Title: Data Classification Policy
Effective Date: February 17, 2026
Amended:
Issuing Authority: Board of Commissioners
Responsible Officer: Director of Information Technology

Category: 500
Number: 507

Purpose

This policy defines how the County of Saginaw classifies and protects information based on its sensitivity, legal requirements, and potential impact if disclosed. It supports compliance with Criminal Justice Information **(CJI)**, Personally Identifiable Information **(PII)**, Electronic Protected Health Information **(ePHI)**, and Payment Card Industry Data Security Standards **(PCI DSS)**. The goal is to ensure appropriate handling, storage, access, and disposal of County data.

Responsibility

Users: All County employees, elected officials, judges, contractors, temporary staff, and vendors are responsible for following this policy when creating, accessing, storing, transmitting, or disposing of County data.

Management: County leadership must ensure that staff understand data sensitivity levels and follow secure handling practices.

County of Saginaw Information Technology (COSIT): Is responsible for maintaining classification guidelines, providing secure technical tools, conducting reviews, and supporting compliance with all applicable regulations.

Scope

This policy applies to all County of Saginaw Elected Officials, Judges, employees, contractors, third-party vendors, or anyone else who handles CJI, PII, ePHI, and/or PCI DSS.

Policy

Before storing and using any new data or information, those identified in the policy scope must classify the data and information.

Public Information

Public information is specifically authorized for broad distribution and may be shared freely without infringing on anyone's privacy or creating risk to individuals or the organization. For example:

- The County of Saginaw website
- Brochures
- Media Releases

Internal Information

Internal information may be shared within the department, as it is not considered sensitive. For example:

- Policies and procedures
- Non-sensitive operational reports

Confidential Information (PII, ePHI, PCI)

- Includes PII, ePHI, and PCI data.
- Access that is limited to authorized personnel.
- Must be encrypted in transit and at rest.
- Paper copies must be locked and secured.
- Information that requires secure disposal methods.
- Third-party systems must comply with relevant standards.

Restricted Information

- Includes Criminal Justice Information (CJI).
- High-risk data that requires the strongest protection.
- Strict need-to-know access.
- MFA required.
- Encrypted storage, transmission, and backups.
- External sharing is prohibited without explicit authorization.

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

Regulatory Information

Category: FBI CJIS Security Policy
Version: 6.0 12/27/2024
Reference: https://le.fbi.gov/file-repository/cjis_security_policy_v6-0_20241227.pdf/view

Category: HIPAA Security Rule
Version: 45 CFR Parts 160 & 164
Reference: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164

Category: Payment Card Industry Data Security Standard (PCI DSS)
Version: 4.0 06/2024
Reference: https://www.pcisecuritystandards.org/document_library/

Category: NIST SP 800-122
Version: 04/06/2010
Reference: https://csrc.nist.gov/pubs/sp/800/122/final

Definitions

Criminal History Record Information (CHRI) is a *subset* of CRI that specifically includes arrest cycles, charges, and disposition information that is protected under the FBI CJIS Security Policy.

Criminal Justice Information (CJI) is any information collected, created, received, or maintained by criminal justice agencies that is needed for law enforcement, public safety, or criminal justice operations.

Criminal Record Information (CRI) is information created, collected, or maintained by a criminal justice agency that documents an individual's interaction with the criminal justice system, including arrest records, booking information, warrants, charges, court data, and correctional or supervision records. CRI may include, but is not limited to, Criminal History Record Information (CHRI) and is considered sensitive data requiring controlled access and protection.

Data classification is the process of organizing information into categories based on its sensitivity, value, and the level of protection it requires. Classification helps an organization determine how data should be accessed, stored, transmitted, and disposed of to reduce risk and comply with legal or regulatory requirements.

Encrypted Storage is the protection of data at rest by converting information into an unreadable format using cryptographic algorithms. Data stored on devices, servers, or cloud platforms can only be accessed or decrypted by authorized users or systems possessing the appropriate encryption keys, helping prevent unauthorized disclosure if the storage medium is lost, stolen, or compromised.

Encrypted Transmission is the process of securing data while it is being sent between systems or networks by encrypting the data in transit. This ensures that information exchanged over wired or wireless connections cannot be intercepted, read, or altered by unauthorized parties, typically using secure protocols such as TLS or VPN.

Encrypted Backups are copies of data that are encrypted before being stored for recovery purposes. This ensures that backup data, whether stored on-site, off-site, or in the cloud, remains protected from unauthorized access while maintaining confidentiality and integrity during storage and restoration operations.

Health Insurance Portability and Accountability Act (HIPAA) is a federal law that sets national standards for safeguarding the privacy and security of health information. HIPAA regulates the use, disclosure, protection, and breach notification requirements for Protected Health Information (PHI) and Electronic Protected Health Information (ePHI). Covered entities and business associates must comply with the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule.

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.

Payment Card Industry Data Security Standards (PCI DSS) is a global security standard that establishes technical and operational requirements for protecting payment card information. PCI DSS applies to any entity that stores, processes, or transmits credit card data and mandates controls for securing cardholder data, preventing fraud, and safeguarding sensitive authentication information.

Personally Identifiable Information (PII) is any data that can identify an individual on its own or when combined with other information. PII includes both direct identifiers (which uniquely identify a person) and indirect identifiers (which can be used to identify someone when linked with other data).

Virtual Private Network (VPN) is a secure technology that creates an encrypted connection between a user, device, or network and a remote system over a public or untrusted network, such as the internet. By encrypting data in transit and masking network traffic, a VPN helps ensure confidentiality, integrity, and secure access to internal resources, while reducing the risk of unauthorized access, interception, or data exposure.