Town of Hudson Backup and Retention Policy

The goal of this document is to describe the Town of Hudson's backup environment, retention policy, backup schedule, and recovery testing policy.

Table of Contents

Town of Hudson Backup and Retention Policy

Backup Configurations

Backup System

The Town of Hudson's data, application databases, email server storage databases, and email messages are backed up daily. Using Backup software, the data is backed up to local network storage located in secure area. Once all data is backed up to the local network storage, the data is encrypted and replicated offsite. This provides a secondary location to be used in a disaster recovery scenario.

Backup Jobs and Retention

Incremental Backup

The Town of Hudson backup software performs incremental backups that allow for immediate restoration of files. Incremental backups are run three times daily.

Full Backup

Daily onsite backups for the Town of Hudson's servers are performed according to the applicable server's schedule. Encrypted copies of the backups are synchronized offsite for disaster recovery.

Email Backup

The Town of Hudson's email servers are backed up offsite on a daily basis. All Town of Hudson email messages sent and received are archived via backup software.

Retention

Data Daily Backup:	730 Days (Up to 2 Years)
Data Weekly Backup:	156 Weeks (Up to 3 Years)
Data Monthly Backup:	84 Months (Up to 7 Years)
Data Yearly Backup:	7 Years
Email Server Backup	Forever
Email Message Backup	Forever

Backup Schedule

Incremental Backup: 7 am, 12 pm, 5 pm daily
Full Backup: Daily between 6 pm and 3 am
Email Server Backup: Daily between 4 pm and 11 pm
Email Message Archiver: Continuous

Town of Hudson Backup and Retention Policy

Backup Procedures

Daily Tasks
Every morning, prior to 9am, the backup administrator reviews the status for the previous day's backup jobs (on Mondays, review the entire weekend's activity) to verify that all jobs completed successfully. Any errors or unsuccessful jobs must be investigated to determine the cause and action taken immediately to complete unsuccessful jobs. The IT Director is notified immediately of any unsuccessful backup jobs.

Recovery Testing
Once per quarter, the Primary and Secondary Backup Administrators conduct recovery tests to verify the recovery procedures and validate the proper functioning of the backup system. Performance of Recovery Tests is logged in the Recovery Test Log. Recovery Testing failures are reported to the IT Director.

The Recovery procedures in this document are used to conduct the recovery test, and the procedures are updated at this time, if needed.

Individual File Recovery Testing
Each quarterly test includes a recovery of individual files. For this test, the backup administrators select several files at random (files that have not been modified since the most recent backup) to restore from the most recent backup. The checksum of the restored files is compared to the original, inability to restore all of the files or any difference in the checksum is noted as a failure.

Full System Recovery Testing
At least once per year, the backup administrators conduct a full system (bare metal) recovery of a backup target. A new Virtual Machine is created, restored fully from the most recent backup of the target, and then tested for completeness of the restore and functionality of the system after restoration.

Testing After Backup System Changes
After any change, upgrade or update to any component of the backup system, including hardware, software or operating system of the backup server, a recovery test is performed. This test includes restoring from backups made prior to the change, as well as conducting a test backup and restore using the new configuration.