HALDIMAND COUNTY
POLICY No. 2009-05

Subject: **INFORMATION TECHNOLOGY BACKUP AND DATA RECOVERY POLICY**

Purpose:

The purpose of this policy is to establish the accountability, responsibility, and expectations for ensuring the integrity of computer-based data retained by the County's Information Systems Division by backing up data to ensure it is not lost and can be recovered in the event of equipment failure, unintentional loss or corruption, inadvertent deletion of files, intentional destruction of data, or disaster.

This policy defines the need for performing periodic computer system backups to ensure that mission critical administrative applications, databases, and users' data are adequately preserved and protected against data loss and destruction. This policy also establishes the accountability, responsibility, and expectations for ensuring the integrity of computer-based data retained by the County's Information Systems Division.

1. POLICY

1.1. *Overview:* This policy defines the backup and recovery policy for data residing on computers within the organization. These systems are typically servers and include file servers, print servers, mail servers, web servers, application servers, databases and directory services. These servers are typically Windows based and include local and remote sites. Desktop computers, laptop computers and handheld devices are not covered by this policy.

1.2. *Backup and Recovery Hardware Platform:* The backup and recovery platform contains a robotic device that performs tape backup and restore functions. Older external tape drive units also exist to be used to carry out restores from older tape formats. The robotic devices and type of tapes are changed as technology changes and capital replacements are made.

1.3. *Administration of Backups:* The Information Systems Division handles the administration of backups through backup application software. The primary application software keeps track of all backups, which includes the policies and backup dates and all other records needed for administration, for the full retention period of the backup. Scheduling is covered in the next section. Each backup is defined by a policy/template. The policy specifies the server, backup type, data type, files to be backed up, scheduling details, tape retention time, media server, media type and robot. All policies and records associated with the administration of backups are themselves fully backed up on tape everyday so that no information will be lost.

1.4. *Scheduling of Backups:* Backups are scheduled to allow users maximum access to data, while ensuring all data and databases are backed up. Because of this, full backups are normally restricted to Friday nights and weekends, while incremental backups run on the remaining weekday evenings. The full backup schedule extends from 7 pm on Friday through to 8 am on the following Monday. The incremental backup schedule starts at 7 pm through to 8 am the following day. A backup can start at any time during these time periods. Haldimand County uses reasonable efforts to backup all modified files daily. Monthly backups take the place of the weekly full backup on the last week of the month.

1.5. *Types of Data to be Backed Up:* Data to be backed up is determined by the policy/template. Systems to be backed up include but are not limited to:

- File Servers which contain application and user data volumes
- Mail Servers which contain user data in the form of e-mail, attachments, calendars, etc. as well as public folders
- Production Database Servers which contain Oracle and SQL databases
- Application Servers which contain applications such as Vailtech and StarGarden
- Backup Servers which contains records of all media written
- Voice Mail servers which contain saved messages and mailbox configurations
- Test and Development Servers which may contain any of the above data
- Web Servers containing the external (Internet) and internal (Intranet) websites

1.5.1. Types of Backups

Full Backups

For all servers, a full backup consists of all the data on the server and is usually performed once per week. The data usually includes operating system data, application data, database data, and user data.

Incremental backups

Incremental backups are used to backup only changes that take place on a daily basis and thus are performed more frequently than the full backups. These backups are usually related to user data.

Database backups (SQL, Oracle)

Database backups are frequently taken to ensure that the most recent data is always available. Hot backups are done while the database is online and being used. These backups take a snapshot of the database to disk and then back it up to tape. Full database exports are completed on a daily basis for Oracle databases which are then backed up to tape.

Shadow Copy

Shadow Copy is a feature available through the Windows operating system that automatically creates point-in-time copies on a scheduled basis of files that have changed. File servers containing user data files with this ability are set to create the point-in-time copies during the normal business work days at 1 ½ hour intervals starting at 10:00 am until 4:00 pm. Once the predetermined amount of space allocated to shadow copy is reached, shadow copy will overwrite the oldest copy. If a document has been accidentally deleted, it can be quickly and easily retrieved.

1.6. *Tape Retention:* The tape retention level specifies how long tapes are kept for recovery purposes. As each tape contains multiple types of data, the following retention periods apply to all types of data:

Daily – 6 weeks
Weekly – 6 weeks
Monthly – Infinity

1.7. *Tape Storage:* Tape media is sent off site to ensure data is safe and accessible in any situation. Monthly tapes are stored offsite for 30 days. These are then stored locally for approximately 6 months and then permanently stored in the records retention centre. Currently the offsite storage is at another County facility where the tapes can be accessed 24 hours a day, 7 days a week, 365 days a year and can be onsite within 60 minutes. Daily and weekly tapes are stored offsite at a County facility and can be onsite within 10 minutes.

1.8. *Tape Drive Cleaning:* The tape drive library cleans tapes automatically as required.

1.9. *Recovery of Data:* This policy also accommodates the recovery of data.

1.9.1. Authorization for User Initiated Restore

Users that need files recovered must submit a request to the HelpDesk Portal. The request must include the reason for the restore and the criticality.

1.9.2. Information Required Regarding Restore

The following information must be included:

(i) the path and name of the file
(ii) the destination of the file
(iii) whether the file can be overwritten
(iv) file creation date (if known) and the last time it was changed
(v) the date and time it was deleted or destroyed

After verifying the information above, it is up to the Information Systems staff to do the following:

(i) Confirm user is requesting his/her own file
(ii) Confirm user is restoring data to his/her own directory
(iii) Carefully confirm with user, if user is restoring many files and directories from an earlier date, that this is what he/she wants and tell him/her the impact of such a restore
(iv) Carefully confirm with user if there are any ambiguities

If there are any concerns regarding the restore, it must be escalated to the Manager of Information Systems before starting the restore.

1.9.3. Timing of Restores

Restores must be scheduled so they do not interfere with access to data or (whenever possible) with the backup window.

1.9.4. Testing

The ability to restore data from backups shall be tested when new backup hardware or software is implemented or changed. Testing will also be conducted on a semi-annual basis through the actual process of recovering data for staff or, if no requests have been made to recover data, restoring random data.

1.10. *Disaster Recovery*

In the event of hardware failure, the recovery method and time will depend on the server and its function. If a server hosting corporate database applications fails, the application server with the test environment can be loaded with the previous night's database export within approximately four hours. In the event of a hardware failure of other servers, a new server environment must be created, loaded and configured with the applicable operating system and applications, before restoring the data. With the County's evolution to virtualization, a new "virtual server" environment may be created eliminating the need to have "extra" or "backup" hardware.

The "IT Disaster Recovery and Business Continuity Policy" and the "IT Disaster Recovery and Business Continuity Plan" further addresses disaster recovery and business continuity.

2. DEFINITIONS

2.1 *Archive*: refers to the saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage space.

2.2 *Backup:* refers to the saving of files onto magnetic tape, disk, or other offline mass **storage media for the purpose of preventing loss of data in the event of equipment** failure or destruction.

- *Full Backup:* all files are backed up
- *Incremental Backup:* all files modified since the last backup of any type are backed up

2.3 *Restore:* refers to the process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

3. RESPONSIBILITIES

3.1. *Information Systems Division:* The I.S. Division is responsible to ensure regular backups are scheduled and completed. This group is responsible for the backup software administration and controls backup policies, scheduling, media servers and robots. Staff also monitor for successful completion of backups and for overall backup performance on a daily basis. Regarding tapes, the I.S. Division ensures that sufficient media levels are available in the libraries to support the backup workload and also performs offsite tape vaulting procedures. In addition, it is the responsibility of the I.S. Division to carry out requests for data recoveries and ensuring the successful completion of restores.

3.2. *Staff requesting restores:* Staff requesting files / data to be restored must submit the request through the HelpDesk Portal.

4. REFERENCES

4.1. *Haldimand County – IT Disaster and Business Continuity Policy*

4.2. *Haldimand County – IT Disaster and Business Continuity Plan*

Topical Index	Corporate Services
Policy Number	2009-05
Short Title	Information Technology Backup and Data Recovery Policy
SMT Approval Date	September 2, 2009
Council in Committee	October 26, 2009 Recommendation # 28
Council Approval Date	November 2, 2009 Resolution # 306-09
Originating Department	CS-IS-02-2009 and CS-IS-03-2009 (Supplementary)
Revisions	