Remote User Connections to the State of Indiana Network

Standard ID
IOT-CS-SEC-124

Published Date
2/11/2013

Effective Date
2/11/2013

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
11.0 Protective Technology (PR.PT)

11.4 PR.PT-4

11.4.1 Network Protection

Purpose
Provides requirements for the mandatory use of 2-factor authentication to the State network by users from home and other “off-site” locations.

Scope
IOT Supported Entities

Statement
Users must self enroll in the two-factor authentication system. To do so, they must have:

- A unique phone number (e.g. - land line, state provided cell phone, personal cell phone)
- An email address (does not have to be a State of Indiana email address)

The two-factor authentication solution will be used for all remote connections via VPN and Citrix (the only type of remote connections authorized for State of Indiana network users). In the event a call cannot be completed to authenticate, a secondary means of connecting will be available.

Roles
All Personnel

Responsibilities
Agencies shall develop a process enabling two-factor authentication via phone. IOT shall establish contract for and oversee operation of the two-factor authentication scheme.

Management Commitment
Management is responsible for ensuring their agency is meeting the requirements written within this Standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT regarding issues with two-factor authentication mechanisms.
Compliance
Users that attempt to bypass State provisioned two-factor authentication without approval may be subject to termination.

Exceptions
Exceptions will be handled on a case by case basis through the State CISO.