HPOL#09
Logical Access Control

(Version 1.0)

Table of Contents

9.1. SCOPE AND OBJECTIVES

In order to safeguard information and computing resources from various business and environmental threats, systems and procedures should be developed and implemented by the government organization for protecting them from unauthorized modification, disclosure or destruction and to ensure that information remains accurate, confidential, and is available when required.

The administration of user access to the organization's automated information should apply the principles of least privilege and be on the basis of "need to know / need to do". The procedures should be administered to ensure that the appropriate level of access control is applied to protect the information in each application and system.

This document addresses policies related to the logical access security of the government organization's information resources.

9.2. POLICY STATEMENT

9.2.1. BUSINESS REQUIREMENT FOR ACCESS CONTROL

9.2.1.1. Access Control Policy

9.2.1.1.1. Access to information must be specifically authorized in accordance with the government organization's User Access Control procedures.

9.2.1.1.2. Access to information will be controlled on the basis of business and security requirements, and access control rules defined for each information system.

9.2.1.1.3. All government organization users must be allowed access only to those critical business information assets and processes, which are required for performing their job duties.

9.2.1.1.4. Access to critical business information assets and activation of user accounts for contractors, consultants, temporary workers, or vendor personnel must only be in effect when the individual is actively performing service for the government organization.

9.2.1.1.5. For contractors, consultants, or vendor personnel, access to government organization critical business information assets, will be provided only on the basis of a contractual agreement.

Explanatory Notes

This agreement will, at a minimum, provide:

- *The terms and conditions under which access is provided.*
- *The responsibilities of the contractors, consultants or vendor personnel.*
- *Agreement by the contractors, consultants or vendor personnel to abide by the government organization's Security Policies.*

9.2.1.1.6. Individuals being involuntarily terminated are subject to the government organization's "Personnel Security Infrastructure" Policy.

9.2.2. USER ACCESS MANAGEMENT

9.2.2.1. User Registration

9.2.2.1.1. The registration and termination of users must be in accordance with User Registration and Termination Procedures.

9.2.2.1.2. All users of information resources must have a unique user ID and authorization from the system owner or management, to access the government organization's information assets.

9.2.2.1.3. All users must be provided with a written statement of their access rights and terms and conditions for usage of these rights, which should be formally accepted.

9.2.2.1.4. No users are provided access before the full completion of authorization procedures.

9.2.2.1.5. A formal record of all registered users must be maintained.

Explanatory Notes

This record must be checked periodically for unused, redundant, or expired user accesses or accounts, or incorrect privileges.

9.2.2.1.6. Redundant user ID's must not be re-issued to new users.

9.2.2.1.7. Accounts that are inactive for a pre-determined maximum number of days must be disabled.

Explanatory Notes

The cause for the inactive accounts should also be established.

9.2.2.1.8. User accounts of personnel transferred to different government organization Sections must be reviewed for appropriate privileges.

9.2.2.1.9. New accounts that have not been logged within a pre-defined maximum number of days must be disabled.

9.2.2.1.10. User accounts of personnel defined in the systems of the government organization must be removed immediately upon their termination.

9.2.2.1.11. All third party personnel requiring access to the government organization's information systems must follow Third Party Access Authorization procedures for registration, to access the government organization's information assets.

9.2.2.2. Privilege Management

9.2.2.2.1. All privileges to users must be assigned through a formal authorization procedure and the government organization must ensure that no privileges are assigned before the completion of authorization procedures.

9.2.2.2.2. All privileges must be allocated as and when required on a "need to know" basis.

9.2.2.2.3. Detailed records must be maintained for all privileges allocated.

9.2.2.3. Review of User Access Rights

9.2.2.3.1. All user access rights must be reviewed periodically.

Explanatory Notes

Review of all special privileged access rights (e.g. administrator accounts) must be carried out at more frequent intervals than that of other users of the system.

9.2.3. USER PASSWORD MANAGEMENT

9.2.3.1. Password Policy

9.2.3.1.1. All information systems of the government organization must require identification and authentication through passwords, pass-phrases, one-time passwords and similar password mechanisms.

9.2.3.1.2. Passwords for the government organization's systems must be created in accordance with this policy and the organization's password rules and guidelines for password configuration, composition, validity, and usage.

9.2.3.1.3. The government organization's information systems (access control programs) must be configured (where such configuration is possible) to fulfil the requirements of this policy and the organization's password rules, guidelines and procedures.

9.2.3.1.4. Passwords must be regarded as confidential information and must not be disclosed to any other person except in accordance with the government organization's password management procedures for safekeeping of passwords.

9.2.3.1.5. Users are responsible and liable for all actions performed by using their user ID(s) and password(s).

Explanatory Notes

Liability for actions performed will include but not be limited to transactions, information retrieval or communication on the government organization's information systems.

9.2.3.2. Password Validity Policy

9.2.3.2.1. All passwords must be changed after predetermined intervals.

Explanatory Notes

System-level and production environment passwords (e.g., root, admin, application administration accounts, etc.) must be changed at more frequent intervals than that of user-level passwords (e.g., application user, email, Web, desktop computer, etc.).

9.2.3.2.2. In case of forgotten passwords, temporary passwords should be issued only after positive identification of the user.

9.2.3.3. User Account Lock-out Policy

9.2.3.3.1. The government organization's information systems must be configured (where this is possible) to lock the user ID and prevent user access to the information system where an incorrect password has been used for a predetermined number of times in sequence.

9.2.3.3.2. Locked out user accounts must be reactivated in accordance with formal procedures to reactivate user accounts developed and implemented for this purpose.

Explanatory Notes

Such procedures must require identification of the user and determination of the reason for the lockout as a minimum for re-instating the user account and providing a new user password.

9.2.3.4. Password Uniqueness Policy

9.2.3.4.1. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

9.2.3.4.2. Passwords used for government organization accounts must not be the same as passwords used for access by other institutions.

9.2.3.4.3. Passwords must be checked to ensure that they are not identical to any of a predetermined number of previous passwords for the same account.

9.2.3.4.4. The same password must not be used for multiple government organization access needs.

9.2.3.5. Password Communication

9.2.3.5.1. Passwords must not be revealed in conversations, inserted into e-mail messages (where encryption options are unavailable) or other forms of electronic communication.

9.2.3.5.2. Passwords must not be written down, stored on any information system or storage device except in accordance with the government organization's password management procedures for safekeeping of passwords.

9.2.3.5.3. Initial temporary passwords must be conveyed in a secure manner.

Explanatory Notes

Passwords could be conveyed verbally in person, in hardcopy sealed envelop with confirmation of receipt, etc. Wherever encryption options are available, conveying of initial temporary passwords via e-mail should be considered.

9.2.3.5.4. All users must be forced to change their temporary passwords on first logon.

9.2.3.6. Password Composition

9.2.3.6.1. Guidelines should be developed for the composition of passwords.

Explanatory Notes

All user-level and system-level passwords must conform, at a minimum, to the guidelines described below:

- *Passwords must contain both upper and lower case characters (e.g., a-z, A-Z)*
- *Passwords must have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./*

- *Passwords must be at least eight alphanumeric characters long.*
- *Passwords must not be a word in any language, slang, dialect, jargon, etc.*
- *Passwords must not be based on personal information, names of family, friends, relations, colleagues, etc.*

9.2.3.7. Password Confidentiality

9.2.3.7.1. Passwords must never be written down or stored on-line. As far as possible, they should be easy to remember.

9.2.3.7.2. Passwords must not be revealed on any questionnaires or security forms.

9.2.3.7.3. Passwords must not be revealed to family members or co-workers.

9.2.3.7.4. Passwords are not to be displayed on the screen when entered.

9.2.3.7.5. Password files are stored in an encrypted form within the application, separately from the application data, to prevent any unauthorized access.

9.2.3.7.6. Vendor default passwords are not to be retained in the systems following the installation of any application or operating system software.

9.2.4. USER RESPONSIBILITIES

9.2.4.1. Unattended User Equipment

9.2.4.1.1. Procedures must be defined for access control of unattended user equipment.

Explanatory Notes

All users must at a minimum enable password-protected screen savers (where this is possible) on unattended user equipment including but not limited to user desktops, portable computers / laptops, and servers.

9.2.4.1.2. Each user must terminate active sessions when activities are finished.

9.2.4.1.3. Users must log off after completion of their tasks.

9.2.5. NETWORK ACCESS CONTROL

9.2.5.1. Policy on Use of Network Services

9.2.5.1.1. Access to networks and network services must be specifically authorized in accordance with the government organization's User Access Control procedures.

9.2.5.1.2. Access to networks and network services will be controlled on the basis of business and security requirements, and access control rules defined for each network.

Explanatory Notes

These rules will at a minimum take into account the following:

- *Security requirements of the network or network service(s).*
- *An identified business requirement for the user to have access to the network or network service ("need to know/access" principle).*
- *The user's security classification and the security classification of the network / network service.*
- *Legal and/or contractual obligations to restrict or protect access to assets.*
- *Definition of user access profiles and management of user access rights throughout the Information Systems network of the government organization.*

9.2.5.2. Enforced Path

9.2.5.2.1. Users should only be allowed access to networks and network resources through a pre-defined path commonly called an 'enforced path'.

Explanatory Notes

Users should not be allowed the flexibility of selecting other routes between the users' terminal and the network service to which the user is allowed to access.

9.2.5.3. User Authentication for External Connections

9.2.5.3.1. Remote user access to the government organization's networks should be subject to appropriate user authentication methods.

Explanatory Notes

The user authentication method used will depend on the user's security classification and the security classification of the network or network service to be accessed.

9.2.5.3.2. Dial-up access to the government organization's resources must be in accordance with the organization's Dial-up procedures and associated guidelines.

9.2.5.3.3. All remote users must dial-in to centralized communications servers.

9.2.5.3.4. The telephone numbers used for dial-in should not use the same exchange as the organization's published numbers.

9.2.5.3.5. Data lines must not be attached to the government organization's information network unless specifically authorized by management.

9.2.5.3.6. Network services must be disabled when using modems.

9.2.5.3.7. Access to internal networks from a remote site must be performed using cryptographic controls.

9.2.5.4. Node Authentication

9.2.5.4.1. Connections by remote computer systems must be authenticated.

Explanatory Notes

This authentication must be at the application computer and/or network level.

9.2.5.5. Remote Diagnostic Port Protection

9.2.5.5.1. All remote diagnostic connections for maintenance, support and special services (such as administration) must be secured and controlled.

9.2.5.5.2. Only authorized maintenance and support engineers should be allowed access to the diagnostic port.

Explanatory Notes

This connectivity should be provided only as and when required. After usage, connectivity must be disabled.

9.2.5.6. Segregation in Networks

9.2.5.6.1. The government organization's information systems network must be divided into logical segments based on the access requirements.

Explanatory Notes

The criteria for division of networks should consider the relative cost and performance impact of incorporating suitable technology.

9.2.5.6.2. Internal networks must be segregated from the external network with different perimeter security controls on each of the networks.

9.2.5.6.3. The connectivity between internal and external networks must be controlled.

9.2.5.7. Network Connection Control

9.2.5.7.1. All external connections by business partners and citizens must be documented and authorized in accordance with the defined "Request for Connectivity" procedure.

Explanatory Notes

A Service Policy Table must be formulated for each service that is allowed through each firewall. The table should list the service, the direction of the service, the business risks associated with allowing the service, and the business justification for allowing the service.

9.2.5.8. Network Routing Control

9.2.5.8.1. Appropriate routing control mechanisms must be deployed to restrict information flows to designated network paths within the control of the government organization.

9.2.5.8.2. Network routing controls must be based on positive source and destination address checking mechanisms.

9.2.5.9. Security of Network Services

9.2.5.9.1. The government organization must obtain detailed descriptions of the security attributes of all external value added services used (if any) from external network services providers.

9.2.5.9.2. The security attributes of all external value added services must establish the confidentiality, integrity, and availability of business applications and the level of controls (if any) required to be applied by the government organization.

9.2.5.9.3. A description of the security controls must be included in the agreement of the service.

9.2.6. OPERATING SYSTEM ACCESS CONTROL

9.2.6.1. Automatic Terminal Identification

9.2.6.1.1. Automatic terminal identification must be used when it is important that transactions are only initiated from a specific terminal or location.

9.2.6.2. Terminal Log-on Procedures

9.2.6.2.1. The terminal logon procedure must disclose a minimum amount of information about the system.

9.2.6.2.2. Personnel designated by management must set the password management system to suspend the user ID after a predefined number of consecutive unsuccessful attempts.

9.2.6.2.3. On suspension of the user ID, personnel designated by management must receive approval from the user's supervisor to reset the user ID.

9.2.6.2.4. A legal banner must appear on all government organization systems prior to login to the system.

9.2.6.2.5. Offices located outside the country must supplement this banner with an appropriate message in their local language.

Explanatory Notes

At no point in the banner or the supplement must the system be identified by organization name.

9.2.6.2.6. The logon procedure must not identify the system or application until the logon process has been successfully completed.

9.2.6.2.7. The system must validate the logon information only on completion of all input data.

9.2.6.2.8. After a rejected logon attempt, the logon procedures must terminate.

Explanatory Notes

The procedure must not explain which piece of information (the user ID or password) was the reason for the logon termination.

9.2.6.2.9. The logon procedures must set a maximum number of attempts and maximum time allowed for the logon process.

Explanatory Notes

If the number of attempts and/or the time is exceeded, the system must terminate the logon process and suspend the user ID.

9.2.6.2.10. On successful completion of logon, the logon procedures must display the date/time of the previous successful logon, and the number and date/time of unsuccessful logon attempts since the last successful logon.

9.2.6.3. User Identification and Authentication

9.2.6.3.1. The government organization must identify and authenticate all users uniquely before granting the appropriate system access.

9.2.6.3.2. The user ID naming convention must be consistent and documented.

9.2.6.3.3. User IDs must not be shared among users.

9.2.6.4. Use of System Programs

9.2.6.4.1. Access to and use of system programs must be restricted and controlled.

9.2.6.4.2. Use of system programs must be limited to authorized individuals.

9.2.6.4.3. All actions performed by an individual on system programs must be logged.

9.2.6.4.4. All unnecessary system utilities and software, including compiler programs, must be removed.

9.2.6.5. Use of System Utilities

9.2.6.5.1. Access to system tools that have the capability to override system and application controls are restricted from all users, except those with documented authorization. System tools shall be protected against unauthorized access.

9.2.6.5.2. Access to system utilities is limited to the minimum practical number of authorized individuals.

9.2.6.5.3. All access to system utilities is logged to facilitate the identification of inappropriate use.

9.2.6.5.4. Ad hoc use of system utilities is not allowed unless specifically authorized.

9.2.6.6. Duress Alarm to Safeguard Users

9.2.6.6.1. Assigning of duress alarms should be based on risk assessment.

9.2.6.6.2. Formal responsibilities and procedures for responding to a duress alarm should be defined by management of the government organization.

9.2.6.7. Terminal Time-out

9.2.6.7.1. After a defined period of inactivity, access to information services is locked and the display of information cleared.

Explanatory Notes

Re-authentication to the information service is needed to unlock access. Time out periods are set based upon risk assessment.

If terminal time out or workstation locking is not available, at a minimum, password protected screen savers are employed. If employees are required to leave their machines unattended for extended periods they will log off or shut down.

9.2.6.8. Limitation of Connection Time

9.2.6.8.1. Wherever possible, for high-risk systems, or for users or systems where access is only required during business hours, active sessions shall be limited to a specified timeframe.

9.2.7. APPLICATION ACCESS CONTROL

9.2.7.1. Information Access Restriction

9.2.7.1.1. Access to the government organization's information resources and applications must be restricted to users who require them and should be in accordance with the information Access Control and Asset Classification procedures.

9.2.7.1.2. All users must have controlled access to all information resources and business applications of the government organization, in accordance with their requirements.

Explanatory Notes

Controlled access would include but not be limited to Read, Write, Modify, Execute, and/or Full control.

9.2.7.1.3. The owner/s of information resources and business applications must review the access rights based on criticality of information and/or at regular predefined time intervals.

9.2.7.2. Sensitive System Isolation

9.2.7.2.1. All sensitive systems must have an isolated and highly secured computing architecture.

9.2.8. MONITORING

9.2.8.1. Monitoring System Access and Use

9.2.8.1.1. All event details on information systems must be logged and stored for a predetermined period.

9.2.8.1.2. All information systems and business applications must be monitored and the results of such monitoring must be reviewed periodically.

9.2.8.1.3. All real-time clocks must be synchronized and reviewed for inaccuracy and drift.

9.2.8.1.4. All unsuccessful login attempts to critical servers must be recorded, investigated, and if necessary, escalated to management.

9.2.9. ACCESS CONTROLS - OTHER

9.2.9.1. Mobile Computing and Remote Access

9.2.9.1.1. All mobile computing facilities must be used in a secured environment.

Explanatory Notes

Mobile computing facilities will include but not be limited to laptop computers, palm top computers, notebooks, and mobile phones.

Where possible, cryptographic controls for communication purposes should be used.

9.2.9.1.2. All mobile computing facilities must not be left unattended and must be physically secured.

9.2.9.1.3. All mobile computing facilities must have boot passwords and/or other security controls.

Explanatory Notes

Boot passwords are the passwords required for authentication, in order to 'start/switch-on' the system.

9.2.9.1.4. All personnel using remote access must be provided with a secure connection to the government organization's information system network.

Explanatory Notes

Secure connections would include but not be limited to Secure Socket Layer and Virtual Private Network.

9.2.9.1.5. The maintenance and support, audit, monitoring, training on security controls and practices, management of access rights, and physical security for remote access, must be in accordance with the government organization's defined procedures.

9.2.9.1.6. The government organization must restrict remote access to specific times and durations for all personnel availing themselves of these facilities.