



Network User Identification and Authentication Good Practice Guide



contents

<u>1</u>	<u>Introduction to Good Practice Guides</u>	<u>3</u>
<u>2</u>	<u>Network User Identification and Authentication Overview</u>	<u>3</u>
<u>3</u>	<u>Network User Identification and Authentication Good Practice Guidelines</u>	<u>4</u>
3.1	General Policy on User Identification and Authentication	4
3.2	Passwords Confidentiality	4
3.3	Password Composition, Length and Validity Good Practice	5
3.4	Password Composition, Length and Validity Better Practice	6
3.5	Lockout of User Accounts after Failed Logon Attempts	6
3.6	Password Administration	7
3.7	Login/Logout Processes	7
3.8	User Account Management	7
3.9	Termination of User Access	8
<u>4</u>	<u>Appendix A: Definitions</u>	<u>8</u>
<u>5</u>	<u>Appendix B: Checklists</u>	<u>9</u>
5.1	Good Practice Checklist	9
<u>6</u>	<u>Document Control</u>	<u>12</u>

1 INTRODUCTION TO GOOD PRACTICE GUIDES

This document is a good practice guide concerning network user identification and authentication techniques used 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 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 NETWORK USER IDENTIFICATION AND AUTHENTICATION OVERVIEW

CGIAR Centers understand and promote the importance of information and knowledge sharing in today's environment. However, for sensitive information and research information not yet released to the public, the security of information and the restriction of this information from unauthorised users is important. Network user identification and authentication via unique identifier (ID) and sound password choice offer the front line of protection for user accounts. A poorly chosen user password may result in the compromise of a center's entire network.

This document is developed to communicate recommended controls for securing user identification and authentication credentials through the use of User IDs and passwords, where these are used for accessing a CGIAR Center's network environment.

3 NETWORK USER IDENTIFICATION AND AUTHENTICATION GOOD PRACTICE GUIDELINES

3.1 General Policy on User Identification and Authentication

- 3.1.1 Identification and authentication of users should be required for all user access into Center networks. CGIAR centers should assign unique user IDs to all users so that activities performed can be linked to the responsible user.
- 3.1.2 The unique User-IDs utilised should not give any indication of the user's privilege level – eg. 'Supervisor' or 'Administrator'. This helps to make it harder for someone outside the organisation to identify accounts that they may want to try to gain access with.
- 3.1.3 Users should be made responsible and accountable for all actions including information retrieval or communication on the Center's network performed under their user-ID(s) and password(s). The core principle is that security is everyone's responsibility – and everyone has a responsibility to protect their own "identity" on the Center computer systems.
- 3.1.4 Users should not be allowed to use a computer system which is logged into a center's network unless supervised by the owner or person responsible for the logged in account.

3.2 Passwords Confidentiality

The confidentiality of passwords is critical to the protection of any sensitive CGIAR center information and of CGIAR center systems. In many cases, passwords offer the first line of defence in stopping unauthorised and malicious users from accessing a user's personal account, or from accessing CGIAR systems. It is paramount that the passwords used are adequately protected and remain secret.

It is recommended that CGIAR centers maintain a policy which contains the following password confidentiality requirements.

- 3.2.1 Users should maintain the secrecy of any personal CGIAR access passwords.
- 3.2.2 Initial passwords for all new user accounts, or reset passwords assigned when a user forgets their password, should be given to users in a secure manner. The use of unprotected (clear text) e-mail messages should be avoided.
- 3.2.3 When provided a password, users should be required to change it to a different password that they choose, after first logging in to the system.
- 3.2.4 If the initial or reset password is not used within a period of time – 5 days is suggested – then that account should be suspended until needed, and a new password be created and issued. Where the technology allows, it is recommended that this process be automated.
- 3.2.5 Passwords and user IDs should not be shared with other users unless required for critical business, legal or emergency purposes. In such cases, responsibility for any misuse should remain with the owner of the user ID.

If knowledge of a password presents a single point of failure (i.e. only one person knows the password required for access to a system, and it is required for that system to operate), the user should advise their manager so that the dependency can be investigated and resolved. Resolution may include advising management of the password, provided lack of segregation of duties issues do not arise, or

alternatively, ensuring a second account with similar privileges is maintained (though accessible only by appropriately privileged users, or stored in a secured location).

- 3.2.6 Passwords should be masked (ie, should appear as **** or similar) on the computer screen when users are entering them.
- 3.2.7 Passwords should not be written or stored either physically nor electronically in plain text or unencrypted. If the password must be written down, it should be stored in a secured storage unit accessible only by the password owner.

3.3 Password Composition, Length and Validity Good Practice

It is recommended that CGIAR centers maintain a policy which contains the following password composition, length and validity requirements:

- 3.3.1 System and security administrator passwords should be reviewed and updated / revoked prior to any change in administrative responsibility, such as the current administrator leaving the organisation or changing roles.
- 3.3.2 Passwords should be changed regularly, on a basis relative to the minimum length of the password. The longer the password length, the less frequent the password needs to be changed. Furthermore, service account passwords should be changed at least annually, unless a more frequent change is required by the system or service.

Minimum Length	Duration
8 characters	90 days
9 characters	180 days
12 characters	365 days

- 3.3.3 Passwords should be changed immediately if they become, or are suspected of having become, compromised.
- 3.3.4 Strong passwords should be utilised. This means that passwords should:
- Be different to the last five (5) used
 - Be different to all passwords used in the past 6 months
 - Have at least a minimum password length of eight (8) characters
 - Contain at least one upper case character (A-Z) and one lower case character (a-z)
 - Have at least one numeric or non-alphanumeric character as well as letters

- 3.3.5 Where possible, passwords should not be identifiable with the user (such as first name, last name, spouse name friends, relations, colleagues, or other easily guessed names). This is rarely able to be technically enforced so is recommended for inclusion in awareness programs for staff.
- 3.3.6 The length and composition of passwords should be automatically enforced by the system at the time of construction.
- 3.3.7 NULL (blank) passwords should be prohibited.

3.4 Password Composition, Length and Validity Better Practice

In addition to the above good practice controls, the following better practice controls are also recommended:

- 3.4.1 System and security administrator passwords (e.g., root, enable, Administrator, SYSTEM) should be a minimum of twelve characters long.
- 3.4.2 System and Security Administrator passwords should be changed regularly on a basis relative to their password length.

Minimum Length	Duration
8 characters	60 days
9 characters	90 days
12 characters	180 days

- 3.4.3 Stronger password composition should include the following:
 - Have at least a minimum password length of twelve (12) characters
 - Have at least one numeric and one non-alphanumeric character as well as letters
- 3.4.4 Where possible, utilise passphrases rather than password. A passphrase uses a string of words rather than a single word, or randomised alphanumeric. For example a passphrase could be "rowRowRowYourBoat3times?".
- 3.4.5 For systems requiring additional security, the use of two factor authentication (2FA) such as the use of one-time passwords generated by a token or sent via SMS to a user's phone, or the use of digital certificates or biometrics, is recommended. Such additional security is recommended for situations including:
 - Authenticating users connecting via remote access solutions
 - Authenticating users connecting to complete administrative tasks
 - Authenticating users connecting to high-security environments (if applicable)

3.5 Lockout of User Accounts after Failed Logon Attempts

It is recommended that CGIAR centers maintain a policy which contains the following account lockout requirements.

- 3.5.1 User IDs should be locked and users prevented access to the network after a maximum of four (4) consecutive invalid login attempts for that User ID.
- 3.5.2 Locked Out user accounts should be reactivated after a period of time, not less than 30 minutes. An alternative scheme for lock out is to increase the time of lock out between each incorrect attempt, starting from one minute of lock out, then 2 minutes, 4 minutes, 8 minutes or permanent lockout until lifted by helpdesk.
- 3.5.3 The User IDs for users with privileges such as root, administrator or supervisor should not be suspended as their suspension could create a denial of an essential service. Instead a time delay should be implemented after each invalid attempt to make brute force guessing attacks more difficult.

3.6 Password Administration

It is recommended that CGIAR centers maintain a policy which contains the following password administration requirements.

- 3.6.1 Accounts should be suspended if the user does not replace the initial or reset password within five (5) days.
- 3.6.2 Default user accounts and passwords should be immediately altered following installation of systems or software.
- 3.6.3 Passwords should not be set to never expire.

3.7 Login/Logout Processes

It is recommended that CGIAR centers maintain a policy which contains the following password login / logout requirements.

- 3.7.1 The login screen for multi-user computers (apart from those on a visitors or public network) should include a special notice that:
 - The system may only be accessed by authorized users
 - Users who login accept that they are authorized to do so
 - Unauthorized system usage or abuse is subject to disciplinary actions
 - System usage may be monitored and logged
- 3.7.2 If there has been no activity on a computer terminal, workstation or desktop computer for at least 15 minutes, the system should automatically blank the screen and suspend or lock the session. Reestablishment of the session should take place only after the user has provided the correct password. This suspension period can be shortened for administrators and users of confidential data or be lengthened for systems intended for broad use.

3.8 User Account Management

It is recommended that CGIAR centers maintain a policy which contains the following user account management requirements.

- 3.8.1 Generic network user accounts should be disabled or locked down where possible.
- 3.8.2 Redundant user-IDs (ie, an account of a staff member who has left the center) should not be reissued to other users. This is not intended to imply that any given user ID should only be used once, but rather that after a user has left, their account should be closed and any information attached to that account removed. The old/existing account should not simply be given to a new user instead of creating a new account.
- 3.8.3 User accounts should be disabled if they have been inactive for a preset period of time (often set to 90 days, but variable depending on the system privileges which the account is linked to), even if the staff member is still active in the center.
- 3.8.4 Privileged access rights should be assigned to different user accounts than those used for day to day activities. Where possible, each user should have a separate privileged account unique to that user.
- 3.8.5 Where a clear business benefit exists, the creation and use of a shared user-ID for a group of users may be used. Appropriate monitoring of these accounts and logs of use should be maintained by the system owner.

3.9 Termination of User Access

It is recommended that CGIAR centers maintain a policy which contains the following user access termination requirements.

- 3.9.1 In case of voluntary or scheduled termination of employment of a user, the Center should immediately remove the User ID upon the departure of the user to remove their access to the network, unless extension of the account is required for center purposes.
- 3.9.2 Where continued existence and use of an account is required after a user has left employment of a center, authorisation is required by the IT Manager and relevant center managers. Additionally, if extension is approved and where necessary, the user of the extended account may be limited to 'read only' privileges.
- 3.9.3 In case of a user being subject to involuntary termination of employment for cause, the Center should close the User ID, and access to the network, immediately that the decision on termination is made. The Center should implement appropriate "end of employment" procedures to ensure the necessary authority is promptly communicated to the network administrator in such cases.

4 APPENDIX A: DEFINITIONS

Clear text: Messages or text that is non encrypted or does not need to be deciphered to be in its original form.

Non-alphanumeric character: Characters that are neither numbers nor letters, so typically symbols such as !@#\$%^&*()_~"?'><.,\

Passphrase: Similar to a password, a passphrase is a password that is constructed using a sentence, so is often longer (and therefore more difficult to attack / crack) than regular passwords. An example would be "ThisPasswordIsStrongerThanARegularPassword"

Service account passwords: Passwords which are set for system level administrative accounts. These may be known by an entire team or a number of staff collectively, as opposed to personal passwords which are usually only known by an individual user.

5 APPENDIX B: CHECKLISTS

The following checklists are designed to assist CGIAR centers that wish to adopt any or all of the good 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.

5.1 Good Practice Checklist

Guideline Number	Guideline	Tick if center currently adhere to this guideline
Section 3.1 – General Policy on User Identification and Authentication		
3.1.1	<ul style="list-style-type: none"> ▪ Assign unique user IDs to all users 	<input type="checkbox"/>
3.1.2	<ul style="list-style-type: none"> ▪ User-IDs should not indicate privilege levels 	<input type="checkbox"/>
3.1.3	<ul style="list-style-type: none"> ▪ Users should be held accountable for all activity from their account 	<input type="checkbox"/>
3.1.4	<ul style="list-style-type: none"> ▪ Users should not be allowed to use a computer system which is logged into a center's network unless supervised by the owner or person responsible for the logged in account. 	<input type="checkbox"/>
3.2 Passwords Confidentiality		
3.2.1	<ul style="list-style-type: none"> ▪ Users should maintain secrecy of personal CGIAR access passwords 	<input type="checkbox"/>
3.2.2	<ul style="list-style-type: none"> ▪ Initial or reset passwords should be communicated in a secure manner 	<input type="checkbox"/>
3.2.3	<ul style="list-style-type: none"> ▪ Users should be required to change initial / reset passwords after logging into the system 	<input type="checkbox"/>
3.2.4	<ul style="list-style-type: none"> ▪ Initial or reset passwords not used within a period of time and the related account should be suspended until needed upon which a new password is created / issued 	<input type="checkbox"/>
3.2.5	<ul style="list-style-type: none"> ▪ Passwords and user IDs should not be shared with other users 	<input type="checkbox"/>
3.2.6	<ul style="list-style-type: none"> ▪ Passwords should be masked on the computer screen 	<input type="checkbox"/>
3.2.7	<ul style="list-style-type: none"> ▪ Passwords should not be written or stored either physically nor electronically in plain text or unencrypted 	<input type="checkbox"/>
3.3 Passwords Composition, Length and Validity Good Practice		
3.3.1	<ul style="list-style-type: none"> ▪ System and security administrator passwords should be reviewed and updated / revoked prior to any change in administrative responsibility 	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adhere to this guideline
3.3.2	<ul style="list-style-type: none"> ▪ System and Security Administrator passwords should be changed at least every 120 days 	<input type="checkbox"/>
3.3.3	<ul style="list-style-type: none"> ▪ Passwords should be changed at least every two months, with a maximum lifetime of 90 days and a minimum lifetime of two days 	<input type="checkbox"/>
3.3.4	<ul style="list-style-type: none"> ▪ Passwords should be changed immediately if they become, or are suspected of having become, compromised. 	<input type="checkbox"/>
3.3.5	<ul style="list-style-type: none"> ▪ Strong passwords should be utilised. This means that passwords should: <ul style="list-style-type: none"> ▪ Be different to the last five (5) used ▪ Be different to all passwords used in the past 6 months ▪ Have at least a minimum password length of eight (8) characters ▪ Contain at least one upper case character (A-Z) and one lower case character (a-z) ▪ Have at least one numeric or non-alphanumeric character as well as letters 	<input type="checkbox"/>
3.3.6	<ul style="list-style-type: none"> ▪ The length and composition of passwords should be automatically enforced by the system at the time of construction. 	<input type="checkbox"/>
3.3.7	<ul style="list-style-type: none"> ▪ NULL (blank) passwords should be prohibited. 	<input type="checkbox"/>
3.4 Passwords Composition, Length and Validity Better Practice		
3.4.1	<ul style="list-style-type: none"> ▪ System and security administrator passwords should be a minimum of twelve characters long. 	<input type="checkbox"/>
3.4.2	<ul style="list-style-type: none"> ▪ System and Security Administrator passwords should be changed regularly dependent on length and system criticality 	<input type="checkbox"/>
3.4.3	<ul style="list-style-type: none"> ▪ Stronger password composition should include the following: <ul style="list-style-type: none"> ▪ Have at least a minimum password length of twelve (12) characters ▪ Have at least one numeric and one non-alphanumeric character as well as letters 	<input type="checkbox"/>
3.4.4	<ul style="list-style-type: none"> ▪ Passphrases should be utilised rather than passwords 	<input type="checkbox"/>
3.4.5	<ul style="list-style-type: none"> ▪ Systems requiring additional security require two factor authentication, for example: <ul style="list-style-type: none"> ▪ Authenticating users connecting via remote access solutions 	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adhere to this guideline
	<ul style="list-style-type: none"> ▪ Authenticating users connecting to complete administrative tasks ▪ Authenticating users connecting to high-security environments (if applicable) 	
3.5 Lockout of User Accounts after Failed Logon Attempts		
3.5.1	<ul style="list-style-type: none"> ▪ User IDs should be locked and users prevented access to the network after a maximum of four (4) consecutive invalid login attempts 	<input type="checkbox"/>
3.5.2	<ul style="list-style-type: none"> ▪ Locked Out user accounts should be reactivated after a period of time 	<input type="checkbox"/>
3.5.3	<ul style="list-style-type: none"> ▪ User IDs for users with privileges such as root, administrator or supervisor should not be suspended 	<input type="checkbox"/>
3.6 Password Administration		
3.6.1	<ul style="list-style-type: none"> ▪ Accounts should be suspended if the user does not replace the initial or reset password within five (5) days. 	<input type="checkbox"/>
3.6.2	<ul style="list-style-type: none"> ▪ Default vendor passwords should be immediately altered following installation of systems or software. 	<input type="checkbox"/>
3.6.3	<ul style="list-style-type: none"> ▪ Passwords should not be set to never expire 	<input type="checkbox"/>
3.7 Login / Logout Processes		
3.7.1	<ul style="list-style-type: none"> ▪ The login screen for multi-user computers (apart from those on a visitors or public network) should include a special notice that: <ul style="list-style-type: none"> ▪ The system may only be accessed by authorized users ▪ Users who login accept that they are authorized to do so ▪ Unauthorized system usage or abuse is subject to disciplinary actions ▪ System usage may be monitored and logged 	<input type="checkbox"/>
3.7.2	<ul style="list-style-type: none"> ▪ If a terminal is idle for 15 minutes, the system should automatically blank the screen and suspend or lock the session 	<input type="checkbox"/>
3.8 User Account Management		
3.8.1	<ul style="list-style-type: none"> ▪ Generic network user accounts should be disabled or locked down where possible. 	<input type="checkbox"/>
3.8.2	<ul style="list-style-type: none"> ▪ Redundant user-IDs should not be reissued to other users. 	<input type="checkbox"/>

Guideline Number	Guideline	Tick if center currently adhere to this guideline
3.8.3	<ul style="list-style-type: none"> Privileged access rights should be assigned to different user accounts than those used for day to day activities. 	<input type="checkbox"/>
3.8.4	<ul style="list-style-type: none"> Creation and use of a shared user-ID for a group of users may be used. Appropriate monitoring of these accounts and logs of use should be maintained by the system owner. 	<input type="checkbox"/>
3.9 Termination of User Access		
3.9.1	<ul style="list-style-type: none"> Upon voluntary / scheduled termination of users, the user ID should be disabled and access removed from the network, unless required elsewhere 	<input type="checkbox"/>
3.9.2	<ul style="list-style-type: none"> Upon involuntary termination of users, the user ID should be disabled and access removed from the network, as soon as the decision of termination is made. 	<input type="checkbox"/>

6 DOCUMENT CONTROL

Version Control Log

Version	Description	Date
1.00	Third revision following 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/> "