State of Vermont

Third Party Connectivity Policy

Date: 11-02-10
Approved by: Tom Pelham
Policy Number:

Contents

1.0 Introduction 3

1.1 Authority 3

1.2 Purpose 3

1.3 Scope 3

2.0 Policy 4

2.1 General 4

2.2. Supporting Provisions 4

3.0 Policy Notification 6

1.0 Introduction

1.1 Authority

The State of Vermont is authorized to undertake the development of enterprise architecture policies and standards. The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), “to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government.”

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that the policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by the agency must explicitly state the more stringent requirements. Agencies shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

1.2 Purpose

The State of Vermont engages third parties in the conduct of its business and to assist the State in providing goods and services to its citizens. In some instances third parties need to connect to the State network, GOVnet, in order to transact business and complete activities related to these contractual relationships. It is the responsibility of the State to protect its enterprise information and infrastructure by setting policy and procedures for the secure, auditable connections of non-State equipment and personnel.

1.3 Scope

This policy applies to all third parties and non-state employees who conduct business with the State and are required to connect to GOVnet in order to fulfill the duties of the contract or agreement with the State. Connections to the inside of the State network by or for third parties (i.e. non-State government entities) that directly connect to non-public Agency/Department resources fall under this policy, regardless of whether a Telco circuit, VLAN or VPN technology is used for the connection.

2.0 Policy

2.1 General

All new extranet connectivity will go through a security review with the Office of the CIO. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed. Third party connectivity solutions, together with equipment that connects through this solution and the personnel who use it must adhere to the IT policies set by the State of Vermont and other applicable policies of Agencies and Department with whom they partner.

The State will set connectivity standards. Use of various technologies and solutions may change over time. Third party network connections may be required to change connectivity solutions based on new standards established by the State. Generally, third parties are not allowed to connect directly to GOVnet at State locations with non-State equipment. Connections may be authorized for special VLANS that are established specifically for third party activity and those that provide internet-only access.

All new connection requests between third parties and Agencies/Departments require that the third party and State representatives agree to an agreement to be signed by the secretary/commissioner/designated authority of the sponsoring department as well as a representative from the third party who is legally empowered to sign on behalf of the third part. The signed document is to be kept on file with the relevant Department. Documents pertaining to the connections into GOVnet are to be kept on file with the Office of the CIO.

2.2. Supporting Provisions

These provisions support the policy and form the basis for third party agreements.

A. **Business Case.** All production extranet communications must be accompanied by a valid business justification, in writing, that is approved by the IT manager and designated authority in the Agency/Department requesting the connectivity. Connections must be approved by the Office of the CIO.

B. **Point of contact.** The sponsoring department must designate two persons to be the points of contact (POC) for the extranet connection; one state employee and one representative from the third party. Each POC acts on behalf of the sponsoring department, and is responsible for those portions of this policy and the signed agreement(s) that pertain to the extranet connection. In the event that either POC changes, the partner extranet organization must be informed within

fourteen (14) calendar days. The sponsoring department is also responsible for notifying the GOVnet management group.

C. **Establishing Connectivity.** Sponsoring departments within the State of Vermont that wish to establish connectivity to a third party are to file a new site request with the Office of the CIO to review the request and evaluate any security issues. If the proposed connection is to terminate within a local segment at the department, the sponsoring department must engage the personnel responsible for security within the department network. The sponsoring department must provide full and complete information as to the nature of the proposed access to the Office of the CIO as requested.

   All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will an agency/department solely rely upon the third party to protect the State of Vermont's network or resources.

D. **Modifying or Changing Connectivity and Access.** The sponsoring department is responsible for notifying the Office of the CIO when there is a material change in their originally provided information so that security and connectivity evolve accordingly. Such changes in access must be accompanied by a valid business justification, and are subject to security review.

E. **Audits.** Sponsoring departments will conduct annual audits to determine compliance with this policy, State and applicable Federal regulations as well as any contractual agreements, of all third party connections, and provide the results of those audits to the Office of the CIO. Additionally, the CIO may monitor the status of third party connections and review the network activity with the sponsoring department.

F. **Terminating Access.** When a third party no longer requires access, the sponsoring department within state government must notify the Office of the CIO. The Office of the CIO or the sponsoring department will then terminate the access. Unapproved connections and/or connections that are no longer being used to conduct state business will be terminated. The Office of the CIO will notify the POC or sponsoring department prior to taking action unless a security incident involves a risk to other agencies/departments. In that event, the connection will be terminated immediately until appropriate safeguards have been restored. If illegal or other prohibited activity is detected through audit or

normal network monitoring, access will be terminated immediately and appropriate actions taken.

3.0 Policy Notification

Each state agency is responsible for ensuring that employees are aware of where policies are located on websites. Agencies are also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.