



STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2024

191 - Data Classification Standard

Purpose

The Data Classification Standard is intended to provide standardization for identification and classification of information assets, to facilitate the use of appropriate security, privacy, and compliance measures to protect the confidentiality, integrity, and availability of the information (data) and associated Information Technology (IT) resources according to its value and/or risk(s) to the agencies.

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact on the State if that data is disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate to safeguard that data. Executive Branch Agencies shall develop policies, procedures, or processes for their own State information and systems to protect State information, where applicable.

Standard

All information assets managed by Executive Branch Agencies shall be identified and categorized. For those agencies bound by any data marking regulatory compliance requirements and expectations, they shall label their data as appropriate, to satisfy the aforementioned requirements. Some examples of data labels include Classified, Restricted, Sensitive, Public, Protected, or Confidential. These labels are determined by the impact level of high, moderate, low, or none as determined by the Executive Branch Agencies and based on the three principles of security: 1) confidentiality, 2) integrity, and 3) availability. Classified information assets have a high impact level, restricted information assets have a moderate impact level, sensitive and public information assets have low impact levels. Information assets that have data at multiple classifications shall be identified, categorized, and labeled as the highest identified classification level. Agencies shall reflect their controls through the quarterly reporting process to DOA-DET.

See the table below for one example of the confidentiality principle of data classification.



**STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION**

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2024

Classification	Adverse Business Impact	Description	Examples (not an exhaustive list)
Classified or Confidential	High	Any data where the unauthorized disclosure, alteration, loss, or destruction may cause personal or organizational financial loss or the unauthorized release of which would be a violation of a statute, act or law; constitute a violation of confidentiality agreed to as a condition of possessing or producing or transmitting data; cause significant reputational harm to the organization; or require the organization to self-report to the U.S. government and/or provide a public notice if the data is inappropriately accessed.	Subject to regulatory or compliance requirements (e.g., FTI, HIPAA, IRS, DMCA, PCI, PHI, PII, etc.). Data with contractual language requiring a confidential or high classification level of information/data. Information assets at this level shall limit access to authorized individuals only and shall employ encryption of data at rest, in use, and in transit (AC-21).
Restricted	Moderate	Any data, if released to unauthorized individuals, could have a mildly adverse impact on the organization’s mission, safety, finances, or reputation. Data not specifically identified in another level is categorized as a “Moderate Risk”.	Information assets at this level can be shared with individuals external to the agency and do not require encryption of data at rest or in use (AC-21).
Sensitive	Low	Any data where the unauthorized disclosure, alteration, loss, or destruction would have a low impact on the mission, safety, finances, or reputation of the organization.	Information assets at this level can be shared with individuals external to the agency and do not require encryption of data at rest, in use, or in transit (AC-21).
Public	Insignificant	Data that if breached owing to accidental or malicious activity would have an insignificant impact on the organization’s activities and objectives.	Information assets at this level can be shared publicly and do not require encryption of data at rest, in use, or in transit (AC-21).

Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies. Agency or State Agency may be used interchangeably with Executive Branch Agency.

State information - Any information that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.

State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to network devices, servers,



**STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION**

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2024

databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed the agency.

Information Asset – All information and information systems and environments that have value to an organization.

Compliance References

- IRS Pub. 1075
- NIST 800-53 Revision 5
- NIST 800-60 Vol 1 and 2
- FIPS 199

Exception Process

Exceptions to any Executive Branch Agency’s Security Policies or Standards shall follow the Executive Branch Risk Exception Procedure.

Document History/Owner

This standard was developed as required by the State of Wisconsin Information Technology Security Policy Handbook, under the authority of Wis. Stat. § 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
2.0	11/03/20	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	11/11/20
3.0	06/24/22	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	06/24/22
4.0	07/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	08/01/23
5.0	7/2/24	Reviewed with Agency Security Officers and IT Directors and	Reviewer: WI ISAC and Enterprise IT	7/30/24



STATE OF WISCONSIN DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2024

		changes were incorporated	Author: DOA/DET/BOS	
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				

Authorized and approved by:

Troy Stairwalt, State of Wisconsin Chief Information Security Officer

DocuSigned by:
Troy Stairwalt
Signature

7/31/2024 | 4:05 PM CDT

Print/Type
Title

Date