Title: Access Control Management
Category: 500
Effective Date:
Number: 503
Amended:
Issuing Authority: Board of Commissioners
Responsible Officer: Director, Information Technology

Purpose

This policy establishes standards for granting, managing, and revoking user access to County of Saginaw Digital Assets, including but not limited to: systems, networks, applications, and data.

Responsibility

The County of Saginaw Information Technology **(COSIT)** is responsible for confirming that the requested access is appropriate for the job role and employs Least Privilege methodology.

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 to create, modify, or remove access to County of Saginaw Digital Assets.

A. Grant Access

1. Access to systems or data must be requested through the IT Help Desk ticket system and must include the following information:
    - Identity of the requester.
    - Business justification.
    - Requested system(s) or data access.
    - Start and end dates if temporary.
2. All access must be approved by the system owner, data steward, or information owner.
3. Access must be provisioned based on the principle of Least Privilege.
4. Role-Based Access Control (RBAC) should be implemented where technically feasible.
5. Custom or non-standard access must be explicitly justified and documented.
6. The use of generic user accounts is strictly prohibited as a foundational security principle to ensure individual accountability, protect sensitive information, and mitigate risks associated with unauthorized access. Exceptions to this policy may be authorized only under extraordinary circumstances where operational necessity or technical constraints necessitate such access, and solely at the discretion of the Director of Information Technology. Any authorized exceptions must be documented, accompanied by a formal risk assessment, and subjected to periodic review to ensure compliance with organizational security standards.

B. Revocation of Access

1. When appropriately notified by a County department, COSIT will institute procedures for revoking user account access. Revocation of access applies to employee or contractor separation of any kind.
2. All access will be revoked immediately upon:
    - Termination of employment or contract.
    - Role changes that no longer require access.
    - Conclusion of temporary or project-based assignments.
    - Detection of unauthorized or malicious activity.
3. Target timeframe for revocation is:
    - Within.8.business.hours of separation notice to COSIT.
    - Immediately.after notice, if termination is involuntary.
4. Department heads, managers, and supervisors will support COSIT by routinely validating user accounts and providing confirmation of active accounts and NOTICE of any change in the user relationship to the County that would or may require revocation of an account or access. The process of validating user accounts will occur at a minimum quarterly, or as determined appropriate by COSIT. Failure to provide validation of user accounts may result in revocation of same.
5. COSIT may utilize scripts to detect accounts that are inactive for 30, 60, or 90 days, orphaned accounts or accounts with no login activity or ownership.
6. Password self-service mechanisms (if deployed) must not allow separated employees to re-enable their own account(s).

C. Requirement of Multi-Factor Authentication (MFA) for Externally Exposed Applications

1. MFA is required for all externally accessible applications and services, regardless of the user’s role or the system's sensitivity level.

2. Acceptable forms of second-factor authentication include:
    - Time-based One-Time Passwords.
    - Hardware or software tokens.
    - Push notification-based approvals.

D. Require MFA for Remote Network Access

1. Must use a centralized authentication system.
2. All enterprise user accounts, including remote, on-prem, & hybrid, must authenticate through this system.
3. Password policies, session timeouts, and lockout rules must be centrally managed and enforced through the enterprise managed authentication.
4. Disable or heavily restrict local authentication mechanisms.

E. Require MFA for Administrative Access

1. MFA for privileged accounts is required and will be enforced regardless of internal or external access paths.
2. Privileged or administrative accounts, including but not limited to the following, must always use MFA:
    - Domain administrators.
    - Cloud root or super-admin roles.
    - Database administrators.
    - Network or firewall administrators.
3. MFA technologies used must be pre-approved by the IT Security team.
4. Due to susceptibility to interception or SIM swapping, SMS-based MFA will generally not be approved unless no other method is feasible.

F. <u>Create and Maintain Inventory of Authentication Systems</u>

1. Access to systems and data will generally be granted based on defined roles and not on a per user basis, to minimize the excess privilege and enforce consistent access management.
2. Access will generally be managed through the enterprise-managed authentication system to minimize role overlaps or unintended privilege escalation.

G. <u>Centralized Access Control</u>

1. All systems, applications, and platforms must integrate with a centralized identity provider or another approved IAM platform.
2. All user authentication and access provisioning must be performed through the centralized access control system.
3. Stand alone or siloed authentication systems are prohibited unless an exception is documented, justified, and approved by IT Security.
4. Whenever technically feasible, systems should use Single Sign-On backed by centralized directory services to simplify user experience and enhance security.
5. All centralized access systems must include the following:
    - Password complexity and expiration policies
    - Multi-Factor Authentication (MFA) for externally accessible systems
    - Session timeouts and idle lockouts
6. Failed login attempts must be logged, and account lockout thresholds must be defined.
7. Any legacy systems that cannot integrate with the centralized access control system must:
    - Be documented and assessed for risk
    - Have compensating controls in place (e.g., MFA, VPN restriction)
    - Be prioritized for upgrade or retirement

H. Role-Based Access Control

1. Access must be granted based on defined.roles.or.security.groups, rather than individual user assignments whenever possible.
2. Role definitions and group membership must be documented and reviewed annually for accuracy and relevance.

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

REFRENCE SOURCES:

Category: HIPAA Administrative Safeguards
Type: Standard
Reference: 45 CFR §164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(C)

Category: HIPAA Technical Safeguards
Type: Standard
Reference: 164.312(a)(2)(i)

Category: CJISSECPOL
Version: 6.0
Reference: AC-1, AC-2, AC-2(1), AC-3, AC-5, AC-6, AC-6(1), AC6-(7), AC-17, AC-19, AU-9(4) IA-2(1), IA-2(2), IA-4, IA-5, IA-8(2), CM-8

RECOMMENDED PRACTICES:

Category: CIS
Version: 8.1
Control: 5
Reference: IG 1, IG 2, IG 3

NIST: SP 800-171 Rev 2, SP 800-63B

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.

Centralized Authentication System is a security architecture where a single, central service manages and validates user authentication across multiple systems, applications, or services within an organization.

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.

Hybrid System refers to an environment that combines on-premises infrastructure with cloud-based services, enabling organizations to leverage the benefits of both deployment models.

Least Privilege is a cybersecurity principle that dictates users, systems, applications, or processes should be granted only the minimum level of access rights and permissions necessary to perform their specific tasks or functions—nothing more.

Multifactor Authentication or 2FA / 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.

On-Premises Systems refer to hardware and software that are physically hosted and operated within an organization's own facilities, rather than in the cloud or at a third-party data center.

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.

Role Based Access Control (RBAC) is a security model used to restrict system access based on a user's role within an organization. Instead of assigning permissions to individual users, permissions are assigned to roles, and users are assigned to those roles.

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.

Single Sign-On (SSO) is an authentication method that enables a user to securely access multiple independent applications, systems, or services with a single set of login credentials. Instead of maintaining separate usernames and passwords for each resource, the user authenticates once through a trusted identity provider, which then issues tokens or assertions to grant access across authorized systems.

Time-Based One-Time Password (TOTP) is a type of two-factor authentication (2FA) method that generates a unique, temporary passcode based on the current time and a shared secret key.

Token is a digital object used to represent and verify a user's identity, session, or access rights. Tokens are typically issued after successful authentication and are used in place of repeatedly entering credentials like a username and password.

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, contractors, third-party vendors, or anyone else who has a County of Saginaw user account and/or an account to County of Saginaw applications that interact with a product, service, system, or technology to achieve specific goals or fulfill needs.