CMSGu2011-08

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Access Control

CERT-MU

National Computer Board
Mauritius

September 2011

Issue No. 8

Version 1.0

Table of Contents

Tables and Figures

Tables

Figures

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

This guideline covers physical and logical access controls, but lays more emphasis on logical access control in order to give users a broad idea of how to restrict access to systems and data.

1.2 Audience

This document, which technical in nature, provides the background for system administrators, information security officers, system owners and data owners to set controls on their systems to protect confidential information. It also helps organisations to manage user accounts, passwords and remote accesses.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document’s content, the targeted audience and the document’s structure.

Section 2 presents a background on physical and logical access controls.

Section 3 provides details on managing accounts.

Section 4 gives an insight on managing passwords.

Section 5 presents an overview on remote access.

Section 6 concludes the document.

Section 7 comprises a list of references that have been used in this document.

2.0 Background

Access control is, in fact, a daily happening. A lock on a car door is basically a form of access control. A PIN on an ATM system at a bank is another means of access control. The possession of access control is of primary importance when people need to secure important, confidential, or sensitive information and equipment.

2.1 Physical Access Control

Physical access control restricts entrance to a property, a building, or a room to authorised persons. Physical access control can be achieved by a human (a security guard or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems. Within these environments, physical key management may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.

An access control system is meant to check who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Previously this was partially achieved through locks and keys. When a door is locked only someone with a key can enter through the door depending on how the lock is configured. Mechanical locks and keys do not allow restriction of the key holder to specific times or dates. Mechanical locks and keys do not provide records of the key used on any specific door and the keys can be easily duplicated or transferred to an unauthorised person. When a mechanical key is lost or the key holder is no longer authorised to use the protected area, the locks must be re-keyed.

Electronic access control uses computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is denied, the door remains locked and any attempt to access the restricted area is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

2.2 Logical Access Control

While physical access control protects IT systems through physical barriers, logical access control protects IT systems and data by verifying and validating authorised users, authorising user access to IT systems and data, and restricting transactions (read, write, execute, delete) according to the user's authorisation level. Logical access control requirements are defined in the following three areas:

- Account Management
- Password Management
- Remote Access

Organisations should develop and document logical access control policies and processes that encompass all three elements.

Logical access controls are a technical means of implementing access policies. Development of the access control policies should be directed by the Head of the organisation/department, with the assistance of the Information Security Officer, System Owners, and Data Owners. The access control policies must provide protection of IT systems and data corresponding to sensitivity and risk. Development of such policies requires balancing the interests of security (sensitivity and risk) against what is needed to accomplish the agency's mission (operational requirements, user-friendliness, and cost), as illustrated in Figure 1.

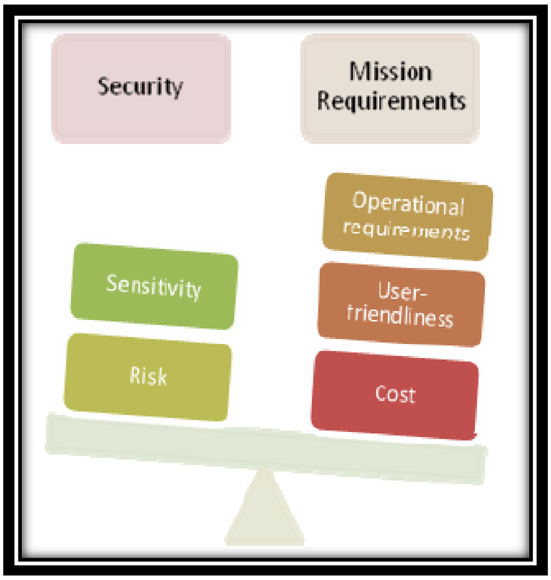

Figure 1 Balance Mission Requirements Against Sensitivity and Risk

Integrated identity and access management is a maturing domain of IT security. Organisations should consider solutions that provide automated and integrated management of the following:

- User identity
- Access requests
- Account creation and termination
- Account privileges
- Passwords, including self-service password resets

3.0 Account Management

Effective account management is vital to providing Logical Access Control in line with sensitivity and risk. It consists of the processes of requesting, authorising, administering, and terminating accounts which access IT systems and data, as illustrated in Figure 2.

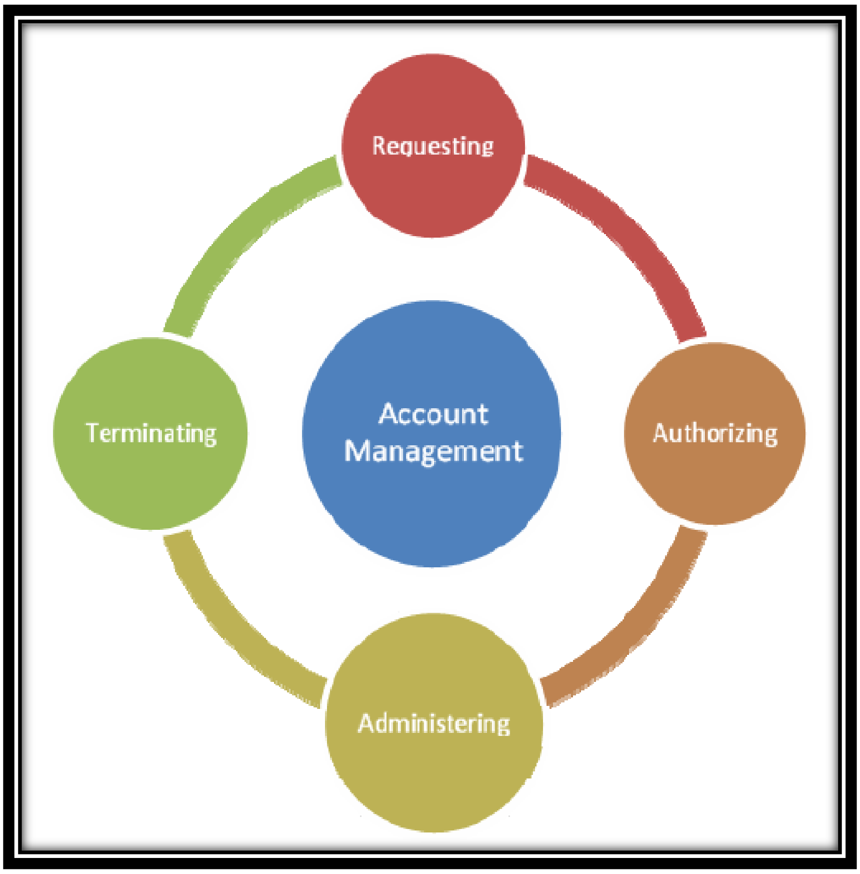

Figure 2 Account Management Cycle

3.1 Defining Identification, Authorisation, and Authentication

As shown in Figure 3, System and Data Owners develop the requirements for identification, authorisation, and authentication to access an IT system according to the sensitivity and risk of the IT system and the data it processes.

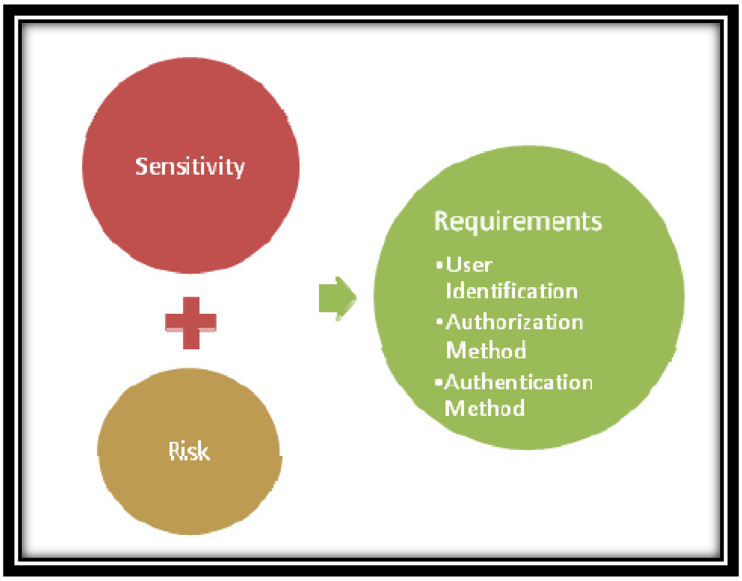

Figure 3 Defining Requirements

Passwords are specifically required for access to all sensitive IT systems and are recommended for all IT systems. Organisations should document policies and procedures that require User IDs and passwords to be passed on to users separately.

Other authentication methods should be considered according to risk and sensitivity. In determining sensitivity level for customer-facing systems, organisations should consider:

- Whether to allow customer access to the data raises the sensitivity level of the data,
- Whether customers have access only to data regarding themselves, or
- Whether they have access to data regarding others, and the appropriate corresponding sensitivity level

Besides, organisations should document policies and procedures that require user acknowledgement of an Information Security Access Agreement prior to receiving access to an IT system. The nature of this agreement will vary depending on the role of the user.

For internal IT systems, and for customer-facing IT systems, where customers have access only to data regarding themselves, the Information Security Access Agreement should document requirements that users:

- Safeguard access control mechanisms such as user IDs and passwords and to use only those access control mechanisms specifically assigned to them
- Receive specific authorisation for any additional access required

- Comply with all applicable security policies, procedures, and standards
- Report any violation of the agreement to the head of the department

Moreover, for customer-facing IT systems where customers have access to data regarding others, the Information Security Access Agreement should document the following:

- Authorised use and disclosure of the data to which the customer user is granted access
- Responsibilities for protection of the data to which the customer user is granted access
- Terms and conditions of the agreement
- Legal liabilities under the agreement

3.2 Access Requests

Organisations must establish policies and procedures for requests and authorisation for access to IT systems and data. The policy and procedures must require that access is authorised using the principle of least privilege. Access to IT systems and data may only be granted with the approval of the user's supervisor and the System Owner. "Guest" or shared accounts are not allowed. These requirements for internal IT systems are illustrated in Figure 4.

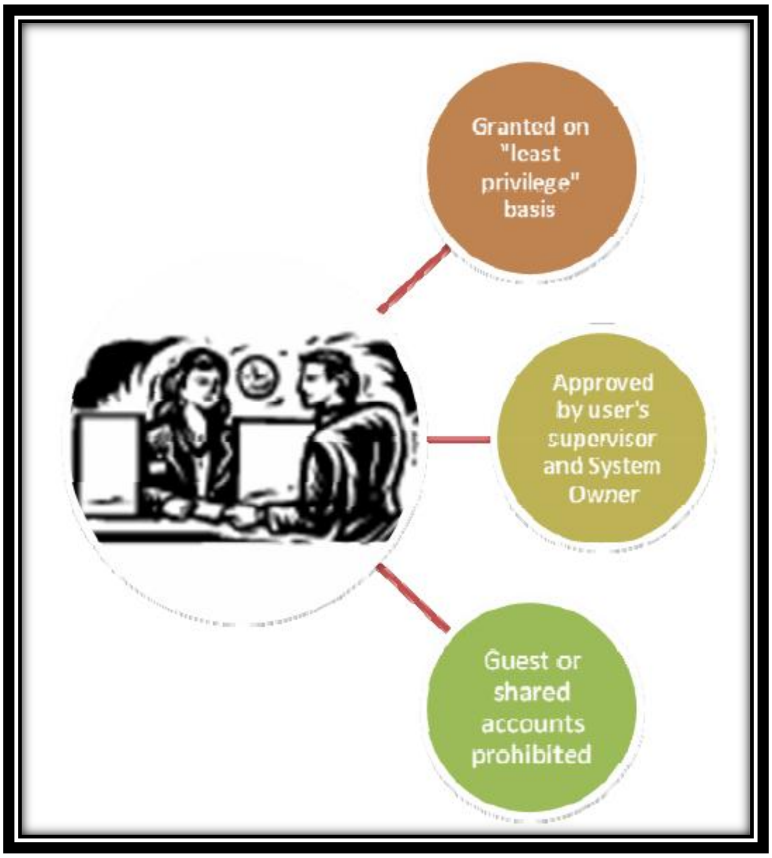
Granted on "least privilege" basis
Approved by user's supervisor and System Owner
Guest or shared accounts prohibited

Figure 4 IT System Access Request Requirements for Internal IT Systems

Organisations should document policies and procedures for requests and authorisation for access to IT systems and data that reflect the differentiation of sensitivity. In particular, organisations should document appropriate access requests and authorisation requirements for customer-facing IT systems, since customers do not have a supervisor to approve the request. Furthermore, organisations may, at their discretion, wish to allow approval of access requests for low sensitivity systems by the System Owner in order to reduce the administrative burden of these low sensitivity systems on the System Owner.

3.2.1 Least Privilege

Access to IT systems and data must be granted on the basis of least privilege. The principle of least privilege allows organisations to provide access only to those systems that users require for performing their tasks. Least privilege requires that organisations must authorise the most restrictive access level necessary for users to perform these functions. Adhering to least privilege principle enhances protection of IT systems and data.

3.2.2 Role-based Access Control

Role-based access control grants access to IT systems and data to users based on their roles within the organisation or as customers of the organisation, rather than on individual users. Organisations should adopt role-based access control as part of their account management policies.

The use of role-based access control is recommended because it simplifies the administration of user access rights by associating these rights with a limited number of standardised roles. This association of access rights with standardised roles also assists in maintaining the principle of least privilege. Organisations should adopt access control policies that prohibit assignment of multiple roles to a single user that can combine to violate separation of duties requirements.

3.2.3 Approval

Before granting access to IT systems and data, organisations must have documentation of the access request. For IT systems with sensitivity of medium and higher, the request must be approved by the System Owner, and, for internal systems, by the user’s supervisor. While the System Owner approves the request based on need to know relative to the data, the user’s supervisor approves the request based on job requirements.

3.2.4 Prohibition of "Guest" or Shared Accounts

Individual accountability is essential for IT systems security. Organisations must not authorise the creation of accounts that can be used anonymously or by more than one person. A guest account enables anonymous access to an IT system, while a shared account (or shared password) hides individual accountability within a group. Both types of accounts, and the sharing of passwords or other logical access methods, are forbidden.

3.3 Account Maintenance

Established accounts require maintenance on a continuous basis to strengthen IT security. Accounts must be validated periodically to determine if the access is still necessary and meets the requirements of least privilege. If not, the access level must be changed or the account disabled/deleted. Organisations should document policies and procedures for the account maintenance activities and requirements described in Figure 5.

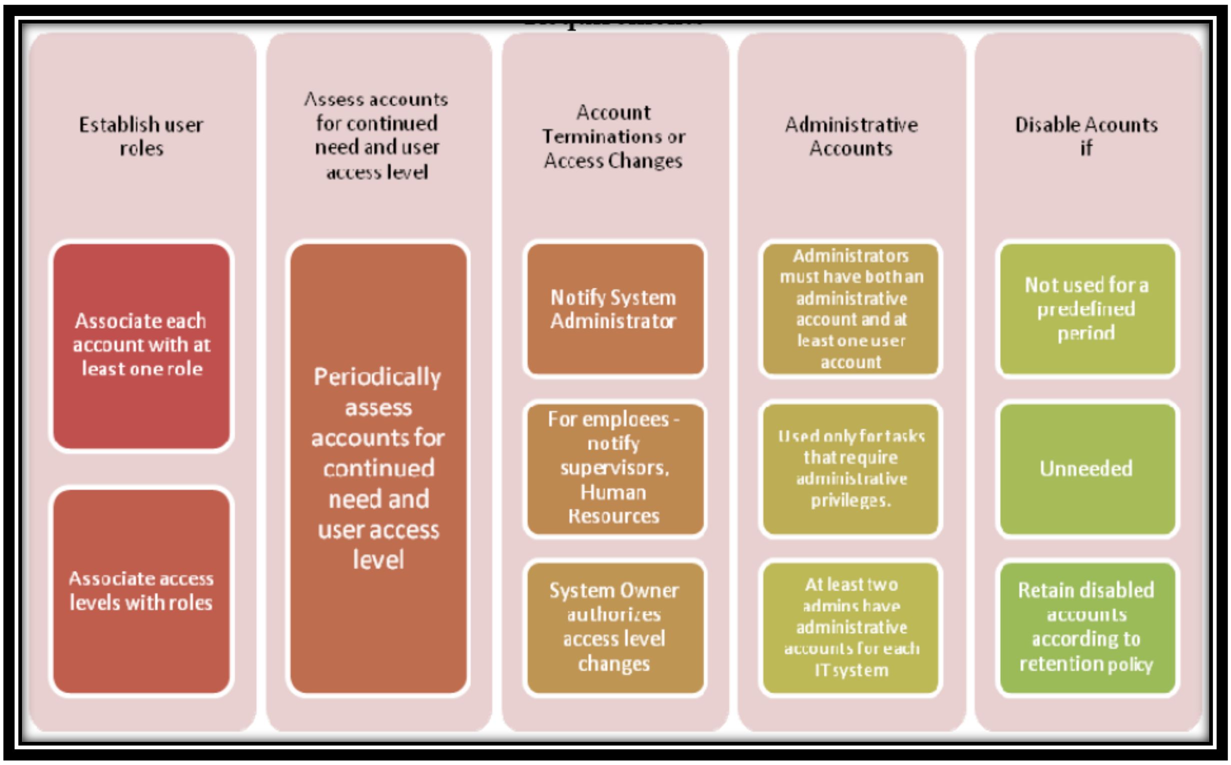
Establish user roles
Associate each account with at least one role
Associate access levels with roles
Assess accounts for continued need and user access level
Periodically assess accounts for continued need and user access level
Account Terminations or Access Changes
Notify System Administrator
For emploees - notify supervisors, Human Resources
System Owner authorizes access level changes
Administrative Accounts
Administrators must have both an administrative account and at least one user account
Used only for tasks that require administrative privileges.
At least two admins have administrative accounts for each IT system
Disable Acounts if
Not used for a predefined period
Unneeded
Retain disabled accounts according to retention policy

Figure 5 Account Maintenance Activities and Requirements

4.0 Password Management

Passwords are required for accounts on sensitive IT systems and recommended for access to all IT systems. Organisations must document their password management policies and procedures. These policies and procedures must include requirements for the following:

- Password complexity
- Secure delivery of new passwords to users
- User activities to keep passwords secure
- Password administration
- Responding to lost, stolen or compromised passwords
- Resetting passwords
- Session controls
- Changing vendor default passwords

4.1 Password Requirements

Organisations must document password length, complexity, duration, and reuse requirements according to risk and sensitivity. Password requirements for each IT system should be documented in policies and procedures for the IT system. These password characteristics are defined in Table 1.

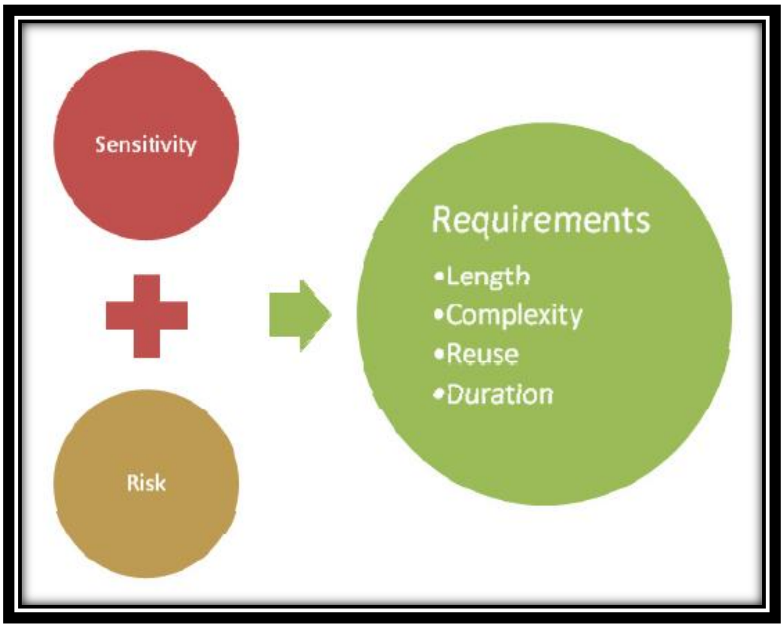

Figure 6 Password Requirements

In accordance with IT security best practice, organisations should require passwords that:

- Are at least eight characters long
- Contain a combination of letters, numbers, and special characters/symbols
- Are forced to be changed at least every 90 days
- Cannot be reused for at least 12 months
- Are masked during entry and encrypted during transmission and storage

Most operating systems have configurable password generators that will enable the IT system to generate passwords that conform to these requirements in accordance with the System Owner's password policy for each IT system. Table 2 below explains password requirement terms in more detail.

Length	The minimum and maximum number of characters allowed in the password.
Complexity	The variety of characters required or allowed in the password. Character variety includes letters, numbers, and symbols (e.g. %, $, _). A password containing upper and lower-case letters, numbers, and symbols is the most complex.
Reuse	The amount of time that must pass before a previous password may be reused. Limiting reuse reduces risk by preventing users from repeatedly using the same one, two or three passwords.
Duration	The maximum amount of time that may pass before a user is required to establish a new password.

Table 1 Password Requirements Terms

4.2 Initial and Replacement Passwords

Organisations should document policies and procedures for distribution of initial and replacement passwords. Any new password provided to a user (either for initial use or as a replacement) must be unique. In this context "unique" means the password cannot be common to any two or more new users (e.g. the IT system name, or "abc123"), nor can it be derived from public information (e.g. the user's last name and phone extension). The best practice is to use a password generator configured to the password policy of the IT system. Initial or replacement passwords must be securely delivered to the user and the user must be required to change the initial or replacement password immediately upon its first use.

4.3 User Management of Passwords

Organisations must document the responsibilities that users of IT systems have for the management of passwords. In particular, policy must reflect the characteristics shown in Figure 7. Users must agree to the responsibilities prior to being granted access.

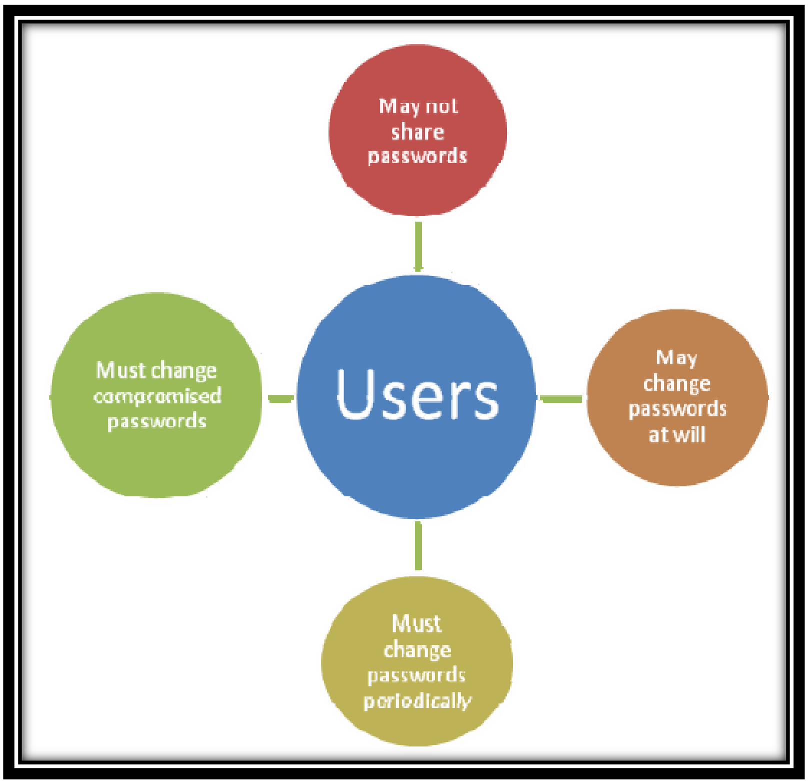
May not share passwords
Must change compromised passwords
Users
May change passwords at will
Must change passwords periodically

Figure 7 User Password Management Responsibilities

4.4 Password Maintenance

System Owners must document password maintenance practices to be followed by System Administrators for each IT system. At a minimum, these practices must cover those listed in Figure 8.

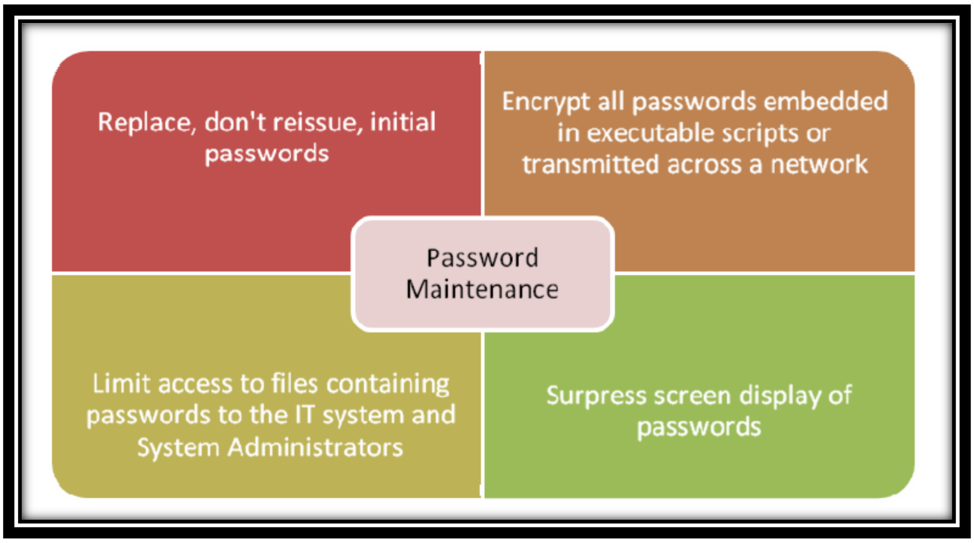
Replace, don't reissue, initial passwords
Encrypt all passwords embedded in executable scripts or transmitted across a network
Password Maintenance
Limit access to files containing passwords to the IT system and System Administrators
Surpress screen display of passwords

Figure 8 Password Maintenance Requirements

4.5 Lost, Stolen, Compromised Passwords

Organisations must document procedures for handling lost, stolen, or compromised passwords. At a minimum these procedures must require users to:

- Immediately report, to the head of the department, the loss, theft, or compromise of passwords; and
- Immediately change their password, in case it is compromised.

Organisations should establish and adhere to consistent, secure processes for verifying user identity before providing a replacement password.

4.6 Password Reset Process

Organisations should document policies and procedures for resetting user passwords. These policies and procedures should require that users authenticate their identities before having their passwords reset. Where possible and where required by IT system or data sensitivity, organisations should document policies that require the following criteria:

- Verification of the user's identity prior to delivery of the reset password to the user
- Logging delivery of the reset password
- The user to change the reset password on first use

In many cases, it will be required that users be able to request and receive password resets by means of a telephone call to a help desk. In such cases, hand delivery of the reset password to the user may not be viable. In these cases, organisations should document policies that require verification of the user's identity via information known only to the help desk and the user, in addition to the other requirements described above.

4.7 Session Controls

Organisations should document session controls to prevent the compromise of passwords and the unauthorised use of established accounts. Organisations should adopt session controls commensurate with sensitivity and risk; at a minimum these controls should:

- Lock user accounts after no more than three unsuccessful login attempts in a row and delay login for no less than 30 minutes, or require an administrator to reset the account before allowing login.
- Lock user sessions after inactivity of no more than 10 minutes until the user re-establishes access using appropriate identification and authorisation procedures (i.e. user ID and password); and
- Terminate user sessions after inactivity of no more than 60 minutes.

4.8 Default Vendor Passwords

IT hardware and software products are often supplied with default passwords that are set by the vendor. To protect against compromise of IT systems and data by means of these passwords, organisations should document policies and procedures that require default vendor passwords to be changed before IT hardware and software is placed into production.

5.0 Remote Access

Remote Access to sensitive IT systems and data may pose serious risks to the organisation. Organisations must document the policies and procedures in order to manage these risks.

5.1 Encryption of Remote Access Sessions

All remote access to sensitive IT systems and data must be encrypted. The encryption must begin with the initiation of the session, include all user identification and authentication, and not end until the session is terminated.

5.1.1 Remote Access Encryption Techniques

The two most widely used remote access encryption techniques are Virtual Private Networks (VPNs) and link encryption. VPNs are primarily used when the remote access occurs through an open network, such as the Internet, while link encryption is used primarily when the remote access occurs through a closed network, such as a dial-up connection. Figures 9 and 10 illustrate these two remote access methods.

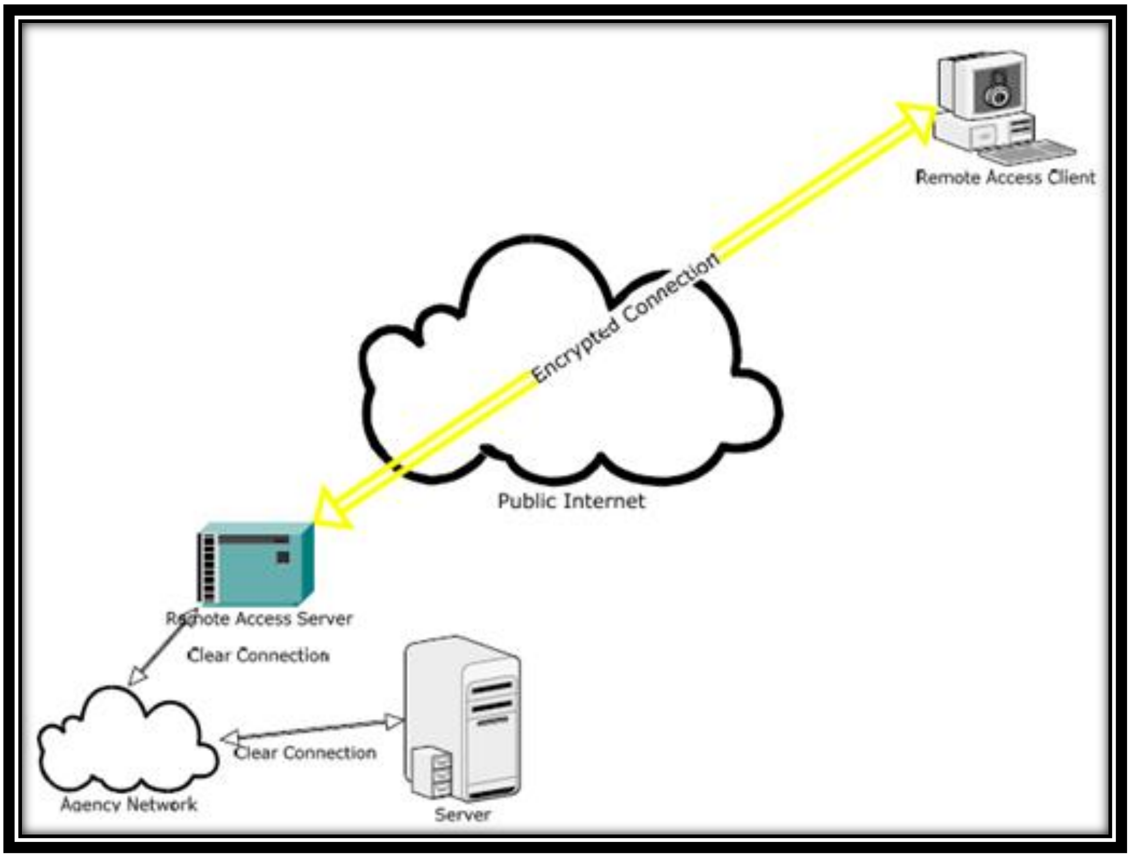

Figure 9 VPN Remote Access

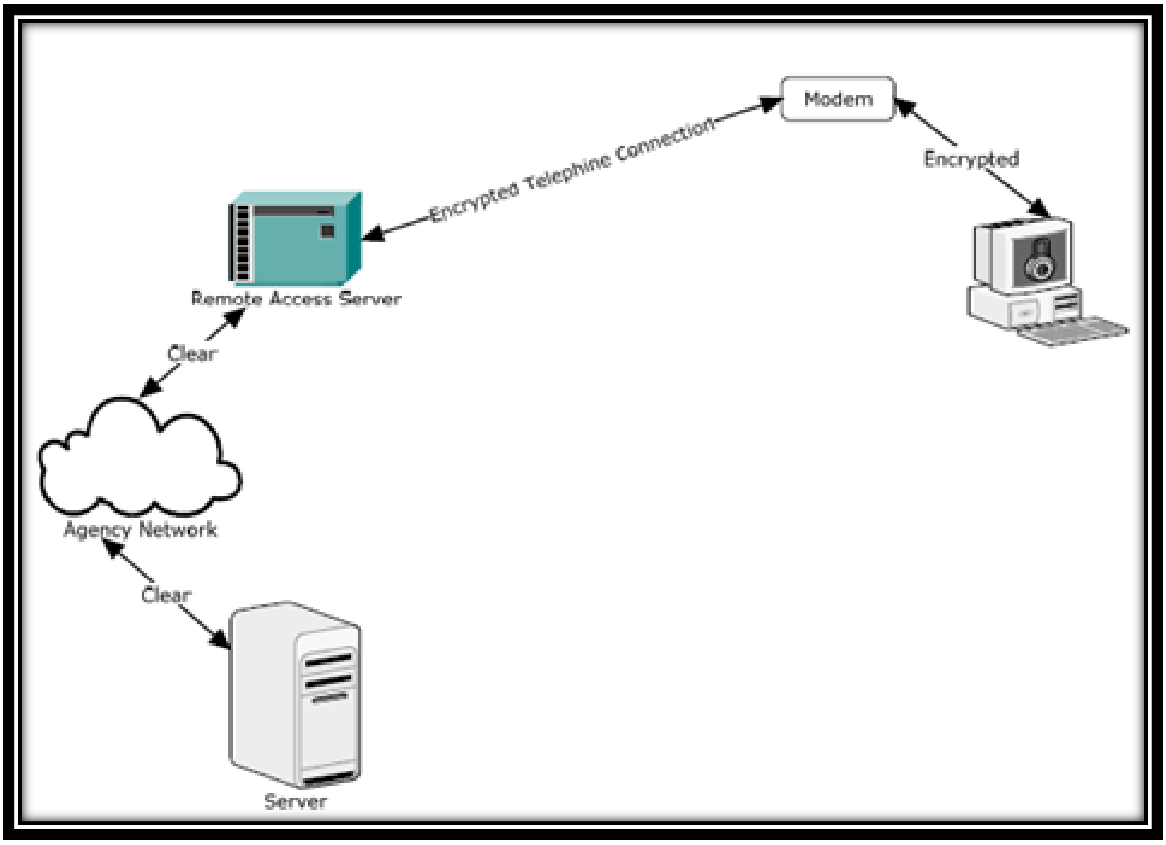

Figure 10 Link Encryption Figure

The administration of specific remote access technologies is beyond the scope of this guideline. Organisations are advised to seek detailed guidance on securing remote access from third-party remote access providers or vendors of the remote access solutions.

5.2 Remote Access Service Hardening

Equipment providing remote access services must be hardened physically (e.g. stored in lockable spaces) and logically (e.g. access protected with passwords, tokens, etc.), as shown in Figure 11. These protections increase the security of the implemented remote access solutions.

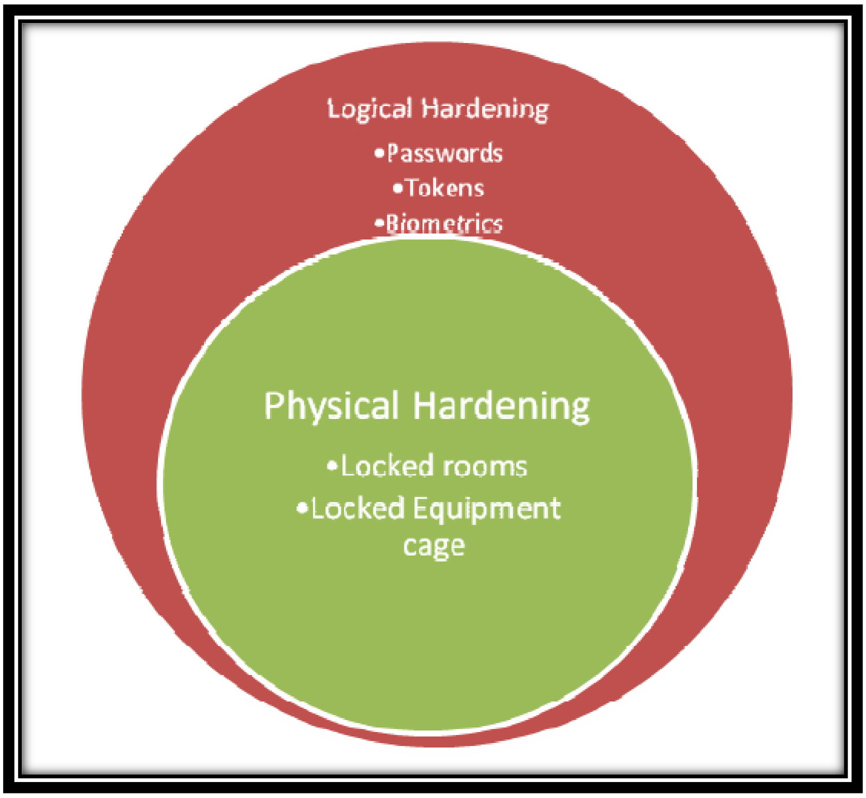

Figure 11 Remote Access Equipment Hardening

5.3 Remote Access Records

Organisations must maintain auditable records of remote access attempts and sessions. Because of transaction volumes, these logs should be automatically generated - most remote access solutions provide this capability. Organisations have to protect these logs as sensitive information.

5.4 Training

Users must be trained on the remote access policies and procedures before they receive remote access authorisation.

6.0 Conclusion

Access control can play a key role in securing a building and its surroundings. It is also very useful in controlling access to systems, files and data. This document provided an overview of the different mechanisms that can be used to restrict access, namely through passwords and permissions depending on roles. Access control, however, has to be employed as part of a well understood and concise policy to fully meet its objectives.

7.0 References

- Virginia Information Technologies Agency (VITA): Information Technology Logical Access Control Guideline
- Wikipedia: http://en.wikipedia.org
- New York City Police Department: Guidelines On Access Control, Screening & Monitoring