Stark County Board of Developmental Disabilities

Policy 6.04 Data Classification	Effective: 4/27/21
Chapter 6: Information Technology	Page 1 of 4

DATA CLASSIFICATION

POLICY

Information is an asset to the Board, just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to Board operations and the confidentiality of its contents. Once this has been determined, the Board can take steps to ensure that data is treated appropriately.

This data classification policy is necessary to provide a framework for securing data from risks including, but not limited to, unauthorized destruction, modification, disclosure, access, use, and removal. The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified.

The scope of this policy covers all Board data stored on Board-owned, Board-leased, and otherwise Board-provided systems and media, regardless of location. Also covered by the policy are hardcopies of Board data, such as printouts, faxes, notes, etc.

Historical Resolution Information

Date	Resolution Number
1/24/15	01-07-15
3/27/18	03-18-18
4/27/21	04-16-21

Reviewer(s):

Information Technology Manager

DATA CLASSIFICATION

PROCEDURE

Classification of Data

Data residing on Board systems must be continually evaluated and classified into the following categories:

1. *Personal* – includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.

2. *Public* – includes already-released marketing material, commonly known information, etc. There are no requirements for public information.

3. *Operational* – includes data for basic business operations, communications with vendors, employees, etc. (non-confidential).

4. *Critical* – any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.

5. *Confidential* – any information deemed proprietary to the agency. All medical information and other information protected by HIPAA. See the IT Confidentiality Policy for more detailed information about how to handle confidential data.

Storage of Data

The following guidelines apply to storage of the different types of Board data:

1. *Personal* – There are no requirements for personal information.

2. *Public* – There are no requirements for public information.

3. *Operational* – Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

4. *Critical* – Critical data should be stored on a server that gets the most frequent backups (refer to the IT Backup Policy for additional information). Some type of system- or disk-level redundancy is encouraged.

5. *Confidential* – Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

Transmission of Data

The following guidelines apply to transmission of the different types of Board data:

1. *Personal* – There are no requirements for personal information.

2. *Public* – There are no requirements for public information.

3. *Operational* – No specific requirements apply to transmission of Operational Data; however, as a general rule, the data should not be transmitted unless necessary for business purposes.

4. *Critical* – There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.

5. *Confidential* – Confidential data must not be: 1) transmitted outside the Board network without the use of strong encryption, or 2) left on voicemail systems, either inside or outside the Board's network.

Destruction of Data

The following guidelines apply to the destruction of the different types of Board data:

1. *Personal* – There are no requirements for personal information.

2. *Public* – There are no requirements for public information.

3. *Operational* – There are no requirements for the destruction of Operational Data, though shredding is encouraged.

4. *Critical* – There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.

5. *Confidential* – Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents – cross cut shredding is recommended**.**

- Storage media (CD's, DVD's) – physical destruction is required.

- Hard Drives/Systems/Mobile Storage Media – at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the Board must use the most secure commercially-available methods for data wiping. Alternatively, the Board has the option of physically destroying the storage media.

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

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Backup To copy data to a second location, solely for the purpose of safe keeping of that data.

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 Data Device A data storage device that is small and portable. Including but not exclusive to USB drives, flash drives, memory cards, or portable hard disk or solid state drives.

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.