



Email Management and Security Good Practice Guide

August 2009



contents

<u>1</u>	<u>Introduction to Good Practice Guides</u>	<u>3</u>
<u>2</u>	<u>Email Management and Security Overview</u>	<u>3</u>
2.1	Understanding 'Good' and 'Better' Practice	4
<u>3</u>	<u>Email Management and Security Good Practice</u>	<u>5</u>
3.2	Mobile Device Emails	7
<u>4</u>	<u>Email Management and Security Better Practice</u>	<u>7</u>
4.1	Encryption of Emails	7
<u>5</u>	<u>Appendix A: Definitions</u>	<u>8</u>
<u>6</u>	<u>Appendix B: Checklists</u>	<u>8</u>
6.1	Good Practice Checklist	8
<u>7</u>	<u>Document Control</u>	<u>10</u>

1 INTRODUCTION TO GOOD PRACTICE GUIDES

This document is a good practice guide concerning the secure use and management of e-mail 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 depending 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 EMAIL MANAGEMENT AND SECURITY OVERVIEW

Engaging in good practices with regard to the security management of e-mail is crucial – whilst the use of e-mail as a medium of communication has become ubiquitous, it is inherently an insecure form of communication. E-mails can be easily intercepted and read by those determined to know their content. While much of the work of the CGIAR centers is inherently of a public good nature, there will be many cases where information is of a nature that it should be closely held by a center, either indefinitely or for a certain period of time. For this reason, it is imperative that sensitive information is not sent or received via e-mail by staff within CGIAR centers unless regard is had to the good practices identified in this document. Specific risks that may eventuate if email usage and security is not managed properly include:

- **Unauthorised information disclosure** – The use of e-mail within CGIAR centers introduces the risk of both accidental and malicious information disclosure through:
 - Mismanaged e-mail recipient lists that result in the unintended delivery of e-mails to certain 3rd parties;
 - Eavesdropping attacks in which a fraudulent party is able to intercept and examine the contents of e-mails containing sensitive information; or
 - Deliberate or accidental forwarding by staff of sensitive information such as research-in-progress, and private, personal, or financial data.
- **Viruses and unrestricted active content** – Infection and the propagation of a virus, worm or other form of malicious software via e-mail may compromise the confidentiality of data stored, processed or transmitted on computers located within CGIAR centers, and may lead to further infections within CGIAR ICT networks.
- **Loss of network availability** - The availability of CGIAR networks can be impaired if unauthorised broadcast messages or self-propagating messages are sent or received, such as though e-mail bombing or spam.
- **Legal liability** - CGIAR centers may be legally liable if staff send inappropriate, misleading or incorrect information using e-mail.

2.1 Understanding ‘Good’ and ‘Better’ Practice

Although this document predominantly contains good practices for email management and security, these are also supplemented by a number of guidelines which provide for a higher level of security, considered “better” or “best” practice. The difference between good and better practice in the context of CGIAR centers is defined below:

- **Good Practice** - An appropriate set of security controls for most CGIAR centers. Focus is applied to the use of technologies which are already likely to be in place, and an attempt is made to minimise the complexity of the solutions and the management overhead of the environment.
- **Better Practice** - A higher standard, to provide further guidance to CGIAR centers who have identified their systems or networks as being at an increased risk of attack, where more sensitive information and systems are housed, and where additional resources are available.

The email systems and all information contained in the systems (for example, email messages, document attachments, access logs, etc.) are the property of CGIAR centers. Hence, it is important to ensure that those systems and information are managed in accordance with the good practices in this guide in order to mitigate any potential security threats.

3 EMAIL MANAGEMENT AND SECURITY GOOD PRACTICE

For controls listed below which include surveillance measures, it is the responsibility of individual centers to research and maintain awareness of the legal, regulatory and compliance environments which surround workplace surveillance and monitoring in their respective host countries (including state or provinces where such level of regulation is in place).

There may be restrictions in place or requirements that must be fulfilled prior to any surveillance activity, such as notification of the users or staff to be monitored, and restrictions on monitoring of data in transit. Examples of such legislation include the Electronic Communications Privacy Act (USA) and the Workplace Surveillance Act (NSW, Australia).

3.1.1 It is recommended for CGIAR centers to maintain a policy statement which reserves the right to record, store and inspect all email communications and logs of such communications. Logs of email communications should capture the following information:

- Sender
- All receivers
- Subject or title
- Filenames of any attached files
- Partial message content (first 200 characters)

3.1.2 CGIAR centers should maintain a policy of notifying email account users about their surveillance and monitoring controls and practices. These should include the center's right to be able to monitor, search, review, disclose, or intercept information contained in center owned email systems (such as messages, document attachments and access logs) for legitimate purposes such as:

- monitoring performance
- ensuring compliance with the policies of the center
- detecting and preventing misuse of the email systems
- troubleshooting hardware and software problems
- complying with legal and regulatory requests for information
- investigating disclosure of confidential research, proprietary information, or conduct that may be illegal or adversely affect the center or its associates.

An example of how a data investigation process could be carried out is detailed below:

- a) An IT manager is allowed to perform the investigation, but only with the approval of at least two senior managers from the senior management group of the Center.
- b) The person concerned must be informed, unless the inspection relates to a criminal or potentially criminal matter.
- c) No other staff can perform investigation actions even if delegated by the approved IT Manager unless protocol a) and b) of this process have occurred for the staff member.
- d) A system-enforced audit trail should be maintained to allow the investigation process to be reconstructed if required.

- 3.1.3 It is recommended CGIAR centers maintain a policy which requires that every message that passes through their email systems is scanned to check for computer viruses, worms, or other executable items that could pose a threat to the security of the center's network and data. Infected email messages should not be delivered to the user.
- 3.1.4 It is recommended CGIAR centers maintain a policy which requires that every email message that passes through CGIAR email systems is scanned to check its contents based on predetermined criteria, such as the following:
- Bad SMTP headers
 - Invalidated source IP addresses
 - Bad domain names
 - Spam
 - The use of offensive language (in this case profanities)
 - Attachments containing inappropriate or malicious material (including viruses, worms and trojans)
- If the message does not pass the criteria, the message should not be delivered to the user and the system administrator should receive an automatic alert. Note that gateway anti-virus inspection software should be sourced from a different vendor from the vendor used to supply end-user anti-virus software.
- 3.1.5 It is recommended that CGIAR centers maintain a policy which requires that users only use software and systems for accessing email services that have been approved for use by the CGIAR center in question.
- 3.1.6 It is recommended that CGIAR maintain a policy which requires retention and archiving of all incoming and outgoing email messages, including attachments, which pass through email systems. Administrators should archive messages to an off-line storage medium at least every six months and purge those messages from the on-line storage medium, however this period can be modified if required to comply with the relevant regulations of the hosting country (which will generally be the country in which the mail server is located).
- 3.1.7 Centers should establish a retention period for archived email messages stored off line in accordance with the laws of the relevant host country (which will generally be the country in which the mail server is located) as well as any other Center or CGIAR-wide requirements included in a broader policy on records management.
- 3.1.8 It is recommended that CGIAR centers maintain a policy which states a maximum email storage capacity determined and enforced by that center. The maximum storage capacity will depend on the available resources of each center. A process of documenting and managing exception to the maximum storage capacity for individuals based on appropriate justification should be put in place in each CGIAR center.
- 3.1.9 It is recommended that CGIAR centers maintain a policy which prohibits automatic forwarding of messages from CGIAR email accounts to any untrusted email addresses except for legitimate purposes specifically approved by the IT manager or the HR Unit (such as in cases of departing staff).
- 3.1.10 Email servers should be configured in a manner which helps reduce the chances of centre email addresses being added to email blacklists. CGIAR should maintain a policy which includes the following controls to support this requirement:
- a) Ensure that the identity of each center mail server within the internal infrastructure correctly identifies itself to other connecting mail servers. At a technical level, this is generally implemented through ensuring that the fully qualified domain name used by the mail server to

identify itself across the Internet is the same as the fully qualified domain name that is specified for the MX record and the DNS hosting provider for each center.

- b) Ensure that center emails cannot be relayed externally.
- c) Ensure that systems and workstations are and remain malware free.

3.2 Mobile Device Emails

Mobile devices such as laptops, smart phones, PDAs and other devices can be utilised for email. While these devices are convenient, they require additional security controls to minimise any introduced risks.

- 3.2.1 It is recommended that center policies and orientation material should encourage users to avoid opening and sending emails in situations where the security of a mobile devices' network connection is unknown (for example, public wireless networks or Internet cafes), unless encrypted or secured connections are utilised between the device and email servers.

4 EMAIL MANAGEMENT AND SECURITY BETTER PRACTICE

4.1 Encryption of Emails

- 4.1.1 A number of solutions exist for the encryption of email. For centers with the resources and technical capability, center policies should require use of a gateway solution (such as Tumbleweed MailGate or PGP Universal) that utilises strong PKI and digital certificate architecture. For other centers, a point solution is recommended such as PGP Desktop.
- 4.1.2 For web based email access, any form of email encryption (such as SSL) configured correctly that is interoperable with internal email gateways can be utilised.
- 4.1.3 When accessing email services using connections such as POP and IMAP access, center policies should require encryption via SSL.

5 APPENDIX A: DEFINITIONS

Domain names: Refers to a name (for example, test.com) that is used to represent an IP address or a set of IP addresses.

Email: The electronic transmission of information through a mail protocol such as Simple Mail Transport Protocol (SMTP). Emails can be sent in either HTML or plain-text format.

Email systems: The network components and the software that allow transmission of electronic messages. These include the email server, the gateways, routers, as well as client email applications.

Encryption: Refers to the process of encoding emails using a specific algorithm to ensure the contents is unreadable to everyone except the sender and intended recipient of the message. Email encryption is often achieved using public/private key cryptography through software such as PGP (Pretty Good Privacy).

Mailing list: Refers to a list of email addresses identified by a single email address. When an e-mail message is sent to the mailing list email address, it is automatically forwarded to all the addresses in the list.

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

Signature: Email signatures can refer to one of two concepts: firstly, the generation of a hash of a message that uniquely identifies the sender of the message and proves to the recipient that the message has not been altered during transmission. It can also refer to the consistent addition of certain information to the text of all email messages, such as names, addresses, and phone numbers.

SMTP headers: SMTP (Simple Mail Transfer Protocol) is used to send email messages on the Internet between servers and from a mail client to a mail server. The SMTP header refers to text automatically inserted at the beginning of an email message by client mail programs and added to by all the mail servers en route to the destination. Each node adds more text, including from/to addresses, subject, content type, time stamp and identification data, which allows the path of the message from source to destination to be tracked.

Spam: The sending of unsolicited emails, often advertising a product or service or containing malicious file attachments. Spam emails are often sent in bulk to a large number of email addresses that may be harvested using a variety of techniques.

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.

6 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.

6.1 Good Practice Checklist

Guideline Number	Guideline	Tick if center currently adheres to this guideline

Guideline Number	Guideline	Tick if center currently adheres to this guideline
Section 3 – Email Management and Security Good Practice		
Section 3.1 – Email management		
3.1.1	<ul style="list-style-type: none"> ▪ Centers reserve right to record/store/emails ▪ Logs of email communications capture appropriate information 	<input type="checkbox"/>
3.1.2	<ul style="list-style-type: none"> ▪ Centers able to monitor/search/review/disclose/intercept information contained in email systems (subject to legal/compliance/regulatory environments) 	<input type="checkbox"/>
3.1.3	<ul style="list-style-type: none"> ▪ Emails subjected to scanning for viruses/worms/malicious executable files ▪ Infected emails not delivered to user 	<input type="checkbox"/>
3.1.4	<ul style="list-style-type: none"> ▪ Emails subjected to appropriate scanning based on identified criteria ▪ Messages failing to pass criteria not delivered, and system administrator alerted 	<input type="checkbox"/>
3.1.5	<ul style="list-style-type: none"> ▪ Only approved software/systems for accessing email used 	<input type="checkbox"/>
3.1.6	<ul style="list-style-type: none"> ▪ Center retains and archives all email messages ▪ Messages archived to off line storage every 6 months (or another appropriate period) and purged from on line storage 	<input type="checkbox"/>
3.1.7	<ul style="list-style-type: none"> ▪ Emails retained for at least two years 	<input type="checkbox"/>
3.1.8	<ul style="list-style-type: none"> ▪ Users allowed a maximum email storage capacity determined by each center ▪ Process in place for documenting and managing exceptions to maximum storage capacity 	<input type="checkbox"/>
3.1.9	<ul style="list-style-type: none"> ▪ Automatic forwarding of messages from CGIAR email accounts to any untrusted email addresses be prohibited 	<input type="checkbox"/>
3.1.10a	<ul style="list-style-type: none"> ▪ Ensure that the identity of each center mail server within the internal infrastructure correctly identifies itself to other connecting mail servers 	<input type="checkbox"/>
3.1.10b	<ul style="list-style-type: none"> ▪ Ensure that center emails cannot be relayed externally 	<input type="checkbox"/>
3.1.10c	<ul style="list-style-type: none"> ▪ Ensure that systems and workstations are and remain malware free 	<input type="checkbox"/>
Section 3.2 – Mobile Device Email		
3.2.1	<ul style="list-style-type: none"> ▪ Encrypted or secured connections utilised for mobile device email connections 	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adheres to this guideline
Section 4 – Email Management Better Practice		
Section 4.1 – Encryption of Emails		
4.1.1	<ul style="list-style-type: none"> Email encryption should be implemented either with a gateway solution or a point solution 	<input type="checkbox"/>
4.1.2	<ul style="list-style-type: none"> Web based email access should utilise encryption such as SSL 	<input type="checkbox"/>
4.1.3	<ul style="list-style-type: none"> Connections to email services such as POP and IMAP should be encrypted using SSL 	<input type="checkbox"/>

7 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/> "