



Sensible Use of Bandwidth Good Practice Guide

August 2009



contents

<u>1</u>	<u>Introduction to Good Practice Guides</u>	<u>3</u>
<u>2</u>	<u>Sensible Use of Bandwidth Overview</u>	<u>3</u>
<u>3</u>	<u>Applicability of Sensible Use of Bandwidth Good Practice Guidelines</u>	<u>3</u>
<u>4</u>	<u>Sensible Use of Bandwidth Good Practice Guidelines</u>	<u>4</u>
4.1	Bandwidth Accountability & Monitoring	4
4.2	Bandwidth Usage Limitations	4
4.3	Disciplinary Processes	4
<u>5</u>	<u>Bandwidth Management Controls</u>	<u>5</u>
5.1	Internal Bandwidth Prioritisation – Good Practice	5
5.2	Internal Bandwidth Prioritisation – Better Practice	5
<u>6</u>	<u>Appendix A: Definitions</u>	<u>6</u>
<u>7</u>	<u>Appendix B: Checklists</u>	<u>7</u>
7.1	Good Practice Checklist	7
<u>8</u>	<u>Document Control</u>	<u>8</u>

1 INTRODUCTION TO GOOD PRACTICE GUIDES

This document is a good practice guide concerning bandwidth usage in 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 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 SENSIBLE USE OF BANDWIDTH OVERVIEW

Ensuring that bandwidth is utilised and managed appropriately helps to maintain the operative efficiency of CGIAR centers communication and research. Inefficient Internet use can cost CGIAR centers significant amounts in network resources, financing and lost productivity.

This document outlines the recommended restrictions and usage practices surrounding network bandwidth management in CGIAR centers.

3 APPLICABILITY OF SENSIBLE USE OF BANDWIDTH GOOD PRACTICE GUIDELINES

The recommendations outlined in this document will be most applicable to low-bandwidth sites. For facilities with the following attributes:

- High bandwidth connections; and/or
- No usage quotas or limits from Internet Service Providers; and
- No excess-usage costs; and
- No issues with quality of service; then

a decision from the IT department can be made regarding which sections of this document do not apply.

4 SENSIBLE USE OF BANDWIDTH GOOD PRACTICE GUIDELINES

4.1 Bandwidth Accountability & Monitoring

- 4.1.1 Center policies should identify users as being responsible for all Internet traffic generated by their workstation on the CGIAR network.
- 4.1.2 It is recommended that center policies require bandwidth usage to be monitored and reviewed as determined on a per-user or per-system basis. Where specific limits have been set for a center, quotas should be provided to users to assist them in ensuring total bandwidth usage (including both traffic into or out of the CGIAR center's network) is managed appropriately.
- 4.1.3 If bandwidth quotas are used, users should be provided with a means to review their usage and performance against the quota.

4.2 Bandwidth Usage Limitations

- 4.2.1 Center policies should include bandwidth quota requirements determined by the center and communicated to center staff. To enforce bandwidth quotas, proxy based solutions readily available on the Internet are recommended (for example RhinoSoft AllegroSurf – www.allegrosurf.com).
- 4.2.2 It is recommended that where users require considerable bandwidth for services such as streaming media, downloading large files, or performing system updates, the user should follow their center's policy on the appropriate timing for such activities (for example downloading large files overnight rather than during the business day, and pausing the download if it flows over to the next business day). Alternatively, users can approach their research leaders, operations leaders as well as the IT team to seek permission or assistance in downloading the files as soon as possible. Transfer limits which limit bandwidth throughput may be utilised for low priority business hour downloads to ensure that other business bandwidth usage can continue unaffected.
- 4.2.3 CGIAR centers should ensure policies require restriction of resource-heavy services in cases where they are not utilised for center-related purposes.
- 4.2.4 CGIAR center should maintain a policy which requires setup of appropriate file size limits for upload or download over center services or protocols. For example:
 - Don't send an email with attachments over 5MB
 - Don't download a file over 50MB through any protocol without asking and gaining approval from the center's IT department

Note that these size limits are indicative only; individual centers should determine approach limits based on bandwidth/quota limits and research requirements.

E-mail size constraints can be set using parameters in Center mail systems. It is recommended that where a mail server denies emails due to size constraints, that it returns an email to the sender notifying them that the email was rejected for this reason. This applies to both outgoing email from internal senders or incoming email from external senders.

4.3 Disciplinary Processes

- 4.3.1 CGIAR center policies should outline a disciplinary process applicable to when users abuse bandwidth, providing for issuing a warning initially, followed by further action if the behavior persists.

5 BANDWIDTH MANAGEMENT CONTROLS

Internal Bandwidth prioritisation controls have been included in this document to assist centers in the management of bandwidth use to ensure the quality and availability of bandwidth resources to high prioritised systems. It is recommended that these controls are included in relevant CGIAR center policies.

5.1 Internal Bandwidth Prioritisation – Good Practice

- 5.1.1 Bandwidth is to be prioritised for center related usage, such as performing research tasks and operations. If necessary, non-center related access to bandwidth may be curtailed in order to ensure center data can continue to be sent / received.
- 5.1.2 There are some cases where broadband enabled services such as VoIP may exist on shared bandwidth and data environments. Centers should maintain policies and procedures to ensure that users do not utilise large amounts of bandwidth if that could disrupt the availability of these services.

5.2 Internal Bandwidth Prioritisation – Better Practice

- 5.2.1 CGIAR centers can utilise Quality of Service (QoS) mechanisms in place to manage the priorities of bandwidth utilisation for different services, users, applications etc. over internal network connections, to ensure steady throughput for these connections. It is recommended that these are utilised, and that any traffic related to core center operations should be prioritised. Any non center related bandwidth should be deprioritised.

Implementing QoS¹ will depend on the services that it is being introduced for. For example a VoIP system will usually have QoS configuration capability available from the management console.

Administrators should determine which applications require QoS controls, and prioritise which are the most critical for the center. Following this, class lists should be setup listing these priorities, then applied to all infrastructure that will be supporting the QoS services (routers, switches, etc).

¹ Further information regarding implementation of QoS is readily available on the Internet (eg. <http://www.ciscopress.com/articles/article.asp?p=471096>).

6 APPENDIX A: DEFINITIONS

Bandwidth: Refers to the amount of data throughput going into or out of a network. In this case, the amount of data flow between the Internet and the CGIAR center's network.

Peer to peer technology: Computer network connections where hosts such as workstations or personal computers can connect directly to one another, without the need for servers inbetween.

Quality of Service (QoS): Quality of Service features provide the ability to prioritise bandwidth utilisation across a network, over data sources, data types, users and other network criteria.

7 APPENDIX B: CHECKLISTS

The following checklists are 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 and better practices to be identified, after which centers can assess whether addressing those gaps will be feasible.

7.1 Good Practice Checklist

Guideline Number	Guideline	Tick if center currently adhere to this guideline
Section 4.1 – Bandwidth Accountability & Monitoring		
4.1.1	<ul style="list-style-type: none"> Users held responsible and accountable for all Internet traffic generated by their workstation 	<input type="checkbox"/>
4.1.2	<ul style="list-style-type: none"> Usage is monitored and reviewed on a per-user or per-system basis 	<input type="checkbox"/>
4.1.3	<ul style="list-style-type: none"> If bandwidth quotas are used, users should be provided with a means to review their usage and performance against the quota 	<input type="checkbox"/>
Section 4.2 Bandwidth Usage Limitations		
4.2.1	<ul style="list-style-type: none"> Bandwidth quotas for each user should be determined by CGIAR centers and communicated to CGIAR center staff 	<input type="checkbox"/>
4.2.2	<ul style="list-style-type: none"> Users with heavy bandwidth resource requirements (streaming, large downloads etc) should time activities outside of center peak usage 	<input type="checkbox"/>
4.2.3	<ul style="list-style-type: none"> Restrict a number of specific resource-heavy services in cases where they are not utilised for center-related purposes (p2p, music / video streaming) 	<input type="checkbox"/>
4.2.4	<ul style="list-style-type: none"> Set appropriate file size limits for upload or download over center services or protocols 	<input type="checkbox"/>
Section 4.3 Disciplinary Processes		
4.3.1	<ul style="list-style-type: none"> Utilise disciplinary process where users exceed bandwidth usage quotas 	<input type="checkbox"/>
Appendix A: Bandwidth Prioritisation – Good Practice		
5.1.1	<ul style="list-style-type: none"> Bandwidth is to be prioritised for center use. If necessary, end-user access to bandwidth may be curtailed in order to ensure center data can continue to be sent / received 	<input type="checkbox"/>
5.1.2	<ul style="list-style-type: none"> Centers should ensure that users do not utilise large amounts of bandwidth if that could disrupt the availability 	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adhere to this guideline
	of these services	
Appendix A: Bandwidth Prioritisation – Better Practice		
5.2.1	<ul style="list-style-type: none"> ▪ Utilise Quality of Service mechanisms to control network bandwidth priorities 	<input type="checkbox"/>

8 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/> "