Title: Account Management
Effective Date:
Amended:
Issuing Authority: Board of Commissioners
Responsible Officer: Director, Information Technology

Category: 500
Number: 502

Purpose

This policy establishes standards for the management of credentials and user accounts to ensure compliance with rules for interaction with, and usage of county owned Digital Assets, thus facilitating the protection of sensitive information.

Responsibility

County of Saginaw Information Technology (COSIT) is responsible for all user account and credential management functions. Account information is relayed to other county-wide elected and department units within the County of Saginaw, as required or needed.

Scope

This policy applies to the following covered individuals: all County of Saginaw Elected Officials, Judges, employees, contracted individuals or entities, third-party vendors, and anyone else who has a County of Saginaw user account and/or an account to County of Saginaw applications. Anyone covered individual who fails to comply with this, or any County of Saginaw policy, is subject to disciplinary action outlined in the County of Saginaw Standards of Conduct.

Policy

This policy establishes rules and controls for managing credentials and user accounts that access the County of Saginaw's Digital Assets.

A. Establishment and Maintenance of an Inventory of Accounts

1. The user account inventory includes the following types of accounts:
    a. User
    b. Administrative
    c. Service
2. The user account inventory at a minimum contains the following details:
    a. Account type
    b. Person's name
    c. Assigned username
    d. Start/Stop dates
    e. Business Unit
    f. Account Status (i.e., enabled, disabled)
    g. Validate all active accounts are authorized
3. As a foundational security principle to ensure individual accountability, protect sensitive information, and mitigate risks associated with unauthorized access, the use of generic user

accounts is prohibited. Exceptions to this policy may be authorized only under extraordinary circumstances where operational necessity or technical constraints necessitate such access. Granting such a request is solely at the discretion of the Director of Information Technology.

   a. An authorized exception granting use of a generic user account must be documented, accompanied by a formal risk assessment, and subjected to periodic review to ensure compliance with organizational security standards.

B. Use Unique Passwords Required

1. COSIT is responsible for updating, enforcing, and communicating any password requirement modifications as necessary.
2. Password Requirements:
   a. All default passwords must be changed at initial login.
   b. Be unique.
   c. Passwords that are created by users must not also be used for personal accounts.
   d. Passwords must not be shared by users.
   e. Passwords must never be written down.

C. Dormant Accounts

1. Any accounts that are inactive for a period of 45 days, shall be deleted or disabled.
2. Accounts of individuals on extended leave, as defined by Human Resources, must be disabled.
3. All user accounts that have not been accessed within 14 business days of creation, must be disabled.
4. Department heads must routinely validate user accounts and provide COSIT written confirmation of active accounts. The process of validating user accounts will occur at a minimum quarterly, or as determined appropriate by COSIT.
5. COSIT will utilize scripts to detect accounts that are inactive for 30, 60, or 90 days, orphaned accounts or accounts with no login activity or ownership.

D. Restrict Administrator Privileges

1. Administrator and privileged accounts shall be utilized for authorized installation and maintenance activities and must be secured with multi-factor authentication (MFA).
2. Administrator accounts must be unique and assigned to a specific individual, unless technically constrained by a system or application.

E. Inventory of Service Accounts

1. The service account inventory must contain the following:
   a. Department Owner
   b. Review Date
   c. Service Account Purpose
2. Regular reviews of service accounts should be performed at a minimum of quarterly but can occur more frequently if needed or requested by COSIT.

F. Centralized Account Management

1. User accounts should be managed through a central directory or identity service whenever it is possible.

G. <u>Account Termination</u>

1. In the event of user separation of any kind, when appropriately notified by the responsible department, COSIT will provide procedures for revoking user account access.
2. Each County Departments shall notify COSIT immediately upon an employee's separation.
3. All user credentials must be revoked immediately upon employee separation.
4. Password self-service mechanisms (if deployed) must not allow separated employees to re-enable their own account(s).

H. <u>Just-in-Time Access Expiration</u>

1. Just-in-time expiration will be implemented by COSIT to ensure elevated privileges are granted only when needed and automatically expire after a predefined time or a specific purpose has been fulfilled.

County Administrator / Legal Counsel Review

The County Administrator has determined that this Policy, as submitted to the Board of Commissioners, contains the necessary substance in order to carry out the purpose of the policy. County Civil Counsel has determined that this Policy, as submitted, contains content that appears to be legal activities of the Saginaw County Board of Commissioners.

Approved as to Substance:

____
Saginaw County Administrator

Approved as to Legal Content:

____
Saginaw County Civil Counsel

REFERENCE SOURCES:

Category: HIPAA Administrative Safeguards
Type: Standard
Reference: 45 CFR §164.308(a)(4)(i)
Category: HIPAA Physical Safeguards
Type: Standard
Reference: 45 CFR §164.312(a)(2)(i)

Category: CJISSECPOL
Version: 6.0
Reference: AC-2, AC-2(1), AC-2(3), IA-5(1), IA-6(2), IA-6(5)

RECOMMENDED PRACTICES:

Category: CIS
Version: 8.1
Control: 5
Reference: IG1, IG2, IG3

NIST: SP 800-53 Rev. 5 AC1, AC-2, AC-5, AC-6, SP 800-207

Definitions

Administrator or privilege accounts are user accounts that have elevated access privileges beyond those of standard user accounts. These accounts are typically used by system administrators, IT personnel, and other high-level users to perform critical tasks such as installing software, modifying system configurations, accessing sensitive data, and managing user accounts.

Asset is anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

Asset Inventory is a register, repository or comprehensive list of an enterprise’s assets and specific information about those assets.

Credentials are the authentication factors—such as usernames, passwords, PINs, cryptographic keys, digital certificates, or biometric data—used to verify and grant an individual, system, or application authorized access to digital resources. Credentials serve as proof of identity and are a core component of access control, security, and compliance.

Digital Assets are the electronic resources including, but not limited to, County of Saginaw systems, networks, applications, and data (to be clear, Digital Assets includes both physical devices and digital information)that Saginaw County owns, controls, or relies upon to conduct business, including hardware, such as computers, servers, tablets, and mobile devices, as well as software, data, communications, intellectual property, and online accounts.

Multifactor Authentication or MFA is a security process that requires users to provide two or more verification factors to access a resource, such as an application, online account, or network. These factors typically fall into three categories:

1. *Something You Know:* Includes passwords, PINs, or security questions.
2. *Something You Have:* Physical security tokens, mobile phones, or hardware keys.
3. *Something You Are*: Biometric verification methods like fingerprints, facial recognition, or voice recognition.

Network is a collection of interconnected devices, such as computers, servers, and printers, that communicate with each other to exchange data and share resources. These networks can be established using physical connections like cables or wireless technologies. Communication protocols, such as TCP/IP, are used to manage the flow of data between devices.

Orphaned user accounts are accounts that remain active within a system, application, or directory after the associated individual—such as an employee, contractor, or vendor—no longer requires access or is no longer affiliated with the organization. These accounts no longer have a valid owner or business purpose but may still retain access rights, privileges, or data.

Password is a sequence of characters used in computing to authenticate a user's identity and authorize access to various digital systems, such as computers, websites, and mobile devices. It is designed to be a secret known only to the authorized user and is often paired with a username for verification purposes.

Rules are formally prescribed principles or directives issued by an authority—such as a legislature, regulatory body, court, or governing organization—that establish standards of conduct, procedures, or operations. They are legally binding within their applicable scope, and noncompliance may result in penalties, enforcement actions, or other legal consequences.

Service Accounts are specialized accounts used by applications, services, or systems to authenticate and perform automated tasks.

User Login Names are comprised of a unique sequence of characters used to identify a user and allow them to access a computer system, network, or online account.

Users are County of Saginaw Elected Officials, Judges, employees, contracted individuals or entities, third-party vendors, and anyone else who has a County of Saginaw user account and/or an account to County of Saginaw applications.