
3.1.12	<ul style="list-style-type: none"> Removable media are virus scanned prior to files stored on them being accessed using CGIAR workstations 	<input type="checkbox"/>
Section 3.2 – Workstation Configuration		
Configuration Requirements		
3.2.1	<ul style="list-style-type: none"> Workstations incorporate settings identified in 3.2.1 	<input type="checkbox"/>
3.2.2	<ul style="list-style-type: none"> Users of workstations are not permitted to change network configuration details of a CGIAR workstation without permission from the IT manager 	<input type="checkbox"/>
3.2.3	<ul style="list-style-type: none"> CGIAR Workstation operating systems kept up to date 	<input type="checkbox"/>
3.2.4	<ul style="list-style-type: none"> Non-center ICT maintenance personnel sign an NDA before being given access to workstations. Alternatively NDA entered into with company employing the maintenance personnel Non-center ICT maintenance personnel escorted/closely monitored while in Center's facility. 	<input type="checkbox"/>
3.2.5	<ul style="list-style-type: none"> Workstations are secured by attachment to a fixed point or other appropriate anti-theft mechanism 	<input type="checkbox"/>
3.2.6	<ul style="list-style-type: none"> Workstations only used the authorized user unless permission is given for another party to use a particular workstation 	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adhere to this guideline
3.2.7	<ul style="list-style-type: none"> Proper notification given to center IT manager before physical transfer of a desktop is made from one location to another 	<input type="checkbox"/>
3.2.8	<ul style="list-style-type: none"> Users of workstations do not install any software or hardware that could compromise security unless there is a legitimate business purpose 	<input type="checkbox"/>
Standard Operating Environment (SOE)		
3.2.9	<ul style="list-style-type: none"> All workstations within CGIAR centers have a common SOE build, with deviations for a workstation approved by the IT manager 	<input type="checkbox"/>
3.2.10	<ul style="list-style-type: none"> After installation of SOE build on CGIAR workstation, all necessary operating system patches and service packs are installed 	<input type="checkbox"/>
3.2.11	<ul style="list-style-type: none"> Installation of additional software on workstations in CGIAR centers occurs only after verification that software is from reputable source and where necessary, virus scanned 	<input type="checkbox"/>

6 DOCUMENT CONTROL

Version Control Log

Version	Description	Date
1.00	Third revision following client feedback	19 Jun 2009
1.10	First published edition	24 Aug 2009

Copyright & Legal

This guideline, prepared specifically for **Consultative Group for International Agricultural Research**, is the intellectual property of SIFT Pty Limited. When finalised, SIFT Pty Limited authorises CGIAR to reproduce or disseminate this guideline as necessary to further the aims and goals of CGIAR, under a Creative Commons Attribution-Noncommercial-Share Alike 2.5 Australia License

In no event shall SIFT Pty Limited be liable to anyone for special, incidental, collateral, or consequential damages arising out of the use of this information.

SIFT® is a Registered Trademark of SIFT Pty Ltd. Many designations used by manufacturers and sellers to distinguish their products are claimed as trademarks or other proprietary rights. Where designations appear, and when the editorial staff were aware of a claim, the designations have been shown. Other trademarks, registered trademarks, and service marks are the property of their respective owners.

Copyright © 2009 SIFT Pty Limited. Originated in Australia.

The first published version provided by SIFT Pty Limited, and future versions with modifications made by the CGIAR, as coordinated through the CGIAR ICTKM Program and the CGIAR Internal Auditing Unit, are being distributed by these Units in accordance with the terms of the above license, which can be found at <http://creativecommons.org/licenses/by-nc-sa/2.5/au/> "