Information Technology Branch Access Control Technical Standard

Information Management,
Administrative Directive A1461

Cyber Security Technical Standard # 5

November 20, 2014

Approved: **Date**: November 20, 2014

1. Purpose

This technical standard identifies the requirements to ensure that access controls will be identified, implemented and managed appropriately for Information Technology Branch systems. Access control restrictions on systems mitigate the risk of security threats such as internal and external intrusions.

2. Scope

This technical standard is intended to apply to people, equipment, application systems and processes that fall within the direct organizational control and support responsibilities of the Information Technology Branch of Corporate Services Department.

3. Exceptions and Compensating Controls

In cases where business requirements or technology limitations prevent direct compliance with an implementation expectation, compensating controls can be proposed that meet the statement objective. If an interpretation is required, contact the Program Manager, IT Security and Risk Assurance Program, Information Technology Branch for guidance. Special cases where exceptions are required to meet business requirements or technology limitations need to be documented and approved.

4. Technical Standards and Implementation Expectations

Implementation expectations establish baseline behaviors and actions that are consistent with industry standards or best practices to meet the technical standard statements. It is the intention of this section to establish baseline security requirements in support of business operations, not to impede business operations or define specific technologies or methodologies.

The technical standards do not provide exacting and prescriptive guidance on exactly how to perform everything stated within the standard. In most cases, additional specific how-to procedures will need to be developed.

4.1. Business Requirements for Access Control Technical Standard

4.1.1. Access to information technology systems must be consistent with business needs and be based on security requirements.

4.1.1.1. Implementation Expectations

<u>Access control procedures</u>

The IT Branch is responsible for establishing, documenting and approving access control procedures which should:

- Support and enable business requirements;
- Consider 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 unique user identifiers or system process identifiers to ensure

that all accesses are auditable; and,
- Have permissions assigned to roles rather than individual user identifiers where possible.

Review of access control procedures
The IT Branch should conduct periodic reviews of the access control procedures as part of an ongoing process for risk management, security, and privacy. Reviews should be conducted:
- At least annually;
- Prior to the introduction of new or significantly changed systems, other services or major technology changes; and
- When the threat environment changes or significant high-risk vulnerabilities arise.

4.2. User Access Management Technical Standard

4.2.1. There must be a formal user registration and de-registration process for granting access to information technology systems.

4.2.1.1. Implementation Expectations

The IT Branch is responsible for managing access to the information technology systems under their control and should implement registration processes which, where feasible:

- Access rights are approved by an appropriate individual to ensure access requests are consistent with job responsibilities;
- Maintains records of access rights approvals;
- Ensures access rights are consistent with the data uses;
- Ensures each user is assigned a unique identifier for accessing information technology systems;
- Restricts access by using predefined role permissions; and
- Provides secure and separate transmission of the user identifier and password to the user.

De-registration
The IT Branch should formally assign responsibilities and implement processes where feasible to:
- Remove access privileges for Employees no longer with the organization;
- Promptly review access rights whenever a user changes duties and responsibilities;
- When there is a change of status a review of access privileges for Employees on extended absence or temporary assignments is performed within a period of time as defined by business requirements;
- Remove access privileges for Employees terminated for cause concurrent with notification to individual; and,
- Regularly check for and remove inactive or redundant user identifiers.

4.2.2. The allocation and use of information technology system privileges must be restricted and controlled.

4.2.2.1. Implementation Expectations

The IT Branch is responsible for authorizing information technology system administrator level privileges and should:

- Identify and document the administrator level privileges associated with information technology systems;
- Ensure the process for requesting and approving access to administrator level privileges is validated by the Application/Information Owner;
- Ensure processes are implemented to remove administrator level privileges from users concurrent with changes in job status;
- Limit access to the fewest number of users needed to operate or maintain the information technology system;
- Ensure the access rights granted are limited to and consistent with the users' job function, responsibilities and least privilege;
- Maintain a record of users granted access to administrator level privileges; and
- Implement processes for regular review of authorizations in place to confirm that access is still needed, and that the least number of users needed have access.

4.2.3. The issuance of authentication credentials must be controlled through a formal management process.

4.2.3.1. Implementation Expectations

Passwords are permitted as a single-factor authentication method. The following applies:

- Passwords will only be issued to users whose identity is confirmed prior to issuance;
- Individuals with the authority to reset passwords should transmit new or reset passwords to the user in a secure manner (e.g., using encryption, using a secondary channel);
- Whenever technically possible temporary passwords should be unique to each individual and should not be easily guessable;
- Passwords should never be stored in an unprotected form; and,
- Default passwords provided by technology vendors should be changed to be compliant with IT Branch guidance during the installation of the technology (hardware or software).

A two-factor authentication credential will combine two distinct factors of something a user knows, something a user has or something a user is. Two-factor authentication is suitable for authenticating users to sensitive information and associated information technology systems. Two-factor is also used for remote access to information technology systems or other uses as determined by a risk assessment.

Information technology systems or services issuing two-factor authentication credentials should ensure the following requirements are implemented:

- Two-factor credentials will be issued to users whose identity is confirmed prior to issuance;
- Credentials should be designed so that compromise of either factor does not compromise the credential, as each factor can be subject to different threats and vulnerabilities; and
- The authority issuing the credential will review all holders of active credentials and verify that all holders are entitled to the credential.

4.2.4. Application/Information Owners and Information Custodians must formally review user access rights at regular intervals.

4.2.4.1. Implementation Expectations

Application/Information Owners and Information Custodians should implement formal processes for the regular review of access rights. Access rights should be reviewed where feasible:

- At least annually;
- When a user's status changes as the result of a promotion, demotion, removal from a user group, re-assignment, transfer or other change that may affect a user's need to access information; and
- As part a major reorganization, or the introduction of new technology or applications.

Review of access rights should 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; and,
- Confirmations that changes to access rights are logged and auditable.

4.3. Network Access Control Technical Standard

4.3.1. Users must only be provided access to the information technology systems they have been specifically authorized to use.

4.3.1.1. Implementation Expectations

Access to network services should be restricted to authorized users and authorized information technology applications. All devices accessing IT Branch internal networks should be managed to ensure that they are configured and used in a manner consistent with guidance.

IT Branch may approve access to City networks by devices managed by other parties provided that:

- A legitimate business reason is demonstrated (e.g. consultant contracted to the City needing to connect a laptop to the City network);
- The device undergoes an initial review to ensure it meets City security requirements prior to accessing the network;
- The device is subject to periodic reviews to ensure it continues to meet

City security requirements; and
- The device and usage of the device is subject to monitoring for acceptable use.

Network connections with external organizations should meet the following requirements:
- Connections should be encrypted;
- Connections should terminate at the appropriate firewall;
- Connections should be authenticated; and,
- The business arrangement, including terms of use of the connection, should be documented.

4.3.2. Remote access to internal information technology systems for the purpose of administrating those systems with use of administrator level privileges requires two-factor authentication.

4.3.2.1. Implementation Expectations

The intention of this statement is to require two-factor authentication in high risk scenarios where system administrators (e.g. domain administrators, server administrators, database administrators, etc.) are accessing information technology systems from external locations to perform maintenance on those systems with powerful administrator accounts.

Two factor authentication provides additional control to administer systems remotely. This standard is not intended to require two factor authentication for regular user activities, although, a risk assessment may determine that two factor is required for some regular user account activities where activities originate from a remote location or a non-IT Branch managed device.

4.3.3. Groups of users, information technology systems must be segregated on networks.

4.3.3.1. Implementation Expectations

The IT Branch should segregate information technology applications, infrastructure and users to support business requirements for connectivity and access control based on the principles of least privilege, management of risk and segregation of duties.

The IT Branch should establish network perimeters and control traffic flow between networks. Network traffic flow control points, such as firewalls, routers, switches, security gateways, VPN gateways or proxy servers, should be implemented at points throughout the network to provide the required level of control.

The implementation of techniques and technologies selected for network segregation should consider the following:
- The classification of information, and associated information technology application and infrastructure;

- The trustworthiness of the network, based on the amount of uncontrolled malicious traffic present, the level of device identification and authentication in the networks and sensitivity to eavesdropping;
- Transparency, usability and management costs of network segregation technologies; and,
- The availability of compensating controls for detection, prevention and correction of malicious network traffic and unauthorized access attempts.

4.4. Operating System Access Control Technical Standard

4.4.1. Access to information technology operating systems must use a secure logon process.

4.4.1.1. Implementation Expectations

Information displayed during logon

The IT Branch should configure logon processes to minimize the opportunity for unauthorized access. This includes:

- Not displaying details about backend information technologies and infrastructure (e.g., operating system information, network details) prior to successful completion of the logon process to avoid providing an unauthorized user with any unnecessary assistance;
- Displaying a general warning notice that the information technology systems be accessed only by authorized users;
- Validating logon information only on completion of all input data; and,
- Not displaying passwords in clear text as they are entered.

Unsuccessful logon attempts

The IT Branch should configure logon processes to:

- Record unsuccessful logon attempts;
- Allow a limited number of unsuccessful logon attempts before taking an action; and,
- Force a time delay or reject further logon attempts if the limited number of consecutive unsuccessful logon attempts is reached.

Password transmission

The IT Branch should ensure logon processes are configured to prevent transmission of passwords in clear text.

4.4.2. All users must be issued a unique identifier for their use only, and an approved authentication technique must be used to substantiate the identity of the user.

4.4.2.1. Implementation Expectations

Allocation of unique identifier

The IT Branch should ensure users are issued unique user identifiers (user logon id's) to be used only by the authorized user. The documented and approved process for allocating and managing unique identifiers should include:

- A single point of contact to:

  - manage the assignment and issuance of user identifiers,
  - ensure that users, except for administrator users, are not issued multiple identifiers for any one information technology system or platform, and,
  - record user status (e.g., Employee, contractor);
- Identification of those Employees or positions authorized to request new user identifiers; and
- Conducting annual reviews to confirm the continued requirement for the user identifier.

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

<u>Shared user identifiers</u>
In exceptional circumstances, where there is a clear requirement, the use of a shared user identifier (shared ID) for a group of users with a specific business purpose can be used, provided:

- A process is in place for requesting and approving the use of shared ID's that includes appropriate approval(s) prior to use;
- A most responsible person (employee) and delegate within the job function using the shared ID is designated to maintain a record (list) of employees using the shared ID;
- A process is implemented to change the password on a shared ID when employees on the list change job status (e.g., transfer, promotion, termination) or a new employee is added to the list;
- Access is controlled and restricted for shared IDs, and they;
  - are not used for administrator functions;
  - are restricted to specific workstations within a business area; and,
- A process is implemented for regular review of shared IDs in place to confirm that they are still required.

4.4.3. A password management system should be in place to provide an effective, interactive facility that ensures quality passwords.

4.4.3.1. Implementation Expectations

The IT Branch should implement password management systems that:

- Enforce the use of individual user identifiers and passwords per system;
- Enforce user change of temporary passwords at first logon and after password reset by an Information Custodian;
- Enforce regular user password change, including advance warning of impending expiry;
- Prevent re-use of passwords for a specified number of times;
- Prevent passwords from being viewed on-screen;
- Where possible, store password files separately from application and system data;
- Ensure password management systems are protected from unauthorized access and manipulation; and,
- Store and transmit passwords in protected (e.g., encrypted) form.

4.4.4. Operating system sessions must be terminated or require re-authentication after a pre-defined period of inactivity.

4.4.4.1. Implementation Expectations

The IT Branch should define and implement automatic termination or re-authentication of active sessions after a pre-determined period of inactivity.

Information technology systems should have session time-outs managed by operating system access, application or infrastructure controls.

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

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

4.5. Application Access Control Technical Standard

4.5.1. Access to information technology application functions and information must be restricted in accordance with the access control procedures as defined by business requirements.

4.5.1.1. Implementation Expectations

The IT Branch should ensure that access control procedures for their applications are implemented. The access control procedures should specify:

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

The access control procedures should specify acceptable authentication methods for users accessing applications (e.g. single factor, two- factor).

4.6. Mobile Computing Technical Standard

4.6.1. Appropriate controls must be implemented to mitigate security risks associated with the use of portable computing devices such as laptops, tablets, smart phones or mobile devices.

4.6.1.1. Implementation Expectations

<u>Administrative safeguards</u>
To ensure that sufficient safeguards are implemented to protect information commensurate with its sensitivity, a risk assessment should be performed prior to permitting use of portable computing devices.

Users will take reasonable measures, such as maintaining personal possession or visual scrutiny of the device or storing the device out of sight using a locking device, to safeguard portable computing devices that have been assigned or issued to them from loss, theft or damage.

Users should report all losses or thefts of portable computing devices, including identification of what information was stored on the device, and all unauthorized disclosure of information residing on mobile computing devices immediately upon discovery.

Minimum technical safeguards

Minimum information protection safeguards for the use of portable computing devices can include:

- Encryption of all stored data to prevent information loss resulting from the theft of the mobile or remote device;
- Encryption of data transmitted via public network;
- Access control permissions on a portable storage device should be applied;
- Regularly maintained data backups of critical information stored on portable computing devices using backup facilities to protect against information loss; and,
- Physical security of the device should be maintained to protect (e.g. use of locking devices where appropriate) against asset and information loss.

5. Reference

Further information can be found in:

- ISO 27002, Chapter 11 – Access Control