Procedure: Data Loss Prevention	**Last Update:** December 3, 2018

References (Statues/Resos/Policies):
Policy – Information Security 5.4.2, Credit Card Payments 4.8.1, Records Management 1.2.2, 45 CFR 160.103; C.R.S. § 6-1-713 – 713.5, 24-73-101 et seq

Purpose:
The purpose of the Data Loss Prevention procedure is to prevent the transmission of sensitive information without encryption to intended recipients external to the County.

A. Definitions

1. DLP: Data Loss Prevention

2. Sensitive Information: Information that is protected against unwarranted disclosure. Sensitive information includes but is not limited to:
   - Personally Identifiable Information (PII)
   - Protected Health Information (HIPAA)
   - Credit Card Holder Data (PCI)
   - Criminal Justice Information Services (CJIS)

3. Encryption: The process of encoding messages or information in such a way that only the intended or authorized recipient(s) can access the data.

B. Applicability: All Jefferson County employees and contractors using the email infrastructure provided by the County IT Services Division.

C. Procedure

1. All outgoing emails will be scanned for the following sensitive information types: PII, HIPAA, PCI, and CJIS.

2. If any of the information types are found, the email will be encrypted automatically prior to being sent to the intended recipient.

D. Track, Report and Audit

1. A record of all emails encrypted using the DLP policies will be kept and reviewed upon request. This data will be kept available for 6 months. Any data past 6 months will be purged from the system.