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

Site-to-Site VPN Interconnections Policy

1.0 Purpose

1.1 This policy outlines the guidelines and security requirements for establishing and maintaining Site-to-Site Virtual Private Network (VPN) connections to networks owned or operated by the State of Maine. This policy applies to all Site-to-Site VPN interconnections, irrespective of whether the connections are established on State-owned devices and networks or those managed by Partner Organizations.

2.0 Definitions

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

2.2 *Partner Organizations:* Refers to any entity, either internal or external to the State of Maine government, seeking to establish a Site-to-Site VPN connection to access State of Maine resources or conduct official business. This includes State of Maine agencies establishing connections between internal networks and external entities such as private businesses, non-profit organizations, educational institutions, and other government entities outside of the Government of the State of Maine. All Partner Organizations, regardless of their affiliation with the State, are subject to the security requirements and procedures outlined in this policy.

2.3 *Post-Quantum Cryptography (PQC) Safe VPN*: A VPN that uses encryption algorithms resistant to attacks from quantum computers, ensuring future security.

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

2.5 *Sensitive Data:* As defined in this policy, refers to any information protected under federal or state law whose unauthorized access, use, or disclosure could cause significant harm or legal consequences. Further information on data classification can be found in the Data Classification Policy[1].

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

2.6 *Site-to-Site VPN*: A secure, encrypted connection between two or more private networks over a public or private network.

2.7 *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.

2.8 *Virtual Private Network (VPN)*: A secure tunnel that encrypts internet traffic, allowing users to access a private network remotely.

3.0 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 Site-to-Site VPN connections established and utilized to access State of Maine resources or to conduct official business on networks owned or operated by the State of Maine. This includes connections established on both State-owned and third-party devices and networks.

5.0 Applicability

5.1 This Policy applies to:

- 5.1.1 All Personnel, both employees and contractors/vendors, within the Maine State Executive Branch;
- 5.1.2 All Information Assets in use within the Maine State Executive Branch; and
- 5.1.3 Information Assets from other branches of Maine State Government that are reliant upon the State Wide Area Network (WAN) for their operation.

6.0 Responsibilities

6.1 Agency Management:

- 6.1.1 Shall be accountable for ensuring that all agency systems and networks utilizing Site-to-Site VPNs adhere to this policy.
- 6.1.2 Shall limit Site-to-Site VPN usage to situations where it is essential for fulfilling official duties and no secure alternatives are available.
- 6.1.3 Shall immediately report any security incidents or breaches involving a Site-to-Site VPN connection between the State of Maine and a third-party to OIT, as outlined in Cyber Incident Response Policy and Procedures (IR-1)[2] (Internal-only).
- 6.1.4 Shall participate in annual tabletop exercises to test incident response plans specific to Site-to-Site VPN scenarios.
- 6.1.5 Shall collaborate with OIT in executing and enforcing this policy.

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

6.2 Chief Information Officer (CIO):
- 6.2.1 Owns and interprets this Policy.

6.3 Chief Information Security Officer (CISO):
- 6.3.1 Shall be responsible for the implementation, enforcement, and ongoing maintenance of this policy.
- 6.3.2 Shall provide guidance and support to Partner Organizations in meeting the policy's requirements.
- 6.3.3 Shall handle or facilitate all external notifications and communications in the event of a data breach in accordance with State policies and laws.
- 6.3.4 Shall advise on the implementation of security controls and develop and maintain incident response procedures specific to Site-to-Site VPNs.
- 6.3.5 Shall authorize and approve all Site-to-Site VPN connections, ensuring alignment with the outlined security standards.
- 6.3.6 Shall conduct or facilitate comprehensive security assessments of Partner Organizations and their infrastructure as described.
- 6.3.7 Shall participate in regular reviews of Site-to-Site VPN connections, at a minimum annually, to assess their continued need and compliance.
- 6.3.8 Shall direct the Security Architecture and Integrations Team who:
  - 6.3.8.1 Shall assess the implementation architecture to verify adherence to State of Maine information security policies. And;
  - 6.3.8.2 Shall collaborate with Partner Organizations to confirm alignment with security best practices and frameworks, as per this policy.
- 6.3.9 Shall direct the Security Operations Center (SOC) Team who:
  - 6.3.9.1 Shall assess of the implementation architecture to determine its effect on security operations.
  - 6.3.9.2 Shall collaborate with Partner Organizations to ensure that Site-to-Site VPNs are integrated into the State's SOC SIEM system and other security tools to enable continuous monitoring and incident response capabilities.

6.4 Partner Organizations seeking to establish Site-to-Site VPN:
- 6.4.1 Shall demonstrate continuous compliance with all security requirements outlined in this policy and any additional terms and conditions agreed upon with the State.
- 6.4.2 Shall promptly notify the State of any security incidents or breaches affecting their Site-to-Site VPN service.
- 6.4.3 Shall cooperate with the State in investigations and incident response efforts related to Site-to-Site VPNs.
- 6.4.4 Shall securely return or destroy all State data transmitted or stored via Site-to-Site VPNs upon termination of the agreement, in accordance with State policies.
- 6.4.5 Shall participate in regular security reviews and audits conducted by the State.

6.5 State of Maine Enterprise Architecture and Policy Team:

6.5.1 Shall define and confirm the data classification standards referenced in this policy and Data Classification Policy.[3]

6.5.2 Shall establish and maintain the data retention and disposal policies referenced in this policy and Media Protection Policy and Procedures (MP-1)[4] (Internal-only).

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

6.6 State of Maine Networking:

6.6.1 Shall be responsible for the configuration, implementation, maintenance, and monitoring of the State's side of the Site-to-Site VPN infrastructure.

6.6.2 Shall implement and manage tools and processes to monitor the performance of all VPN connections (if applicable).

6.6.3 Shall implement appropriate network segmentation and access controls to isolate Site-to-Site VPN traffic.

6.6.4 Shall cooperate with Partner Organizations to troubleshoot and resolve any technical issues.

6.6.5 Shall maintain up-to-date documentation of the Site-to-Site VPN configurations and any changes made. Any and all changes must be made and documented as described in the Change Management Policy.[5]

6.6.6 Shall have the authority to disable or block Site-to-Site VPN connections at any time, without notice, upon discovery of any security or performance issues, as per this policy.

7.0 Directives

7.1 All Site-to-Site VPN connections ("VPN" or "VPN connections") established to access State of Maine ("the State") resources or conduct official business must be explicitly authorized and approved by the CIO or a designated security authority. These connections must adhere to the OIT security standards outlined in this document and any other relevant security policies.

7.2 VPN usage shall be limited to situations where it is essential for fulfilling official duties and no secure alternatives provided by OIT are available.

7.3 All Site-to-Site VPN connections shall utilize certificate-based authentication (Public Key Infrastructure (PKI)). Certificates will be issued and controlled by either the State of Maine, through its designated Certificate Authority (CA), or a mutually agreed upon third-party CA, under the strict oversight and approval of the State of Maine, which reserves the right to make final decisions on all matters pertaining to PKI.

---

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

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

[5] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf

7.4 **Key Exchange Requirements**

7.4.1 To establish secure cryptographic communications, the initial exchange of asymmetric keys must adhere to the following requirements:

7.4.1.1 Approved Methods:

7.4.1.1.1 Manual Out-of-Band Delivery: Physical exchange of key material via trusted couriers or secure storage devices (e.g., hardware security modules).

7.4.1.1.2 Dedicated Secure Channels within a VPN: Utilizing a mutually authenticated and encrypted VPN tunnel.

7.4.1.1.3 Secure Digital Transfer: Employing a FIPS 140-3[6] validated cryptographic module to digitally sign and encrypt the key material prior to transmission over an authenticated and encrypted channel (e.g., Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol Secure (FTPS), Secure File Transfer Protocol (SFTP)).

7.4.1.2 Prohibited Methods:

7.4.1.2.1 Unencrypted or insecure communication channels (e.g., email, chat apps without verified End-to-End Encryption) must not be used for key exchange due to their susceptibility to compromise.

7.4.2 Failure to comply with these requirements may result in the exposure of cryptographic keys, leading to the compromise of sensitive information and potential security breaches.

7.5 The lifecycle of a VPN connection shall be managed in three distinct stages: pre-connection, connection, and post-connection, each with specific requirements and responsibilities that must be adhered to:

7.5.1 Pre-Connection Stage

7.5.1.1 All entities seeking to establish a Site-to-Site VPN connection to State of Maine resources must fulfill the following requirements:

7.5.1.1.1 Security Assessment: Undergo a comprehensive security assessment conducted by the State CISO, a designated authority, or a mutually agreed upon third-party security assessment firm.

7.5.1.1.2 Compliance and Best Practices: Demonstrate compliance with National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5[7] security controls relevant to VPNs and maintain appropriate certifications (e.g., ISO 27001[8]) while adhering to industry best practices.

7.5.1.1.3 Incident Response Plan: Have a formally documented incident response plan outlining procedures to effectively address and

[6] https://csrc.nist.gov/pubs/fips/140-3/final

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

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

mitigate security incidents and breaches. In the event of any such incident, the entity shall promptly notify the State of Maine within 24 hours, followed by written confirmation detailing the nature and scope of the incident, actions taken to mitigate the issue, and measures implemented to prevent recurrence.

7.5.1.1.4 Technical Documentation: Provide detailed technical documentation outlining their VPN solution, including architecture, encryption protocols, authentication mechanisms, and logging capabilities.

7.5.1.1.5 Logging and Auditing: Agree to enable robust logging and auditing mechanisms and be prepared to send logs to the State of Maine upon request.

7.5.1.1.6 Patch Management: Commit to adhering to a strict patch management policy for their VPN application or appliance. Remediation timelines for vulnerabilities are as follows:

7.5.1.1.6.1 Critical: Within 48 hours

7.5.1.1.6.2 High: Within 96 hours

7.5.1.1.6.3 Medium: Within 7 calendar days

7.5.1.1.6.4 Low: Within 30 calendar days

7.5.1.1.7 Contractual Agreement: Agree to the State's contractual terms and conditions regarding data handling, security, and liability. These terms can be found at the "IT Service Contract (IT-SC)" link at this page Office of (Maine) State Procurement Services. (Applicable only to non State of Maine entities.)

7.5.1.1.8 State Audit Rights: Agree to the State's right to audit both virtually and on-site at any given time while the contract or agreement is in effect.

7.5.1.1.9 Encryption Protocols: Utilize strong encryption protocols, as advised by the State's Security Architecture and Integrations Team, such as AES-256 for symmetric encryption and CRYSTALS-Kyber for post-quantum cryptography (PQC) readiness in key establishment and agreement. Additionally, maintain a proactive plan to transition to a PQC-safe VPN solution when available.

7.5.1.1.10 VPN Protocols: Utilize modern VPN protocols, as advised by the State's Security Architecture and Integrations Team (e.g., OpenVPN, WireGuard, or IKEv2/IPSec).

7.5.1.1.11 Zero Trust Principles: Agree to allow and transition to Zero Trust Principles as they are implemented by the State (e.g., continuous verification, and least privilege access).

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

7.5.2 Connection Stage:

7.5.2.1 The following technical requirements must be met during the operation of the VPN connection:

7.5.2.1.1 Strong Encryption: Utilize strong encryption protocols (e.g., AES-256/CRYSTALS-Kyber) at all times.

7.5.2.1.2 Logging and Auditing: Enable robust logging and auditing mechanisms to track all VPN activity, supplementing and complying with Risk Assessment Policy and Procedures (RA-1).[9]

7.5.2.1.3 Network Segmentation: Isolate VPN traffic from sensitive systems using network segmentation. Ensure both connecting parties adhere to the principle of least access.

7.5.2.1.4 Vulnerability Scanning and Penetration Testing: Allow regular vulnerability scanning and penetration testing on the VPN infrastructure without prior notice by the State.

7.5.2.1.5 Security Awareness Training:

7.5.2.1.5.1 Partner Organizations shall provide regular security awareness training (semi-annual minimum) to all personnel involved in the management and operation of the Site-to-Site VPN connection. This training should focus on (but not limited to):

7.5.2.1.5.1.1 Shared Fate: Emphasize that a Site-to-Site VPN connection creates a shared security environment. A security breach or vulnerability on either side of the connection can potentially impact both the Partner Organization and the State of Maine's networks.

7.5.2.1.5.1.2 Risks Associated with Site-to-Site VPNs: Educate personnel about the specific risks involved with Site-to-Site VPNs, such as unauthorized access, data interception, and misconfiguration. Highlight the importance of strong encryption, secure authentication methods, and network segmentation.

7.5.2.1.5.1.3 Best Practices for Secure Site-to-Site VPN Management: Provide guidance on best practices for managing Site-to-Site VPNs securely.

7.5.3 Post-Connection Stage

7.5.3.1 Upon termination of the agreement or cessation of need for access to State of Maine resources via a Site-to-Site VPN connection, the following procedures will be followed:

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

7.5.3.1.1 Access Revocation: All access to State resources will be immediately revoked.

7.5.3.1.2 Connection Termination: The VPN connection will be terminated and all associated routes removed from any and all routing tables.

7.5.3.1.3 Credential and Configuration Removal: All VPN-related credentials, PKI, and configurations will be securely deleted and removed from all systems and devices.

7.5.3.1.4 Final Audit: A final audit of VPN activity may be conducted at the State's discretion to ensure no unauthorized access or data exfiltration occurred.

7.6 **Monitoring and Management:**

7.6.1 The State reserves the right to implement the following monitoring and management practices:

7.6.1.1 Performance Monitoring: OIT will utilize appropriate tools and processes to monitor the performance of all VPN connections. This includes but is not limited to monitoring metrics such as latency, throughput, packet loss, and connection uptime. Performance thresholds will be established for each metric, and alerts will be generated when these thresholds are exceeded. Regular reports on VPN performance will be provided to relevant stakeholders, including OIT management, the CISO, and agency representatives.

7.6.1.2 Security Monitoring: OIT will monitor VPN connections for anomalies or suspicious activity. Traffic may be regularly inspected by an IDS/IPS system, including SSL/TLS break and inspection. The State may also implement a network-based Data Loss Prevention (DLP) solution to monitor traffic and ensure compliance with applicable agreements, contracts, laws, and regulations.

7.6.1.3 Incident Response: All parties must maintain and follow documented incident response procedures to promptly address and mitigate any security incidents or breaches related to VPN connections.

7.6.1.4 Regular Reviews: OIT will conduct regular reviews to assess the continued need for each VPN connection and ensure its ongoing compliance with security requirements.

7.6.1.5 Annual Review and Key Rotation: An annual review will be conducted for each connection to assess its policies, procedures, and necessity. Cryptographic keys and passwords will be rotated during this review.

7.6.1.6 Termination Right: The State reserves the right to terminate any VPN connection at any time for any reason.

7.7 **Data Retention and Destruction:**

7.7.1 Any State of Maine data transmitted, stored, or processed in connection with the VPN will be securely returned or destroyed in accordance with Media Protection Policy and Procedures (MP-1)[10] (Internal-only).

7.8 **VPN Split Tunneling:**

7.8.1 While split tunneling is often associated with end-user VPNs, it's important to recognize that site-to-site VPNs can also be impacted. Misconfigurations in split tunneling by either party can lead to unintended traffic exposure, potential disclosure of sensitive network information, or unauthorized access to resources. Therefore, the following policy regarding split tunneling shall be enforced:

7.8.1.1 Permitted Use of Split Tunneling:

7.8.1.1.1 Split tunneling may be permitted on a case-by-case basis, subject to explicit written authorization from the CIO or designated security authority. This authorization will only be granted under the following conditions:

7.8.1.1.1.1 Strong Justification: The requesting entity must demonstrate a compelling business need for selective routing that cannot be met through alternative means.

7.8.1.1.1.2 Risk Assessment: A thorough risk assessment must be conducted to identify and mitigate potential security risks associated with the specific use case.

7.8.1.1.1.3 Technical Controls: Appropriate technical controls, such as application-level traffic filtering and network segmentation, must be implemented to ensure that only authorized traffic bypasses the VPN.

7.8.1.1.1.4 Monitoring and Auditing: Robust logging and auditing mechanisms must be in place to monitor and track all traffic, both through the VPN and directly to the internet.

7.8.1.2 Prohibited Use of Split Tunneling:

7.8.1.2.1 Split tunneling is strictly prohibited for the following types of traffic:

7.8.1.2.1.1 TLP:Amber or TLP: Red data: Any traffic containing TLP:Amber (sensitive) or TLP: Red (restricted) data, as defined by the Data Classification Policy.[11]

7.8.1.2.1.2 Access to State Resources: All traffic accessing State of Maine resources, including applications, databases, and file shares.

7.8.1.2.1.3 High-Risk Activities: Activities deemed high-risk, such as financial transactions or access to critical infrastructure.

---

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

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

7.9 **Data Ownership and Residency:**

7.9.1 Ownership: All State of Maine data transmitted or stored via the VPN remains the property of the State and must be returned or securely destroyed upon contract or agreement termination per Media Protection Policy and Procedures (MP-1)[12] (Internal-only).

7.9.2 Residency: All data transmitted or stored in relation to this VPN connection and associated network must remain within the continental United States or Canada. No data shall be transmitted to or stored in any foreign country without explicit written authorization from the CIO or designated security authority.

7.10 **Data Breach Notification:**

7.10.1 In the event of a data breach or suspected data breach resulting from or potentially involving a State of Maine Site-to-Site VPN connection, the following notification procedures will be followed, in accordance with the Maine "Notice of Risk to Personal Data Act[13]" and other relevant state and federal laws:

7.10.1.1 Internal Notification:

7.10.1.1.1 The entity responsible for the VPN connection is required to report the data breach or suspected breach to OIT within 24 hours of discovery. OIT will promptly inform the CIO, CISO, relevant agency heads, legal counsel, and initiate incident response protocols as outlined in the State's data breach response plan or other previously agreed-upon documented procedures.

7.10.1.2 External Notification and Public Communication:

7.10.1.2.1 All external notifications and communications regarding the data breach will be handled exclusively by the State of Maine. Entities involved in the VPN connection are prohibited from making any public statements or disclosing information about the breach without prior written authorization from the State.

7.11 **Additional Security Requirements:**

7.11.1 Mobile Device Prohibition: Due to inherent security risks, the use of Site-to-Site VPNs on mobile devices (including but not limited to smartphones, tablets, and laptops) to access State of Maine resources is generally prohibited unless explicitly authorized by the CIO or a designated security authority.

7.11.2 Annual Tabletop Exercises: Designated personnel from entities utilizing State of Maine Site-to-Site VPN connections and relevant State of Maine personnel shall participate in annual tabletop exercises to simulate various security incident

---

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

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

scenarios, including data breaches, unauthorized access, and malware infections. These exercises aim to test and validate the effectiveness of incident response plans, identify areas for improvement, and ensure a coordinated response in the event of an actual incident.

7.12 **Cybersecurity Insurance Requirement:**

7.12.1 To mitigate the financial risks associated with potential data breaches or cyber attacks, all non-government Partner Organizations integrating their systems with the State of Maine's systems must maintain comprehensive cybersecurity insurance coverage. This requirement does not apply to State of Maine entities. This insurance should be adequate to cover the costs incurred in the event of a security incident, including but not limited to:

7.12.1.1 Forensic investigation and remediation

7.12.1.2 Legal fees and settlements

7.12.1.3 Notification to affected individuals

7.12.1.4 Credit monitoring and identity theft protection services

7.12.1.5 Business interruption and recovery expenses

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

7.13 **Incident Response Retainer:**

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

7.13.1.1 24/7 Availability: Access to IR experts around the clock to address incidents promptly.

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

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

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

7.13.2 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.

8.0 Consolidated Process to Establish a Site-to-Site VPN Connection:

Site-to-Site VPN Interconnections Policy

8.1 To establish a Site-to-Site VPN connection between a Partner Organization's network and the State of Maine's network, the following process must be followed. All submissions must include a 90-day lead time for review and approval. Failure to provide adequate documentation and adhere to the lead time may result in automatic disapproval of the request.

- 8.1.1 Vendor Proposal:
  - 8.1.1.1 The Partner Organization submits a formal request (including a proposed contract/agreement) to OIT, detailing the purpose of the VPN connection and why no other secure alternatives exist (aligned with Official Business), technical specifications, and evidence of compliance with the State of Maine's Site-to-Site VPN Interconnections Policy. The proposal must also include:
    - 8.1.1.1.1 Commitment to patch management and incident response.
    - 8.1.1.1.2 Agreement to enable logging/auditing and send logs to the State.
    - 8.1.1.1.3 Agreement to adopt Zero Trust Principles (when applicable or employed by the State)
    - 8.1.1.1.4 Agreement to State's use of IDS/IPS (potentially with SSL/TLS break and inspect).
    - 8.1.1.1.5 Justification, risk assessment, and technical controls for split tunneling (if applicable).
    - 8.1.1.1.6 Proof of cybersecurity insurance and IR retainer (if applicable).
- 8.1.2 OIT Security & Business Review:
  - 8.1.2.1 OIT Security reviews the technical aspects of the proposal and conducts a risk assessment. Simultaneously, the relevant business unit assesses the justification for the VPN connection. Both parties provide sign-off upon approval.
- 8.1.3 OIT Networking and Firewall Team Review:
  - 8.1.3.1 The Networking and Firewall team reviews the technical details of the proposed VPN connection to ensure compatibility and security within the State's network infrastructure and applicable policies and laws.
- 8.1.4 Legal Review and Contract Signing:
  - 8.1.4.1 The State's legal team reviews the proposed contract/agreement, ensuring it aligns with all policy requirements and legal considerations. Upon approval, the contract is signed by authorized State representatives.
  - 8.1.4.2 All security requirements, including those outlined in this policy and additional controls determined in the risk assessment, are incorporated into the final agreement.
- 8.1.5 OIT-Led Implementation and Configuration:
  - 8.1.5.1 OIT assumes full responsibility for the technical implementation on the State's side, including:
    - 8.1.5.1.1 Configuring network and firewall settings for a secure connection.
    - 8.1.5.1.2 Implementing approved authentication mechanisms.

8.1.5.1.3 Establishing access controls and permissions in accordance with this policy.

8.1.6 OIT Security Validation and Continuous Monitoring:

8.1.6.1 OIT Security validates the implemented connection to confirm adherence to approved security controls.

8.1.6.2 Ongoing monitoring of the Partner Organization's access and activities is conducted through automated tools, log analysis, and periodic audits to ensure continuous compliance.

8.1.7 Notification: Once the VPN connection is established and validated, the relevant Partner Organization and the Helpdesk are notified of the new connection, along with any specific instructions or access details.

8.2 Important Note: Any changes to the established VPN connection must follow the Change Management Policy[14].

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. Additionally, 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[15]

10.6 Waiver Process: Waiver Policy[16]

10.7 Distribution: Internet[17]

[14] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/ChangeManagementPolicy.pdf
[15] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[16] http://www.maine.gov/oit/policies/waiver.pdf
[17] https://www.maine.gov/oit/policies-standards