World Agroforestry Centre Policy Series MG/C/4/2009

ICT Privacy and Acceptable Use Policy

One of the policies on information security and business continuity which will be audited by the CGIAR Internal Audit Unit for all Centres given (a) their network inter-linkage through Active Directory and (b) the inter-reliance of many Centres for information backup and recovery of hosted outreach sites.

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	20/09/2009	Ian Moore	Final draft circulated to staff
1.1	30/11/2009	Ian Moore	Revised following SLT guidance

Document Control

The ICT Manager of the common services unit providing ICT Services to the World Agroforestry Centre (ICRAF) and the International Livestock Research Institute (ILRI) will maintain control of the document which will be reviewed every two years in conjunction with the ICT Steering Group.

Proposed updates will be presented to the Centres' senior management for adoption according to their organizational arrangements for approval of ICT policies. Upon acceptance by the Centres, the update will come into force.

Any discretionary controls added by a Centre may be reviewed annually; however updates may occur more frequently if deemed necessary.

Purpose

The purpose of this document is to communicate the Centre's policy on acceptable use of ICT resources at the Centre and to outline expectations of privacy. The policy is in place to protect the employee and the Centre. Inappropriate use can expose the Centre to risks at both a technical level (with potential damage being caused to ICT infrastructure) and at operational level (with misuse of Internet resources leading to possible reputational damage to centres and a loss in productivity)

The Centre's intentions for publishing an ICT Privacy and Acceptable Use Policy are not to impose restrictions that are contrary to the Centre's established culture of openness, trust and integrity. The Centre is committed to protecting the Centre's employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every Centre employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

This document incorporates the CGIAR Internal Audit Unit's (IAU) recommended best practices. All Centres will be reviewed by the IAU to ensure that they have implemented the recommended best practices, in all their offices. A shared CGIAR electronic network exists (through the implementation of Active Directory) and which has, as a result, created an inter-dependency among the Centres with regard to network security. It is therefore important that all Centres are reviewed against a common set of ICT security guidelines.

Scope

This document covers an individual's privacy expectations and the acceptable use of the Centre's ICT resources by employees, contractors, consultants, and other staff of the Centre and hosted organisations including all personnel affiliated with partners and third parties. This policy applies to all ICT equipment that is owned or leased by the Centre.

1. Privacy

1.1. While the Centre desires to provide a reasonable level of privacy, be aware that information assets our employees, agents, independent contractors or visitors create, distribute, access, or manage, including all documents, messages or other content created, sent or received over ICT systems or stored on ICT systems are and shall remain the property of the Centre. This unavoidably limits personal privacy and the Centre cannot ensure, and you should not assume,

the confidentiality of any documents, messages or other content sent or received through, or stored on, ICT systems controlled by the Centre or its agents.

1.2. The Centre does not routinely examine or disclose information on its ICT systems. Nonetheless, subject to the procedures detailed below, the Centre may deny you access to any ICT system and may examine or disclose information on these systems under the following conditions:

- when required by and consistent with law;
- when the Centre has reason to believe that a violation of law or of the Centre policies is threatened or has taken place;
- when there are compelling circumstances where failure to act may result in significant harm to the Centre or an individual associated with the Centre; or
- under time-dependent, operational circumstances.

1.3. The ICT Department will facilitate the first 3 conditions only upon the request of the Director General or the Head of Human Resources. For circumstances covered by the last condition, upon the request of your theme or Division/Theme Director (ILRI) or Regional Coordinator/Global Project Leader/Division Director (ICRAF), the ICT Department will forward the requested content or information created, received or stored by you to the person needing it and send an e-mail to you informing you that such action has been taken.

1.4. During the performance of their duties, ICT Department staff occasionally need to monitor transmissions, observe certain transactional information, or observe information considered as private. Such unavoidable inspection is limited to the least invasive degree of inspection required to perform their duties and ICT Department staff will not disclose any legitimate information observed. However, they will report violations of law or policy discovered in the course of their duties.

2. E-mail Privacy

2.1. The Centre's policy regarding e-mail privacy is covered under the Privacy statements in section 1 relating to ICT systems in general.

2.2. E-mail messages that you send can never be considered private as once received by the recipient you no-longer have control over what happens to the message.

2.3. Upon your departure from the Centre, there is no guarantee of privacy of the information contained in your e-mailbox or archive folder(s). It is recommended that, prior to your departure; you delete all private and personal e-mail from your Centre e-mailbox and from your e-mail archive folder(s).

3. File Storage Privacy

3.1. The Centre's policy regarding the privacy of the files stored on network drives, computers or other media belonging to the Centre is covered under the Privacy statements in section 1 relating to ICT systems in general.

3.2. Because of their shared nature, any shared folders are not considered to be private. The Centre will not access information on your local hard drives without your permission. However, you should not treat your local hard drives as private, because there is no mechanism to guarantee their privacy.

3.3. Confidential files should be stored on secure network folders. Personal files should be stored on personal removable media such as external hard disks, data sticks, DVDs, or CDs.

3.4. The final backup and archive of local hard drives and the network folders that is made upon your departure is not considered to be private. It is recommended that you delete any private or personal files from your local drives and network folders before you depart.

4. Telephone System Privacy

4.1. The Centre's policy regarding telephone conversations and voicemail privacy is covered under the Privacy statements in section 1 relating to ICT systems in general.

4.2. If you intend to record a telephone or VoIP (gTalk, Skype) call you must first inform all participants that the call will be recorded. The privacy of telephone conversations is protected by law. Without court approval, in many jurisdictions it is illegal to record or monitor telephone conversations without advising the participants that the call is being monitored or recorded.

4.3. The use of the Centre telephone equipment creates transaction records (which include the number called and the time and length of the call) that are available to budget managers, directors, and senior administrative staff as part of routine accounting procedures. This information is not considered private.

5. Acceptable Use

5.1. Users of the Centres ICT Systems are expected to use them responsibly and securely in a manner that minimises the risk of detrimental impact to the Centre. That is, to comply with all applicable country and local laws, with this and other Centre policies, and with normal standards of professional and personal courtesy and conduct.

5.2. All information stored or transmitted through the Centre's ICT systems must conform to law and the Centre policies regarding protection of intellectual property, including laws and policies regarding licensing, copyright, patents, and trademarks. You should assume that material created by others, in electronic or other forms, is protected by copyright unless such material includes an explicit statement that it is not protected or unless such material is clearly in the public domain.

5.3. The Centre's ICT systems should be used primarily for research and business purposes. Some incidental personal use of the Centre's ICT systems by staff is allowed as long as:

- it does not consume more than a trivial amount of system resources;
- it does not interfere with your productivity or that of others;

- the activity is legal and in compliance with Centre codes of conduct or anti-harassment policies;
- sensitive information or systems belonging to the Centre are not placed at risk of compromise;
- it does not pre-empt any research activity of the Centre.

5.4. The Centre's ICT systems must not be used for:

- Unlawful, fraudulent or libellous activities;
- commercial purposes not under the auspices of the Centre;
- personal financial gain;
- political activities;
- engaging in any form of intelligence collection from the Centre's information assets;
- activities that put the reputation of the Centre or its employees at risk;
- activities that violate other Centre policies or guidelines.

5.5. The Centre will not take any responsibility for the security of any personal information transmitted by staff (such as for personal e-commerce transactions or banking transactions) using the Centre provided Internet connections or email system, including any consequential losses sustained as a result of the transmission of this information.

5.6. The Centre retains the right to deny access to any ICT system and may examine or disclose online information that the Centre ICT systems have been used to access in line with the Privacy statements in section 1.

6. E-mail Acceptable Use

6.1. The Centre's policy regarding acceptable use of e-mail is covered under the Acceptable Use statements in section 5 relating to ICT systems in general.

6.2. All staff are eligible to an email account on the Centre's email system. Therefore all business communications of the Centre sent via email should be sent using an official Centre email account except in exceptional circumstances where a valid business case exists.

6.3. Use of personal web-based email accounts is permitted from within the Centre's network for personal communications; however users should treat attached files and website links as potentially harmful and refrain from downloading or following either of these from computers used for official Centre work. Staff should not use personal email accounts for work purposes except in exceptional circumstances where a valid business case exists.

6.4. Email accounts are only for use by the person who has been assigned the account. You should not allow anyone else access to your account and should not share your email account passwords with other individuals in any circumstances. However, in some situations, it may be necessary for this to occur. In such situations, access to another party's email account should only occur where the person who owns the email account has provided a written request to their senior manager, which is subsequently approved. The request should:

- Identify who the email account will be accessed by and how long this arrangement will be in place; and
- Contain an acknowledgement by the owner of the email account that they will continue to be responsible for all activity on the account.

6.5. Internal mailing lists should not be published or distributed to non-staff members. Internal mailing lists typically contain email accounts and addresses used to distribute email messages to all or a subset of the Centre's staff.

6.6. Users should not forge, attempt to forge, disguise or attempt to disguise the user's identity for email messages sent using the Centre's email systems.

6.7. Email is an inherently insecure form of communicating information. It is recommended that highly confidential information should not be sent by email to external parties. ICT can assist to encrypt messages containing highly confidential information that have to be sent by email.

6.8. To minimise the threat from viruses and malicious code entering a computer, automatic loading of pictures, as well as downloading and processing of active content within messages should be disabled by default. Users should not execute any untrusted programs that are received either via personal or Centre email accounts, nor should users install any software upgrades or patches received via these accounts unless received from a reliable source and the code has been tested to ensure it does not contain viruses or malware.

6.9. In addition to the types of usage listed in section 5.4, the Centre's e-mail system should not be used to:

- send any information that incites crime or other unlawful activities (as defined in either the sending or receiving country, or any country through which the information is routed);
- send any messages that violate the intellectual property, proprietary, personal or contractual right of any third parties;
- produce, distribute or forward "chain mail", or other unsolicited messages and personal mass mailings including "spam" or to operate businesses, or make solicitations for personal gain, political or religious causes, or outside organizations;
- produce, distribute or forward any material that is offensive, defamatory, or threatening to others. These may include statements, messages, or images consisting of pornographic material, ethnic slurs, racial epithets, or anything that may be construed as harassing, offensive, or insulting to others based on race, religion, national origin, colour, marital status, gender orientation, citizenship status, age, disability, or physical appearance;
- intentionally engage in practices that impede the availability of electronic communications services;
- send email messages that contain configuration details of any networks or servers within he Centre to public newsgroups or mailing lists. This includes internal machine addresses, server names, server types, or software version numbers.

6.10. To facilitate communications and to properly identify the sending party all e-mail messages sent through the Centre's email system should contain a signature that includes:

- Sender's Full Name
- Position Title
- Centre Name and Address
- Email address
- Web site URL of centre
- Phone and fax numbers (including relevant area codes)
- The management approved disclaimer statement

6.11. To minimise risks and liability from the misuse of information contained in email messages the following disclaimer should be added manually to all external or internal email messages when:

a. the message contains confidential information;
b. the message content provides advice;
c. the message contains official documents or information from the Centre, especially when agreements are being discussed;
d. you do not want the message forwarded to any other recipients.

In the case of point d, it is recommended that the disclaimer statement is edited to include the name(s) of the intended recipient(s) to replace the text "the addressee".

DISCLAIMER NOTICE - this e-mail message (including any attachments) is intended for the addressee only, and the information that it contains may be confidential, legally privileged and protected by law. Access by the intended recipient only is authorized. It is not intended to constitute a binding contract unless expressly stated. Any liability (in negligence or otherwise) arising from any third party acting, or refraining from acting, on any information contained in this e-mail is hereby excluded. If you are not the intended recipient, please notify the author immediately and delete this e-mail (including any attachments) immediately in its entirety. Do not disclose the contents to any other person use it for any purpose or store or copy the information in any medium. Copyright in this e-mail and attachments created by us, belongs to <Centre Name>. <Centre Abbr> also asserts the right to be identified as such and object to any misuse.

7. Internet Acceptable Use

7.1. Acceptable use of the Internet by employees, agents, independent contractors and visitors is covered under the Acceptable Use statements in section 5 relating to ICT systems in general.

7.2. When issuing statements, comments or opinions on websites, blogs, forums and similar electronic venues, either as an individual or on behalf of the Centre or other individuals, it is important to maintain the corporate image of the Centre. All statements, comments or opinions

should therefore be expressed in a professional and non-offensive manner and in accordance with the Centre's external communications policies.

7.3. When using web pages that require a user ID and password for access, it is recommended that staff do not use the same ID and password as is used for access to any internal systems, networks or applications with the Centre.

7.4. Where staff engage in ecommerce transactions for official purposes over the Internet, using corporate credit card or banking information, they should first ensure that the organisation with whom they are dealing is reputable and legitimate, and that such transactions can be completed in a secure fashion (for example, through use of SSL). Computer systems used to conduct such "secure" or "sensitive" activities over the Internet should not also be used for other activities that require the installation of arbitrary software applications, especially those downloaded from the Internet.

7.5. Sensitive or confidential information belonging to the Centre (such as non-public research data or passwords used to gain access to systems and devices within a Centre) should not be posted to public newsgroups, forums, blogs or websites. Extreme caution should be taken if sensitive data needs to be transmitted over the internet, this should only take place if the information is in encrypted form. ICT can assist in the use of file encryption solutions such as PGP (via email) and SecureZIP. Alternatively, the information can be transmitted through the use of protocols that use encryption such as Secure FTP.

7.6. Before downloading files from the internet, via applications or when using communication tools (skype, gTalk, gotomeeting) the staff member should:

- ensure that files are obtained from a trusted, reputable source to minimise the risk of downloading viruses and malicious code;
- check the legality of downloading the information, particularly with respect to copyright permission;
- not download unlicensed software or violate limitations on the use of particular software as imposed by any licence agreements. Most downloaded software, including shareware and freeware, is copyrighted and subject to license, which sets limitations on its use;
- not redistribute downloaded material unless the owner has given permission for them to do so either directly or in the copyright/license terms.

7.7. In addition to the types of usage listed in section 5.4, the Centre provided Internet connections should not be used for:

- use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization;
- requesting, accessing, posting, or downloading of any material that incites crime or terrorism (as defined in either the receiving or hosting country, or any country through which the information is routed).

- creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs;
- misuse of, disclosing without proper authorisation, or altering personnel information (e.g., making unauthorized changes to personnel files, or sharing personnel data with unauthorized parties);
- wilful or negligent introduction of computer viruses, trojan horses or other destructive programs onto the Centre's systems or networks or into external systems and networks;
- unauthorised decryption or attempt at decryption of any system or user passwords or any other user's encrypted files;
- intentionally engaging in practices that impede the availability of any of the Centre or third-party;
- any unauthorized, deliberate action that damages or disrupts computing systems, networks or electronic communications services that alters their normal performance, or causes them to malfunction;
- packet sniffing, packet spoofing, or use of any other means to gain unauthorised access to information, a computer system, or network;

7.8. In particular the following categories of web sites should not be accessed from the Centre's computer systems. Where appropriate these categories of sites will be blocked through web filtering. Exceptions can be configured upon a written email request to their senior manager who will give approval to the ICT Manager to make the change if the sites have been incorrectly categorised or if required for work purposes:

- adult content, nudity;
- gambling, games;
- illegal or questionable, military and extremist, racism and hate; and
- hacking, proxy avoidance, peer-to-peer file sharing.

7.9. The Centre will log details of all Internet content that is accessed, including the following information:

- URL of content accessed
- Time and date of access
- The computer or user that accessed the content

The log file should contain records of content accessed in the preceding 90 days. In addition, backups of the log file should be performed regularly to ensure that content accessed in the past year can be reviewed by accessing these backups.

8. Copying and Printing Acceptable Use

8.1. Acceptable use of copying and printing facilities by employees, agents, independent contractors and visitors is covered under the Acceptable Use statement in section 5 relating to ICT systems in general.

8.2. Use of the copying and printing facilities for personal use is permitted as long as the cost is charged to the staff's personal account and that the criteria outlined in section 5.3 are met.

9. Telephone systems Acceptable Use

9.1. Acceptable use of telephone facilities by employees, agents, independent contractors and visitors is covered under the Acceptable Use statement in section 5 relating to ICT systems in general.

9.2. Use of the telephone facilities for personal use is permitted as long as the cost is charged to the staff's personal account and that the criteria outlined in section 5.3 are met.

10. Related Documentation

10.1. Network Infrastructure Security Policy

10.2. Network User Identification and Authentication Policy

10.3. Workstation Security Policy

10.4. Internet and Email Security Policy

11. Compliance and Waivers

11.1. Compliance with this policy by users, network administrators, or others responsible for implementation of the policy, is mandatory. Procedures are in place to monitor compliance with this policy.

11.2. Violations of this policy may result in disciplinary action in accordance with the human resources policies of the Centre.

11.3. Requests for waivers of this policy shall be formally submitted to the Senior Manager. The requests shall set out the justification, duration of the proposed waiver and how the increased risk arising from the waiver will be managed. Requests will be approved by the Senior Manager of the person making the request, in consultation with the ICT Manager and will be documented in the form of a management letter.

11.4. Approved waivers shall be monitored to ensure that the conditions of the waivers are being observed.

Definitions

- **ICT systems:** include but are not limited to computer equipment, software, operating systems, database systems (including Finance and HR), storage media, network accounts, e-mail, internet

access, copying and printing systems, the telephone system (including voicemail), network backups and electronic archives, including systems hosted or controlled by third-party vendors of the Centre. Since technology changes quickly, other systems may be added to this definition as appropriate.

- **Disclaimer:** Text added to a document to explicitly state how the content of the message can or cannot be used.
- **Senior Manager:** The person on the Centre's management committee (MC/SLT) who has responsibility for the person making the request.