191 – Data Classification Standard

Purpose

The Data Classification Standard is intended to provide standardization for identification, classification, and labeling 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. To identify how to maintain systems, applications, and integrations in order to ensure data confidentiality, integrity, and availability.

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the State if that data be 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 are to 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 must be identified, categorized, and labeled. 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 must be identified, categorized, and labeled as the highest identified classification level. Agencies are to reflect their controls through the annual reporting process to DOA-DET.

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

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 must limit access to authorized individuals only and must 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.

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, 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 has 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 Agencies Security Policies, Procedures or Standards must follow the Executive Branch Agencies 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 Wisconsin State Statute 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
1.0	10/15/18	Submitted to and approved by the IT Executive Steering Committee	Reviewer: ITESC Author: DOA/DET	10/15/18
1.0	10/29/19	Reviewed with Agency Security Officers and feedback collected. Planning for making revisions.	Bureau of Security	10/29/19
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
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:

Alan Greenberg, CISO

DocuSigned by:
Alan Greenberg
7062227F849B429...

7/8/2022 | 1:55 PM CDT

Print/Type
Title

Signature

Date