Policy & Standard Background

Name: Data Classification Standard

New

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

The 2017 version of OCIO 141.10 section 4.1 describes the four categories of data processed by agency systems. The new standard builds upon this section by highlighting the impact of agency mission and business objectives, and data aggregation, on data classification. It also requires agencies to perform an IT risk assessment on its Category 3 and 4 data to identify data protection requirements which may exceed compliance requirements.

What is the business case for the policy/standard?

Legal requirements and the data use demands of an agencies mission impact the categorization of that data. This standard ensures that consistent requirements guide data categorization.

What are the key objectives of the policy/standard?

- **Agencies use uniform standards when categorizing data.**
- **Agencies identify Category 3 and Category 4 data security requirements that may exceed compliance requirements.**

How does policy/standard promote or support alignment with strategies?

This policy ensures that agencies consider legal requirements and mission-related use when categorizing data. It also ensures that these factors inform agency data protection strategies.

What are the implementation considerations?

Agencies must validate that their data classification schemes meet the requirements in this standard.

How will we know if the policy is successful?

- **Agencies will be able to provide a risk assessment identifying the risks of processing Category 3 and Category 4 data.**
- **Agencies will be able to map their data classification schemes to this standard.**

State CIO Adopted:
TSB Approved:
Sunset Review:

Replaces:
IT Security Standard 141.10 (4.1)
December 11, 2017

DATA CLASSIFICATION STANDARD

See Also:

RCW 43.105.450 Office of Cybersecurity
RCW 43.105.020 (22) "State agency"
RCW 39.26.340 Data Sharing- Contractors
RCW 39.24.240 Data Sharing - Agencies

1. Agencies must classify data into categories based on its sensitivity and handling requirements.

a. Agency data classifications must translate to or include the following classification categories:

i. Category 1 - Public Information

Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.

ii. Category 2 - Sensitive Information

Sensitive information is not specifically protected from disclosure by law but is for official use only. Sensitive information is generally not released to the public unless specifically requested.

iii. Category 3 – Confidential Information

Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to:

A. Personal information as defined in RCW 42.56.590 and RCW 19.255.010.
B. Information about public employees as defined in RCW 42.56.250.
C. Lists of individuals for commercial purposes as defined in RCW 42.56.070(8)
D. Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

iv. Category 4. - Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

A. Especially strict handling requirements are dictated, such as by statutes, regulations, agreements, or other external compliance mandates.
B. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

b. Refer to the Risk Management Policy and Risk Assessment Standard for management of risk based on these classifications.

2. Agencies must consider certain factors when categorizing data.

a. Agencies must identify and understand all laws, regulations, policies, and standards that apply to their data and ensure applicable requirements are met.
b. Agencies must take their missions and business objectives into consideration when evaluating their data classifications.
c. Agencies must consider how combining or aggregating data may change the sensitivity of the data.
d. In general, the sensitivity of a given data element is likely to be greater in combination than in isolation (e.g., association of an account number with the identity of an individual and or

institution).

e. When data is newly combined or aggregated its classification level should be reviewed.
f. Agency Data Sharing: Refer to the Data Sharing Policy.

REFERENCES

1. NIST 800-60: Guide for Mapping Types of Information & Information Systems to Security Categories.
2. Definition of Terms Used in WaTech Policies and Reports.
3. Data Sharing Policy.
4. Risk Management Policy.
5. Risk Assessment Standard.
6. RCW 42.56.590 Personal information—Notice of security breaches.
7. RCW 19.255.010 Personal information—Notice of security breaches.
8. RCW 42.56.250 Employment and Licensing.
9. RCW 42.56.070 (8) Documents and indexes to be made public—Statement of costs.
10. RCW 42.56.420 Security.
11. NIST Cybersecurity Framework Mapping
    - Identify.Asset Management-5: Resources are prioritized based on their classification, criticality, and business value.
    - Identify.Risk Assessment-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.

CONTACT INFORMATION

- For questions about this policy, please contact the WaTech Policy Mailbox.
- For technical security questions or to submit risk assessments, please contact the WaTech Risk Management Mailbox.
- For technical security questions or to request a Design Review, please contact sdr@watech.wa.gov.