Maine State Government
Department of Administrative & Financial Services
Office of Information Technology (OIT)

Vendor Identity System Integration Policy

1.0 Purpose

1.1 This policy establishes security requirements for connecting Vendor Identity Management systems (IdMs) with State of Maine identity systems, including but not limited to Active Directory (AD). Ensuring data confidentiality, integrity, and availability (CIA) while enabling authorized vendor access.

2.0 Definitions

2.1 *Active Directory (AD):* Microsoft's directory service used to manage resources on a network.

2.2 *Federation:* A trust relationship between identity providers that allows users to access resources across domains.

2.3 *Identity Governance and Administration (IGA):* A set of processes and technologies for managing digital identities, including the provisioning, de-provisioning, and governance of user accounts and access privileges.

2.4 *Identity Management System (IdM):* A system for managing user identities and access permissions within an organization or across organizations.

2.5 *Information Assets:* The full spectrum of all I.T. products, including business applications, system software, development tools, utilities, appliances, etc.

2.6 *Least Privilege:* The principle of granting users only the minimum necessary access to perform their job functions.

2.7 *Lightweight Directory Access Protocol (LDAP):* An open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. LDAP is often used for authentication and authorization purposes, but can also be used to manage and query directory information.

2.8 *OpenID Connect (OIDC):* An identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner.

2.9 *Privileged Access:* Elevated permissions that grant access to sensitive systems or data, including, but not limited to, Domain Administrators, Schema Administrators, and Enterprise Administrators within AD or equivalent roles in other State identity systems.

2.10 *Privileged Access Management (PAM):* A cybersecurity strategy for managing and controlling privileged access and permissions for users, accounts, processes, and systems across an IT environment.

2.11 *Security Assertion Markup Language (SAML):* An open standard for exchanging authentication and authorization data between parties, often used in federation.

2.12 *State Identity Systems:* Encompasses all systems used to manage and authenticate user identities within the State of Maine's IT environment, including AD and any other identity and access management (IAM) platforms or services used by the State.

2.13 *Security Information and Event Management (SIEM):* A system that collects and analyzes security logs from various sources to detect and respond to potential threats.

2.14 *Secure Sockets Layer (SSL)/Transport Layer Security (TLS): Break and Inspect Procedures:* The process of decrypting and analyzing encrypted web traffic to identify potential threats or policy violations.

2.15 *Zero Trust Architecture:* A security model that requires all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

3.0 Policy Conflict

3.1 In the event of a conflict between this policy and any applicable law or union contract, the terms of the law or contract shall prevail. If this policy conflicts with any established security procedure, the more stringent or secure provision shall prevail.

4.0 Scope

4.1 This policy covers all connections between vendor IdMs and State identity systems, regardless of the technology used (e.g., SAML, LDAP, OIDC).

5.0 Applicability

5.1 This policy applies to the following entities who manage or interact with vendor IdMs and State identity systems as defined in the scope:

5.1.1 All Personnel, both employees and contractors/vendors, within the Maine State Executive Branch;

5.1.2 All Personnel who manage or interact with vendor IdMs and State identity systems;

5.1.3 Any other authorized vendors or entities whose IdMs integrate with the State’s identity systems.

6.0 Responsibilities

6.1 Agency Management:

6.1.1 Manage vendor relationships and contracts within their agency complying with all provisions of this policy and any other applicable State of Maine policies.

6.1.2 Ensure that vendors comply with this policy and all other relevant State of Maine IT security policies.

6.1.3 Report any security incidents or suspected breaches involving vendor access to OIT immediately.

6.1.4 Collaborate with OIT to define and implement appropriate access controls for vendors.

6.1.5 Ensure individual employees and contractors within the agency who interact with vendor IdMs or State identity systems are aware of and adhere to this policy.

6.2 OIT Chief Information Officer (CIO):

6.2.1 Owns and interprets this Policy.

6.2.2 Approves or designates an approver for all vendor integrations with the State of Maine's identity systems.

6.3 OIT Chief Information Security Officer (CISO):

6.3.1 Shall be responsible for the implementation, enforcement, and ongoing maintenance of this policy.

6.3.2 Facilitates monitoring of vendor access to State identity systems for compliance with this policy.

6.3.3 Shall direct the Security Architecture and Integrations Team who:

6.3.3.1 Conducts or oversees security assessments of vendor IdMs and proposed integrations;

6.3.3.2 Shall facilitate the review of proposed integrations to ensure compliance with State of Maine information security policies. And;

6.3.3.3 Shall coordinate validation that those integrations adhere to security best practices as defined by established frameworks, industry best practices and all provisions of this policy.

6.3.4 Shall direct the Security Operations Center (SOC) Team who:

6.3.4.1 Investigates and responds to security incidents involving vendor access.

6.3.4.2 Shall coordinate the review of the implementation architecture to determine its impact on security operations.

6.3.4.3 Shall facilitate collaboration to ensure vendor IdMs are integrated with the State's SOC SIEM and other security tools to facilitate activity monitoring and security alerting.

6.4 State of Maine Enterprise Architecture and Policy Team:

6.4.1 Define and enforce the data classification standards referenced in this policy and Data Classification Policy.[1]

6.4.2 Establish and maintain the data retention and disposal policies referenced in this policy and Media Protection Policy and Procedures (MP-1)[2] (Internal-only).

6.4.3 Assess the implementation architecture to verify adherence to State of Maine policies, architecture principles, and standards as outlined in this policy.

6.5 Vendors

6.5.1 Comply with all security standards and policies outlined in this document and any other relevant State of Maine IT security policies.

6.5.2 Undergo a security assessment of their IdM system or proposed integration as required by OIT.

6.5.3 Report immediately any data breaches or suspected data breaches involving State of Maine data to OIT as outlined in Cyber Incident Response Policy and Procedures (IR-1)[3] (Internal-only).

6.5.4 Cooperate fully with OIT in any incident response and investigation.

7.0 Directives

7.1 All integrations between vendor IdMs and the State of Maine's identity systems must receive formal approval from OIT's CIO or a designated security authority before implementation. The State of Maine will ensure these integrations adhere to the security standards and policies outlined in this document and any other relevant State of Maine IT security policies, as well as recognized security standards such as NIST SP 800-53[4] or ISO 27001.[5]

7.2 Prior to approval by the CIO, vendors must undergo a security risk assessment of their IdM system or proposed integration. The assessment will be conducted by the State of Maine or an approved third-party security assessment firm and will determine the vendor's risk tier, which will inform the level of security controls required for the integration.

7.3 State of Maine Audit Rights: The State of Maine reserves the right to audit vendor IdM systems both virtually and on-site at any given time while the contract or agreement is in effect.

7.4 Intrusion Detection/Prevention System (IDS/IPS): Vendors agree to the use of an IDS/IPS by the State of Maine, which may include SSL/TLS break and inspect procedures.

[1] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf

[2] https://stateofmaine.sharepoint.com/:b:/r/sites/MaineIT/Shared%20Documents/Policies/MediaProtectionPolicy.pdf

[3] https://stateofmaine.sharepoint.com/:b:/r/sites/MaineIT/Shared%20Documents/Policies/IncidentResponsePolicy.pdf

[4] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[5] https://www.iso.org/standard/27001

7.5 Termination Right: The State of Maine reserves the right to terminate any connections, at any time for any reason.

7.6 **Authentication and Authorization:**

7.6.1 Federated Identity: To ensure the highest level of security for the State of Maine's identity systems, federated identity solutions (e.g., SAML 2.0 or OIDC) shall be the mandatory method for vendor access. Vendors currently utilizing alternative methods must transition to a federated identity solution during their contract renewal process. Vendors currently using Active Directory shall immediately adopt the mandatory security requirements outlined in Appendix A, serving as an interim measure until full transition to federated identity is achieved. Failure to comply with these requirements may result in contract non-renewal. In exceptional cases where a federated identity solution is demonstrably not feasible, vendors may request an exception, accompanied by a detailed justification and comprehensive risk assessment, for review and approval by the CIO or designated security authority.

7.6.2 Multi-Factor Authentication (MFA): Vendors are required to implement MFA for all vendor access to the State of Maine's environment. MFA must be based on one of the following:

7.6.2.1 FIDO2-compliant hardware token

7.6.2.2 Time-based One-Time Password (TOTP) algorithm

7.6.2.3 Hardware security key

7.6.3 In alignment with the State's ongoing transition towards a Zero Trust security model, Vendors are expected to ensure that their solutions support and adhere to the State's Zero Trust principles and implementation as the State adopts them.

7.6.4 Least Privilege and Granular Access Control: Vendor access shall strictly adhere to the principle of least privilege, granting only the minimum access necessary to fulfill the specific duties and responsibilities outlined in the vendor's contract or agreement.

7.6.5 The State of Maine will implement a more granular approach to access control, using role-based access control (RBAC) and/or attribute-based access control (ABAC) to grant permissions based on specific roles or attributes. This will ensure that vendors have access only to the resources they need to perform their job functions.

7.7 **Operational Security Controls:**

7.7.1 Secure Transmission: Vendors must ensure that all communication between their IdMs and the State of Maine's identity systems is encrypted in transit using strong cryptographic protocols (e.g., TLS 1.2 or higher).

7.7.2 Termination: Upon termination or expiration of a vendor contract, or if a vendor relationship is otherwise discontinued, the State of Maine will immediately and completely revoke all vendor access to the State's identity systems. This includes disabling accounts, revoking credentials, and removing any associated permissions.

7.7.3 Logging: Vendors must log all authentications and access attempts, including successful and failed attempts, with relevant details such as user ID, timestamp, logging action or event code, and source IP address. These logs must be retained for a minimum of one year (or as otherwise specified in the State's log retention policy) and be made available to OIT upon request. Logs must be in a format that is compatible with Risk Assessment Policy and Procedures (RA-1)[6].

7.7.4 The State of Maine will implement a PAM solution to control and monitor privileged access to both vendor and State systems. This will help mitigate the risk of insider threats and unauthorized access.

7.7.5 Vendors will implement a SIEM solution and allow transmission to the State of Maine's SIEM system. This would enable centralized monitoring and analysis of security events for proactive threat detection and incident response.

7.7.6 Endpoint Security: Vendors are required to implement robust endpoint security measures on devices accessing State identity systems. This includes, but is not limited to, antivirus/anti-malware software, firewalls, and intrusion detection systems.

7.8 **Incident Response and Data Breach Notification:**

7.8.1 In the event of a data breach or suspected data breach resulting from or potentially involving State of Maine data accessed through the vendor's IdM system or integration with State identity systems, the following notification procedures will be followed, in accordance with the Maine "Notice of Risk to Personal Data Act"[7] and other relevant state and federal laws:

7.8.2 **Vendor Reporting Requirements:**

7.8.2.1 Vendors are required to report any data breach or suspected data breach involving State of Maine data accessed through the vendor's IdM system or AD integration to OIT via the designated communication channel (e.g., secure email, hotline) within 24 hours of discovery.

7.8.2.2 The report must include a detailed description of the incident, the data involved, the estimated number of individuals affected, and the actions taken to mitigate the breach.

7.8.2.3 Vendors must cooperate fully with the State of Maine's incident response procedures, promptly providing any additional information or assistance requested by OIT.

7.8.3 **OIT Responsibilities:**

7.8.3.1 Upon receiving a data breach report, OIT will immediately notify the CIO, CISO, relevant agency heads, and legal counsel.

7.8.3.2 Incident response protocols, as outlined in Cyber Incident Response Policy and Procedures (IR-1)[8] (Internal-only) will be initiated.

7.8.3.3 OIT will lead the investigation and remediation efforts, coordinating with the vendor as needed.

7.8.3.4 OIT will manage all external notifications and public communications regarding the data breach, following applicable state and federal laws.

[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/RiskAssessmentPolicyProcedure.pdf

[7] https://legislature.maine.gov/legis/statutes/10/title10ch210-B.pdf

[8] https://stateofmaine.sharepoint.com/:b:/r/sites/MaineIT/Shared%20Documents/Policies/IncidentResponsePolicy.pdf

7.8.3.5 Vendors are prohibited from making any public statements or disclosing information about the breach without prior written authorization from the State.

7.9 **Vendor Monitoring and Compliance:**

7.9.1 **OIT Responsibilities:**

7.9.1.1 Activity Monitoring: OIT may implement continuous monitoring of vendor activities within the State's identity systems to detect anomalies, unauthorized access attempts, or suspicious behavior. This may include automated tools and real-time alerts to ensure prompt response to potential security incidents.

7.9.1.2 Log Collection and Review: OIT will collect and analyze vendor-generated logs related to access and changes within the State's identity systems for auditing and compliance purposes.

7.9.1.3 Security Alerts: OIT will implement alerting mechanisms to notify appropriate personnel of potential security incidents or breaches.

7.9.1.4 Compliance Reviews: OIT will conduct regular reviews to assess vendor compliance with the security standards and policies outlined in this document. This includes verifying the continued necessity of access privileges, ensuring adherence to the principle of least privilege, and validating the effectiveness of security controls.

7.9.2 **Vendor Responsibilities:**

7.9.2.1 Incident Response: In the event of a security incident or breach involving a vendor IdM system or integration with State identity systems, the vendor is required to cooperate fully with the State of Maine's incident response procedures. This includes promptly reporting incidents, participating in investigations, and implementing corrective actions as directed by the State.

7.9.2.2 Remediation: Vendors are responsible for implementing any corrective actions identified by OIT to address security deficiencies or vulnerabilities in their IdM systems or integrations.

7.9.2.3 Reporting: Vendors must provide regular reports to OIT on their security posture, including vulnerability assessments, penetration testing results, and incident response activities.

7.9.2.4 Compliance: Vendors must maintain ongoing compliance with the security standards and policies outlined in this document and any other relevant State of Maine IT security policies. Failure to maintain compliance may result in the suspension or termination of access to State identity systems and potential legal action.

7.9.2.5 Vendor Third-Party Risk Management: Vendors are responsible for ensuring that their subcontractors or third-party service providers (if allowed by the agreement or contract with the State) who may access or process State data also adhere to the security standards and policies outlined in this document. Vendors must include appropriate security provisions in their contracts or agreements with these third parties and conduct due diligence to assess their security posture.

7.10 **Cybersecurity Insurance Requirement:**

7.10.1 To mitigate the financial risks associated with potential data breaches or cyber attacks, all vendors integrating their IdM systems with the State of Maine's identity systems must maintain comprehensive cybersecurity insurance coverage. This insurance should be adequate to cover the costs incurred in the event of a security incident, including but not limited to:

7.10.1.1 Forensic investigation and remediation

7.10.1.2 Legal fees and settlements

7.10.1.3 Notification to affected individuals

7.10.1.4 Credit monitoring and identity theft protection services

7.10.1.5 Business interruption and recovery expenses

7.10.2 The minimum required coverage limits will be specified in the vendor contract and may be subject to periodic review and adjustment based on the nature of the vendor's services and the potential risks involved. The State of Maine reserves the right to request proof of insurance from vendors at any time and to review the adequacy of coverage.

7.11 **Incident Response Retainer:**

7.11.1 To ensure a swift and effective response to potential security incidents, the State of Maine strongly recommends, but does not require, that all vendors maintain a retainer with a reputable provider of Incident Response (IR) services. This retainer should include:

7.11.1.1 24/7 Availability: Access to IR experts around the clock to address incidents promptly.

7.11.1.2 Forensic Investigation: Capabilities to conduct thorough investigations to determine the cause and extent of an incident.

7.11.1.3 Containment and Remediation: Expertise in isolating and neutralizing threats, as well as restoring affected systems and data.

7.11.1.4 Legal and Regulatory Guidance: Assistance with navigating legal and regulatory requirements related to data breaches and other security incidents.

7.11.2 Maintaining an IR retainer can significantly reduce the time and resources required to respond to an incident, minimizing potential damage and ensuring a faster recovery.

7.12 **Additional Security Requirements:**

7.12.1 **Annual Tabletop Exercises:** OIT will conduct regular tabletop exercises with vendors to simulate various security incident scenarios. These exercises will help evaluate the effectiveness of the incident response plan, identify areas for improvement, and ensure all parties understand their roles and responsibilities in responding to security events.

7.12.2 **Data Classification and Handling:** State data accessed by vendors shall be classified according to the Data Classification Policy.[9] Vendors must adhere to the handling and protection requirements associated with each data classification level.

7.12.3 **Training and Awareness for State Employees:** OIT will develop and implement regular training and awareness programs for all State employees who interact with vendor IdMs or State identity systems. These programs will cover the security risks associated with vendor access, best practices for secure interactions, and the importance of adhering to this policy. See Awareness and Training Policy and Procedures[10] for more information.

7.12.4 **Data Loss Prevention (DLP) Measures:** The State of Maine may implement DLP measures to monitor and control the movement of sensitive data within its identity systems and ensure compliance with applicable agreements, contracts, laws, and regulations.

7.12.5 **Specific Guidance for Cloud-Based IdMs:** Vendors using cloud-based IdM solutions must ensure that the cloud provider's security controls align with the State of Maine's security standards and policies. This includes considerations for data residency, encryption, access management, and incident response capabilities. Vendors must provide evidence of the cloud provider's compliance with relevant security standards and certifications (e.g., ISO 27001,[11] SOC 2).

8.0 Integration Request and Implementation Process

8.1 To establish a secure connection between a vendor IdM and the State of Maine's identity systems, the following process must be followed and all submissions must have a 90-day lead for review and approval. Failure to provide adequate documentation and lead time may result in an automatic disapproval of the request.

8.1.1 Entity Request for Connection:

8.1.1.1 Any Entity's Role: An entity (e.g., State of Maine agency, vendor, partner organization) identifies a legitimate need to connect their systems or services with the State of Maine's identity systems.

8.1.1.2 Formal Request Submission: The entity submits a formal request to OIT, outlining the purpose of the connection, the technical details of the integration, and a comprehensive justification for the request.

8.1.2 OIT Security and Risk Assessment:

8.1.2.1 OIT's Role: Upon receiving the request, OIT initiates a thorough security and risk assessment of the proposed connection. This includes:

8.1.2.1.1 Evaluating the entity's security posture and adherence to relevant security standards and policies.

8.1.2.1.2 Assessing the potential risks associated with the connection, considering the sensitivity of data involved, the level of access required, and the entity's role and responsibilities.

8.1.2.1.3 Conducting a security assessment of the entity's systems, if necessary.

[9] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf

[10] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/SecurityAwarenessTrainingPolicy.pdf

[11] https://www.iso.org/standard/27001

8.1.2.1.4 Determining the appropriate security controls for the connection, such as MFA requirements, encryption protocols, logging requirements, and monitoring mechanisms.

8.1.3 OIT-Entity Consultation and Approval:

8.1.3.1 OIT's Role: OIT consults with the requesting entity to discuss the findings of the security and risk assessment, explain the recommended security controls, and address any concerns or questions. The State of Maine will purely report on the issues; it is the entity's responsibility to secure their networks and systems.

8.1.3.2 Approval Process: Based on the assessment and consultation, OIT seeks approval from the appropriate authority within the State of Maine to proceed with the connection. This may involved the agency head, the CIO, CISO, and/or other designated officials, depending on the nature and scope of the connection.

8.1.4 Legal Review and Agreement Finalization:

8.1.4.1 OIT's Role: OIT collaborates with the State's legal team to review the proposed contract, agreement, or memorandum of understanding (MOU) with the entity. All security requirements, including those outlined in this policy and the additional controls determined in the risk assessment, are incorporated into the final agreement.

8.1.4.2 Agreement Security Provision: OIT ensures that the agreement includes all provisions as outlined in this policy.

8.1.5 OIT-Led Implementation and Configuration:

8.1.5.1 OIT's Role: OIT assumes full responsibility for the technical implementation and configuration of the connection between the entity's systems and the State's identity systems. This includes:

8.1.5.1.1 Configuring network and firewall settings to establish a secure connection.

8.1.5.1.2 Implementing the approved authentication mechanisms, ensuring compliance with security best practices.

8.1.5.1.3 Setting up access controls and permissions in accordance with this policy and other applicable State policies.

8.1.6 OIT Security Validation and Continuous Monitoring:

8.1.6.1 OIT's Role: OIT validates the implemented connection to confirm its adherence to the approved security controls. Ongoing monitoring of the entity's access and activities may be conducted through automated tools, log analysis, real-time alerts, and periodic audits to ensure continuous compliance with security requirements.

9.0 Compliance

9.1 Non-compliance with these procedures jeopardizes the security of State of Maine data and systems and may result in the immediate revocation of access and the termination of any relevant agreements or contracts. Additioinally, if a cyber attack on the State of Maine is traced to a violation of this policy, the responsible entity may be held liable for remediation costs and may face legal action.

10.0 Document Information

10.1 Initial Issue Date: October 18, 2024

10.2 Latest Revision Date: October 18, 2024

10.3 Point of Contact: Enterprise.Architect@Maine.gov

10.4 Approved by: Chief Information Officer, OIT

10.5 Legal Citation: Title 5, Chapter 163: Office of Information Technology[12]

10.6 Waiver Process: See the Waiver Policy[13]

10.7 Distribution: Internet[14]

[12] http://legislature.maine.gov/statutes/5/title5ch163sec0.html

[13] https://www.maine.gov/oit/policies/waiver.pdf

[14] https://www.maine.gov/oit/policies-standards