



---

# Internet Security Good Practice Guide

August 2009



contents

<b><u>1</u></b>	<b><u>Introduction to Good Practice Guides</u></b>	<b><u>3</u></b>
<b><u>2</u></b>	<b><u>Internet Security Overview</u></b>	<b><u>3</u></b>
<b><u>3</u></b>	<b><u>Internet Security Good Practice Guidelines</u></b>	<b><u>4</u></b>
<b><u>4</u></b>	<b><u>Appendix A: Definitions</u></b>	<b><u>6</u></b>
<b><u>5</u></b>	<b><u>Appendix B: Checklists</u></b>	<b><u>6</u></b>
5.1	Good Practice Checklist	6
<b><u>6</u></b>	<b><u>Document Control</u></b>	<b><u>8</u></b>

## **1 INTRODUCTION TO GOOD PRACTICE GUIDES**

---

This document is a good practice guide concerning Internet 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 and Acceptable Use 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 and acceptable use. 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 based on the risk profile of each center.

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 INTERNET SECURITY OVERVIEW**

---

The Internet provides access to an array of information, resources and services that provide potential opportunities and benefits which aid and support the work of CGIAR research centers. However, if Internet use within centers is not securely managed, it can expose those centers to risks at both a technical level (with potential damage being caused to ICT infrastructure) and an operational level (with misuse of Internet resources leading to possible reputational damage to centers and a loss in productivity).

These guidelines establish a set of good practice measures that CGIAR centers should adopt to ensure a sufficient level of protection is provided in response to the security risks presented by Internet use within centers.

## 3 INTERNET SECURITY GOOD PRACTICE GUIDELINES

---

### Authentication

- 3.1.1 CGIAR policies should require all staff in CGIAR centers to provide authentication credentials before being granted Internet access. These credentials are to be presented in addition to any initial authentication required to connect to the center network (e.g. via active directory). Note that in some instances this authentication process can be performed transparently (ie through 'single sign on') depending on the technology used. For example, a proxy server can be configured to authenticate users requiring Internet access using Active Directory.

Note that access by visitors to the Internet is covered in the Network Infrastructure Security Good Practice Guide.

### Filtering of Internet Access

- 3.1.2 It is recommended that centers include policy requirements for all Internet traffic in CGIAR centers (inbound and outbound) to pass through an anti-virus gateway. If this is not possible, then at a minimum, up-to-date anti malware software should be installed and running on center workstations with Internet connectivity.

### External Connections

- 3.1.3 It is recommended that CGIAR centers should have a policy requiring workstations connected to CGIAR center networks not to be used by staff to establish a separate direct connection (for example, through a modem, wireless connection or similar) to other external networks (including the Internet).
- 3.1.4 CGIAR center policies should include a requirement that workstations connected to CGIAR center networks via a VPN connection must not utilise split tunnelling; in particular, all internet access in these situations should be provided through the VPN, rather than through a separate, direct Internet connection.
- 3.1.5 It is recommended that center policies include a requirement stating that under no circumstances should external connections be established that allow unauthorised parties to gain access to the internal networks of CGIAR centers. More detail on specific guidelines regarding this requirement are available in the Network Infrastructure Security Good Practice Guide.
- 3.1.6 CGIAR center policies should include controls limiting access to internal networks. Access to internal networks from the Internet (for example, via VPN) should only be allowed for users that have been approved for such access by the center's designated IT staff. Ideally, authentication for VPN users should use a minimum of two factors.

### Internet Services

- 3.1.7 CGIAR centers should establish the standard Internet services to be provided to users, such as:
- Email
  - Internet Browsing
  - Access to the Center's research website and intranets

In addition, access to additional services may be provided with the approval of each center's IT manager.

- 3.1.8 It is recommended that center policies include a requirement for creating logs that record all requests (both inbound and outbound) for Internet services. The relevant policy should also require the generated audit logs to be reviewed on a daily basis by the designated IT staff of the center. Logging functionality can be provided through the use of automated software tools.
- 3.1.9 FTP servers hosted by CGIAR centers that accept connections from the Internet should be located in a DMZ. These FTP services can accept anonymous connections but in these circumstances read-only access to the server should be all that is permitted, and access to content on the server should be restricted to non-confidential information.
- 3.1.10 All FTP and SSH sessions, whether to servers hosted externally or hosted by CGIAR centers should be logged and monitored

### Internet Facing Firewalls

All firewalls located in CGIAR centers should be configured in accordance with the configuration guidelines and policy recommendations provided in the Network Infrastructure Security Good Practice Guide. In addition, the following guidelines apply specifically to Internet facing firewalls:

- 3.1.11 Logging of all firewall related activities (including maintenance activities) should be performed at all times
- 3.1.12 An explicit "deny all" rule should be implemented as the last rule in the filtering configuration of Internet facing firewalls to allow for logging of rejected connection attempts to any relevant Internet services
- 3.1.13 Backup firewall configuration files stored offline should only be viewable by designated IT staff.
- 3.1.14 Internet facing firewalls should use Network Address Translation (NAT) where possible.

### Password Protected Web Pages

- 3.1.15 CGIAR centers should make clear to staff, through orientation materials, network user guides and other permanently available information, that when using web pages that require a user ID and password for access, it is recommended that they do not use the same ID and password as is used for access to any internal systems, networks or applications with CGIAR centers.

## 4 APPENDIX A: DEFINITIONS

---

**Authentication:** The process of identifying an individual, usually based on a username and password. Authentication is distinct from authorisation, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access privileges of the individual. Three types of factors can be used to provide authentication: a) something you know (e.g. a password), b) something you have (e.g. a certificate or card), and c) something you are (e.g. a fingerprint or retinal pattern). Using any two in conjunction is known as two-factor authentication.

**Email:** The electronic transmission of information through a mail protocol such as Simple Mail Transfer Protocol (SMTP).

**Encryption:** The process by which data is re-arranged into an unreadable or unintelligible form for confidentiality, transmission or other security purposes

**File Transfer Protocol (FTP):** A standard Internet protocol that is used to exchange files between computers on the Internet. FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to download programs and other files to your computer from other servers.

**Firewall:** Security device (either hardware or software based) that is used to restrict access in communication networks. They prevent computer access between networks, or networks and applications, and only allow access to services that are expressly registered. They also keep logs of all activity, which may be used in investigations.

**Network Address Translation (NAT):** A feature typically employed by firewalls/routers that interface between external and internal facing networks. NAT allows the allocation of multiple IP addresses to machines located in internal networks, without the existence of these machines being revealed on the external network. Instead, only a single or small number of IP addresses are advertised to the external network, which are then mapped by the router/firewall to the machines on the internal network.

## 5 APPENDIX B: CHECKLISTS

---

The following checklist is designed to assist CGIAR centers that wish to adopt any or all of the good and better 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 adheres to this guideline
Section 3 – Internet Security Good Practices		
Authentication		
3.1.1	<ul style="list-style-type: none"> <li>▪ Staff provide authentication credentials before being granted internet access</li> </ul>	<input type="checkbox"/>
Filtering of Internet Access		

Guideline Number	Guideline	Tick if center currently adheres to this guideline
3.1.2	<ul style="list-style-type: none"> <li>Internet traffic passes through anti-virus gateway or workstations with Internet connectivity use anti-malware software</li> </ul>	<input type="checkbox"/>
<b>External Connections</b>		
3.1.3	<ul style="list-style-type: none"> <li>Workstations connected to internal networks are not used by staff to establish separate direct connections to external networks</li> </ul>	<input type="checkbox"/>
3.1.4	<ul style="list-style-type: none"> <li>Workstations connected to internal networks via VPN do not utilise split tunneling</li> </ul>	<input type="checkbox"/>
3.1.5	<ul style="list-style-type: none"> <li>Unauthorised parties not able to gain access to internal networks via external connections</li> </ul>	<input type="checkbox"/>
3.1.6	<ul style="list-style-type: none"> <li>Internal network access via VPN etc only allowed for approved users. Authentication for VPN users uses a minimum of 2 factors if possible.</li> </ul>	<input type="checkbox"/>
<b>Internet Services</b>		
3.1.7	<ul style="list-style-type: none"> <li>Access to web browsing, email, internal website and intranets provided</li> <li>Access to other services provided based on approval of center IT manager.</li> </ul>	<input type="checkbox"/>
3.1.8	<ul style="list-style-type: none"> <li>Logs created that record all requests for Internet services, which are reviewed daily by designated IT staff</li> </ul>	<input type="checkbox"/>
3.1.9	<ul style="list-style-type: none"> <li>FTP servers hosted by centers should be located in a DMZ.</li> <li>Where anonymous FTP connections allowed, read only access should be all that is permitted, and access should only be allowed to non-confidential information.</li> </ul>	<input type="checkbox"/>
3.1.10	<ul style="list-style-type: none"> <li>FTP and SSH sessions logged and monitored</li> </ul>	<input type="checkbox"/>
<b>Internet Facing Firewalls</b>		
3.1.11	<ul style="list-style-type: none"> <li>Logging of firewall related activities performed at all times</li> </ul>	<input type="checkbox"/>
3.1.12	<ul style="list-style-type: none"> <li>Deny all rule implemented as last rule in filtering configuration</li> </ul>	<input type="checkbox"/>
3.1.13	<ul style="list-style-type: none"> <li>Backup configuration files stored offline viewable by designated IT staff</li> </ul>	<input type="checkbox"/>
3.1.14	<ul style="list-style-type: none"> <li>Firewalls use Network Address Translation where possible</li> </ul>	<input type="checkbox"/>
<b>Password Protected Web Pages</b>		

Guideline Number	Guideline	Tick if center currently adheres to this guideline
3.1.15	<ul style="list-style-type: none"> <li>▪ Staff do not use passwords and user ID for web pages that are also used to access internal systems/networks/applications</li> </ul>	<input type="checkbox"/>

## 6 DOCUMENT CONTROL

---

### Version Control Log

Version	Description	Date
1.00	Third revision from 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/>