Maine State Government
Dept. of Administrative & Financial Services

Data Management and Governance Practice
Data Sharing Agreement Guidelines Whitepaper

This data sharing guidelines whitepaper outlines the procedures and criteria for sharing and integrating data among the state's departments and agencies. The people of Maine place significant trust in the government by providing a vast amount of personal data, and it is crucial for the government to honor that trust by managing the data responsibly and effectively.

Effective decision-making and fulfilling state obligations require quality information. This involves exchanging data among various agencies and external sources. Ensuring this exchange is efficient, secure, and standardized across departments is crucial. This document is not a policy but is designed to provide guidance on effective data exchange.

Following the guidelines outlined in this document will enhance the state agencies' capacity to safely and securely share data while complying with all applicable Federal and State laws.

Table of Contents

1.0 Why a Data Sharing Agreement Guidelines Whitepaper?

The purpose of this guidelines whitepaper is:

- To provide guidance for state departments and agencies to manage data exchange.
- To create consistency between state agencies regarding data sharing.

When done correctly, data sharing enhances data value and efficiency, drives growth, and improves program, service delivery, and business outcomes. It is an integral part of State of Maine's (SOM's) operations as it allows departments and agencies to access relevant data to derive meaningful insights.

Data sharing is essential for effective policy making and improvement for SOM. It affects departments and agencies by:

- Enhancing data privacy and security with secure, lawful, and governed data exchange instructions.
- Identifying and removing data siloes to enable collaborative decision-making.
- Improving readiness for mandated data sharing by focusing on data, analytics, and quality instead of just compliance.
- Reducing duplicated efforts and redundant spending on the same data assets.

2.0 Applicability

This document applies to all SOM Executive Branch employees, vendors and sub-contractors, covering all Executive Branch information assets regardless of their hosting location.

3.0 Overcoming Data Sharing Barriers

Data sharing is a critical capability for digital transformation; however, there is a lack of consistency in sharing data at scale. State agencies must address issues of internal data retention and the risk of external data misappropriation. Additionally, agencies may be apprehensive of sharing data due to real or perceived regulatory

constraints, fear, outdated or inflexible data management and governance policies, or insufficient tools and technologies.

These challenges can be mitigated through a combination of data governance and organizational change management solutions. Firstly, SOM can collaborate to implement standardized data formats and protocols that ensure compatibility across various systems and departments, thus facilitating seamless data exchange. Secondly, fostering a collaborative culture among departments and agencies is essential. By encouraging cross-departmental teams to communicate and share expertise, data, and resources, our state can overcome internal data retention issues and promote data sharing with confidence. Open lines of communication between departments and agencies will enable the timely dissemination of updates and new regulatory requirements, ensuring that all parties remain well-informed.

4.0 Responsibilities and Management

Numerous responsibilities facilitate data sharing and utilization. These obligations are as follows:

MaineIT Management:

- Ensures that the underlying technical details of the actual exchange comply with industry best practices of security and privacy.
- Manage data sharing with external vendors to ensure that they comply with industry best practices.

Agreement Administrators:

- Serves as official points-of-contact at the agency and departmental levels.

Data Officers and Stewards:

- Reviews data sharing MoAs and DSAs regularly for compliance.
- Responsible for checking data transmission logs for compliance with industry best practices of security and privacy, regulations and laws.

5.0 Data Exchange

Data shared under this guideline shall be categorized as either standing or ad hoc data exchange. They are summarized below:

Standing Data Exchange	Ad Hoc Data Exchange
Routine/ regular data exchange to support ongoing collaboration	Temporary/ one-time basis for emergency response or specific needs
Require formal governance structures to oversee data ownership or stewardship	Should specify the duration for usage and disposal
Requires well-defined access protocols to ensure only authorized users can interact with shared data	Should have the same formal governance structures and access protocols as standing data exchange
Requires periodic review of relevance, and alignment with applicable laws and regulations	

6.0 Data Exchange Recommendations

To exchange data effectively and reliably, it is crucial to:

- Align data sharing with specific goals and outcomes.
- Recognize how data sharing propels innovation, coordination, and improves service delivery.
- Collaborate to update data management practices and promote a culture of data sharing rather than data ownership.
- Implement data fabric architecture to change a siloed environment into a coordinated one.

7.0 Authorized and Unauthorized Use

Authorized Users are individuals who require access to receive, examine, analyze, and interpret confidential information within a department or agency. They have a legitimate need-to-know within specific agency data systems to perform essential job functions.

Authorized Use	Unauthorized Use
Releasing data to only authorized users responsible for transmitting all data requests and maintaining a log of all data requested and received	Using data for non-compliant purposes or projects
Keeping data separate from all other data files	Disclosing or sharing sensitive data with external parties
Limiting data use to only the activities described in a signed MoA or DSA	

8.0 Parties

Effective data exchange typically involves two parties, categorized as transmitting and receiving entities. Both parties have distinct responsibilities. The transmitting entity is responsible for collecting and maintaining the data, while the receiving entity requests access to this information. Please refer to MaineIT Data Exchange Policy for information on the duties of the transmitting and receiving departments or agencies.

9.0 Data Disposal

Upon completion of the project or the intended purpose for data sharing, all data shared with the Receiving Party including archival and backup copies, shall be destroyed in accordance with General Schedule 9.3

Data from the parent system or source does not need to be decommissioned or deleted. Instead, the receiving entity's access to that source, and any copies made, should be revoked. For these purposes, the custodian of records would be the owner of the original data and should follow its records retention schedules as applicable.

10.0 Education, Awareness and Training

To enhance responsible data exchange practices and reduce the likelihood of data security incidents, it is important that each department and agency ensure that personnel are directly involved in creating, overseeing, and implementing data exchanges participate in and complete all applicable SOM Security Awareness Training modules and orientation.

The training will be assigned by Data Officers and will encompass topics such as:

- Relevant data protection laws, such as FERPA and HIPAA
- Departmental data policies and procedures
- Acceptable data handling, storage, and transmission practices
- Reporting procedures for suspected data breaches
- Updates in department and agency data security policies and procedures.
- Emerging data threats and vulnerabilities.

- Lessons from recent data security incidents.

11.0 Related MaineIT Policies

In order to facilitate agency staff's understanding and adherence to the technical compliance standards set forth by MaineIT during the development, implementation, and review of Data Sharing Agreements, please consult the policies listed below.

Certification	Reporting	Access Reviews
Please see Security Awareness and Training Policy (AT-1) for detailed information.	Please see Cyber Incident Reporting Procedures (IR-6) for details. For vendors, please refer to MaineIT Confidentiality and Non-Disclosure Agreement (NDA) for detailed information.	Please refer to Access Control Policy (AC-1) and Access Control Procedures for Users (AC-2) for information on access reviews.

12.0 Enforcement

It is the responsibility of each party's data leaders to ensure that the guidelines for data sharing agreements are adhered to in accordance with their organization's policies, procedures, and regulatory environment.

13.0 Insurance Requirements

To mitigate risks associated with data exchange, SOM has Cyber Liability Insurance that covers various departments and agencies within the Executive Branch and for MaineIT services to Constitutional Offices. This insurance covers data recovery costs that the state incurs due to damages arising from data or security breaches. Additionally, it provides "Post Breach Remedial Services" after an incident involving unauthorized access or use of SOM's computer systems, data breaches, unauthorized access or disclosure of data, and other security incidents. It is the responsibility of external vendors to have their own Cyber Liability Insurance.

14.0 Termination Requirements

Data Sharing Agreements/MOA's become effective immediately upon signature by authorized representatives of the participating departments and agencies. They remain in effect until the stated purpose for data sharing is completed, applicable laws or regulations governing the shared data change, the guidelines are amended or renewed by the participating departments and agencies and determinations on ad-hoc versus standing data exchange termination differences are resolved.

Any party may withdraw from an active data sharing agreement/MOA by providing 30 days' written notice to the other participating parties, which can be either business or calendar days.

If there are concerns about misuse of data or intentional unauthorized disclosures, please consult with the Office of the Attorney General to determine if immediate termination is appropriate.

15.0 Policy References

Please refer to the MaineIT Data Exchange Policy for information on the following:

- Data transmission
- Storage and handling requirements
- Non-waiver of rights

Please refer to the Remote Housing Policy for information on the following:

- Landing requirements
- Offshore requirements

For information on data breach or security incident, please see Cyber Incident Reporting Procedures (IR-6).

For information on MaineIT's four levels of data classification, please refer to the Data Classification Policy.

Data Sharing Checklist

Parties and Effective Dates	Identify sending and receiving parties, and effective dates (duration) of the DSA
Purpose	Clearly identify the reason for data sharing
Access to Data	Outline the criteria and restrictions for accessing data, and identify authorized users
Data Exchange	Specify whether the data exchange is ad hoc or standing
Data Transmission Terms & Conditions	Detail the criteria for transmitting, storing, and maintaining data to ensure compliance with laws and regulations
Reliance	Describe the transmitting parties' reliance on the receiving party to adhere to the DSA terms
Data Breach or Security Incident	Detail the protocol for notifying involved parties of a data breach or security incident, with an emphasis on immediate communication
Data Disposal	Provide instructions for the receiving party on the acceptable disposal of data received via the DSA
Enforcement	Outline each party's responsibility to adhere to the data sharing guidelines within their organization's policies
Jurisdiction and General Provisions	Include specific terms, requirements, provisions, and information relevant to the parties and their respective regulatory environments.
Termination of Agreement	State that the agreement is effective upon signature and remains valid until its purpose is fulfilled, the end date is reached, or relevant laws change. Allow for early termination, requiring written notification 30 calendar days prior. If there are concerns about misuse of data or intentional disclosures, please consult with the Office of the Attorney General to determine if immediate termination is appropriate.
Authorized Representatives(s)	Identify the authorized signatories on behalf of agencies