Data Protection Categorization Standard

From the Office of the Chief Information Officer, State of Minnesota

Version: 1.7
Effective Date: 1/1/2016
Revised: 10/1/2023
Approved: John Israel, State Chief Information Security Officer **Date:** 1/31/2024

Standard Statement

All State data must be categorized as either High, Moderate or Low based on its protection requirements. Factors to be considered in assessing protection requirements include, but are not limited to, the impact to individuals or the State if the data is improperly disclosed or modified and the value of data to attackers. Systems, paper or electronic media and physical locations must be protected according to the highest category of data that they store, process, or transmit. Data is owned by the agencies and each agency must identify and categorize their data based on its protection requirements.

Table 1. Data Protection Categorization Controls

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization

1	Data Protection Categorization	State agencies must identify, categorize, and document the common data elements used within the agency.
		
		All data is categorized as one of the following:
		
		• **High:** Data that is highly sensitive and/or protected by law or regulation. This includes, but is not limited to:
		  ○ Protected Health Information (PHI) data as defined in the HIPAA Regulation (45 C.F.R., Sec. 160.103).
		  ○ Social Security Administration (SSA) Data
		  ○ Criminal Justice Information (CJI) data as defined in the FBI Criminal Justice Information Services (CJIS) Security Policy.
		  ○ Government issued ID Numbers (e.g., Social Security Numbers, Driver's license numbers / State ID Card numbers, Passport Numbers)
		  ○ Federal Tax Information (FTI) data as defined in IRS Publication 1075.
		  ○ Payment Card Industry (PCI) Account Data as defined by the Payment Card Industry Data Security Standards (PCI DSS).
		  ○ Bank account numbers excluding State-owned bank account numbers.
		• **Moderate:** Data that does not meet the definition of Low or High. This includes, but is not limited to:
		  ○ System security information.
		  ○ Not public names.
		  ○ Not public addresses.
		  ○ Not public phone numbers.
		  ○ IP addresses.
		• **Low:** Data that is defined by Minnesota Statutes Chapter 13 as "public" and is intended to be available to the public.
			Low
			
			Moderate
			
			High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
2	System Protection Categorization	Systems must be categorized as follows: • Systems must be categorized based on the highest categorized data the system stores, processes, or transmits. • Security and authentication systems must be categorized based on the highest categorized system or data that they are protecting.	Low Moderate High
3	Record Retention	State data storage must be kept to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following: • Handling and retaining information within systems and information output from systems in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. • Specific retention requirements for cardholder data and other regulated data. • Processes for secure deletion of data when no longer needed. • A quarterly process for identifying and securely deleting stored data with a Data Protection Categorization of High that exceeds defined retention.	High
4	Sensitive Authentication Data	Payment Card Industry sensitive authentication data (full track data, card validation code or value, and PIN data) must not be stored after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.	High
5	Recordkeeping	A log of all requests for FTI, including receipt and disposal of returns or return information must be maintained. This includes any medium containing FTI, such as computer tapes, cartridges, CDs, or data received electronically.	High

Control Number	Control Name	Control Detail	Applicable Data Protection Categorization
6	Publicly Accessible Content	Processes must be in place to ensure not public information is not published on publicly accessible systems. Processes must include: • Designating individuals that are authorized to post information onto publicly accessible systems. • Training authorized individuals to ensure that publicly accessible information does not contain nonpublic information. • Reviewing the proposed content of information prior to posting onto publicly accessible systems to ensure that nonpublic information is not included. • Reviewing the content on publicly accessible systems for nonpublic information bi-weekly and removes such information, if discovered.	Low Moderate High

Reason for the Standard

Categorization of data is a critical part of data management, which includes identifying and implementing appropriate security controls to support the confidentiality, availability, and integrity of data. The categorization determines the baseline security controls for the protection of the data. These controls are identified within the Enterprise Information Security Standards. The protection requirements follow the data between systems, media, and physical locations.

Roles & Responsibilities

- Employees, Vendors, and Contractors
    - Be aware of and follow relevant information security policies, standards, and procedures.
    - Ensure information security is incorporated into processes and procedures.
    - Ensure contract language with vendors and contractors includes required information security controls.
    - Consult with information security staff on the purchase and procurement of information technology systems or services.
    - Contact information security staff or email GRC@state.mn.us with questions about the information security policies, standards, or procedures.
- Supervisors and Managers
    - Ensure employees and contractors are proficient in the information security policies, standards and procedures that are relevant to their role.
    - Hold employees accountable for following the information security policies, standards, and procedures.

    - Information Technology Personnel
    - Apply appropriate controls to the design, operation and maintenance of systems, processes, and procedures in conformance with the information security policies, standards, and procedures.
- Information Security Personnel
    - Develop, maintain, and assess compliance with the information security policies, standards, and procedures.
    - Develop, maintain, and implement a comprehensive information security program.
    - Provide training on information security policies, standards, and procedures.
    - Assist agencies and personnel with understanding and implementing information security policies, standards, and procedures.
    - Notify appropriate personnel of applicable threats, vulnerabilities and risks to State data or systems.
- Agency Data Practices Personnel
    - Assist agencies and personnel with questions on proper data use, collection, storage, destruction, and disclosure.

Applicability

This standard applies to all departments, agencies, offices, councils, boards, commissions, and other entities in the executive branch of Minnesota State Government.

Related Information

Information Security and Risk Management Program Policy

Minnesota Statutes Chapter 13

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Federal Information Security Management Act (FISMA)

Criminal Justice Information Services (CJIS) Security Policy

IRS Publication 1075

Payment Card Industry Data Security Standard (PCI DSS)

State Standards and Authoritative Source Cross Mapping

Glossary of Information Security Terms

History

Version	Description	Date
1.0	Initial Release	4/21/2015
1.1	Added Compliance Enforcement Date	12/29/2015
1.2	Updated Compliance Enforcement Date	12/20/2016
1.3	Updated Compliance Enforcement Date	10/26/2017
1.4	Scheduled Document Refresh	3/10/2020
1.5	Scheduled Document Refresh	11/1/2021
1.6	Grammatical updates	10/1/2022
1.7	Clarified “not public” info; version number and revision date updated	10/1/2023

Contact

GRC@state.mn.us