City of Milwaukee

City of Milwaukee

Access Control Standard

NIST Reference:	Implementation Date :	Revision Number :
AC – Access Control	DRAFT	0.1

ACCESS CONTROL STANDARD

OVERVIEW

Account management and access control includes the process of requesting, creating, issuing, modifying and disabling user accounts; enabling and disabling access to resources and applications; establishing conditions for group and role membership; tracking accounts and their respective access authorizations; and managing these functions.

ACCOUNT MANAGEMENT

Account management and access control require that roles are defined and assigned for each resource and application. A listing of authorized users in these roles must be documented and maintained. Each role may belong to one or more individuals depending on the application. User accounts should be reviewed annually.

INDIVIDUAL ACCOUNTS

1. User accounts will be created after a request is received; either through email or RITS (Request IT Support) by authorized departmental personnel. The accounts will follow the standard naming convention of first initial followed by the first five (5) letters of the last name.
2. User account permissions and level of system access are assigned based upon an individual's role.
3. If an individual has several departmental roles, with conflicting levels of access, the most restrictive policy applies.
4. Upon creation or reset of an account, the system should prompt the user to create an initial password that complies with the Password Complexity Standard. In cases where this is not possible, the initial password must be unique, comply with the Password Complexity Standard, and require that the user change the password upon the first use.

PRIVILEGED ACCOUNTS

1. A privileged account is an account that provides increased access and requires additional authorization. Examples include a network, system or security administrator account. The use of privileged accounts must be compliant with the principle of least privilege. Access will be restricted to only those programs or processes specifically needed to perform authorized business tasks and no more.
2. Authorized individuals with privileged access, such as account administrator, will be issued additional accounts. Privileged access will not be assigned to standard user accounts.
3. The passwords to system and service accounts essential to the operation of an information system must be known or accessible to more than a single person. Such passwords must meet complexity requirements, be stored in a

secure manner, and changed on a schedule relative to the risk of exposure or at a minimum when those with knowledge of the password terminate or are reassigned.

ACCEPTABLE USE

In order to safeguard the City of Milwaukee's information resources, department and agencies should adopt an acceptable use agreement. Inappropriate use exposes the City to risks including attacks, compromise of network systems and services, and legal issues. This agreement applies to all employees, contractors, and consultants and should be signed before access is given to City information resources.

PASSWORD COMPLEXITY REQUIREMENTS

All passwords are to be treated as sensitive, confidential information and therefore need to meet the following requirements for AD and applications:

1. All passwords must be at least eight characters long.
2. All passwords must be alphanumeric (Contain at least one (1) letter and number).
3. All passwords must set to change at least every 60 days.

UNSUCCESSFUL LOGIN ATTEMPTS

The number of unsuccessful consecutive attempts by a user to enter a password and log into a system or application is limited to no more than ten (10) attempts after which accounts will be locked. Only authorized account administrators can unlock locked accounts. If necessary password resets will follow password complexity requirements.

SESSION LOCK

Session lock helps prevent unauthorized access to devices when the currently signed-in user leaves without locking the desktop. The Active Directory security policy setting **Interactive Logon: Machine inactivity limit**, will be set to 15 minutes, (900 seconds). If the amount of inactive time exceeds the inactivity limit set by this policy, then the user's session locks by invoking the screen saver. Screen Savers should be active on the destination machine with password authentication required. Exceptions to this setting will be based on the need for high availability.

REVISION HISTORY

Revision	Date	Changes
0.0	January 29, 2007	Initial Release
0.1	July 9, 2019	Format Revision