

Security Addendum

1.0 Purpose

This document describes the policy under which outside organizations connect to Tennessee Bureau of Investigation networks for the purpose of transacting business related to the Tennessee Bureau of Investigation.

2.0 Scope

Connections between outside organizations that require access to non-public Tennessee Bureau of Investigation resources fall under this policy, regardless of whether a Telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection.

3.0 Policy

3.1 Pre-Requisites

3.1.1 Security Review

All new extranet connectivity will go through a security review with the Tennessee Bureau of Investigation information security department. 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. Access must be allowed to the site for on site security reviews within 24 hours of notice of intent from Tennessee Bureau of Investigation.

3.1.2 Site documentation

All site documentation related to the connection between the organization and Tennessee Bureau of Investigation must be maintained by the organization connecting to Tennessee Bureau of Investigation. All such documents must be submitted to Tennessee Bureau of Investigation upon initial connection and at anytime changes are made on site, regardless of how direct or indirect the change is. Example of such documents might include number of computers and the operating systems they are running, a list of routers and firewalls, and possible schematic drawings of all equipment showing interconnectivity.

3.1.3 Point Of Contact

The connecting organization must designate a person to be the Point Of Contact (POC). The POC acts on behalf of the connection organization, and is responsible for those portions of this policy that pertain to it. In the event that the POC changes, the Tennessee Bureau of Investigation must be informed within a timely manner.

3.2 Modifying or Changing Connectivity and Access

All changes in access must be accompanied with all relevant documentation, and are subject to security review. The connecting organization is responsible for notifying the Tennessee Bureau of Investigation when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

3.3 Terminating Access

When access is no longer required the connecting organization must notify Tennessee Bureau of Investigation. Should a security incident or a finding that a connection has been deprecated and is no longer being used to conduct official Tennessee Bureau of Investigation business necessitate a modification of existing permissions, or termination of connectivity, Tennessee Bureau of Investigation will notify the POC of the connecting organization of the change prior to taking any action.

THIS AFGREEMENT will become effective on _____.

IN WITNESS WHEREOF, the parties hereto caused this Agreement to be executed by the proper officers and officials.

TENNESSEE BUREAU OF INVESTIGATION:

Mark R. Gwyn, Director

Date

Agency Representative

Date