CITY OF RICHMOND

INFORMATION TECHNOLOGY BACKUP POLICY 2016

I. PURPOSE:

To establish a policy and procedures for backing up City information that is stored electronically in a computerized form to ensure its safety in the event of a severe hardware interruption, software interruption, virus attack or other disaster. This includes backing up information from disk storage or other media for offsite storage for all City servers maintained by the Information Technology Department including mid-range systems.

II. POLICY:

A. Proper disaster recovery planning includes backing up server information including mid-range systems. Every server supported by the Information Technology Department on the City’s network will be backed up to special disk backup media. The frequency of backups will depend on the significance of the information and its frequency of change. Daily and weekly backup media will be stored offsite from the main City Hall. Monthly and annual tape backup media will be stored offsite approximately ninety miles or more from the City of Richmond for disaster recovery purposes. See cloud based replication and cloud offsite storage. Procedures for recovery and restoration of the information will be documented and stored at the offsite storage location(s).

B. The results of every backup job are to be automatically logged each day and stored for one year.

III. BACKUP SCHEDULE:

<u>Standard network backup email files databases, etc.</u>

Frequency: Server to disk backup daily. Incremental backup every day and full backups on a weekly basis.

In house storage: backup replications /uploads continuously to the cloud (Barracuda) local servers.

Retention policy: emails and databases: keep 3 days to incremental files two weeks in house.

IV. REDUNDANCY:

Redundancy Cloud Replication (unlimited data)

Storage: saves to external cloud continuously (three cloud locations in North America – Campbell CA, Ann Arbor, MI and Atlanta, GA).

Restore (all data) from external cloud: seven years available for annual backups.

V. TESTING:

Testing backups

Restores performed on random files a minimum of once per quarter.

VI. DEFINITIONS:

Backup policy

An organization's procedures and rules for ensuring that adequate amounts and types of backups are made, including suitably frequent testing of the process for restoring the original production system from the backup copies.

Backup rotation scheme

A method for effectively backing up data where multiple media are systematically moved from storage to usage in the backup process and back to storage. There are several different schemes. Each takes a different approach to balance the need for a long retention period with frequently backing up changes. Some schemes are more complicated than others.\

Backup site

A place where business can continue after a data loss event. Such a site may have ready access to the backups or possibly even a continuously updated mirror.

Backup software

Computer software applications that are used for performing the backing up of data, i.e., the systematic generation of backup copies.

Backup window

The period of time that a system is available to perform a backup procedure. Backup procedures can have detrimental effects to system and network performance, sometimes requiring the primary use of the system to be suspended. These effects can be mitigated by arranging a backup window with the users or owners of the system(s).

Cloud backup

Is a strategy for backing up data that involves sending a copy of the data over a proprietary or public network to an off-site server.

Cloud replication

Is the process of copying production data to a device at a remote location for data protection or disaster recovery purposes.

Copy backup

Backs up the selected files, but does not mark the files as backed up (reset the archive bit). This is found in the backup with Windows 2003.

Cumulative incremental backup

A differential backup used by NetBackup.

Daily backup

Incremental backup of files that have changed today

Data salvaging/recovery

The process of recovering data from storage devices when the normal operational methods are impossible. This process is typically performed by specialists in controlled environments with special tools. For example, a crashed hard disk may still have data on it even though it doesn't work properly. A data salvage specialist might be able to recover much of the original data by opening it up in a clean room and tinkering with the internal parts.

Differential backup

A cumulative backup of all changes made since the last full backup. The advantage to this is the quicker recovery time, requiring only a full backup and the latest differential backup to restore the system. The disadvantage is that for each day elapsed since the last full backup; more data needs to be backed up, especially if a majority of the data has been changed.

Disaster recovery

The process of recovering after a business disaster and restoring or recreating data. One of the main purposes of creating backups is to facilitate a successful

Disaster recovery. For maximum effectiveness, this process should be planned in advance and audited.

Disk cloning

The process of copying the contents of one computer hard disk to another disk or to an *image file* (see *disk image* below) for later recovery.

Disk image

Single file or storage device containing the complete contents and structure representing a data storage medium or device, such as a hard drive, tape drive, floppy disk, CD/DVD/BD, or USB flash drive.

FlashBackup

A term used for *raw partition backup* used by NetBackup Advanced Client. In NBAC, support is limited to the VxFS (Veritas), ufs (Solaris), Online JFS (HP-UX), and NTFS (Windows) filesystem types. Similar to the UNIX utility *dump*.

Full backup

A backup of all (selected) files on the system. In contrast to a drive image, this does not included the file allocation tables, partition structure and boot sectors.

Hot backup

A backup of a database that is still running, and so changes may be made to the data while it is being backed up. Some database engines keep a record of all entries changed, including the complete new value. This can be used to resolve changes made during the backup.

Incremental backup

A backup that only contains the files that have changed since the most recent backup (either full or incremental). The advantage of this is quicker backup times, as only changed files need to be saved. The disadvantage is longer recovery times, as the latest full backup, and all incremental backups up to the date of data loss need to be restored.

Media spanning

Sometimes a backup job is larger than a single destination storage medium. In this case, the job must be broken up into fragments that can be distributed across multiple storage media.

Multiplexing

The practice of combining multiple backup data streams into a single stream that can be written to a single storage device. For example, backing up 4 PCs to a single tape drive at once.

Multistreaming

The practice of creating multiple backup data streams from a single system to multiple storage devices. For example, backing up a single database to 4 tape drives at once.

Normal backup

Full backup used by Windows Server 2003.

Near store

Provisionally backing up data to a local staging backup device, possibly for later archival backup to a remote store device.

Open file backup

The ability to back up a file while it is in use by another application.

Remote store

Backing up data to an offsite permanent backup facility, either directly from the live data source or else from an intermediate near store device.

Restore time

The amount of time required to bring a desired data set back from the backup media.

Retention time

The amount of time in which a given set of data will remain available for restore. Some backup products rely on daily copies of data and measure retention in terms of days. Others retain a number of copies of data changes regardless of the amount of time.

Site-to-site backup

Backup, over the internet, to an offsite location under the user's control. Similar to remote backup except that the owner of the data maintains control of the storage location.

Synthetic backup

A term used by NetBackup for a restorable backup image that is synthesized on the backup server from a previous full backup and all the incremental backups since then. It is equivalent to what a full backup would be if it were taken at the time of the last incremental backup.

Tape library

A storage device which contains tape drives, slots to hold tape cartridges, a barcode reader to identify tape cartridges and an automated method for physically moving tapes within the device. These devices can store immense amounts of data.

Rue image restore

A term used by NetBackup and Backup Exec for the collection of file deletion and file movement records so that an accurate restore can be performed. For instance, consider a system that has a directory with 5 documents in it on Friday. On Saturday, the system gets a full backup that includes those 5 documents. On Monday, the owner of those documents deletes 2 of them and updates 1 of the 3 remaining. That updated document gets backed up as part of The Monday night incremental backup. On Tuesday afternoon the system crashes. If we perform a normal restore of the full backup from Saturday and the incremental backup from Monday to the fresh system, we will have restored the 2 documents that were

Intentionally deleted. True image restore keeps track of the deletions with each incremental backup and prevents the deleted files from being inappropriately restored.

Trusted paper key

A machine-readable print of a cryptographic key.

Virtual Tape Library (VTL)

A storage device that appears to be a tape library to backup software, but actually stores data by some other means. A VTL can be configured as a temporary storage location before data is actually sent to real tapes or it can be the final storage location itself.