# DuPage County

| | |
|---|---|
| Confidential Data Policy | Created: 10/15/2016 |
| Section of: County Security Policies | Modified: |
| Target Audience: All Staff | Page 1 of 2 |

## 1. Purpose

The purpose of this policy is to detail how Confidential Data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of Confidential Data, and outlines specific security controls to protect this data.

## 2. Scope

The scope of this policy covers all County data stored on County-owned, County-leased, and otherwise County-provided systems and media, regardless of location. Also covered by the policy are hardcopies of County data, such as printouts, faxes, notes, etc. This policy is not meant to replace or otherwise supersede the Identity Protection Policy, policy 9.5, located in the DuPage County Employee Policy Manual.

## 3. Policy

### 3.1 Restatement of Definition of Confidential Data (from Data Classification Policy – Section 4.1.3)

Confidential Data: Information that must be guarded due to legal, proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Confidential Data is information that is restricted to certain employees of DuPage County who have a legitimate purpose for accessing such data. Data Owners may designate data as Confidential. Disclosure to parties outside of DuPage County should be authorized by the County Board and/or the State's Attorney's Office. Some examples of Confidential Data are: Social Security numbers, credit card numbers, bank account numbers, and protected health information, as defined by HIPAA.

### 3.2 Treatment of Confidential Data

#### 3.2.1 Storage

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

#### 3.2.2 Transmission

Confidential data must not be transmitted outside the County network without the use of strong encryption or left on voicemail systems, either inside or outside of the County.

#### 3.2.3 Destruction

Confidential data must be destroyed in a manner that makes recovery of the information impossible, either by shredding, data wiping using the most secure commercially available data wiping technology, or by physically destroying the storage media.

## 4. Applicability of Other Policies

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

## 5. Enforcement

This policy will be enforced by the Department Head or Elected Official. 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 County property (physical or intellectual) are suspected, the County may report such activities to the applicable authorities.

## 6. Revision History

Revision 1.0, 10/15/2016