Stark County Board of Developmental Disabilities

IT REMOTE ACCESS

POLICY

It is often necessary to provide access to Board information resources to employees or others working outside the Board's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

This policy is provided to define standards for accessing Board information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

The scope of this policy covers all employees, contractors, and external parties that access Board resources over a third-party network, whether such access is performed with Board-provided or non-Board-provided equipment.

Historical Resolution Information		Reviewer(s):
Date	**Resolution Number**	Information Technology Manager
10/26/10	10-104-10	
9/26/15	09-50-15	Superintendent
1/22/19	01-03-19	

IT REMOTE ACCESS

PROCEDURE

Prohibited Actions

Remote access to Board systems is only to be offered through a Board-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a Board system without the approval of the IT Manager.
- Remotely accessing Board systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the IT Manager.
- Use of non-Board-provided remote access software.
- Split Tunneling to connect to an insecure network in addition to the Board network, or in order to bypass security restrictions.

Use of Non-Board-Provided Machines

Accessing the Board network through home or public machines can present a security risk, as the Board cannot completely control the security of the system accessing the network. Use of non-Board-provided machines to access the Board network is permitted as long as this policy is adhered to, and as long as the machine meets the following criteria:

- It has up-to-date antivirus software installed.
- All software is accessed through the Board's Citrix environment.

When accessing the network remotely, users must not store confidential information on home or public machines.

Client Software

The Board will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access.

Network Access

There are no restrictions on what information or network segments users can access when working remotely, however the level of access should not exceed the access a user receives when working in the office. Two factor authentication should be used.

Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the Board's network must be timed out after 1 hour of inactivity.

Applicability of Other Policies

This document is part of the Board's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of Board property (physical or intellectual) are suspected, the Board may report such activities to the applicable authorities.

Definitions

Modem A hardware device that allows a computer to send and receive digital information over a telephone line.

Remote Access The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

Split Tunneling A method of accessing a local network and a public network, such as the Internet, using the same connection.

Timeout A technique that drops or closes a connection after a certain period of inactivity.

Two Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.