Stark County Board of Developmental Disabilities

RETENTION

<u>POLICY</u>

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the Board's guidelines on retention are consistently applied throughout the organization.

The purpose of this policy is to specify the Board's guidelines for retaining different types of data.

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.

Note that the need to retain certain information can be mandated by local, state, or federal regulations. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

Historical Resolution Information	Reviewer(s):
Date　　　　　　　**Resolution Number** 10/26/10 3/28/15　　　　03-19-15	Director of IT

Stark County Board of Developmental Disabilities

RETENTION

PROCEDURE

I. **Reasons for Data Retention**
   The Board does not wish to simply adopt a "save everything" mentality.   That is
   not practical or cost-effective, and would place an excessive burden on the IT Staff to
   manage the constantly-growing amount of data.

   Some data, however, must be retained in order to protect the Board's interests,
   preserve evidence, and generally conform to good business practices.   Some
   reasons for data retention include:

   A. Litigation

   B. Accident investigation

   C. Security incident investigation

   D. Regulatory requirements

   E. Intellectual property preservation

II. **Data Duplication**
   As data storage increases in size and decreases in cost, Boards often err on the side
   of storing data in several places on the network.   A common example of this is
   where a single file may be stored on a local user's machine, on a central file server,
   and again on a backup system.   When identifying and classifying the Board's data,
   it is important to also understand where that data may be stored, particularly as
   duplicate copies, so that this policy may be applied to all duplicates of the
   information.

III. **Retention Requirements**
   This section sets guidelines for retaining the different types of Board data.

   A. **Personal** - There are no retention requirements for personal data.   In fact,
      the Board requires that it be deleted or destroyed when it is no longer
      needed.

   B. **Public** - Public data must be retained according to the timelines as set forth
      in the County's Schedule of Records Retention and Disposition.

   C. **Operational** - Most Board data will fall in this category.   Operational data
      must be retained according to the timelines as set forth in the county's
      Schedule of Records Retention and Disposition.

Stark County Board of Developmental Disabilities

     D. **Critical** - Critical data must be retained according to the timelines as set forth in the County's Schedule of Records Retention and Disposition.

     E. **Confidential** - Confidential data must be retained according to the timelines as set forth in the County's Schedule of Records Retention and Disposition and any state or federal requirements.

IV. **Retention of Encrypted Data**
If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

V. **Data Destruction**
Data destruction is a critical component of a data retention policy.   Data destruction ensures that the Board will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, the Board must actively destroy the data covered by this policy.   If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered.   Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the Board's executive team.

The Board specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or Board policy.

VI. **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.

VII. **Enforcement**
This policy will be enforced by the IT Director 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.

Stark County Board of Developmental Disabilities

Definitions

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 and secure without the key.   Used to protect data during transmission or while stored.

Encryption Key   An alphanumeric series of characters that enables data to be encrypted and decrypted.