Maine State Government

Department of Administrative and Financial Services

Office of Information Technology (OIT)

Data Classification Policy

1.0. Purpose

The State's information assets are essential resources that must be protected from unauthorized use, access, disclosure, modification, loss or deletion. This policy describes the process for classifying and labeling State of Maine information assets. Proper classification of State information assets enables agencies to conduct their business through effective management of risk to information confidentiality, integrity, and availability. It also allows for implementation of appropriate information security controls that support each agency's mission in a cost-effective manner.

2.0. Definitions

2.1. *Confidentiality, Integrity, and Availability (CIA):*

2.1.1. *Confidentiality*: The security objective of confidentiality is defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (FIPS 199).

2.1.2. *Integrity*: The security objective of integrity is defined as guarding against improper modification or destruction of information assets, which includes ensuring information nonrepudiation and authenticity (FIPS 199).

2.1.3. *Availability*: The security objective of availability is defined as ensuring the timely and reliable access to and use of information assets (FIPS 199).

2.2. *Data*: A representation of information in a formalized manner suitable for communication, interpretation, or processing. Data can be processed by humans or by automatic (electronic) means. Examples of data may include, but are not limited to, documents, emails, transcripts, images, audio, or video stored electronically, databases, logs, or journals.

2.3. *Data Classification*: The taxonomy of organizing data into categories, so that data may be used and protected efficiently.

2.4. *Information Asset:* A body of information, defined and managed as a single unit, so that it can be understood, shared, protected, and utilized effectively. Information assets have recognizable and manageable value, risk, content, and lifecycles. Information assets could come in any media form, for example, paper, or electronic format (CDs, USBs, Hard Disk Drives [HDDs], etc.). It could be structured (databases, etc.) or unstructured (emails, etc.). It includes tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) and intangible assets (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation); its value is determined by stakeholders in consideration of loss concerns across the entire system life cycle, including but not limited to business or mission concerns.(*NIST, SP 800-160 Vol. 2 Rev. 1*)

2.5. *Information Asset Owners*: Ownership of Information Assets is listed in the OIT Information Systems Contingency Plan (CP-2)[1] (Intranet only).

2.6. *Personally Identifiable Information (PII)*: Information that can be used to distinguish or trace the identity of an individual (for example, name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual (such as date and place of birth, mother's maiden name, etc.)., please see Maine Public Law 10 MRSA § 1347. It also includes personally identifiable information protected from disclosure under Federal or State privacy laws.

3.0. Applicability

3.1. This Policy applies to:

3.1.1. All State of Maine Executive Branch personnel, both employees and contractors.

3.1.2. Executive Branch data and information assets, irrespective of hosting location; and

3.1.3. Information assets from other Maine State Government branches that use the State network or are co-hosted with Executive Branch information assets.

4.0. Responsibilities

4.1. Agency Business Partners

4.1.1. Serve as the fiduciary steward and custodian of their data.

4.1.2. Serve as the classification authority for the data and information that the agency collects or maintains in fulfilling its mission.

[1] https://inet.state.me.us/oit/policies/documents/InformationSystemsContingencyPlan.pdf

4.1.3. Classify agency data in accordance with this Policy, all applicable Federal and State statutory and regulatory compliance requirements, and Office of Information Technology (OIT) policies, procedures, and standards.

4.1.4. Agency Business Partners assign Agency staff to ensure the data the agency generates or manages is categorized in compliance with this Policy.

4.1.5. In collaboration with OIT Information Asset Owners and I.T. Procurement, holds internal and contracted parties that are responsible for State information assets accountable to this Policy.

4.1.6. Develops and implements Agency-level policy and procedures to meet additional statutory requirements or Agency-specific requirements for safeguarding State information assets.

4.2. Chief Information Security Officer (CISO)

4.2.1. Serves as the final authority for resolving any data classification conflicts or under this Policy.

4.3. OIT Information Asset Owners

4.3.1. Comply with this Policy.

4.3.2. In collaboration with Agency Business Partners and I.T. Procurement, hold internal and contracted parties that are responsible for State information assets accountable to this Policy.

4.3.3. Ensure data being managed through the assigned information assets are designed and implemented to achieve the security required based on the classification assigned by the Agency Business Partner.

4.4. OIT Information Security Office (ISO)

4.4.1. Owns, executes, and enforces this Policy.

4.4.2. Provides oversight of the security tools, practices, and procedures to protect agency and State data.

4.4.3. Communicates required controls to the OIT Information Asset Owners and Agency Business Partners based on the assigned classification of an Information Asset.

4.5. State of Maine Chief Data Officer

4.5.1. Owns the governance of data to provide stewardship to the data management program for the State of Maine.

5.0. **Benefits of Classifying Data**

5.1. State agencies rely upon State data, information system assets and information systems to successfully conduct critical missions. As reliance upon these assets and systems has grown, so has their complexity within our current risk environment. As a mission-essential function, information security must be conducted in a manner that reduces the risks to the information entrusted to the agency, its overall mission, and its ability to do business and serve Maine citizens.

5.2. Proper classification of State information assets enables agencies to conduct their business through effective management of risk to information confidentiality, integrity, and availability. It also allows for implementation of appropriate information security controls that support their mission in a cost-effective manner.

5.3. Conversely, an incorrect information asset or system categorization can result in either over-protecting the asset or system, which wastes valuable security resources, or under-protecting it and placing important operations and assets at risk. The aggregation of such mistakes at the enterprise level can further compound the problem. The failure to secure and protect the confidentiality, integrity and availability (CIA) of data in a highly networked environment can damage or shut down systems that operate critical infrastructure, financial and business transactions, and vital government functions. Such unauthorized disclosure can compromise data and result in legal and regulatory non-compliance.

5.4. The initial security categorization should occur as early as possible in the initiation, planning, and procurement or development phases of a technology solution (or system) to ensure the appropriate security requirements and security controls are applied with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability).

6.0. Data Classification Process

6.1. State data is classified in accordance with this Policy to ensure appropriate protections and consistency throughout the data life cycle.

6.1.1. To classify data, the data type must first be identified, which includes assessing the value, legal requirements, sensitivity, and criticality (i.e., integrity and availability needs) of the data, which informs impact determinations. Agencies classify data according to its sensitivity and its legal and regulatory compliance requirements.

6.1.1.1. Classification of data and ensuing security controls are guided by a wide array of federal and state statutory and regulatory requirements (See Appendix A). Data classification must also be considered in the development of agency Memorandums of Agreement and other similar types of data sharing agreements.

6.1.2. The four (4) model data classification schema (i.e., Public, Internal, Sensitive, and Restricted) was adopted to be the foundation for the State's classification schema.

6.1.3. To determine what information goes into which schema, Federal Information Processing Standards (FIPS) 199 security objectives were used to categorize data based on its level of CIA. These three core cybersecurity objectives are described as follows:

6.1.3.1. Confidentiality – preventing unauthorized disclosure of information;
6.1.3.2. Integrity – preventing unauthorized modification of information; and
6.1.3.3. Availability – providing timely access to information.

6.1.4. For each of these objectives, an information type is assigned an impact level of no impact, low, moderate, or high, depending on what security implications would result from a failure to achieve said objective. Each objectives is individually rated as no impact, low, moderate, or high impact. For example, an information asset may have a confidentiality level of "high", an integrity level of "moderate", and an availability level of "low" (e.g., HML (See Appendix B, Table 1 for additional details).

6.1.5. When classifying the impact, the agency should consider how the information/ information systems is used to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

6.2. An information asset must be classified based on the highest level necessitated by its individual data elements. The control baselines selected for systems are commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, or the State if there is a loss of CIA. The high-water mark concept is used to determine the impact level of the system described as follows:

6.2.1. A low-impact system is defined as a system in which all three of the security objectives are low.

6.2.2. A moderate-impact system is a system in which at least one of the security objectives is moderate and no security objective is high.

6.2.3. A high-impact system is a system in which at least one security objective is high.

6.3. Merging of information which creates a new information asset or situations that create the potential for merging (e.g., backup tape with multiple files) must be evaluated to determine if a new classification of the merged data is warranted.

6.4. The results of security classification inform the selection of security control baselines to protect systems and information.

6.5. Agencies should use a risk-based approach to protecting the confidentiality of PII.[2] In brief, NIST guidance on determining the PII confidentiality impact levels of data (see NIST SP 800-122), is based on six factors:

6.5.1. Identifiability: How easily PII can be used to identify specific individuals.

6.5.2. Quantity of PII: How many individuals are identified in the information.

[2] Agencies are responsible for compliance with a combination of laws, regulations, and other mandates related to protecting PII and should seek appropriate guidance from legal counsel and privacy officers as appropriate.

6.5.3. Data Field Sensitivity: The sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together.

6.5.4. Context of Use: The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated.

6.5.5. Obligation to Protect Confidentiality: Any laws, regulations, or mandates governing the obligation to protect PII.

6.5.6. Access to and Location of PII: The nature of authorized access to PII.

6.5.6.1. The more frequently and widely PII is accessed, the more opportunities exist for compromise of confidentiality.

6.5.6.2. PII being accessed from outside the direct control of the organization, such as by being stored on, or accessed from, remote workers' devices or other systems, for example web applications, carries a higher risk.

6.6. The overall classification of any Information Asset is pegged to the classification of the data that it transacts, and is irrespective of lifecycle and/or environment, for example, Production, Test, Staging, Training, Quality assurance, etc. For instance, if production data is copied, into a lower (less restrictive and lower classification) environment, then the lower environment must be treated just as the production environment with respect to security, compliance, privacy, etc.

6.7. System information (e.g., network routing tables, password files, cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed by the information system to ensure confidentiality, integrity, and availability.

6.8. For net-new applications, configuration changes, or information assets utilizing Agency data, prior to Deployment Certification, Agency Business Partners and OIT Information Asset Owners collaborate to classify the data that will be used. The OIT Information Security Office validates the data classification.

6.8.1. The CISO resolves conflicts as provided above, see Section 4.2.

6.9. Agencies may use the guidance provided (see Appendix C) and the Information Asset Classification Worksheets (Appendix E) to assist with their data classification decisions for security objectives (CIA). Owners should consult with subject matter experts who have specific knowledge about the information asset. The ISO may also be called upon to advise and assist agencies in determining the classification.

6.10. For existing applications, configuration changes, or information assets utilizing Agency data, as part of risk assessments (see Risk Assessment Policy and Procedures), Agency Business Partners and OIT Information Asset Owners collaborate to classify the data used (see Risk Assessment Policy and Procedures). The ISO validates the assigned data classification when needed.

7.0. **Data Sharing Protocol (TLP)**

7.1. The Traffic Light Protocol (TLP) was established by the Forum of Incident Response Security Teams (FIRST) to facilitate greater sharing of potentially sensitive information and more effective collaboration. The Cybersecurity and Infrastructure Security Agency (CISA) and various federal and state partners have adopted TLP to establish boundaries and build trust within the cybersecurity community. By quickly understanding each other's expected sharing boundaries, entities can foster timely, actionable, and effective information sharing to mitigate and even prevent cyber incidents.

7.2. In addition to data classification, all State agencies should assign data a corresponding TLP label to facilitate information sharing among state and federal partners to ensure appropriate data sharing boundaries are established and maintained.

7.3. TLP is a set of four labels used to indicate the sharing boundaries to be applied by the recipients. The four TLP labels are: TLP: RED, TLP:AMBER, TLP:GREEN, and TLP:WHITE as follows:

7.3.1. TLP: White: Information that the organization has permission or authority to release publicly and, therefore, does not need confidentiality protection.

7.3.2. TLP: Green: Limited adverse effect on organizational operations, organizational assets, or individuals resulting in minor degradation to an organization's ability to carry out its mission, minor financial loss, and/or minor harm to individuals.

7.3.3. TLP: Amber: Serious adverse effect on organizational operations, organizational assets, or individuals including resulting in significant degradation to an organization's ability to carry out its mission, significant financial loss, and/or significant but non-life-threatening harm to individuals.

7.3.4. TLP: Red: Severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals resulting in severe degradation to or a complete loss of an organization's ability to carry out its mission, severe financial loss, and/or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

7.4. See Appendix D (Table 3) for alignment between TLP labels and the State's data classification schema.

7.5. See Appendix F for an overview of how to manage information sharing using the TLP rating system.

7.6. See Appendix G for examples of how to TLP ratings apply to selected OIT data handling policies and procedures.

8.0. **References**

8.1. The following sources were used in the development of the schemas for data classification:

8.1.1. *FIPS Publication 199, Standard s for Security Categorization of Federal Information and Information Systems*: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf; and *FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems:* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

8.1.2. *NIST SP 800-53, Recommended Security Controls for Federal Information Systems Rev. 3:* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf;

8.1.3. *NIST SP 800-60 Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories:* http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800- 60_Vol1-Rev1.pdf

8.1.4. *NIST SP 800-60 Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf

8.1.5. *NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII):* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf

9.0. **Initial Issue Date**: February 3, 2023

10.0. **Latest Revision Date:** February 3, 2023

11.0. **Point of Contact:** Enterprise.Architect@Maine.Gov

12.0. **Approved By:** Chief Information Officer, OIT

13.0. **Legal Citation**: Title 5, Chapter 163: Office of Information Technology

14.0. **Waiver Process:** Waiver Policy

15.0. **Distribution:** Internet

Appendix A. Data Classification – Summary of Applicable State and Federal Standards, Policies and Laws

The laws, regulations, and guidance documents cited in this Table include various terms and definitions used to describe personal information; it is not intended to be a comprehensive list. Note that additional security controls may be required for certain data types based on federal and state statutory and regulatory requirements.

TABLE 1: SUMMARY OF STATE AND FEDERAL STANDARDS, POLICIES AND LAWS BASED ON DATA TYPE

Type of Data	Applicable State & Federal Standards, Policies, and Laws (*not intended to be an exhaustive list*)
☐Publicly available information	▪ NIST 800-171 ▪ Maine Freedom of Access Act (Title 1 MRSA c. 13)
☐ Confidential Personally Identifiable Information (PII)	▪ State of Maine Breach Notification Law ▪ National Institute of Standards & Technology: NIST SP 800-53 Revision 5 "Moderate" risk controls ▪ Privacy Act of 1974, 5 U.S.C. 552a. ▪ Security regulations from the U.S. DHHS, Administration for Children and Families, Office of Child Support Enforcement Program, Office of Child Support Enforcement (OCSE)
☐ Payment Card Information	▪ Payment Card Industry Data Security Standard (PCI DSS) v 3.2 ▪ Nacha Operating Rules (ACH)
☐ Federal Tax Information	▪ Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies: IRS Pub 1075 ▪ IRS Pub 1075 Contractor Language Addendum required
☐ Personal Health Information (PHI) / ☐ Individually Identifiable Health Information (IIHI)	▪ Health Insurance Portability and Accountability Act of 1996 (HIPAA), ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS, 45 C.F.R. § 160.103. ▪ State of Maine HIPAA BAA required ▪ The Health Information Technology for Economic and Clinical Health Act HITECH ▪ Code of Federal Regulations 45 CFR 95.621 ▪
☐ Affordable Care Act Personally Identifiable Information (PII)	▪ Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies IRS Pub 1075 ▪ Minimum Acceptable Risk Standards for Exchanges MARS-E 2.0 (Scroll down the page)
☐ Medicaid Information	▪ Medicaid Information Technology Architecture MITA3.0 ▪ Code of Federal Regulations 45 CFR 95.621
☐ Student Education Data	▪ Family Educational Rights and Privacy Act: FERPA
☐ Personal Information from Motor Vehicle Records	▪ Driver's Privacy Protection Act (Title XXX) ("DPPA") 18 U.S.C. Chapter 123, §§ 2721 – 2725
☐ Criminal Records	▪ Criminal Justice Information Security Policy: CJIS
☐ Social Security Act Data	▪ Service Level Agreements containing language as specified in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration (SSA)
☐ Exempt Records under Maine's FOAA	▪ Various types of personal information exempt from public disclosure under Maine FOAA

Appendix B. Information Asset Classification Categories per FIPS 199

Table 2. Information Asset Classification Categories per FIPS 199

		Potential Impact		
SECURITY OBJECTIVE	**NO IMPACT**	**LOW RISK**	**MEDIUM RISK**	**HIGH RISK**
CONFIDENTIALITY Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	No foreseeable effect on organizational operations, assets or individuals from any unauthorized disclosure of information.	The unauthorized disclosure of information would have little or no adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals, i.e. (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals, i.e. loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Appendix B. Information Asset Classification Categories per FIPS 199

INTEGRITY Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	No foreseeable effect on organizational operations, assets or individuals from unauthorized modification or destruction of information.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
AVAILABILITY Ensuring timely and reliable access to and use of information.	No foreseeable disruption of access to or use of information or an information system is expected to have an effect on organizational operations, assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Appendix C. Additional Guidance for Data Classification

1.0. **Guidance to Inform the Data Classification Process**

1.1. Before determining the classification, it may be beneficial for agencies to familiarize themselves with the following areas:

1.2. Source, Purpose, and Value:

1.2.1. How the information asset is used in supporting business functions.

1.2.2. How often the information asset is used.

1.2.3. How often the information asset is updated.

1.2.4. Dependencies between this information asset and others.

1.2.5. The cost of creating and duplicating the information.

1.3. Legal Requirements:

1.3.1. Laws, regulations, policies, or contracts that mandate special security requirements for the information (e.g., Health Insurance Portability and Accountability Act (HIPAA)).

1.3.2. Retention requirements for the information asset.

1.4. Access Requirements:

1.4.1. Who has/should have access to the information (e.g., people, positions, organizational units).

1.4.2. Whether the information is shared among other units/State Entities, third-parties, Federal/local governments.

1.5. Health and Safety Concerns:

1.5.1. Impact on agency personnel as well as the public.

1.6. Mission:

1.6.1. The overall mission of the State Entity.

1.6.2. The information owner's role (or unit's role) in completing the mission.

1.7. Non-tangible Effects:

1.7.1. Impact if information asset is not available (temporarily or permanently).

1.7.2. The effect of a breach of confidentiality, integrity, or availability on the intangible assets of the State Entity such as reputation, trust and morale.

Appendix D: TLP and Corresponding Alignment with the State Data Classification Scheme

Table 3: TLP and Corresponding Alignment with Data Classification Schema

Data Classification Scheme	TLP Category	PII Confidentiality Impact Level	Availability**
Public	White	No Impact or N/A	Greater than a Month
Internal	Green	Low - a limited adverse effect	Up to a Month
Sensitive	Amber	Moderate -serious adverse effect	1 Week or less
Restricted	Amber*	High - severe or catastrophic adverse effect	Hours to a few days
	Red		

**TLP Amber may be used to encompass information assets classified as Sensitive and Restrictive, depending on CIA impact levels assigned to the data.*

***Availability is provided here for guidance only and is not intended to be determinative or replace the agency's internal assessment.*

Appendix E: Data Classification Worksheets for 3 Security Objectives (CIA)

CONFIDENTIALITY QUESTIONS				
1. Is the information publicly available?	No		Yes	
2. Does the information include or contain Personal, Private, or Sensitive Information (PPSI)?	No		Yes	
	None	Limited	Serious	Severe
3. What impact does unauthorized disclosure of information have on health and personal safety?				
4. What is the financial or agency liability impact of unauthorized disclosure of information?				
5. What impact does unauthorized release of sensitive information have on the agency's mission?				
6. What impact does unauthorized disclosure of information have on the public trust, agency reputation, and public interests?				
7. Is confidentiality mandated by law or regulation? If yes, what is the impact of unauthorized disclosure of information. If no, do not make a selection.				
8. Is the information intended for limited distribution? If yes, what is the impact of unauthorized disclosure. If no, do not make a selection				
CONFIDENTIALITY RATING				

If ALL answers are **GREEN**, the rating is **Low**; if ANY of the answers are **YELLOW** and **NONE** are **RED**, the rating is **MODERATE**; if ANY of the answers are **RED**, the rating is **HIGH**.

Appendix E: Data Classification Worksheets for 3 Security Objectives (CIA)

INTEGRITY QUESTIONS				
1. Does the information include medical records	No		Yes	
2. Is the information (e.g., security logs) relied upon to make critical security decisions?	No		Yes	
	None	Limited	Serious	Severe
3. What impact does unauthorized modification or destruction of information have on health and safety?				
4. What is the financial impact of unauthorized modification or destruction of information?				
5. What impact does unauthorized modification or destruction of information have on the agency's mission?				
6. What impact does unauthorized modification or destruction have on the public trust?				
7. Is integrity addressed by law or regulation? If yes, what is the impact of unauthorized modification or destruction of information. If no, do not make a selection.				
8. Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, what is the impact of unauthorized modification or destruction of information. If no, do not make a selection.				
INTEGRITY RATING				

If ALL answers are **GREEN**, the rating is **Low**; if ANY of the answers are **YELLOW** and **NONE** are **RED**, the rating is **MODERATE**; if ANY of the answers are **RED**, the rating is **HIGH**.

AVAILABILITY QUESTIONS				
Assessment Question				
	As time permits	**Within 1 to 7 days**	**24 hrs. per day/7 days a week**	
1. This information needs to be available:				
Impact Questions				
	None	**Limited**	**Serious**	**Severe**
2. What is the impact to health and safety if the information were not available when needed?				
3. What is the financial impact if the information were not available when needed?				
4. What is the impact to the agency's mission if the information were not available when needed?				
5. What is the impact to public trust if the information were not available when needed?				
AVAILABILITY RATING				

If ALL answers are **GREEN**, the rating is **Low**; if ANY of the answers are **YELLOW** and **NONE** are **RED**, the rating is **MODERATE**; if ANY of the answers are **RED**, the rating is **HIGH**.

_____ _____

Information Owner - print **Date**

_____ _____

ISO/Designated security representative - print **Date**

Appendix F: Traffic Light Protocol User Guidance

Traffic Light Protocol (TLP)

TLP definitions referenced below are provided by the Forum of Incident Response Security Teams (FIRST) and adopted by Cybersecurity and Infrastructure Security Agency (CISA) to facilitate greater sharing of potentially sensitive information and more effective collaboration.

Color	When Should It Be Used?	How May It Be Shared?
TLP: Red **Not for disclosure**, restricted to participants only by specific law, statute, regulation, or rule.	Sources may use **TLP: Red** when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if released, accessed, or misused.	Sources may not share **TLP: Red** information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting. TLP: RED information should be exchanged verbally or in person.[3]
TLP: Amber **Limited disclosure** restricted to a limited group of an organization.	Sources may use **TLP: Amber** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Sources may only share **TLP: Amber** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing which must be adhered to.
TLP: Green **Limited disclosure**, restricted to the State of Maine staff.	Sources may use **TLP: Green** when information is useful for the awareness of all participating organizations as well as with peers within the sector.	Sources may use **TLP: Green** when information is useful for the awareness of all participating organizations as well as with peers within the sector.
TLP: White **Disclosure is not limited**.	Sources may use **TLP: White** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules.	**TLP: White** information may be distributed without restriction.

[3] https://www.cisa.gov/uscert/sites/default/files/tlp/tlp-v1.pdf

Appendix G: TLP Ratings and Data Handling Requirements

In addition to data classification, all State agencies should assign data a corresponding TLP label to facilitate information sharing among state and federal partners to ensure appropriate data sharing boundaries are established and maintained. Data is handled based on its rating in adherence with the following data handling policy requirements; additional handling requirements may be required based on applicable statutory and regulatory requirements. Embedded links have been included to reflect State of Maine resources.

	TLP: White	TLP: Green	TLP: Amber	TLP: Red
Accessible only to authorized personnel.	Not required	Required	Required	Required
Accessible only after authentication and protected from unintended access by unauthorized users (see Identification and Authentication Policy,[4] intranet only).	Not required	Required	Required	Required
Accessible only to authorized users after multi-factor authentication based on the principle of least privilege (see Access Control Policy,[5] Access Control Procedures for Users,[6] and Identification and Authentication Policy,[7] intranet only).	Not required	Not required	Suggested	Required
Sent via secure methods of transmission (see Data Exchange Policy[8]).	Not required	Required	Required	Required

[4] http://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf
[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlPolicy.pdf
[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/AccessControlProceduresForUsers.pdf
[7] http://inet.state.me.us/oit/policies/documents/IdentificationAuthenticationPolicy.pdf
[8] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf

Appendix G: TLP Ratings and Data Handling Requirements

	TLP: White	TLP: Green	TLP: Amber	TLP: Red
Kept physically secure (see Physical and Environmental Protection Policy and Procedures[9]).	Not required	Required	Required	Required
Disposed of securely when no longer needed and when retention requirements have been met (see Media Protection Policy and Procedures,[10] Intranet only).	Not required	Required	Required	Required
Segmented from other data types.	Not required	Not required	Suggested	Required
Encrypted at rest and in-flight, using at least AES-256 encryption or better (see Remote Hosting Policy[11]).	Not required	Required	Required	Required
Adhere to the Data Exchange Policy for any data exchange that either originates or terminates with the Maine State Executive Branch (see Data Exchange Policy[12]).	Not required	Not required	Required	Required
Documents and emails are labeled with the applicable data classification and handled accordingly.	Required	Required	Required	Required
Any cloud service provider transacting data must have an acceptable third-party	Not required	Not required	Required	Required

[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/PhysicalandEnvironmentalProtection.pdf
[10] https://inet.state.me.us/oit/policies/documents/MediaProtectionPolicy.pdf
[11] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RemoteHostingPolicy.pdf
[12] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf

Appendix G: TLP Ratings and Data Handling Requirements

	TLP: White	TLP: Green	TLP: Amber	TLP: Red
audit report (see System and Services Acquisition Policy and Procedures[13]).				
Contracts for services that receive, process, or store data must be located in the continental United States (see System and Services Acquisition Policy and Procedures[14]).	Not required	Not required	Not required	Required
Mobile media and devices that contain data must be in a protected environment at all times, or must be encrypted (see Rules of Behavior).	Not required	Not required	Required	Required
Prohibited from posting, uploading, or sharing on any public website or social media site (see Rules of Behavior).	Not required	Required	Required	Required
Handling instructions for use in test environments.	Not required	Not required	Required	Required

[13] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemAndServicesAcquisitionPolicy.pdf
[14] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SystemAndServicesAcquisitionPolicy.pdf