DuPage County

Backup Policy	Created: 06/25/2015
Section of: County Security Policies	Modified:
Target Audience: Technical	Page 1 of 4

DuPage County is hereinafter referred to as "the County."

1.0 Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

2.0 Scope

This policy applies to all data stored on County systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures. This policy does not apply to systems administered by County-wide Elected Officials.

3.0 Policy

3.1 Identification of Critical Data

The County has identified critical data based on an informal review of information. Data determined to be critical is given the highest priority during the backup process.

3.2 Data to be Backed Up

A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

- All data determined to be critical to County operation and/or employee job function.

- All information stored on the County file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.

- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

3.3 Backup Frequency

Backup frequency is critical to successful data recovery. The County has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

Differential: Monday through Thursday
Full: every Friday
Monthly backups: Last Friday of every month

3.4 Off-Site Rotation

Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the County's uptime requirements. The County has determined that backup media must be rotated off-site three times per week.

3.5 Backup Storage

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, County data, precautions must be taken that are commensurate to the type of data being stored. The County has set the following guidelines for backup storage.

When stored onsite, backup media must stored in a fireproof container in an access-controlled area. When shipped offsite, a hardened facility (i.e., commercial backup service) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media. If a backup service is used, rigorous security procedures must be developed and maintained, which will include, at minimum, credential-verification and signature of the backup service courier. Online backups are allowable if the service meets the criteria specified herein. Confidential data must be encrypted using industry-standard algorithms to protect the County against data loss.

3.6 Backup Retention

When determining the time required for backup retention, the County must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The County has determined that the following will meet all requirements (note that the backup retention policy must confirm to the County's data retention policy and any industry regulations, if applicable):

Differential Backups must be saved for a minimum of one month.
Full weekly Backups must be saved for a minimum of one month.

Full Monthly Backups must be saved on site for six months with a copy of monthly backups stored offsite for 12 months.

3.7 Restoration Procedures & Documentation

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.

3.8 Restoration Testing

Since a backup policy does no good if the restoration process fails it is important to periodically test the restore procedures to eliminate potential problems.

Backup restores must be tested when any change is made that may affect the backup system, as well as twice per year.

3.9 Expiration of Backup Media

Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

3.10 Applicability of Other Policies

This document is part of the County'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.

4.0 Definitions

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

Backup Media Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.

Full Backup A backup that makes a complete copy of the target data.

Incremental Backup A backup that only backs up files that have changed in a designated time period, typically since the last backup was run.

Restoration Also called "recovery." The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

5.0 Revision History

Revision 1.0