METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY **INFORMATION SECURITY POLICY**	POLICY NUMBER: 9
SUBJECT: ACCESS CONTROL AND USER ACCOUNT MANAGEMENT	DISTRIBUTION DATE: 9/15/2017 EFFECTIVE DATE: 10/1/2017
ISSUING AUTHORITY: DIRECTOR OF INFORMATION TECHNOLOGY SERVICES OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this policy is to ensure Metropolitan Government of Nashville and Davidson County (Metropolitan Government) reduces risks to information security by managing accounts that provide access, limiting access to authorized users and preventing unauthorized access to information systems.

POLICY

1. General

   Metropolitan Government shall develop procedures for the effective implementation of security controls covering access control and information system account management. Information system accounts are used to provide access to information technology assets and physical access, in cases where physical access is tied to information system accounts.

   Information system account types include, for example, individual, shared, group, system, guest/anonymous, and service. As set forth below, Metropolitan Government's access control processes are supported through the use of the controls set forth in: (i) business requirements (Section 2.1 below); (ii) user access management (see Section 2.2 below); (iii) user responsibility (see Section 2.3 below); (iv) system and application access control (see Section 2.4 below); (v) segregation of duties (see Section 2.5 below); and (vi) additional security controls (see Section 2.6 below).

2. Detailed

   2.1. Business Requirements of Access Control

   2.1.1. Metropolitan Government shall:

   a. provide access based on business and information security requirements;
   b. determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks;
   c. consider both logical and physical access controls together, where applicable;
   d. give Users and service providers a clear statement of the business requirements to be met by access controls that have been provided.

Two of the frequent principles directing the access control policy are:

a. Need-to-know: you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile);
b. Need-to-use: you are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) you need to perform your task/job/role.

2.1.2. Access to Networks and Network Services

Metropolitan Government shall provide Users with only the access to the network and network services that they have been specifically authorized to use. Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization’s information security management and control. Metropolitan Government shall utilize appropriate technical controls to protect the internal Metropolitan Government network from external networks.

2.1.3. Least Privilege

Metropolitan Government shall employ the principle of least privilege, allowing only authorized accesses for Users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

2.2. User Access Management

Metropolitan Government Departments and Agencies shall include possible impacts to access controls when assessing changes to their information environment.

2.2.1. User Registration and De-registration

Metropolitan Government shall implement a formal user registration and de-registration process to enable assignment of access rights. Providing or revoking access to information or information processing facilities is usually a two-step procedure:

- assigning and enabling, or revoking, a user ID;
- providing, or revoking, access rights to such user ID.

2.2.2. User Access Provisioning

Metropolitan Government shall implement formal user access provisioning to assign or revoke access rights for all user types to all systems and services. Ideally, consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles.

2.2.3. Management of Privileged Access Rights

Metropolitan Government shall implement processes for restricting and controlling the allocation and use of “privileged access rights”. These privileged access rights are generally referred to as “administrative rights”. Inappropriate use of administrative rights (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

2.2.4. Management of Secret Authentication Information of Users

Metropolitan Government shall implement processes that control the allocation of any secret authentication information. Passwords are a commonly used type of secret authentication information and are a common means of verifying a user's identity. Other types of secret authentication information are cryptographic keys and other data stored on hardware tokens (e.g. smart cards) that produce authentication codes.

2.2.5. Review of User Access Rights

Metropolitan Government shall include a review of users' access rights at regular defined intervals as part of access control procedures.

2.2.6. Removal or Adjustment of Access Rights

2.2.6.1. Removal

Metropolitan Government shall confirm that the access rights of all Users to information assets be removed upon termination of their employment, contract or agreement, or adjusted upon change. Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services should be removed or suspended.

2.2.6.2. Modifications

Metropolitan Government shall confirm that changes of User employment or role is reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adjusted include those of physical and logical access. Removal or adjustment can be done by removal, revocation or replacement of keys, identification cards, information processing facilities or subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights. If a departing employee or external party user has known passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract or agreement.

2.2.6.3. Additional Considerations

Access rights for information and assets associated with information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

- whether the termination or change is initiated by the employee, the external party user or by management, and the reason for termination;
- the current responsibilities of the employee, external party user or any other user;
- the value of the assets currently accessible.
- In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee or external party user, e.g. group IDs. In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to

advise all other employees and external party users involved to no longer share this information with the person departing.

In cases of management-initiated termination, disgruntled employees or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they may be tempted to collect information for future use.

2.3. Use of Secret Authentication Information

Metropolitan Government Users shall be required to follow all applicable policies, procedures and standards, including, but not limited to, Metropolitan Government's Acceptable *Use of Information Technology Assets Policy*, with regards to the use of secret authentication information.

2.4. System and Application Access Control

Metropolitan Government shall develop and documents processes to prevent unauthorized access to systems and applications.

2.4.1. Information Access Restriction

Access to information and application system functions shall be restricted in accordance with this policy and shall be restricted based on individual business application requirements.

2.4.2. Secure Log-on Procedures

Access to systems and applications shall be controlled by a secure log-on procedure. A suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

2.4.3. Password Management System

Password management systems shall be interactive and shall ensure quality passwords. A password management system must:

- enforce the use of individual user IDs and passwords to maintain accountability;
- allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
- enforce a choice of quality passwords;
- force users to change their passwords at the first log-on;
- enforce regular password changes and as needed;
- maintain a record of previously used passwords and prevent re-use;
- not display passwords on the screen when being entered;
- store password files separately from application system data;
- and transmit passwords in protected form.

2.4.4. Use of Privileged Utility Programs

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

2.4.5. Access Control to Program Source Code

Access to program source code shall be restricted. Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries.

If the program source code is intended to be published, additional controls to help getting assurance on its integrity (e.g. digital signature) shall be considered.

2.5. Segregation of Duties

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Metropolitan Government shall work to implement segregation of duties, where applicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision shall be considered.

2.6. Additional Security Controls

Metropolitan Government shall, where applicable:

2.6.1. Access and impose additional usage restrictions to further limit access;

2.6.2. Identify parameters that define typical account usage and notify when use is outside those parameters;

2.6.3. Enforce a limit of invalid logon attempts and automatically lock account for a specified period of time;

2.6.4. Display to users a message banner that identifies acceptable use;

2.6.5. Display to users data and time of last logon (access);

2.6.6. Institute session lock and termination settings for a determined period of inactivity; and

2.6.7. Require the creation and use of any "generic" account, an account used by multiple users and whose activity cannot be tracked to a unique user, to be approved via the security exception process;

2.6.8. Implement controls for insider threat monitoring, including abnormal privileged user activity detection;

2.6.9. Develop a documented account lifecycle management, including creation, periodic recertification, and prompt disablement upon role change or termination.

SCOPE, BACKGROUND and GOVERNANCE

This information is set forth in the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the *Metropolitan Government Information Security Glossary*.

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov, or by mailing them to CISO, Information Technology Services Department, 700 2nd Avenue South, Suite 301, P. O. Box 196300, Nashville, TN 37219-6300.

9/15/17

Keith Durbin
Director of Information Technology Services
Metropolitan Government of Nashville and Davidson County

Date

REFERENCES

- ISO 27002: sections *9.1-9.4, A.6.1.2*
- NIST Special Publication 800-53 rev 5, *Security and Privacy Controls for Federal Information Systems and Organizations:* Control numbers – AC2, AC-3, AC-5, AC-6,
- Center for Internet Security Critical Security Benchmark #12, 16, 15
- Criminal Justice Information Services (CJIS) Security Policy ver. 6.0
- NIST Cybersecurity Framework ver. 2.0
- NIST Special Publication 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

REVISION HISTORY

REVISION	DATE	CHANGES
1.0	9/15/17	FINAL

1.1	8/29/2025	Added: 2.6.1. “Implement controls for insider threat monitoring, including abnormal privileged user activity detection; 2.6.2. Develop a documented account lifecycle management, including creation, periodic recertification, and prompt disablement upon role change or termination. Change to reflect use of rev 5 of NIST 800-53 as a reference Change to reflect use of rev 2 of NIST Cybersecurity Framework Change to reflect use of version 6 of CJIS as a reference Change to reflect use of NIST 800-171 r3 as a reference