

THE CITY OF
COLUMBUS

MICHAEL B. COLEMAN, MAYOR

DEPARTMENT OF
TECHNOLOGY

**Request for Proposals
for
Backup System Redesign and Deployment**

Gary R. Cavin, CIO

Table of Contents

1	INTRODUCTION	1
2	SCOPE AND CLASSIFICATION.....	1
2.1	Scope	1
2.2	Classification.....	2
2.3	Budget	3
3	REQUIREMENTS	3
3.1	General Requirements	3
3.2	Bidder Requirements.....	3
4	RFP Process Overview	4
4.1	RFP Questions and Answers	4
4.2	RFP Schedule of Events	4
5	PROPOSAL SUBMISSION REQUIREMENTS	5
5.1	Section One: Transmittal Letter and Offer	5
5.2	Section Two: Competence.....	5
5.3	Section Three: Quality and Feasibility.....	6
5.4	Section Four: Ability	6
5.5	Section Five: Past Performance.....	7
5.6	Section Six: Cost & Payment Terms.....	7
6	EVALUATION CRITERIA AND PROCESS	7
6.1	Step One of Evaluation	7
6.2	Step Two of Evaluation Process	8
7	APPENDICES	9
7.1	Appendix A: Current Scope of Backup Targets.....	9
7.2	Appendix B: Current and Planned System Information	9
7.3	Appendix C: Backup System Service Levels.....	11
7.4	Appendix D: Operational Backup Policy, Standards, and Guidelines.....	12
7.5	Appendix E: Proposed Design and Data Flow	16

1 INTRODUCTION

The City of Columbus is placing this Request for Proposals with the intention to enter into a contract with an experienced Vendor who will provide backup system design, deployment, and documentation services. The City utilizes Symantec Netbackup to meet its needs and intends to continue with this solution for the foreseeable future.

2 SCOPE AND CLASSIFICATION

2.1 Scope

The City is seeking proposals from vendors that have extensive experience assisting data center providers in design, deployment, and documentation of Symantec Netbackup solutions. The City requires the following deliverables from this project.

2.1.1 Finalize Redesign of City of Columbus Backup System

The City requires a vendor to perform all necessary tasks to finalize the redesign of the backup system. This includes a design document, implementation plan, and other recommended artifacts. This has been started by City of Columbus Backup Administrators. The relevant details for the purpose of this RFP have been included in Appendices C through E. The following requirements must be met.

- Utilizes Symantec Netbackup 7.5 or later
- Utilizes existing or newly purchased hardware and software (Appendix B)
- Disk based backup targets, synchronized to a second data center
- Minimal use of tape media
- Follows the draft backup retention guidelines (Appendix C)
- The latest backup of data must be kept offsite from the primary data center

2.1.2 Deploy Redesigned Backup System

Based on redesign per section 2.1.1, the vendor must install, configure, and release to production the redesigned backup system. This includes but is not limited to:

- Installation and configuration of Netbackup media servers
- Configuration of disk and tape hardware to work with the new system
- Migration of existing backup targets to the new system in a phased approach
- Installation and configuration of Symantec Netbackup OpsCenter reporting tool.
- Tuning of the environment for optimal backups, utilizing the Netbackup Tuning and Performance Guide as a baseline.

The following requirements must be met for this deliverable:

- Existing Netbackup 6.5 tapes must be usable to restore archived data if needed
- All data that is currently backed up must continue to be backed up through the upgrade process. No interruptions in service can be experienced.

- Must work within prescribed Department of Technology maintenance windows and change policies. This is typically the third weekend of every month. Exceptions can be made to perform changes between 6:00PM and 6:00AM daily with prior approval.
- No interruption to production systems during normal business hours (6:00AM to 6:00PM M-F)
- A project plan with dates and milestones shall be created and followed throughout implementation. The service provider shall work with a project manager from the City of Columbus to plan and schedule all work.

2.1.3 Documentation and Reporting

Based on deliverables in 2.1.1 and 2.1.3, the vendor will be required to document the new backup system and create metrics and reports that will assist in the ongoing management and administration of the system. This includes but is not limited to:

- Document all system details in the Department of Technology system document template
- Review and edit the Department of Technology Backup Standards and Guidelines document (Appendix D) as necessary, in order to properly align the policies and processes with best practices and technological capabilities
- Provide a list of standard processes, maintenance activities, scheduled tasks, etc., required for effective maintenance of the backup system. Any item should be accompanied by detailed instructions of how to perform the task, frequency, etc.
- Provide access to, or create, standard reports to represent the ongoing health of the backup system to management and backup administrators. This may include, but is not limited to:
 - Backup job success/failure rate per day/week/month
 - Repeat offenders (job failure)
 - Trend: Backup window exceptions
 - Trend: Total amount backed up, per target, per day/week/month
 - Trend: Total amount restored, per day/week/month
 - Others as per best practices
- Provide best practice key performance indicators for backup system health, including definitions, thresholds, and reports.
- Provide knowledge transfer of best practices for future system expansion and system upgrades. This may include the following topics
 - Hardware expansion thresholds for disk, media servers, master server, etc.
 - Scale up vs. scale out

2.2 Classification

Qualified vendors must submit (as described within the specifications) documentation of a minimum of three (3) backup system design and deployment engagements within the past three (3) years, equivalent to the size and complexity of the City's system. Engagements must involve Symantec Netbackup technology solutions. Qualified vendors must have experience providing the services described in this RFP.

2.3 Budget

The estimated budget for this engagement is between \$20,000 and \$50,000. That said, the City is interested in lower cost proposals that meet the requirements detailed in this RFP.

3 REQUIREMENTS

3.1 General Requirements

3.1.1 Term

The proposed contract shall be for services delivered within one (1) year of a certified purchase order. The contract will not automatically renew, but can be extended for an additional year subject to mutual agreement, and approval from proper City authorities.

3.1.2 Pricing

Respondents to this RFP are required to propose hourly rates for the staff offered in their proposal. Hourly rates must include out-of-pocket expenses, including travel expenses. Price proposals that do not offer comprehensive hourly rates (including all out-of-pocket and travel expenses) will not be considered.

3.2 Bidder Requirements

3.2.1 Company Experience

Respondents to this RFP must submit documentation of at least three (3) backup system design and deployment engagements within the past three (3) years, equivalent to the size and complexity of the City's backup system. Engagements must involve Symantec Netbackup technology solutions. Respondents must briefly document capabilities and submit an outline of its experience including data describing the current corporate organizations date of incorporation, ownership, corporate office, number of years in business, total number of employees, services offered, and corporate ethics statement.

3.2.2 Staff Experience

Respondents to this RFP must submit resumes for the staff proposed to deliver service to the City. Staff must have experience delivering the services described in this RFP utilizing Symantec Netbackup solutions. Authorized Symantec Consultant accreditation is preferred. The winning respondent must guarantee that proposed staff will actually deliver services, or where necessary, be substituted for staff with equivalent experience.

3.2.3 References

Respondents to this RFP must provide references to verify capabilities, experience, and work history in delivering the services described in this RFP. A minimum of three (3) references are required. References should consist of projects of a similar scope, complexity, and cost. The reference contact information shall include the customer name, start/end dates of the project, customer e-mail address, street address, telephone number, fax number, and a description of the services provided.

3.2.4 Work Hours

With the exception of relevant tasks associated with section 2.1.2 above, any work under this RFP that will be required to be performed, completed, and managed at City of Columbus premises shall be

conducted during standard business hours (Monday through Friday, 8:00 a.m. – 5:00 p.m. EST, excepting City holidays) unless otherwise agreed upon in advance. As described in section 2.1.2, some tasks must be performed during evening and weekend hours to avoid service interruptions during normal business hours. The City will provide work space for the Vendor. At its sole discretion, the City may arrange remote connectivity at Vendor’s request.

4 RFP PROCESS OVERVIEW

Selection of the winning proposal shall be in accordance with Section 329.14 of Columbus City Codes, 1959. Any agreement or contract entered into will be in accordance with the provisions of Chapter 329 of Columbus City Codes, 1959, the standard agreements for professional services of the Department of Technology, and all other applicable rules and regulations. The Columbus City Codes can be found at <http://ordlink.com/codes/columbus/>.

4.1 RFP Questions and Answers

In order to enable accurate communication with respect to this RFP, to provide Vendors the opportunity to seek clarification on matters pertaining to the RFP requirements, and to enhance the Vendors’ understanding of the City’s needs, the City will accept questions from potential Vendors.

4.1.1 Question process

Specific questions concerning the RFP requirements should be submitted *in writing* before 8:00AM Eastern on May 21, 2012. Written questions must be sent via email to: vendorservices@columbus.gov and include this solicitation number in the subject line. Questions submitted to other email addresses will be ignored.

4.1.2 Answer Process

Written responses to all pertinent questions will be prepared by the City of Columbus and published as an addendum at <http://vendorservices.columbus.gov/e-proc/>. Responses will be sent by May 25, 2012 @ 5:00 p.m. Eastern. This will ensure accurate, consistent responses are provided to all potential Vendors.

4.2 RFP Schedule of Events

The following RFP schedule of events represents the City’s best estimate of the schedule that will be followed. All times are Eastern Time.

Event	Date/Time (if applicable)
RFP Issued	September 10, 2012
Deadline for written questions	September 17, 2012 @ 8:00 AM
City response to questions issued	September 25, 2012 @ 4:00 PM
RFP Due	October 4, 2012 @ 11:00 AM
Notification of finalists	October 12, 2012
Finalist Interviews (as needed)	October 16-17, 2012
Final Award	October 22, 2012
City Council Approval of Contract	November 26, 2012
Project Commencement	December 15, 2012

5 PROPOSAL SUBMISSION REQUIREMENTS

Vendor's response to this RFP should provide a clear and concise description of the Vendor's proposal and capabilities. Emphasis should be on completeness and clarity of content. Vendor shall provide one (1) original and three (3) copies of their proposal. Proposal should be in clear and succinct language, and no longer than fifty (50) pages on twenty-five (25) double-sided sheets, not including samples and/or attachments. Plastic or ringed binders and non-recyclable paper are discouraged. An electronic copy of the proposal must also be submitted on a CD or equivalent storage device. Proposals shall be organized in the following sections:

5.1 Section One: Transmittal Letter and Offer

A dated letter of transmittal on the Vendor's letterhead must be in each submittal and include, but need not be limited to, the following information:

5.1.1 Offer Period

Statement of proposal is valid for 180 days.

5.1.2 Signature

The signature of a person authorized to legally bind the Vendor to the extent of a potential contract agreement with the City.

5.1.3 Identify Materials

Identification of all material enclosures submitted in response to the RFP.

5.1.4 Contact Information

The name, e-mail address, street address, and telephone number of the individuals to which inquiries relating to this RFP should be directed.

5.2 Section Two: Competence

Vendor shall demonstrate through its background and qualifications that it is capable of providing the services described in this RFP by submitting the following information in its response:

5.2.1 Company History/Facts

Vendor should give a brief summary of the company's background. Please use this section to include any pertinent facts not otherwise requested.

5.2.2 City of Columbus Contract Compliance

If you do not have a valid City of Columbus Contract Compliance Number, please see the City's procurement site to obtain one: <http://vendorservices.columbus.gov/e-proc/>. While prospective vendors can respond to this RFP without a contract compliance number, the successful respondent to this RFP must obtain a contract compliance number as a condition of doing business with the City. The City is committed to equal business opportunity, and strongly encourages participation from minority/female business enterprises in this and all City procurement.

5.2.3 Primary business focus

Please include industries served and NAICS codes if applicable.

5.2.4 Qualifications

A brief descriptive statement indicating the Vendor's qualifications to deliver the services requested in this RFP.

5.2.5 Organization size

Provide a description of the Vendor's organization's size, longevity, and clients.

5.2.6 Related experience

Provide information about the Vendor's experience providing backup system design and deployment utilizing Symantec Netbackup solutions. Successful vendor must have completed at least three (3) similar engagements in the past three years that satisfy the requirements outlined in section 3.2.1.

5.2.7 Project staff information

Vendors must propose specific staff to deliver the services requested in this RFP. For each staff person proposed, a resume must be included documenting education and experience that satisfy the requirements outlined in section 3.2.2.

5.3 Section Three: Quality and Feasibility

5.3.1 Proposed Services and Deliverables

Proposals must include a description of proposed services for completing the deliverables outlined in section 2.1.

5.3.2 Service Delivery Plan

Explain your service delivery plan and provide an example project plan with timelines (assuming the start date listed in section 4.2), milestones, and deliverables. Identify all necessary resources, both vendor-provided and City-provided to successfully produce the deliverables within the timeline proposed. Of particular interest is the amount of City-provided time you will need to complete the tasks and deliverables described in section 5.3.1. Proposals that fail to include a fully resourced example project plan with timelines will be considered non-responsive.

5.4 Section Four: Ability

Vendor must demonstrate the ability to complete the project as planned and on schedule.

5.4.1 Workload

Vendor shall provide a calendar covering the proposed service delivery time frame indicating periods when the vendor has the resources available to work on the project, and periods when the vendor will not be available to work on the project. Previous commitments do not need to be disclosed specifically, but should be blocked out on the calendar. Preferred times to commence work on the project should be indicated.

5.4.2 Financial Responsibility

Vendor shall provide documentation of financial responsibility, financial stability, and sufficient financial resources to provide the scope of services to the City in the volume projected and within the time frames required. This documentation may take the form of: a letter of credit or reference from a bank or other financial institution; an insurance policy or bond; audited cash flow and balance sheet statements; or a satisfactory credit rating from a reputable credit rating agency.

5.5 Section Five: Past Performance

Vendor must be able to demonstrate experience providing the services described in this RFP by submitting the contact information of three (3) Professional Reference(s). The reference contact information shall include the name, e-mail address, street address, telephone number, fax number, and a description of the contract amount and service that was provided.

5.6 Section Six: Cost & Payment Terms

5.6.1 Cost

Proposals must identify estimated hours of service to be delivered by each of the staff persons proposed in section 5.2.7, associated hourly rates, and total costs. As described in section 3.1.2, hourly rates must be inclusive of all costs, including travel costs. Proposals identifying separate travel and other out-of-pocket costs will be considered non-responsive. Such costs should be recovered through the hourly rates proposed.

5.6.2 Payment Terms

The City prefers a proposed project payment schedule based on milestone and deliverable achievement. Based on the deliverables outlined in section 5.3.1 and the project plan outlined in section 5.3.2, proposals should include an estimated payment schedule based on completion of the deliverables. The City's standard terms are Net 30 days, but will consider early payment incentives as part of its evaluation. Payment terms that include late payment penalties are not acceptable.

6 EVALUATION CRITERIA AND PROCESS

Proposal responses shall be reviewed, judged, scored, and ranked by an evaluation committee consisting of City staff. Evaluation will be a multi-step process consisting first of a complete proposal submission by Vendor prior to the RFP deadline, a review of the proposals by the City evaluation committee, and then two (2) or more of the highest rated Vendors may be selected with which to hold additional discussions.

6.1 Step One of Evaluation

Evaluation Committee will study the proposals and rate them according to the following:

6.1.1 Vendor's Competence (Section 5.2) - 25 points total this section

Higher points will be given to respondents demonstrating competence to perform the required service as indicated by the education and experience of proposed personnel who would be assigned to perform the work. Particular focus will be paid to the work experience and Symantec Consultant certifications of personnel to be assigned by the vendor to this project, in performing similar projects. Higher points will also be awarded to vendors who can guarantee that equivalent staff will be made available in the event that proposed staff are no longer available.

6.1.2 Quality and Feasibility (Section 5.3) - 25 points total this section

A maximum of fifteen (15) points will be awarded based on the demonstrated understanding of the services needed and deliverables required. Higher points will be awarded to proposals that include quality samples of proposed deliverables, based on the judgment of the evaluation committee.

A maximum of ten (10) points will be awarded based on the quality and feasibility of the proposed service plan described in section 5.3.2. Higher points will be awarded to proposals that provide deliverables sooner, and clearly identify needed City staff hours and other resources necessary for successful delivery.

6.1.3 Ability (Section 5.4) – 10 points this section

Higher points will be awarded to proposals demonstrating that personnel can be made available to meet the City's needs at the time services are needed (section 5.4.1). Higher points will be awarded to proposals by vendors with demonstrated financial stability (section 5.4.2).

6.1.4 Past Performance (section 5.5) – 25 points this section

Vendors must provide reference contact information as described in section 5.5. Higher points will be awarded to vendors with a proven track record of success in providing quality services on projects of a similar size and complexity.

6.1.5 Cost & Payment Terms (section 5.6) – 15 points this section

Fifteen (15) points will be awarded to the lowest cost proposal. Other proposals will be awarded proportionately fewer points. The highest cost proposal will be awarded the fewest points.

6.2 Step Two of Evaluation Process

At the discretion of the evaluation committee, two (2) or more of the highest rated vendors may be selected for holding additional discussions to elaborate upon their qualifications and proposals in follow up interviews with the evaluation committee.

6.2.1 Revisions

The committee may permit revisions of proposals so long as all vendors who are selected for additional discussions are given equal opportunity to revise their proposals.

6.2.2 References/Past performance

Professional references may be contacted to evaluate such factors as quality of work, success in controlling costs, and success in meeting deadlines.

6.2.3 Selection

Vendors selected for this phase will be evaluated using the same criteria outlined in section 6.1, incorporating any additional information provided during the discussions phase. The evaluation committee will recommend an award to the City of Columbus Technology Department Director. With the concurrence of the Director, the City and successful Offeror will negotiate a contract. With approval from the City Council, the City and successful Offeror will execute the contract.

7 APPENDICES

7.1 Appendix A: Current Scope of Backup Targets

- Total Server disk space – Approximately 45 TB
 - Approximately 275 Windows servers (approximately 70% virtual)
 - 9 Unix servers
 - Approximately 20 Linux servers (approximately 60% virtual)
- EMC VNX CIFS file shares – Approximately 50 TB. Utilizes NDMP for backup currently
- Exchange - 990 GB
- SharePoint – 800 GB
- Virtualization solution for the Department of Technology is built on vSphere 5.

7.2 Appendix B: Current and Planned System Information

7.2.1 Current Backup System

- Master Server (1)
 - HP DL360G5
- Media Servers (7)
 - HP DL360 G5
- Disk Targets
 - HP P2000 (20TB)
 - 12 2TB SAS, 7200 rpm
 - HP P2000 (60TB)
 - 12 2TB SAS, 7200 rpm
 - 24 2TB SATA, 7200 rpm
- Tape Silo HP 322e ESL Tape Library (14 LTO3 drives)
- Infrastructure
 - Fiber switches (2) EMC DS5300

7.2.2 New Hardware Allocated for Upgraded Backup System

- Servers
 - HP DL360 G7 (8)
- Disk Storage
 - HP P2000 A (Primary Data Center)
 - 75TB
 - 2TB SAS, 7200 rpm
 - HP P2000 B (Secondary Data Center)
 - 75TB
 - 2TB SAS, 7200 rpm

7.2.3 Software

Symantec Netbackup 6.5 is currently utilized under the capacity licensing model from Symantec. The City of Columbus is entitled to all current versions of the products under that licensing agreement.

The City of Columbus also owns licenses for Symantec Puredisk de-duplication technology, also based on the capacity being utilized.

7.3 Appendix C: Backup System Service Levels

Recovery Tiers			Platinum	Gold	Silver	Bronze
		Description	High Availability	Critical applications	Standard business apps. All virtual servers	Retention Tier. All physical servers by default. Staging/Development environment. Current capabilities.
	Scheme	Specification				
Operational Recovery (OR)	Recovery Granularity	Recovery Granularity	Complete App Restore	Complete App Restore	File Or File System Restore	File Or File System Restore
<i>Per Server, Database, or data set</i>	Recovery Point Objective (RPO)	Amount of Data Loss	< 1 hour	8 Hours	<24 Hour	Best Effort
	Recovery Time Objective (RTO)	Time To Recover Data from point of notification	< 30 Minutes	< 4 hours	Max. 3 business day response 7 GB/Minute Throughput	Best Effort
	Primary Retention Period	Time Data is retained	4 Hours	72 hours	1 month	Per retention schedule
	Secondary Retention Period (Data backup System)	After the primary time period expires, the secondary backup method is the sole source of recovery for older data.	60 days on disk 1 year on tape (email system is not kept on tape)	60 days on disk 1 year on tape	35 days on disk 1 year on tape	14 days on disk 6 months on tape
	Data backup system details		Daily to disk (7 day ret.) Weekly to disk (5 week ret.) Monthly to tape (13 month ret.) Disk target deduplicated			Daily To disk (2 week ret.) Monthly to tape (6 month ret.)
	Technologies Utilized		Clustering Oracle RAC Application Specific synchronization Vmware Fault Tolerance	SAN Snapshot Vmware Snapshot CIFS Snapshots RMAN (Oracle) and SQL Backup	Disk-based backup	Disk/Tape backup only

7.4 Appendix D: Operational Backup Policy, Standards, and Guidelines

Purpose

The purpose of this document is to set the standards and policies that the data backup system must adhere to. This document will provide technical and procedural standards for which the backup system will be designed to. It will also set expectations as to what the backup system will deliver, and address when and how the backup system will be utilized in the overall strategy for DoT, in regards to operational recovery and disaster recovery.

Retention Policy

Record retention policies are kept by the City’s Record Retention Officer. The Department of Technology, and in turn the data backup system, is governed by Administrative Service Retention Schedule. **It is the position of the Department of Technology that the data backup system will only be governed by the applicable retention policies in this schedule, and only those retention policies that specifically deal with data backup media.**

The data backup system primary use is for recovery of damaged or lost files, not as a data retention system. Data files that fall under other City of Columbus retention guidelines are the responsibility of the respective departments. Such files must be maintained in a retrievable form independent of back-ups. Although backup files may contain files that fall under retention policies, back-ups are intended to restore files, not to maintain them for long-term use. An archive location may be provided to keep data files to meet long term retention.

Tiered Recovery Model

Among the large quantities of data stored and managed by the Department of Technology, there are varying degrees of importance of this data to the City. As such, a tiered data recovery model will be established to help focus activities, capital and infrastructure to the most important data systems. As part of the Disaster Recovery project, a draft tiered recovery model was established with some basic measurable metrics (See attached). This model separated out recovery as a result of a widespread outage (disaster recovery) versus individual file or data recovery (operational recovery).

The data backup system is the primary operational recovery tool for the entire Bronze and Silver tiers. Higher tiers require more frequent data backups (8 hours, 1hour, etc.), and require the use of other technologies to provide data backups. The data backup system will still be used within these tiers, but will be a secondary source of recovery.

Official Data Backup System Retention Polices

Schedule Number	Record Title and Description	Retention period
	Silver/Gold/Platinum tier daily backups – disk based data backups for recovery only	7 days
	Silver/Gold/Platinum tier weekly backups – disk based data backups for recovery only	5 weeks
	Silver/Gold/Platinum tier monthly backups – tape based data backups for recovery only	1 year
	Bronze tier daily backups - disk based data backups for recovery only	14 days
	Bronze tier monthly backups - tape based data backups for recovery only	6 months
	Archive tier yearly backups – tape based backups for recovery only, 2 per year	2 years

Operational Guidelines

- All data will be kept on near line storage for a short period of time. The retention time on disk (RTOD) will vary by tier, and will be calculated based on the likelihood of having to restore the data.
- Retention time on tape (RTOT) will be 1 year for all production systems, and 6 months for all test systems. One monthly backups will be pulled to tape
- All disk targets will utilize de-duplication technology to reduce storage requirements.
- An archive tier will be established (pending approval). This will be a write once, read many disk target area for data files that must be retained per City retention policies. The disk archive will be backed up twice a year to tape, and tape archives will be kept for 3 years.
- All backups will be “Full” backups unless specific situations call for different methods. The software system, utilizing de-duplication technology, will only backup files that have changed since the last backup (delta changes).
- Symantec Netbackup software will be utilized to meet the requirements of the system. Operational maintenance of updates and patches will be performed twice a year. Security and emergency patches will be performed as needed based on severity, at the discretion of the System Owner for the Storage, Backup and Recovery Service and/or his designees.
- Database backups – All databases will be backed up according to a standardized process. All databases of the same type (Oracle, SQL, etc.) will be backed up using the same method, to a consistent location (see Database Backups section for more details). Flat files will be picked up from that location by the data backup system, and will be treated consistently with other flat files from that point on.
- A copy of all backup data on disk will be maintained at two locations. Data will be backed up at the primary site and replicated to an off-site location, and will remain on both sets of disks until the prescribed retention period runs out.
- Archive tapes will be kept in the fireproof safe at the Primary data center.
- The standard processes, backup job policies, etc., will be documented in the System Document. Any exceptions to the standard processes will be documented individually in the System Document.

Restore Process

All requests for restores will require a helpdesk ticket be created. Requests for an emergency restore can be expedited to the Backup Administrators without a ticket; however a ticket should be completed as soon as possible with the pertinent details. The service level expectations for file restoration shall follow the standard helpdesk SLA, with impact and urgency being the main factors in the expected resolution time. If a file restore is needed to return an impactful business system to a usable state, the process shall be expedited accordingly. Typically, this situation would be classified as a disaster recovery scenario, rather than an operating recovery. Disaster Recovery scenarios utilize different tools and have separate Service Levels.

Restoration processes are highly dependent on the amount of data being restored. As such, guarantees and service levels regarding restoration times cannot be realistically set on a broad level. What can be established are response times and throughput rates. Response times are set at the helpdesk level as

discussed above. Throughput levels are set at the tier level and are dependent on many technical factors.

Restores requested past the RTOD may be subject to further delays while tapes are located and loaded.

Change Management

The process of adding and removing data items from the backup system is incredibly important to ensuring a reliable backup and restore process. Backup administrators must know when servers are added or removed from the infrastructure to ensure that the system stays efficient and everything that is in scope is being backed up as expected. Backup administrators must be notified of the following changes:

1. New server build
2. Server decommission
3. Server changes (add hard drives, etc.)
4. Enterprise storage add/move/change
5. Changes in service tier

In addition to external activities, changes within the backup system must be documented properly. Any changes in backup jobs, policies, etc. must be documented in the System Document for the backup system.

Special Backup Requests

There are times when a “special backup” must be performed to meet some regulatory or retention requirement. This frequently happens with financial systems that require a snapshot of the closed to be kept for many years. In these circumstances, it will be highly suggested that the Archive data store is utilized to house this information. While a tape backup can be taken, tape technologies frequently expire and cannot be used before the retention period of such data ends, making the tape essentially useless. An online archive location allows for quick access to such data if it is needed.

If a temporary tape backup is needed for some business purpose, a helpdesk request should be placed with the Service Desk. Special backups will require at least 3 business days’ notice, and the same tape retention periods will apply as noted above.

Reporting

Reports are essential to the healthy operation of the data backup system. Reporting, at a minimum, should allow for insight into pass/fail status, timing of backup jobs, how much data was backed up, etc. Standard reports will be dictated and created by the backup administrators, and will be run on request only. On-demand reporting for DoT and departmental system owners will be explored and developed as time permits.

Exclusion Process

At times, some data must be excluded from the backup processes for various reasons. Some files, like databases, are backed up through a separate process and should be excluded by default. Other data is excluded by request. The process for excluding data from the backup system is as follows:

1. Open a helpdesk request to exclude the data from the backup process. The following information must be present:
 - a. Location (file, folder, server, etc.)
 - b. Timeframe to exclude (if applicable)
 - c. Reason for exclusion
 - d. Person requesting and/or approving the exclusion.

Note that this process does not need to be followed for databases that fall under that standard process. However, the exclusions must still be noted in the System Document.

Operations Tape Processing

Operations procedures for tapes will be documented and updated as needed. The procedures will be documented in the System Document.

Special Conditions

Certain data must be handled in special ways. Regulations require that some data be encrypted on transportable media. Others require isolation due to personal information being present. Any special requirement must be documented in the System Document. All requirements shall be able to be upheld through an outside audit. These conditions may require special configurations, policies, or jobs within the data backup system. Any isolated data needs will be provisioned with security enabled on the backup disk devices.

7.5 Appendix E: Proposed Design and Data Flow

