



SECTION L - PROTECTING THE CONFIDENTIALITY OF ELECTRONICALLY STORED INTERNAL AUDIT REPORTS, WORKING PAPERS AND COMMUNICATIONS

Introduction

CGIAR internal auditing relies heavily on electronic storage and transmission of information for the purpose of planning, conducting, reporting and following up on audits and investigations; communicating with Center external auditors and reviewers; reporting on internal audit activity to Center management and Boards, and receiving information of concern to staff who wish to report this to the Internal Auditors. In the course of their work Internal Auditors electronically receive, store and transmit much privileged information which if not properly protected could damage the reputation of the audit function, breach Center policies or privacy laws, or disrupt the effective operation of the audit activities.

This section applies to all internal audit consultants in relation to their work for Center audits and other engagements for the CGIAR IAU, as well as CGIAR IAU and Center Internal Audit staff. References to Internal Audit staff in this Manual section cover them also.

The section covers the basic elements required to effectively protect confidential/sensitive electronic Internal Audit information such as audit reports, audit working papers, internal audit databases, internal audit activity reports, non-public Center documents and data collected for permanent files, audit documents shared by external auditors and external review panels, and audit-related communications between auditors and with audit clients (which are referred to collectively in this section as “IA information”). These elements include:

- classification and labeling of IA information to facilitate secure treatment;
- handling protocols for storage and transmission of IA information;
- protocols for disposal of media which has been used to store confidential IA information. and
- guidance to implementation, for protecting IA information in a mobile computing environment



Electronic copies of IA information may be held in the custody of Internal Audit staff during the course of audits being carried out, for backup purposes, or for archiving for reference by the auditor for future audit work. Copies of this information may also be archived centrally either by the CGIAR Internal Auditing Unit at its office locations in Los Baños, Nairobi, Mexico or Patancheru, or by Center Internal Audit Units at their Center Headquarters.

Media referred to in this Manual section includes desktop computers, laptop computers and other mobile machines such as PDA's and Tablet PCs, and storage media such as external disk drives, thumb drives, CDs and DVDs,

Ref.	Policy and Practice Requirements	IIA Standards and Other references
L.1	<p>Policy: All electronically stored IA information shall be stored, transmitted and disposed at a level of security appropriate to their level of confidentiality. Procedures shall be established and observed for:</p> <ul style="list-style-type: none"> ▪ management of desktops, laptops, other mobile machines and storage media containing IA documents; ▪ the storage of IA documents on Center-managed or other servers, and their transmission through Center-managed communication systems; and ▪ the secure and safe deletion of IA documents from desktops, laptops, other mobile machines and storage media used for storing audit documents, when the computers and storage media are no longer required and are to be decommissioned or transferred back to the host Center for re-use or disposal. 	
L.1-1	<p>Practice requirement:</p> <p>In order to achieve and maintain appropriate protection of all electronically stored IA information:</p> <ul style="list-style-type: none"> ▪ the information shall be clearly identified 	<p>ISO 27001:2005(E) Information Security Management Systems Requirements A.7.1 Responsibility for</p>



Ref.	Policy and Practice Requirements	IIA Standards and Other references
	<p>and filed in an organized fashion by the Internal Audit staff who are responsible for their custody;</p> <ul style="list-style-type: none"> ▪ all such information, other than copies of Center or other documents and data which are already publicly available, shall be classified at a minimum as “confidential” and treated as such in their storage. These documents should only be made available, unless expressly approved by the Center Director General of the Center from which the document originates, to Center management and staff who are otherwise entitled to access the documents, to Internal Audit staff or (upon request) to the external auditors of the Center concerned. In the latter case this shall not include documents relating to the competitive selection of the external auditor, which may include commercial-in-confidence information provided by other audit firms and confidential assessments of the firms. ▪ confidential information shall be further classified as “sensitive” where it relates to investigations by Internal Audit or other parties; information obtained through whistleblower reporting or related to whistleblowers; contains information required by Center policies or applicable privacy laws to be specially handled; Board of Trustees and committee minutes and related documents classified as Board-in-confidence; or information provided by third parties subject to special protection and use conditions. 	<p>assets</p> <p>A.7.1.1 Inventory of Assets</p> <p>A.7.1.2 Ownership of assets</p> <p>A.7.2 Information Classification</p> <p>A.7.2.1 Classification guidelines</p> <p>A.7.2.2 Information labeling and handling</p>
L.1-2	<p>Practice Requirement:</p> <p>The Head of Internal Audit’s approval shall be</p>	



Ref.	Policy and Practice Requirements	IIA Standards and Other references
	<p>obtained to store any information that is classified as sensitive.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ Internal Auditors should minimize the amount of sensitive information stored. In particular, audit files should not normally include information on staff medical matters, staff disciplinary proceedings, selection panel evaluations for hires and promotions, commercial-in-confidence information provided by bidders or proprietary information shared with Centers by private sector partners. If reference to these is necessary for audit purposes, then it is preferable to limit this to cross-referencing of where information is located in the Center concerned. If any such documents are stored they should be encrypted. 	
L.1-3	<p>Practice Requirement:</p> <p>The Internal Audit staff who keeps copies of electronically stored IA information shall be considered “owners” of this IA information. Such individuals have responsibility for controlling the use and security of the information. In the case of IA information which is classified as “sensitive”, the Head of Internal Audit shall ensure that the number of “owners” is limited to what is strictly necessary and that, at all times, who those “owners” are can be readily identified.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ The term “owner” does not mean that the Internal Auditor actually has property rights to the asset. ▪ It is not feasible to maintain registers of 	<p>ISO 27001:2005(E) Information Security Management Systems Requirements A.7.1.2 Ownership of assets</p>



Ref.	Policy and Practice Requirements	IIA Standards and Other references
	<p>who stores copies of particular IA information, at a document level, for all IA information.</p> <ul style="list-style-type: none"> ▪ In cases of confidential/sensitive documents it is preferable that there is only one “owner” and that this principle is only deviated from in exceptional circumstances. Keeping multiple copies of sensitive IA information makes it more difficult to responsibly control the information. 	
L.1-4	<p>Practice Requirement:</p> <p>Encryption should be applied whenever sensitive/confidential information are (a) stored on Center or other servers; (b) stored on machines which do not have appropriate access controls and/or are accessible via the network; and (c) stored on removable media (e.g., CDs, DVDs, and USB drives) or portable media (e.g., PDA’s, tablet PCs, and laptops) which do not have an appropriate level of physical protection.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ For those data stored on portable media (e.g., PDA’s, tablet PCs, laptops), as well as storage media, (e.g., CDs, DVDs, and USB drives) encryption shall be provided through the use of built-in encryption features, a whole disk encryption tool or one that can at least be configured to encrypt all stored data. ▪ For those data contained in a Center host’s database server, encryption shall be provided through the use of whole disk encryption or through features native to the database server software. Encryption capabilities native to database server software may allow for encryption of 	<p>ISO 27001:2005(E) Information Security Management Systems Requirements</p> <p>A.12.3.1 Policy on the use of cryptographic controls</p>



Ref.	Policy and Practice Requirements	IIA Standards and Other references
	<p>specific tables or columns of a database and may also be required to segregate access rights among multiple applications that utilize a single database server.</p> <ul style="list-style-type: none"> ▪ For sensitive/confidential data contained in back-ups and archives, encryption shall be provided to prevent unauthorized access. ▪ Encryption of sensitive/confidential information in storage presents risks to the availability of such information, due to the possibility of encryption key loss. Therefore, at least one copy of any such information shall be stored in a known location having an appropriate level of physical protection in unencrypted form or, if encrypted, the means to decrypt it must be available to more than one person in IAU. 	
L.1-5	<p>Practice Requirement:</p> <p>Information received via the CGIAR IAU whistleblower email account shall only be accessed and downloaded outside of CGIAR networks, and stored on non-Center media.</p>	
L.1-6	<p>Practice Requirement:</p> <p>Where the IA information is housed on the hard drives of a workstation (laptop or desktop), the machine must be in a physically secure location and require a unique logon with a strong password for each individual authorized to use it (i.e. shared accounts and passwords are not permitted). The machines should have adequate anti-virus protection operating and operating systems should be kept up to date with security patches.</p>	



Ref.	Policy and Practice Requirements	IIA Standards and Other references
	<p>Discussion:</p> <ul style="list-style-type: none"> ▪ Generally, Internal Audit staff use machines provided by their host Centers for work purposes. The above requirement should therefore normally be implemented by compliance with Center IT security policies which have equivalent requirements ▪ In the case that IA information is stored on the personal machines of Internal Auditors or IA consultants, equivalent security should be deployed at least in relation to access to the sectors of their machines where IA documents stored for working or backup purposes. 	
L.1-7	<p>Practice Requirement:</p> <p>Internal Auditors shall take appropriate measures to protect portable media from theft/loss when traveling to prevent loss, damage or compromise of IA information.</p> <p>Discussion:</p> <p>The level of security applied to portable media should not be any less than that applied to media kept in the office. There are additional considerations when media is being transported. Internal Auditors should consider the following measures:</p> <ul style="list-style-type: none"> ▪ Ensure adequate insurance cover is in place to protect laptops and other equipment off site. ▪ Carry laptops, and do not surrender laptop bags to baggage handlers or hotel bell staff. They should not be left unattended in public places. 	<p>ISO 27001:2005(E) Information Security Management Systems Requirements</p> <p>A.9.2.5 Security of equipment off-premises.</p>



Ref.	Policy and Practice Requirements	IIA Standards and Other references
	<ul style="list-style-type: none"> ▪ Use a non-descript carrying case, or backpack to carry laptops, to avoid attracting thieves' attention. ▪ Manufacturer's instructions for protecting equipment should be observed at all times, e.g., protection against exposure to strong electromagnetic fields ▪ Consider using computer privacy screens ▪ Apply a cable locking system to secure laptops when left in offices being visited or on desks in hotel rooms. Lock laptops and other portable machines and storage media away in suitcases when left in hotel rooms. ▪ Apply appropriate environmental protection to laptops, e.g. <ul style="list-style-type: none"> ○ Keep out of direct sunlight ○ Keep free of dust ○ Keep free of liquids ○ Keep media away from exposure to magnetic fields, radio equipment or any sources of vibration ▪ When storing or transporting laptops and storage media, adhere to manufacturers' published recommended temperature and humidity levels. ▪ Use CGIAR offices and office equipment, including computers, faxes, printers, and secured network connections, when and where available, during travel. ▪ Avoid use of hotel faxes, copy facilities, and computers in business centers for transmitting, downloading or accessing sensitive documents. ▪ Be careful when logging online in a wireless 	



Ref.	Policy and Practice Requirements	IIA Standards and Other references
	<p>hot spot, such as hotel, café, or airport lounge by verifying that you are logging on to a valid wireless network. This can be done by verifying the network name (SSID) and checking in the “Wireless Connection Window”, for the notice that “you are connecting to a secure connection....” The most likely risk to be mitigated is logging on to someone nearby with a wireless computer attempting to steal your identity.</p> <ul style="list-style-type: none"> ▪ Configure laptops to not auto connect to wireless access points that are listed as “unsecure”. ▪ If required to transfer electronic files to facilitate printing, copying, or projection of presentation materials, be sure to remove data from temporary files, recycle bins and other files on non-owned equipment. ▪ Report actual, attempted, or suspected targeting of information during travel. ▪ Report loss of laptops 	
L.1-8	<p>Practice Requirement:</p> <p>Where machines or portable media are to be returned to the Center for decommissioning or reuse, or otherwise disposed, the Internal Auditor responsible shall ensure that the audit-related contents of the media are deleted. Confidential documents should at least be cleaned to prevent keyboard retrieval and sensitive documents should be fully purged.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ There are four types of media sanitization actions which may be applied: 	<p>ISO 27001:2005(E) Information Security Management Systems Requirements</p> <p>A.10.7.1 Management of removable media</p> <p>A.10.7.2 Disposal of media</p> <p>A.10.7.3 Information handling procedures</p> <p>US National Institute of Standards and Technology</p>



Ref.	Policy and Practice Requirements	IIA Standards and Other references
	<ul style="list-style-type: none"> ○ Disposal – media is discarded with no sanitization considerations – acceptable when the media contains only non-confidential information. ○ Clearing – protects against robust keyboard retrieval attempts. Simple deletion of information is not sufficient as it must be resistant to keystroke recovery attempts from standard devices and data scavenging tools. Overwriting of documents is an acceptable clearing method. ○ Purging – protects against laboratory retrieval attempts using non-standard systems. Certain firmware is available to protect against such attempts. ○ Physically destroying – by disintegration, cross-cut shredding, pulverization, burning and melting of media. This is the only fully secure method. <ul style="list-style-type: none"> ▪ Specific methods for different types of media are contained in the NIST Guidelines for Media Sanitization. ▪ In the case of Center-owned laptops, PDA's or storage media, Internal Auditors should ascertain the procedures and tools used by the Center to sanitize these prior to re-assignment or disposal. For reassignment, use of industry-practice overwriting software should be sufficient to sanitize non-sensitive confidential information. For disposals, software such as KillDisk to permanently destroy drive contents such be sufficient for all documents. ▪ In the case of Auditor-owned laptops or 	<p>Guidelines for Media Sanitization</p> <p>http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf</p>



Ref.	Policy and Practice Requirements	IIA Standards and Other references
	<p>storage media, if Internal Auditors are unsure, unclear or cannot conduct media sanitization in a safe and effective manner, the advice should be sought of a knowledgeable IT professional either at the host Center or from an outside vendor.</p>	
L.1-9	<p>Practice Requirement:</p> <p>Internal Audit staff shall ensure that all audit presentations are removed from non-owned presentation computers. In general, presentations should be kept on flash drives and confidential information that is classified as “sensitive” should not be recorded in the presentation document.</p>	
L.1-10	<p>Practice Requirement:</p> <p>Internal Audit staff entrusted with the custody of electronic IA information shall back this information up in an alternative machine or on storage media, kept in another location, under the same level of security applied to the “original” documents.</p> <p>Discussion:</p> <ul style="list-style-type: none"> ▪ Backup of IA sensitive/ confidential information should be encrypted, whenever technically feasible. ▪ Unencrypted backups should be physically secured and not subject to access by unauthorized person/staff member at any time. 	



<p>L.1-11</p>	<p>Practice Requirement:</p> <p>Confidential information which is classified as “sensitive” shall not be transmitted over the CGIAR email system without being encrypted.</p> <p>Discussion:</p> <p>The following would be acceptable methods of file/email encryption. The last two may be the most practical methods for internal auditors:</p> <p>File/Email Encryption</p> <ul style="list-style-type: none"> ▪ S/MIME signed and encrypted email ▪ PGP/GnuPG encrypted email and files ▪ Password-protected zip files ▪ Password-protected Microsoft Office documents 	
<p>L.1-12</p>	<p>Practice Requirement:</p> <p>Internal Auditors using E-conferencing to obtain or transmit confidential information should understand, and be satisfied with, how the service provider deals with private information and what policies have been implemented to ensure the data is protected at all times.</p>	<p>ISO 27001:2005(E) Information Security Management Systems Requirements</p> <p>A.11.7 Mobile computing and teleworking</p>