City of Lawrence
Administrative Policy

SUBJECT	APPLIES TO
Server Backup Policy	Departments supported by Information Systems

EFFECTIVE DATE	REVISED DATE	
September 1, 2009		

APPROVED BY	TOTAL PAGES	POLICY NUMBER
City Manager	6	107

1.0 Purpose

This policy is intended to define and document the procedures used to protect the data, applications, and configurations on the servers used by the City of Lawrence, Kansas.

2.0 Scope

This policy covers the backups for servers supported by the Information Systems department and does not include the Police Department. This policy is a backup policy only and is not intended to define the primary data storage the City uses in its production network, but rather defines the secondary storage providing the final level of redundancy for the data, applications, and configurations of the City's servers. While this policy is integral to any disaster recovery efforts, it is not intended as a disaster recovery plan or a business continuity plan.

It is the responsibility of all users to store critical data on servers that are covered by this policy. Any data stored on local personal computers and notebooks is not backed up by the Information Systems Department and their protection relies solely on the user.

3.0 Roles

The employees primarily responsible for the operation of the backup policy will be the admin positions in the IS department; specifically, the Database Administrator and the Network/System Administrator. Some specific backup jobs may be assigned to technicians, and technicians may be assigned temporary responsibilities for the backups. The admin and technician positions are managed by the Network Manager who will receive performance measures from the monitoring and auditing of the backups and restores. This document will be maintained by the Network Manager position. The AS/400 is backed up by designated personnel under the supervision of the Director of Information

Systems. Some servers at remote sites may be assigned to onsite personnel in other departments, but Information Systems should monitor their backup logs to verify the correct procedures are being followed.

4.0 **Backup Types**

There are several backup types that will need performed and each server will be reviewed by the primary users, appropriate admin position, and network manager to determine which backup type or combination of types are appropriate for each server. These determinations will be recorded and maintained in a spreadsheet called *Serverlist.xls* and will be stored in the Information Systems departmental folder. The best practice is for backups to be made offsite, so every attempt should be made to backup servers in a secondary facility. The backup types are defined below:

4.1 Bare Machine Backup This type of backup ensures the ability to *restore a machines configuration, applications, and data all from one restore operation*. This includes backups performed using VMware's "Virtual Consolidated Backup. This type of backup can be performed at any frequency that is deemed appropriate. It is appropriate for Application Servers where install media and extensive configuration would be needed to replace a lost server.

4.2 Data Only Backup This method backups *all the stored data on file shares* on a server. The file attributes are typically backed up as well. The data usually consists of files stored by users and these files are often documents (word, excel, .pdf), small databases (MS access), or pictures (.jpg, .tif). Backups are recommended to be performed or archived off-site of the server(s) locations where connectivity allows.

4.3 Email Backup The City of Lawrence's email system is Microsoft Exchange Server and presents some unique backup challenges. The data for all email boxes is stored in a single common data store file and requires a backup agent to make backups of a moment in time. Although the data is backed up daily, there is no guarantee that a specific email may be restored at a future date. The City does not have email archiving capabilities that can ensure each email is retained, thus it is the responsibility of each user to retain any emails that are considered important or critical. Restores from a Microsoft Exchange Backup are labor intensive, as they require establishing a new email server target to restore the data to. Current email configurations do not accommodate the ability to restore individual email boxes or emails.

4.4 SQL Backup This backup method specifically *protects Microsoft SQL databases* from data loss. The Database Administrator creates these jobs and the backups go to offsite disk storage. The frequency of these jobs is determined as-needed by the Database Administrator. This type of backup

should be performed on all SQL databases.

4.5 Oracle Backup The City currently only has one Oracle database, which is the Full Court ® database by Justice Systems. Justice Systems has recommended a specific backup method for their database that includes doing a complete dump of the data and structure files into an ASCII file that can be easily restored if necessary.

4.6 Other Database Backups The City has a variety of other databases that include Microsoft Access ®, Progress, MySQL, IBM, and others. Information Systems will back these up using the "Data Backup Only" method unless a different backup method is recommended or controlled by the developers of the database application.

4.7 AS/400 Backup A daily backup job scheduled entry called DLYSAVLIB is activated in the System i (AS/400) to initiate a daily backup of all non-system data libraries beginning at 02:00 a.m. of each weekday. Currently the saved data will be directed to tape device TAP06. Specifically the DLYSAVLIB job scheduled entry executes the CL program DLYSAVLIB in library CITYGPL. This DLYSAVLIB backup program adheres to IBM-recommended backups of the following libraries:

SAVSECDTA	(saves user profiles)
SAVCFG	(saves configured devices)
SAVLIB *ALLUSR	(saves all user libraries)
SAVDLO	(saves document library objects)
SAVLIB *IBM	(saves IBM libraries)
SAV IFS	(saves IFS objects)

Since the DLYSAVLIB is a job scheduled entry, no operator intervention is required to initiate the daily backup procedure. However each morning, the system operator will be required to remove the tape from TAP06, write the current date on the tape, and place it in the tape rotation box. The system operator will then be required to take the oldest dated tape from the tape rotation box and place it in the TAP06 drive in preparation for the next day's backup.

On Monday morning of each week (or Tuesday following a holiday), the system operator will remove the tape from the TAP06 drive, write the backup date on the tape, and prepare it for Federal Express shipment to the City's disaster recovery provider, Synergistic Online Solutions. A Fed-Ex envelope containing the Monday backup tape should be addressed to:

Synergistic Online Solutions
Attn: Mike Bertrand
339 NW 12th Street
Blue Springs, MO 64015

Synergistic Online Solutions will then load the contents of the backup tape to the disaster recovery AS/400 located in Blue Springs, Missouri. Synergistic will then Fed-Ex this same tape back to arrive usually on Thursday of the same week, where the tape will be placed back into the tape rotation.

A quarterly "System Save" is processed four times per year. Although the daily backup procedure saves all of the changing data and programs on the system, there are still static programs that can only be backed up when the system is in a restricted state, i.e. all users are off the system and no activity is taking place. A SAVSYS backup should be done to backup these remaining static system programs on weekends when the system can be placed in a restricted state. A SAVSYS should be done at least quarterly or more frequently if cumulative PTFs or other major system changes are to be applied. Refer to the IBM system operations guide for steps to complete a SAVSYS procedure. The resulting SAVSYS tape should be stored in the fireproof safe in the Information Systems forms storage area. The schedules for these backups are maintained on the daily work task sheets used by those supporting the AS/400's daily activities.

5.0 **Backup Increments**

5.1 Daily Full Backup is a backup type that backs up *every file* specified in a selection list, and does it once *every day*. This backup is most often used for databases that cannot be backed up with an SQL backup. Restores can be made from one day, one week, one month, or the beginning of the year.

5.2 Weekly Full Backup is a backup type that backs up *every file* specified in a selection list, and does it once *every week*. This type is seldom used. Restores can be made from one week, one month, or the beginning of the year.

5.3 Daily Differential/Weekly Full backup is a backup type that backs up every file specified in a selection list, and does it once every week, then checks daily for files that have changed since the full backup, and backs up those files once every day. This type of backup is the backup method for all file servers. Restores can be made from 1-7 Days ago, one month ago, or the beginning of the year.

5.4 Annual Backups will be made once a year. The media will be removed, and they will be placed in storage until the next annual backups replace them. Annual archived media should be stored in a secure location preferably off-site. Not all servers will have annual backups available.

6.0 **Backup Hardware and Media**

6.1 Primary Backup The primary backup equipment used by the City utilizes an ADIC Scalar 100 tape autoloader unit. The backup unit has a capacity of 75

LTO-2 tapes and contains three LTO-2 backup drives. The backup unit is located at the Waste Water Treatment Plant which allows the majority of equipment being backed up to have the backups stored off-site from the actual servers being protected. The backup software manages the backs up and instructs the tape autoloader to change tapes as necessary. The unit's tape autoloaders rotates the tapes as necessary and the tapes are continually overwritten. Backup data stored on this unit is typically available for the prior three to four weeks of the current backup date.

6.2 Individual Tape Autoloaders The City also has four other smaller tape autoloader libraries dispersed at other locations. These units are Quantum 8 cartridge auto-loaders that use LTO3 tape cartridges. The units are located at Fire Station #5, Wastewater Treatment Plant, Kaw Water Treatment Plant and the Clinton Water Treatment Plant. The data on these units are continually overwritten as required for available backup space.

6.3 Stand-Alone Tape Drives A small number of City servers can not feasibly use the City's primary tape backup system, typically due to slow connectivity communication speeds. These units may have internal or external standalone tape drives using a variety of tape formats. The responsibility for tape rotations for these backups is sometimes assigned to on-site departmental personnel. These types of backups are to be monitored by the Network Administrator position.

6.4 Network Attached Storage (NAS) Backup Units Some databases and other specific data sets are routinely backed up to NAS units connected to the backup server located at the Wastewater Plant. The Database Administrator may more commonly use this method for databases.

6.5 Portable Hard-Drive Storage Units Occasionally backups may be made with portable drive units for a variety of reasons as needs arise.

7.0 **Backup Auditing and Monitoring**

Backup jobs will be monitored on a daily basis by the assigned admin position for success and failure. The statistics of success and failure rates will be reported to the Network Manager and recorded in the performance measures. The Admin positions will occasionally perform restore audits from the backup jobs to verify we are performing restorable backups. These restore audits may be assigned by the Network Manager or IS Director if deemed appropriate. The restore audits will be performed by restoring the backup job to an alternate machine and test functionality of that machine after the restore.

8.0 **Server Backup Listing**

A spreadsheet listing will be maintained to document each server, its related

backup rotation, and target storage unit. The file is to be stored in the documentation directory of the Information Systems documentation folder. The Network Manager is responsible for maintaining oversight of the backup listing, identifying the backup strategy for each server, the target media, and the assignment of personnel responsible for monitoring the backup processes.

9.0 **Obsolete Backups**

9.1 Obsolete Tape Media Before obsolete tapes are discarded they should be physically destroyed LTO-2 and LTO-3 tape cartridges are expected to be reliable for 12-18 months, at the end of their expected life-cycle they should be physically destroyed to prevent access to any data on them.

9.2 Obsolete Disk Storage Media When functional hard-disks are removed from service, they will be prepared for disposal by an automated process that writes “0s” across the entire disk, then sent to a trusted recycling facility. When non-functional hard-disks are disposed of they will be sent to a trusted recycling facility.