Document Version: 1.2
Effective Date: 2021-11-10
Last Reviewed: 2021-11-10

6.24 Access Control Security Standard
Effective: 2021-11-10

1. PURPOSE

Access control policies provide the blueprint for the management of employee access, authorizations and control requirements for computer networks, operating systems, applications, and information. This standard identifies security best practices and responsibilities for administrators and employees.

2. DESCRIPTION

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: IM/IT Standards).

This standard identifies the controls that restrict access to government information and information assets. Access control protects organizations from security threats such as internal and external intrusions. The controls are guided by legislation that protects particular types of information (e.g., personal and other types of confidential information) and by business requirements.

3. AUTHORITY

The Government Chief Information Officer (GCIO) and the **Core Policy and Procedures Manual (CPPM) Chapter 12**.

Section 12.3.3 Policy 5 of the CPPM states: *"Government must appropriately provide access to, manage, preserve and dispose of its records in compliance with the Document Disposal Act, the Freedom of Information and Protection of Privacy Act, and other relevant legislation, policies and standards, in order to:*

- *ensure government accountability;*
- *provide evidence of its activities and organizational structure;*
- *document its responsibilities, rights and entitlements; and*
- *preserve records of enduring value."*

4. APPLICATION/SCOPE

This standard applies to information systems in Ministries, agencies, boards and commissions that are subject to the **Core Policy and Procedures Manual**.

This standard applies to information systems that are custom developed or commercial off the shelf (COTS) and are hosted on-premises or in the cloud.

Owners of information systems should apply this standard after they have determined their access control requirements. Owners of information systems are advised to consult with the Office of the Chief Information Officer (OCIO) Information Security Branch (ISB) to discuss access control requirements for their information systems.

If a Ministry is not able to satisfy the requirements of the Access Control Security Standard, the Ministry may request an Exemption from the Government Chief Information Officer (GCIO).

For more information about the Exemption process, visit https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/exemptions

5. REQUIREMENTS

5.1 Business requirements of access control – Access control policy

5.1.1 Introduction

Access to information systems and services must be consistent with business needs and be based on security requirements to ensure that information and information systems are available for authorized use and protected from unauthorized use.

5.1.2 Requirements

5.1.2 a) Access control policy
Information Owners and Information Custodians are responsible for establishing, documenting and approving access control policies which must:

- Support and enable business requirements;
- Be based on requirements identified in Privacy Impact Assessments and Security Threat and Risk Assessments; and,
- Include classification of assets.

Access control policies must additionally:

- Consider both physical and logical access to assets;
- Apply the need-to-know and least privilege principles;
- Set default access privileges to deny-all prior to granting access;
- Require access by unique user identifiers or system process identifiers to ensure that all access actions are auditable;
- Have permissions assigned to roles rather than individual user identifiers; and,
- Access requirements should be determined at a functional, work unit level.

The access control policy must be communicated to employees as part of awareness training.

5.1.2 b) Access control policy management
Information Owners and Information Custodians are responsible for establishing processes to manage the access control policies, including:

- Ensuring the process is communicated to all employees;
- Documenting processes for employee registration and deregistration;
- Segregating roles and functions (i.e. access requests, access authorization, access administration);
- Defining rules for controlling access to privileged system functions;
- Identifying roles and/or functions which require multi-factor authentication; and,
- Identifying and justifying exceptional cases where there is a need for enhanced employee security screening for sensitive assets.

5.1.2 c) Review of access control policy
Information Owners and Information Custodians must conduct periodic reviews of the access control policies as part of an ongoing process for risk management, security, and privacy. Annual reviews are recommended. Reviews must be conducted:

- Prior to the introduction of new or significantly changed systems, applications or other services or major technology changes;
- When the threat environment changes or new vulnerabilities arise;
- Following significant government or Ministry re-organization as appropriate; and,
- For sensitive and business critical assets, reviews should be conducted more frequently than annually, based on the Security Threat and Risk Assessments of those assets.

5.2 Business requirements of access control – Access to network services

5.2.1 Introduction

Employees must only be provided access to the network services they have been specifically authorized to use by limiting network access to authorized users of specific information systems to support the information system access control policy.

5.2.2 Requirements

5.2.2 a) Access to network services
Information Custodians must enable network services needed to support business requirements (e.g., by explicitly enabling needed services and disabling unneeded services). Access to network services will be controlled at network perimeters, routers, gateways, workstations and servers.

Information system network access must be restricted to the authorized users and systems as defined in the access control policies for the information system, using the principle of least privilege.

5.2.2 b) Management controls and processes
Information Custodians must document processes for management of network access, including processes to:

- Document and review implemented network access controls;
- Identify threats, risks and mitigation factors associated with network services;
- Test network access controls to verify correct implementation; and,
- Assist Information Owners to verify the principle of least privilege is used to minimize access, as specified in the access control policy.

5.2.2 c) Means for accessing networks and network services
Information Custodians must define and implement:

- Permitted network access methods for each network zone (e.g., direct connection, Virtual Private Network, Wi-Fi, remote desktop connection, desktop terminal services); and,
- Minimum security controls required for connection to networks (e.g., patch levels, anti-virus software, firewalls, user and system authentication requirements).

5.3 Business requirements of access control – Remote access

5.3.1 Introduction

Remote access to government information systems must be subject to authentication to identify and authenticate users and systems accessing the government network from remote locations.

5.3.2 Requirements

5.3.2 a) Remote access to government networks or services
Providers of remote network access services for individuals must:

- Perform a Security Threat and Risk Assessment for each remote access service to determine the authentication methods to be implemented. Factors to be considered include information security information security classification of network services, and information and information systems accessible from the remote access service;
- Require remote users to connect through government designated remote access services or security gateways (e.g., Virtual Private Network (VPN), Desktop Terminal Services (DTS), Outlook Web Access);
- Require user identification and authorization prior to permitting each remote network connection; and,
- Require multifactor authentication when accessing sensitive information from untrusted networks (e.g. the Internet).

Providers of remote network access services for interconnection of networks must:

- Perform a Security Threat and Risk Assessment for each remote network interconnection to determine the user and system authentication methods to be implemented. Factors to be considered include:
  - Information security classification of network services, information, and information systems accessible from the remote access service, and,
  - the strength of security controls implemented in the remote network;
- Obtain prior approval to interconnect networks from Information Owners of every information

system accessible from the remotely connected networks; and,
- Require remote network interconnections to connect through government designated remote access services or security gateways (e.g., Virtual Private Network, Third Party Network Gateway).

5.4 Business requirements of access control – Authentication of connections

5.4.1 Introduction

Automatic equipment identification must be used, as appropriate, to authenticate connections from specific locations and equipment to increase assurance of system identification where required by system sensitivity or information security classification.

5.4.2 Requirements

5.4.2 a) Authentication of connections
Information Owners must use automatic equipment identification if the requirement is identified by a Security Threat and Risk Assessment. Factors to consider include:
- The sensitivity and classification of information that may be accessed or stored;
- The physical security of information, information technology assets and location;
- Unauthorized information access by people at the location, either inadvertent or deliberate; and,
- Remote access threats if remote access is utilized.

When Information Owners identify a requirement for connection to a network or information system from a specific location or equipment, the connection may be authenticated using automated equipment. Activities include:
- An identifier must be in, or attached to, the equipment;
- The identifier indicates that the equipment is permitted to connect to specified networks or information systems and must be maintained in the asset inventory;
- The equipment identifier must be inspected, and sessions should be logged to verify that the identifier is being correctly used for access; and,
- Connections must be monitored to detect anomalies, such as unusual session times, overly long sessions, or increased frequency of use.

Good physical security is required to complement the use of equipment identifiers. Reliance should not be placed solely on automated equipment for authentication. The equipment should be secured from tampering by locating it inside a secure facility or ensuring it is under the direct supervision of an individual.

5.5 Business requirements of access control – Diagnostic ports

5.5.1 Introduction

Physical and logical access to diagnostic ports must be securely controlled to prevent unauthorized use of maintenance or diagnostic facilities.

5.5.2 Requirements

5.5.2 a) Protection of diagnostic ports
To prevent bypassing of information system access controls, Information Custodians must implement access control processes for the physical and logical access controls of the ports, services and systems used for diagnostic, maintenance and monitoring activities.

Physical and logical access controls to be considered for implementation include physical locks, locking cabinets, access control lists and filters, network filters and user authentication systems.

Diagnostic ports must be kept inactive until needed and kept active for the minimum time required.

Access to diagnostic ports from remote locations, or by external parties, or service providers must be authorized in agreements, contracts and conditions of use.

Use of diagnostic ports must be logged and monitored for suspicious activity.

5.6 Business requirements of access control – Network connection control

5.6.1 Introduction

The connection capability of users must be restricted in shared networks in accordance with the access control policy of the information system to control network connection to support the access control policy and limit opportunity for unauthorized access.

5.6.2 Requirements

5.6.2 a) Logical and physical network connection control
Information Custodians must restrict the ability of users to physically and logically connect to networks according to the access control policy defined by Information Owners. The techniques used may include:

- Physical cabling protection;
- Physical control of network ports in public areas and meeting rooms;
- Segregated networks for unauthenticated devices;
- User and device authentication prior to issuance of network addresses;
- Router access control lists;
- Scanning for unauthorized network equipment (e.g., unauthorized wireless access points, modems); and,
- Virtual LANs.

Direct network connections to information systems must only be permitted if required for information system function. For example, database server hardware should be placed in a network security zone to prevent direct network connections from employee workstations.

5.6.2 b) Wireless networks
Information Custodians must prevent unauthorized connection to wireless networks through use of identification and authentication techniques as identified in a Security Threat and Risk Assessment.

5.7 Business requirements of access control – Network address control

5.7.1 Introduction

Networks must have routing controls to prevent unauthorized access or bypass of security control points to ensure that computer connections and information flows do not breach the access control policy of the information systems.

5.7.2 Requirements

5.7.2 a) Network address control
Information Custodians must implement mechanisms to prevent unauthorized changes to network routing and traffic flow (e.g., through use of router access control lists).

Security gateways must be considered for network access control points, in accordance with information system's security classification requirements. Gateways may be used to validate source and destination addresses when proxy servers or network address translation are used with secondary identity verification techniques (e.g., user identifier and password, digital certificates).

5.7.2 b) Control of routing information
Information Custodians must implement processes and controls to prevent unauthorized access to, or tampering of, network routing information (e.g., through use of encryption, authenticated routing protocols, access control lists).

5.8 Employee access management – Employee registration

5.8.1 Introduction

There must be a formal employee registration and deregistration for granting access to all information systems to ensure that all access actions are traceable to an identifiable individual or process.

5.8.2 Requirements

5.8.2 a) Registration
Information Owners and Information Custodians are responsible for managing access to the assets under their control and must implement registration processes that:

- Require approval for all access rights being requested;
- Ensure access requests are approved by the Supervisor of the employee requesting access;
- Ensure the reasons for requesting access are consistent with job responsibilities;

- Maintain records of access right approvals;
- Ensure employees understand the conditions of access and, have signed confidentiality agreements where appropriate;
- Ensure access rights are consistent with the data uses as documented in the approved Privacy Impact Assessment;
- Ensure accesses are traceable to an identifiable individual or process;
- Ensure each employee is assigned a single unique identifier for accessing information systems (see Exceptions below);
- Ensure the responsibilities for authorizing access are segregated from the responsibilities for granting access;
- Restrict access by using predefined role permissions;
- Provide secure and separate transmission of the user identifier and password to the employee; and,
- In exceptional cases, where warranted by the information security classification of the asset and supported by a Security Threat and Risk Assessment, ensure enhanced employee security screening or background checks are completed prior to authorizing access.

Exceptions:
Individual employees may have multiple identifiers when:

- Required to meet limitations of technology (e.g., IDIR, MVS); and
- Required to meet unique business requirements provided the rationale is documented and approved by the Information Owner or Information Custodian as appropriate.

5.8.2 b) De-registration
Information Owners and Information Custodians must formally assign responsibilities and implement processes to:

- Remove access privileges for employees no longer with the organization within 5 working days;
- Promptly review access privileges whenever an employee changes duties and responsibilities;
- Promptly review access privileges whenever the employee's branch or department is involved in significant reorganization;
- Review access privileges for employees on extended leave of absence or temporary assignments within 10 working days of the change of status;
- Remove access privileges with concurrent notification to the employee terminated with cause; and,
- Quarterly check for and remove inactive or redundant user identifiers.

5.9 Employee access management – Access provisioning

5.9.1 Introduction

A formal employee access provisioning process must be implemented to assign or revoke access rights for all user types to all systems and services to ensure authorized user access and to prevent unauthorized user access to systems and services.

5.9.2 Requirements

5.9.2 a) Access provisioning process
Information Owners and Information Custodians must implement a formal employee access provisioning process. The provisioning process for assigning or revoking access rights granted to user IDs must include:

- Verifying the use of the information system or service is authorised. Separate approval for access rights from management may also be appropriate;
- Verifying that the level of access granted is appropriate to the access policies and is consistent with other requirements such as segregation of duties;
- Ensuring that access rights are not activated (e.g., by service providers) before authorization procedures are completed;
- Maintaining records of access rights granted to a user ID to access information systems and services;
- Maintaining an independent record of user IDs given access to critical systems.
- Adapting access rights of employees who have changed roles or jobs and immediately removing or blocking access rights of employees who have left the organization; and,
- Periodically reviewing user access rights to information systems or services.

Guidelines:
Employee access roles should be established based on business requirements that summarize access rights into typical user access profiles. Employee access requests and reviews are more easily managed by access roles than by individual access permissions. Consideration should be given to including clauses in employees' contracts and service contracts that specify sanctions if unauthorized access is attempted by employees.

5.10 Employee access management – Use of system privileges

5.10.1 Introduction

The allocation and use of system privileges must be restricted and controlled to prevent unauthorized access to multi-user information systems.

5.10.2 Requirements

5.10.2 a) Managing, restricting and controlling the allocation and use of system privileges
Information Owners and Information Custodians are responsible for authorizing system privileges and must:

- Identify and document the system privileges associated with each information system or service;
- Ensure the process for requesting and approving access for system privileges includes Supervisor approval(s) prior to granting of system privileges;
- Ensure processes are implemented to remove system privileges from employees' accounts concurrent with changes in their job status (e.g., transfer, promotion, termination);

- Limit access to the fewest number of employees needed to operate or maintain the system or service;
- Ensure the access rights granted are consistent with, and are limited to employee job functions and responsibilities;
- Maintain a record of employees granted access with system privileges;
- Ensure use of system privileges is recorded in audit logs that are unalterable by the privileged user;
- Implement processes for ongoing compliance checking on the use of system privileges; and,
- Implement processes for regular review of system privileges authorizations to confirm that access is still needed and that the least number of users needed have access.

User identifiers established to perform regular activities must not be used to perform privileged system functions. Separate user identifiers assigned with system privileges must be used to perform those activities.

Guidelines:

- The design of information systems should include processes for performing regular maintenance activities that avoid the use of system privileges.
- Whenever possible system routines should be used to execute system privileges rather than granting system privileges to individual employees.
- System acquisition and development should encourage use of programs which minimize the need for employees to operate the system with system privileges.

Privileged users should:

- Not be able to read the data of an information asset unless authorized;
- Be able to alter user permissions for an information asset; and,
- Be permitted to view, but not alter, user activity logs as part of security safeguards.

5.10.2 b) Managing the issuance and revocation of privileged user credentials
The issuance of privileged user credentials must have two levels of approval. Use of system privileges should require use of multi-factor authentication.

5.11 Employee access management – Authentication credentials

5.11.1 Introduction

The issuance and revocation of authentication credentials must be controlled through a formal management process to define the formal management processes for issuing passwords.

5.11.2 Requirements

5.11.2 a) Managing the issuance and revocation of authentication credentials
Ministries must formally designate individuals who have the authority to issue and reset passwords. The following applies:

- Passwords must only be issued to employees whose identity has been confirmed;

- Individuals with the authority to reset passwords must transmit new or reset passwords to the employee in a secure manner (e.g., using encryption, using a secondary channel);
- Whenever technically possible, temporary passwords must be unique to each individual and must not be easily guessed;
- Passwords must never be stored in an unprotected form;
- Default passwords provided by technology vendors must be changed to a password compliant with government standards during the installation of the technology (hardware or software); and,
- The revocation of authentication credentials must follow a formal process.

5.12 Employee access management – Access rights review

5.12.1 Introduction

Information Owners must formally review employee access rights at regular intervals to ensure that access rights are only granted to users with a defined "need to know".

5.12.2 Requirements

5.12.2 a) Circumstances and criteria for formal access rights review
Information Owners and Information Custodians must implement formal processes for the regular review of access rights. Access rights must be reviewed:

- Annually;
- More frequently for high value information assets and privileged users;
- When an employee's status changes as the result of a promotion, demotion, removal from a user group, re-assignment, transfer or other change that may affect an employee's need for access;
- As part of a major re-organization, or the introduction of new IT system or application; and,
- When Information Owners change the access control policy.

5.12.2 b) Procedure for formal access rights review
Review of access rights must include the following:

- Confirmation that access rights are based on the need-to-know and least privilege principles;
- Confirmation that all members of the group/role have a need-to-know;
- Reviews and verification of access control lists dated and signed by the reviewer and kept for audit purposes; and,
- Confirmation that changes to access rights are logged and auditable.

Access control logs and reports are government records and must be retained and disposed of in accordance with approved record management schedules.

5.13 Employee access management – Employment status

5.13.1 Introduction

The access rights of employees to information systems must be removed upon termination of employment and reviewed upon change of employment. Physical and logical access rights to information systems and information processing facilities must be managed in relation to the security responsibilities of the job requirements.

5.13.2 Requirements

5.13.2 a) Change of employment status
Supervisors must review access to information systems and information processing facilities when employees change employment, including:

- When employees assume new roles and responsibilities;
- During restructuring of positional or organizational roles and responsibilities;
- When employees commence long-term leave; and,
- When directories, documentation and systems are updated.

5.13.2 b) Action upon termination or change of employment
Supervisors must ensure access to information systems and information processing facilities is removed upon termination of employment or reviewed upon change of employment by:

- Removing or modifying physical and logical access;
- Recovering or revoking access devices, cards and keys; and,
- Updating directories, documentation and systems.

5.13.2 c) Reduction of access rights
Supervisors must ensure access to information systems and information processing facilities is reduced or removed before the employment terminates or changes, based upon the evaluation of risk factors such as:

- Whether the termination or change is initiated by the employee/contactor or by a Supervisor;
- The reason for termination;
- The current responsibilities of the employee/contractor; and,
- The value of the assets currently accessible.

5.14 Employee responsibilities – Passwords

5.14.1 Introduction

Employees must follow security best practices in the selection and use of passwords to maintain the integrity of the unique identifier (user id) by following security best practices.

5.14.2 Requirements

5.14.2 a) Selection of passwords
When selecting passwords employees must:

- Select complex passwords, i.e., a mixture of characters as specified in the *Complex password requirements* (see section 5.14.2 e);
- Keep authentication information confidential;
- Avoid recording authentication information; and,
- Avoid using the same password for multiple accounts.

The effectiveness of access control measures is strengthened when employees adopt security best practices for selecting passwords.

5.14.2 b) Password change
Passwords must be changed:

- During installation of hardware or software that is delivered with a default password;
- Immediately if a password is compromised or if compromise is suspected. If a compromise has taken place or is suspected, the incident must be reported in accordance with the Information Incident Management Policy; and,
- In compliance with password change instructions issued by an automated process (e.g., password life-cycle replacement) or an appropriate authority.

5.14.2 c) Privileged accounts
Privileged accounts have broader and more powerful access rights to information assets. In addition to 5.14.2 a) and b), employees authorized to create or who hold privileged accounts must use passwords which are at least 15 characters where technically feasible.

5.14.2 d) Protection and use of passwords
Passwords are highly sensitive and must be protected by not:

- Sharing or disclosing them;
- Permitting anyone to view them as they are being entered;
- Writing them down;
- Storing other personal identifiers, access codes or tokens with passwords;
- Keeping them in a file on any computer system, including mobile devices, unless that file is encrypted according to the Cryptographic Standards for Information Protection;
- Including them in any automatic or scripted logon process or code; and,
- Using them in accounts used for non-government purposes.

Where a business need is defined to keep written records of passwords, a request for an exemption must be submitted to the Office of the Chief Information Security Officer.

5.14.2 e) Complex password requirements:
The Complex Password standard for government systems requires that a password must:

- Contain a minimum of 10 characters;
- Contain characters from three of the following categories:

- English upper-case characters (A to Z);
- English lower-case characters (a to z);
- numerals (0 to 9);
- non-alphanumeric keyboard symbols (e.g., ! $ # %); and,

- Not contain the username or any proper names of the employee.

For example, the complex password "T#ocitpi7"is derived from the phrase "The number of clowns in the parade is seven". Complexity can be further increased by substituting numbers for vowels.

For mobile devices connecting to the government messaging server, the following password rules apply:

- A password must contain a minimum of 6 characters;
- Controls should be in place to prevent the use of overly simple passwords; and,
- The use of a combination of numbers, symbols, upper- and lower-case characters is recommended to increase the password strength.

Guidelines:
Never divulge your password to anyone. Legitimate IT technical support employees such as systems administrators, helpdesk and security will not ask employees for their passwords.

Authority and Exceptions:
Exception is granted to RACF and VM Secure due to technical product limitations.

5.15 System application access control – Information system controls

5.15.1 Introduction

Access to information systems functions and information must be restricted in accordance with the access control policy to restrict access to application systems functions and information to authorized individuals or systems.

5.15.2 Requirements

5.15.2 a) Information access controls
Information Owners and Information Custodians are responsible for ensuring the implementation of the access control policy for their business applications. Every information system must have an access control policy that specifies access permissions for information and system functions. The access control policy must identify the information and system functions accessible by various classes of users.

The application and information section of the access control policy must specify:

- The information to be controlled;
- The system functions to be controlled; and,
- The roles authorized to access the resources and information, and what types of access are permitted (e.g., Create, Read, Update/Write, Delete, Execute) based on business need.

5.15.2 b) System configuration
Information system access controls must be configurable to allow Information Custodians to modify access permissions without making code changes.

System utilities or functions that can bypass user access controls must be specified in the access control policy. Access to these utilities and functions must be restricted.

5.15.2 c) Publicly accessible information
Information that is publicly accessible must be segregated from non-public information.

5.16 System application access control – Segregation of sensitive information systems

5.16.1 Introduction

Information systems managing data of a sensitive nature must have an isolated dedicated computing environment to ensure that sensitive information systems are segregated from non-sensitive information systems and are not compromised by sharing information technology resources with non-sensitive information systems.

5.16.2 Requirements

5.16.2 a) Segregation of sensitive information systems
Information Owners and Information Custodians must conduct a Security Threat and Risk Assessment to determine the information system's information security classification level. The information system's information security classification level determines which network security zone the information system must reside in.

Network security zones must be established using physical or logical methods, which may include separate network segments, separate servers, firewalls, access control lists and proxy servers.

5.17 System application access control – Secure logon process

5.17.1 Introduction

Access to information systems must use a secure logon process to ensure access to information systems is limited to authorized users and processes.

5.17.2 Requirements

5.17.2 a) Information displayed during logon
Information Owners must ensure that Information Custodians configure logon processes to minimize the opportunity for unauthorized access, which include:

- Not displaying details about backend systems (e.g., operating system information, network details) prior to successful completion of the logon process to avoid providing an unauthorized user with unnecessary assistance;
- Validating logon information only on completion of all input data; and,
- Not displaying passwords in clear text as they are entered.

5.17.2 b) Unsuccessful logon attempts
Information Owners must ensure that Information Custodians configure logon processes to:

- Record unsuccessful logon attempts;
- Allow a limited number of unsuccessful logon attempts;
- Limit the maximum and minimum time allowed for the logon procedure, and if exceeded, the system should terminate the logon; and,
- Force a time delay or reject further logon attempts if the maximum number of consecutive unsuccessful logon attempts is reached.

After three consecutive failed logon attempts for an account, the logon process must:

- Lock the account and require Administrator intervention; or,
- Lock the account for 15 minutes and then allow a further three logon attempts.

5.17.2 c) Password transmission
Information Owners and Information Custodians must ensure logon processes are configured to prevent transmission of passwords in clear text.

Guidelines:
A general warning should be displayed that the information system is accessed only by authorized users.

The logon procedure should permit users to monitor the security of their account by displaying the following information on completion of a successful logon:

- Date and time of the previous successful logon; and,
- Details of any unsuccessful logon attempts since the last successful logon.

5.18 System application access control – User identifiers

5.18.1 Introduction

All employees must be issued a unique identifier for their use only and an approved authentication technique must be used to substantiate the identity of the users to ensure the traceability of each employee's access to information systems.

5.18.2 Requirements

5.18.2 a) Allocation of unique identifier
Information Owners must ensure employees are issued unique user identifiers (user ids) for their use only, except as specified in 5.18.2 c). The documented and approved process for allocating and managing unique identifiers must include:

- A single point of contact to:
  - manage the assignment and issuance of user identifiers,
  - ensure that users, except for privileged users, are not issued multiple identifiers for any one information system or platform, and,
  - record user status (e.g., employee, contractor);
- Identification of those individuals or positions authorized to request new user identifiers;
- Confirmation that the user has been informed of appropriate use policies;
- Automated linkages with the employee's management system (i.e., CHIPS) to identify transfers, terminations and extended leave actions to initiate the suspension or cancellation of user identifiers;
- Linkages with contract management offices and/or contract managers to identify and maintain the status of identifiers issued to contractors; and,
- Conducting annual reviews to confirm the continued requirement for the user identifier.

To segregate roles or functions, privileged users may be issued multiple identifiers for an information system or platform.

5.18.2 b) Authentication of identity
Information Owners must ensure that user identifiers are authenticated by an approved authentication mechanism.

User identifiers authenticated by means other than a password must use a mechanism approved by the Office of the Government Chief Information Officer.

5.18.2 c) Shared user identifiers
In exceptional circumstances, where there is a clear business benefit identified by the Information Owner or Information Custodian, the use of a positional user identifier for a group of users or a specific job can be used, provided:

- Positional user identifiers are not used for privileged users; and,
- The Supervisor responsible for the position using the positional user identifier:
  - Maintains a record of the name of the individual, the user identifier, and the start and end date of use, and,
  - Deactivates the user identifier when not in use by requesting a password reset.

Guidelines:
Processes for issuing and managing information system user identifiers should be coordinated with those used for issuing and managing other identification credentials (e.g., building passes, user identifiers for telecommunications services provided to an individual).

5.19 System application access control – Password management

5.19.1 Introduction

A password management system must be in place to provide an effective, interactive facility that ensures quality passwords to support the operating system access control policy by enforcing password management rules.

5.19.2 Requirements

5.19.2 a) Password management standard
Information Owners and Information Custodians must ensure password management systems:

- Enforce the use of unique user identifiers and passwords;
- Support selection and change of passwords using the Complex Password Standard (see 5.14.2 e));
- Enforce change of temporary passwords at first logon and after a password reset by an Administrator;
- Enforce scheduled user password change, and provide advance warning of impending expiry at least 10 days prior to users;
- Prevent re-use of the same password within 12 months;
- Prevent passwords from being viewed on-screen;
- Store password files separately from application system data;
- Are protected from unauthorized access and manipulation; and,
- Store and transmit passwords in a secure (e.g., encrypted) manner.

Authority and Exceptions:

- Exception granted to RACF due to technical product limitations.
- Exemptions may be approved under specific criteria for non-expiring password usage. The Non-Expiring Password Acceptance Form is available from OCIO Security Operations.

5.20 System application access control – System utility programs

5.20.1 Introduction

Use of system utility programs must be restricted and tightly controlled as they can be used to override system and application controls.

5.20.2 Requirements

5.20.2 a) Restriction and control of system utility programs
Information Owners and Information Custodians must limit use of system utility programs by:

- Defining and documenting authorization levels;
- Restricting the number of users with access to system utility programs;
- Annually reviewing the status of users with permissions to use system utility programs;

- Ensuring that the segregation of duties is maintained when system utilities are used;
- Requiring a secure logon process to be used to access system utilities;
- Ensuring that all system utility programs are identified and their usage logged;
- Segregating system utilities from application software where possible; and,
- Removing or disabling unnecessary and obsolete system utilities and system software.

Guidelines:
Use of system utility programs should be limited to privileged users. Use of system privileges should require use of multiple factors of authentication.

5.21 System application access control – Session time-out

5.21.1 Introduction

Inactive sessions must be shut down after a defined period of inactivity to ensure unattended information system sessions are automatically terminated.

5.21.2 Requirements

5.20.2 a) Session time-out
Information Owners and Information Custodians must define and implement automatic termination or re-authentication of active sessions after a pre-determined period of inactivity.

Government information systems must have session time-outs managed by the operating system access, application or government infrastructure controls.

Application and network sessions must be terminated or require re-authentication after a pre-defined period of inactivity commensurate with the:

- Risks related to the security zone;
- Information security classification of the information being handled; and,
- Risks related to the use of the equipment by multiple users.

The session must be terminated or require re-authentication after a period of no more than 15 minutes of inactivity.

5.22 System application access control – Access restrictions

5.22.1 Introduction

Restrictions on connection times must be used to provide additional security for high value applications to limit opportunities for inappropriate and unauthorized access.

5.22.2 Requirements

5.22.2 a) Limiting access hours
Information Owners and Information Custodians must restrict access hours for high value applications. Restricting access hours includes:

- Limiting access to pre-determined times (e.g., when Ministry support employees are available); and,
- Establishing restrictions for access from high risk public or external locations which are outside the control of the Ministry.

5.22.2 b) Limiting connection duration
Information Owners and Information Custodians must limit the duration of connection times for high value applications. Restricting connection duration includes:

- Limiting session length; and,
- Requiring re-authentication of the user when a session has been inactive for a pre-defined period of time.

5.23 System application access control – Program source libraries

5.23.1 Introduction

Access control must be maintained for program source libraries to protect information systems from unauthorized access or modification.

5.23.2 Requirements

5.22.2 a) Protection of program source libraries
Information Owners and Information Custodians must implement procedures to control access to program source code for information systems to ensure that:

- Program source code is isolated and stored separately from operational information systems;
- Privileged users' access is defined and monitored;
- A change control process is implemented to manage updates of program source libraries and associated items;
- Program source code stored on any media must be protected; and,
- Accesses and changes to program source libraries are logged.

6. SUPPORTING DOCUMENTS

- **Core Policy and Procedures Manual Chapter 12**: https://github.com/bcgov/digital-policy/blob/master/CPPM-Chapter12.md
- **IM/IT Security standards:** https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard#it_sec
- **Identity Standards**: https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards/find-a-standard#id_mgt

7. DEFINITIONS

The following key words in this document are to be interpreted as described in RFC 2119 (see https://tools.ietf.org/html/rfc2119):

- MAY;
- MUST;
- MUST NOT;
- OPTIONAL;
- RECOMMENDED;
- REQUIRED;
- SHALL NOT;
- SHALL;
- SHOULD; and,
- SHOULD NOT

8. REVISION HISTORY

Date	Author	Version	Change Reference
2020-08-01	Clive Brown	v1.1	Update for MFA
2021-04-20	Kristina Petrosyan	v1.2	Records of access rights for critical systems Format to new IM/IT standards template Minor editing changes to improve clarity

9. CONTACTS

For questions or comments regarding this standard, please contact:

Information Security Branch
OCIO, Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca