Stark County Board of Developmental Disabilities

Policy 6.09 Mobile Devices	Effective: 5/25/21
Chapter 6: Information Technology	Page 1 of 4

MOBILE DEVICES

POLICY

The Board recognizes that mobile devices have become a necessary tool for conducting business. With the introduction of mobile devices comes inherent data security risks that must be acknowledged and accounted for. Data on these devices must be secured in the event that the device is lost, stolen, or compromised.

This policy applies to Board data as it relates to mobile devices that are capable of storing data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with Board data.

This policy 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.

Historical Resolution Information		**Reviewer:**
Date	**Resolution Number**	Information Technology Manager
1/24/15	01-07-15	
3/27/18	03-18-18	
5/25/21	05-21-21	

MOBILE DEVICES

PROCEDURE

Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The Board should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

- Laptop locks and cables can be used to secure laptops when in the office or other fixed locations.
- Mobile devices should be kept out of sight when not in use.
- Care should be given when using or transporting mobile devices in busy areas.
- As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.
- The Board should evaluate the data that will be stored on mobile devices. The Board will use mobile device management software to remote wipe data on smart phones and tablets. Sensitive data should not be stored on laptops or other remote devices.
- The Board should continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting Board data. The following sections specify the Board's requirements for data security as it relates to mobile devices.

- **Laptops**
  Whole disk encryption is required. Laptops must require a username and password or biometrics for login.
- **Tablets/Smart Phones**
  Use of encryption is required on tablets/smart phones. Tablets/smart phones must require a password for login.
- **Mobile Storage Media**
  This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storage of Board data on such devices is prohibited unless the USB drive is obtained from the Information Technology department and is encrypted.

- **Portable Media Players**
  No Board data can be stored on personal media players.

- **Other Mobile Devices**
  Unless specifically addressed by this policy, storing Board data on other mobile devices or connecting such devices to Board systems is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the IT Manager.

Connecting to Unsecured Networks

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the Board.

General Guidelines

The following guidelines apply to the use of mobile devices:

- Loss, theft, or other security incident related to a Board-provided mobile device must be reported promptly.

- Confidential data should not be stored on mobile devices. Confidential data should only be accessed via Citrix.

- Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.

- Users are not to store Board data on non-Board-provided mobile equipment unless the device is enrolled with the Board Mobile Device Management software. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA.

Audits

The Board must conduct periodic reviews to ensure policy compliance. A sampling of mobile devices should be taken and audited against this policy on a periodic basis.

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

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Devices A portable device that can be used for certain applications and data storage. Examples are Tablets or Smartphones.

Mobile Device Management (MDM) Software Software designed to remotely manage and secure mobile devices such as Smartphones and Tablets.

Mobile Storage Media A data storage device that utilizes flash memory to store data; often called a USB drive, flash drive, or thumb drive.

Password A sequence of characters that is used to authenticate a user to a file, computer, or network; also known as a passphrase or passcode.

PDA Stands for Personal Digital Assistant. It is a portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Portable Media Player A mobile entertainment device used to play audio and video files. Examples are MP3 players and video players.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.