PUEBLO CITY-COUNTY
LIBRARY
Ideas · Imagination · Information

www.pueblolibrary.org

INFORMATION TECHNOLOGY POLICIES & PROCEDURES

PUEBLO CITY-COUNTY LIBRARY
Ideas · Imagination · Information

www.pueblolibrary.org

TABLE OF CONTENTS

PUEBLO CITY-COUNTY LIBRARY
Ideas · Imagination · Information

www.pueblolibrary.org

INFORMATION TECHNOLOGY

05.01.01 Password Management Policy

Maintaining a strong password is a critical facet of computer and network security. The use of weak passwords places the PCCLD network, and the data within, in jeopardy of being compromised. The purpose of this policy is to establish a standard for the creation, ongoing use, and frequent change of passwords for all technology resources used by PCCLD personnel. This policy will be enforced to ensure the protection of the PCCLD network, computer resources, and to safeguard access to personal and confidential information. All PCCLD personnel, that are considered staff, volunteers, contractors, consultants, and/or any person(s) that require the use of a username and password for the purpose of doing business with PCCLD will be required to adhere to this policy.

- Passwords must be changed at least twice a year.
- All passwords must be a minimum of eight characters and include characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example: !, $, #, %)
- Passwords must not be shared with any person for any reason, unless (1) approved by an immediate supervisor, and/or (2) subpoenaed for legal purposes.

www.pueblolibrary.org

INFORMATION TECHNOLOGY

05.01.01.P1 Password Management Procedures

Creating and maintaining strong passwords help to prevent access to important and confidential information. A strong password prevents unauthorized access to important data and thwart identity theft. Below are some guidelines and steps to help create and maintain strong passwords.

What you should NOT do:

- DO NOT use any iteration of your name, names of family members, pets, or friends.
- DO NOT use important numbers, or series of numbers, such as birth dates, social security numbers, or phone numbers.
- DO NOT use whole dictionary, common, or slang words.
- DO NOT use extended repeated letters or numbers.
- DO NOT use the same password for multiple accounts.

What you should do:

- When creating or changing a password, make the password easy to remember, but complex for someone to guess or crack.
    - Use uppercase and lowercase letters (A-Z, a-z)
    - Use numbers (0-9)
    - Use special characters and symbols (!, @, #, $, %, +, -, \)
    - Use longer characters to strengthen passwords; instead of just a minimum of 8 characters, use 10 or more characters.
- Change passwords often; the more often a password is changed, the more difficult it is for someone to guess or crack the password.
- Instead of a password, use a passphrase increasing protection for your accounts:
    - A passphrase is a sentence or phrase that can be remembered replaced with a combination of the aforementioned characters, e.g., “Silent night, holy night” using a variation of complex characters, a good paraphrase would be “$iLen7N!gh7h0lyN1gh7”

Examples of weak passwords:

- *Bingo* – A common word, too easy to guess or crack.
- *Lisa2009* – Uses a personal name and a common number; easy for a hacker to crack.
- *LG7777* – Uses a repeated number.
- *GJohnson* – Example of a name used in the password; easy to guess.

Examples of strong passwords:

- *$nWNalc@iB* – Uses uppercase and lowercase letters, special characters and numbers.
- *Our@#We@th3rls2Humid!* – A great password is a passphrase. A passphrse is based on a sentence or phrase that you can remember using upper case and lowercase letters, numbers and special characters. A passphrase also works well because it uses more characters; this passphrases uses 21 characters.
- *J'ki2a&O!yF):xP* – Though difficult to remember, the best passwords have a combination of uppercase and lowercase letters, special characters and symbols, are long in character length, and are completely random.

It is a challenge to remember multiple passwords; it is more of a challenge to remember multiple complex passwords. Despite the challenge, it is not good practice to write down passwords. Writing passwords down makes it easier for anyone to find them as most passwords written down are kept near the user's computer. Below are a couple of ways to store and/or remember passwords and ensure confidentiality:

- Utilize a password manager software program. Such programs are installed on the computer to store all accounts, usernames and passwords. The benefit of this software is that the user must remember the password to login to the password manager and from there will have access to all of the accounts without remembering all of the usernames and passwords.
- Use a particular method, such as a hash function, to generate passwords for all accounts. By using this process, the user does not necessarily need to remember all passwords but the method in which the passwords were created. For example, to create a new account for a website called *flowerbasket.com;* the method requires using the first, third and fifth characters of the website name—in this case: f, o, e. Count the number of characters in the website, in this example 16. Create the password by putting together the first, third, and fifth characters with the total number of characters spelled out. To add further complexity, capitalize the third character, replace the last character with a number, and consistently add the same special character. The password for flowerbasket.com would become: "*foEsixtee4$*"

Passwords must not be written down and left in a place where unauthorized personnel might discover them. If it is necessary to write down a password, store the password in a secure location accessible only by the user. Once the password is remembered, destroy the paper or file on which it was written.

If a user suspects a password has been compromised in any way, notify the PCCLD Information Technology Department and immediately change the password. The PCCLD Information Technology Department may periodically use password/passphrase guessing or cracking measures to ensure the use of strong passwords. Should a password/passphrase be cracked during this process, the user of that account may be asked to change his/her password.

In the event an employee is terminated or resigns, Human Resources must notify the Information Technology Department so the employee's account(s) can be disabled or deleted immediately. Should the employee who has been terminated or resigned have password access to accounts with special privileges, passwords to such accounts must be changed immediately.

05.01.01.P2 Backup and Restore Procedures

Overview

This document describes the backup and restore procedures used by the Library's Information Technology Department and the components used to support such procedures. This document is intended as an overview of the practices used, and as such, is to be a living document that is revised based on changes to ensure consistent backups and restoration practices. The PCCLD IT department continues to review its backup practices and evaluate various backup solutions as the solution in place is satisfactory, but not ideal. As the Library develops a comprehensive disaster and continuity plan, this document will be modified as necessary to support the plan.

Data Center and Off-Site Storage Locations

The datacenter contains the majority of the Library's servers, hosted applications, and data storage. The datacenter for the Pueblo City-County Library District resides at the Rawlings Library in the server room next to the IT offices located in the basement. The branch library locations all consist of at least one server that stores original data, and in some cases backup data, for each respective branch and/or other locations. The Pueblo West Library serves as an off-site storage location in which tape backups created at Rawlings are taken and stored in a secure safe. The Pueblo West Library also serves as a fail-over site in which key network operations will be provided in the case of a disaster or emergency that riddles the Rawlings Library inoperable. Though the Pueblo West Library has been designated a fail-over site, additional equipment and services are still required and need to be configured before the site is capable of handling resilient services for the Library district.

Equipment

A Dell PowerEdge 2950 server hosts the primary backup software and serves as the media server for backup agents installed on multiple servers. The server is connected to a Dell PowerVault 124T tape autoloader that contains a single tape drive. The PowerVault device is capable of two (2) magazines with a capacity of eight (8) LTO-3 or LTO-4 tapes (LTO-5 is in draft); our tape autoloader device only contains one (1) magazine. The autoloader uses a robotic device to automate the selection and use of tape media. LTO-3 is the tape media used in the autoloader device. LTO-3 media is capable of storing 400GB uncompressed data and 800GB compressed data. A bank of 30 tapes can be used for backup, tape rotation, and off-site storage.

An internal tape drive is used on the Library's two (2) Sun servers to supplement backups processed on the autoloader device. Both servers contain a SCSI tape drive in which DDS tapes are used for incremental backups. The Sun servers host the Library's integrated library system; one server is the production server and the other serves as a test server. Though both servers include an internal tape drive, only the production server is regularly used. The DG3-150M tapes are capable of storing 20 GB uncompressed data and 40GB compressed data. The DAT72 tapes are capable of storing 36GB uncompressed data and 72GB compressed data. Again, the internal tape drives are used as supplemental backups; the primary backup for the integrated library system is conducted on the media server using Symantec BackupExec 2010.

An EMC AX150i storage area network (SAN) device is used to store data in the first backup phase of the disk-to-disk-to-tape approach. The SAN device contains two (2) disk pools for storage, a 2 TB pool and a 1.3 TB pool. The backup server, also known as the media server, back's up data to the SAN device using iSCSI technology.

Two (2) 4GB IronKey USB storage devices are used to supplement backups for the finance accounting system, Fundware.

Software

The latest version of Symantec's BackupExec software, version 2010 is used to automate backup jobs and manage backup media. BackupExec agent software is installed on the majority of the Library's servers. The agent software is the endpoint in which the media server communicates and manages backup and restore jobs for each server. Special backup agents are used for particular applications such as Microsoft Exchange and SQL Server.

Microsoft's Volume Shadow Copy Service (VSS) is used on Windows Servers to provide limited backup and restore functionality for users. VSS creates incremental copies of data on a daily basis and allows users to retrieve deleted and/or changed files and/or folders for up to 30 days.

CPIO and UFSDUMP are Solaris utilities used to backup local data. Copy In and Out (CPIO) is a native Unix tool used in a nightly Symphony report to backup daily changes made to the Symphony database. Unix File System Dump (UFSDUMP) is another native Unix tool, ufsdump is used to backup changes made to the Symphony database over the weekend.

Microsoft Outlook 2007 includes a feature to recover deleted emails which are archived for up to 7 days after deletion on the Exchange server.

Responsibilities

The responsibility to backup and restore data lie specifically with the IT department. Users will have limited access to restore data such as deleted files and emails, but the backup schedule, data restore from servers, and configuration is handled by the IT department. All members of the IT department will be given an overview of how data is backed up and restored. Though cross-training and knowledge throughout the department is encouraged on these procedures, the primary responsibility to monitor and manage backup and restores will rest with the System Administrator and/or Systems Specialist. Backup and restoration policies, procedures, and changes in backup philosophy will be handled by the IT Manager.

Backup

There are various philosophies and methods used for backup and restores. A disk-to-disk-to-tape, also known as D2D2T, approach is used as the Library's primary backup scheme. This strategy back's up original data stored on disk to a disk pool located on a SAN or NAS, that data is then stored to tape media; tape media is rotated off-site to the Pueblo West Library. In the case of the Fundware system, the Finance department runs a backup utility each day storing the Fundware backup to the IronKey USB storage device. At the end of the week, the USB device is stored in a safety deposit box at Vectra Bank. Despite the backup process used by the Finance department, the Fundware data is included in the overall D2D2T approach.

The main approach to backup the Library's data is D2D2T, but there are instances in which data is backed up directly to disk or tape. In the case of the integrated library system, the job to backup data to disk before going to tape was taking entirely too long. The backup to tape proved to be faster and more efficient so that backup job and schedule changed using additional supplemental backups for faster restore processes.

Backup Types & Occurrences

There are three backup methods generally used in a backup solution; full backup, differential backup, and incremental. All three methods are used for the Library's backup solution. Full backups are used to

backup complete data sets. Differential backups are used to backup data that has changed since the last full backup in a cumulative fashion. Incremental backups will backup data that has changed since the last backup, full or incremental. Archive and copying of data can also be seen as methods for backups. The copy method is used in the Library's backup solution; the archive solution is not really utilized. Please refer to Table 1 to see specifics on each backup job and the frequency of that job.

Tape Rotation

30 LTO-3 tapes are available for use in the PowerVault 124T. 7 tapes are consistently used in the autoloader magazine for automation. 3 – 5 tapes are rotated to Pueblo West each month for off-site storage. The remaining tapes are used after active tapes become full, in which data is on those tapes are erased and re-used in the backup rotation. All tapes are labeled for recognition and proper storage and reuse.

Eight (8) DAT 72GB tapes are available for use in the internal tape drives on the production and test Symphony servers. Only five (5) tapes are used in a daily rotation for incremental backups on the production server. Tapes can be used to restore production data to the test server for testing purposes and/or production roll-over should it be needed. The DG-150M tapes are available but are no longer used on a regular basis due to their storage limitations.

There are two (2) IronKey USB devices in which the Finance department used for rotation and backup purposes. At the end of each week, one of the USB drives are taken to Vectra bank and stored in a safe deposit box. The following week, the USB drive is replaced with the second USB device.

Restore

Test restores will be conducted twice a year on mission critical applications. Scheduled preventive maintenance work orders have been assigned to specific IT members to conduct test restores. Comments regarding the success, failure, and resolution of each restore will be documented in the completed work order ticket. See Figure 1 for a work order restore job assigned to an IT staff member. The process to restore an application and/or data sets will vary depending on the system. If the application is intact, the process will generally involve obtaining the most recent full backup and/or incremental and/or differential backup jobs. As our primary backup software, BackupExec will be used to restore the majority of backup jobs to either a test environment or original productive environment. If an application is not intact, the software will need to be reinstalled, reconfigured, and then restored.

Test restores ensure proper reading of media and restoration of data. The practice of restoring data will be shared among key IT staff members; the procedures of restoring data, and access to data, will be understood as well as the estimated time to complete the process based on the data being restored.

Staff can restore data that has been deleted or changed within 30 days of modification on servers running VSS. Not all servers in the Library's server farm run VSS as there is no need for staff to access certain files or folders. Staff also have the capability to retrieve deleted emails up to 7 days from time of deletion through Microsoft Outlook.

Tape Media Care

All tape media is stored in a secure location, generally in the basement wiring closet at the Rawlings Library, Pueblo West Library in a secure safe, or safe in the IT offices at the Rawlings Library. The room temperature where the tapes are stored are maintained anywhere from 68 – 73 degrees. The number of times an LTO tape can be used is based on the type of tape, number of passes, or uses, and conditions in which the tape us used and stored. The LTO-3 tape media the Library uses has an archival life of 30 years and 1 million passes (equal to 260 full backups). These are the technical specs for LTO-3; tape media can wear sooner than expected depending on the type of use and in improper conditions. All of the DAT72 tapes are stored at the Rawlings Library in the IT office in a secure box. The DAT72 tape media is capable of 2000 passes, or 100 full backups.

It is important the tape drive that is used to backup data to the media is cleaned and checked on a regular basis. If the drive is not cleaned on a regular basis tapes can encounter undue wear and/or result with inconsistent and incomplete backups. After passes or uses manufactures recommend cleanings after a number of hours of uses or number of passes. Many backup devices include a self-cleaning mechanism and many backup solutions include reports that are sent to administrator to clean drives after recommended use. To ensure regularity and quality of backups, tape drive media for the Library's PowerVault 124T takes place once a month.

Destruction & Disposal

As the first phase of disk-to-disk-tape is to store media on disk, ensuring the quality and integrity of the storage media is important. SAN and NAS devices could encounter errors through data corruption and/or disk defragmentation. Disk pools are defragmented at least twice a year. File-system checks are also conducted twice a year to ensure the integrity of the disk pools. Should a disk be found to be corrupt or bad, and cannot be recovered through disk checks or defragmentation, the drive(s) will be removed, wiped to minimum DoD standards, and sent to Metech recycling for proper disposal and destruction.

Destruction and disposal of tape media can, and will, take place for several reasons. First, should the condition of a tape be found to be in a poor state after inspection, the tape will be destroyed and disposed. Second, after the tape has been used through a number of mounts or number of backup passes, the tape will be destroyed and disposed. Third, should backups result in consistent errors either through backups or restores, the media will be disposed and destroyed.

Tape media is destroyed by the process of degaussing. Degaussing means to take a super magnet and run it over the tape media to erase all of the contents on the tape. After the tapes have been degaussed, the tapes are placed in a recycling tote in which Metech Recycling picks up to properly recycling electronic waste.

www.pueblolibrary.org

INFORMATION TECHNOLOGY

05.01.01.S1 Backup Jobs Schedule

Server	Application	Backup Type	Backup Tool	Storage Medium	Frequency	Content Being Backed Up
Achilles	Outlook Web Access	Front end Exchange server contains no data as it retrieves data from the backend server. No backup required.				
Aletheia	Directors Station	Directors Station is not setup yet, therefore no backup schedule is defined.				
Argus	CPS Images	Copy	Windows Copy Command	Zephyr Disk Pool	Image Updates	G:\PCCLDcache G:\PCCLDvDisks
		Full	BackupExec	LTO-3	Bi-Annually	G:\PCCLDcache G:\PCCLDvDisks
Artemis	Test Symphony	Full	UFSDUMP	DAT72	As Needed	/s/sirsi
Atlas	VMWare	Full	Snapshots	Local Disk	After Updates	[atlas_vm_datastore]
Castor	CPS Server	Full	BackupExec	Rhea Disk Pool	After Updates	C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data
Danaus	Terminal Services	Terminal Services service requires no backup.				
	TimeClock	Full	Robocopy	Rhea Disk Pool	Daily	C:\Program Files\Microsoft SQL Server\MSSQL$TIMECLOCKPLUS\Data
Demeter	SAN Disk Pool	Full	BackupExec	LTO-3	Monthly	S:*.*
Dione	Sendmail	Dione is used to forward email notices and reports from Symphony; no backup is needed as no data is stored on this server.				
Gaia	User Data/System State	Full	BackupExec	SAN	Monthly	E:\DepartmentFolders E:\Userdrives E:\Userprofiles
	User Data	Incremental	BackupExec	SAN	Weekly	E:\DepartmentFolders E:\Userdrives E:\Userprofiles
		Incremental	VSS	Local Disk	Daily	G:\
Helios	User Data/System State	Full	BackupExec	SAN	Monthly	G:\Userdrives G:\Userprofiles G:\DepartmentalFolders
	User Data	Incremental	BackupExec	SAN	Weekly	G:\Userdrives G:\Userprofiles G:\DepartmentalFolders
	User Data	Incremental	VSS	Local Disk	Daily	G:\

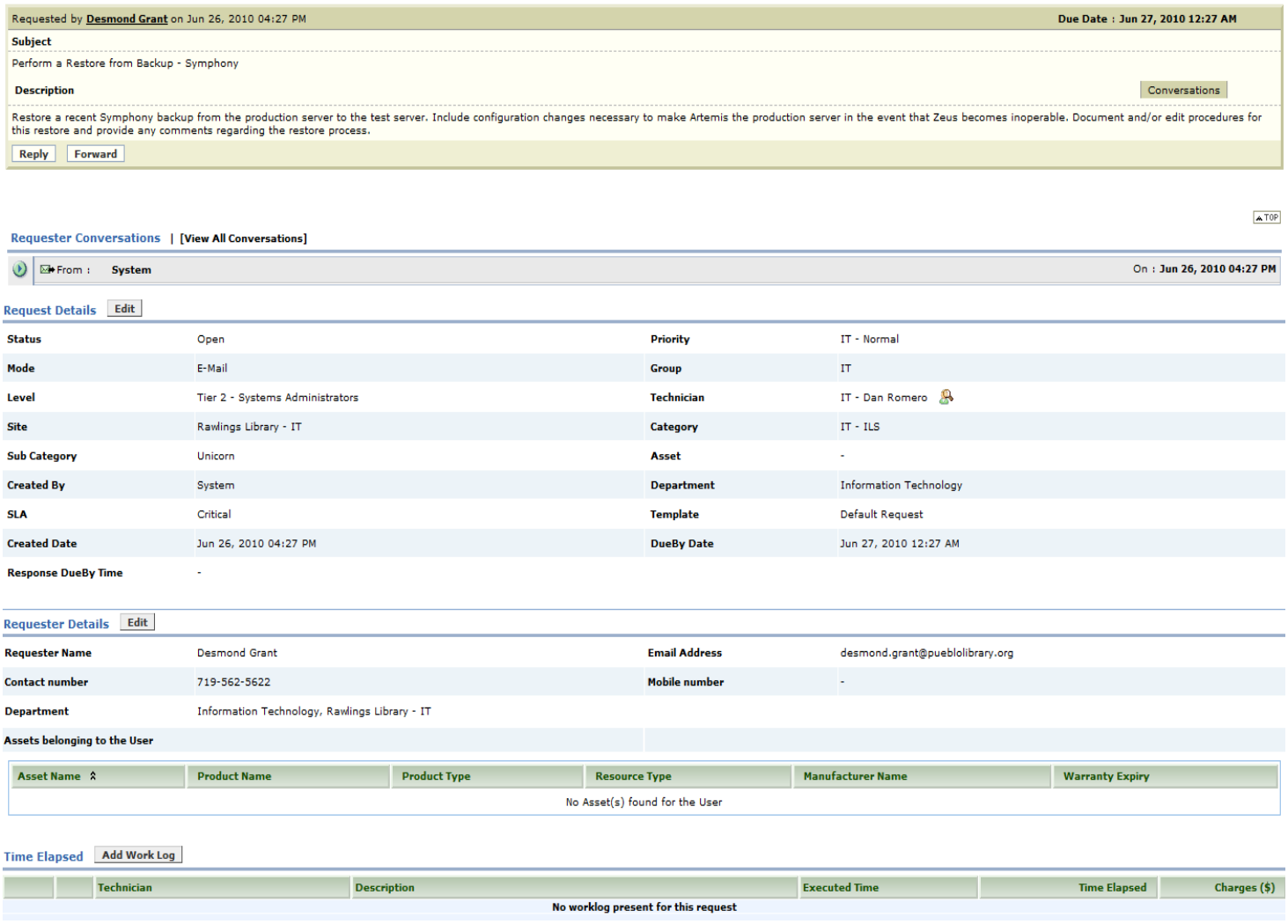
Server	Application	Backup Type	Backup Tool	Storage Medium	Frequency	Content Being Backed Up
Hemera	Optima	Full	BackupExec	SAN	Weekly	C:\Program Files\GNEIL OPTIMA\HRWare\Backup
Hera	Web Files/Folders	Full	BackupExec	SAN	Weekly	C:\windows\system32\logfiles E:\
		Incremental	BackupExec	SAN	Daily	C:\windows\system32\logfiles E:*.*
Hercules	VMWare	This is a test server; no backup jobs are set.				
Hermes	Microsoft Exchange	Full	BackupExec	LTO-3	Weekly	First Storage Group (located on E:\)
		Differential	BackupExec	SAN	Daily	First Storage Group (located on E:\)
Hestia	iBistro	Full	BackupExec	SAN	Weekly	C:\Progra~1\Apache~1\Apache~1 D:*.*
Horae	PW IP Cameras	No backup job has been created; a plan is being formulated on creating a backup job to accommodate the storage generated for live video feeds.				
Hyperion	DHCP	Full	Copy	Theia Disk Pool	After Changes	C:\windows\system32\dhcp
Notus	SVA	Full	BackupExec	SAN	Weekly	D:\sirsi D:\SVA Batch Files
Ophion	FAS	Full	FAS Backup Utility	SAN	Occasional	C:\FASSERV\data
Paean	PA Server	No backup jobs have been created.				
Pandora	User Data/System State	Full	BackupExec	SAN	Monthly	E:\Barkman E:\Userdrives E:\Userprofiles
	User Data	Incremental	BackupExec	SAN	Weekly	E:\DepartmentFolders E:\Userdrives E:\Userprofiles
	User Data	Incremental	VSS	Local Disk	Daily	G:\
Pollux	CPS Backup Server	No backup jobs have been created.				
Plutus	Fundware	Full	Fundware Backup Utility	IronKey USB	Daily	E:\Fundware\Data
		Full	BackupExec	SAN	Weekly	E:\Fundware\Data\Backup
		Incremental	BackupExec	SAN	Daily	E:\Fundware\Data\Backup
Prometheus	SAM	Full	BackupExec	SAN	Weekend	C:\Inetpub E:\Downloads E:\Scripts SQL SAM & SAM Reports DB's
		Incremental	BackupExec	SAN	Daily	SQL SAM & SAM Reports DB's
Proteus	ServiceDesk+	Full	Backup	Local Disk	Daily	E:\\proteus\AdventNet\ME\ServiceDesk

Server	Application	Backup Type	Backup Tool	Storage Medium	Frequency	Content Being Backed Up
Rhea	Backup Config	Full	BackupExec	SAN	Monthly	Symantec BackupExec Config
Theia	Domain Controller	No backup jobs have been created.				
Themis	DNS	Full	Copy	Remote Disk	On Revision	/var/named/chroot
Thetis	WSUS	Update server currently is not being backed up.				
Tyche	MAS90 & ABRA	A backup schedule has not been defined for these applications as we are working on the migration project and the server is not in production.				
Vesta	iBistro	No backup jobs have been created.				
Zephyr	User Data	Full	BackupExec	SAN	Bi-Weekly	E:\userdrive E:\userprofile E:\departmentfolders
		Incremental	VSS	Local Disk	Daily	E:*.*
Zeus	Symphony	Incremental	CPIO	DDS Tape	Mon-Fr	/s/sirsi
		Incremental	Copy	Local Disk	Sun & Mon	/s/sirsi
		Full	BackupExec	LTO-3 Tape	Daily	/s/sirsi
		Sync	rsync	NFS Share (Artemis)	When Needed	/s/sirsi (w/ exclusions)

www.pueblolibrary.org

INFORMATION TECHNOLOGY

05.01.01.S2 Work Order for Restore



Requested by **Desmond Grant** on Jun 26, 2010 04:27 PM — **Due Date : Jun 27, 2010 12:27 AM**

Subject

Perform a Restore from Backup - Symphony

Description — Conversations

Restore a recent Symphony backup from the production server to the test server. Include configuration changes necessary to make Artemis the production server in the event that Zeus becomes inoperable. Document and/or edit procedures for this restore and provide any comments regarding the restore process.

Reply | Forward

TOP

Requester Conversations | **[View All Conversations]**

From : **System** — On : **Jun 26, 2010 04:27 PM**

Request Details Edit

Status	Open	**Priority**	IT - Normal
Mode	E-Mail	**Group**	IT
Level	Tier 2 - Systems Administrators	**Technician**	IT - Dan Romero
Site	Rawlings Library - IT	**Category**	IT - ILS
Sub Category	Unicorn	**Asset**	-
Created By	System	**Department**	Information Technology
SLA	Critical	**Template**	Default Request
Created Date	Jun 26, 2010 04:27 PM	**DueBy Date**	Jun 27, 2010 12:27 AM
Response DueBy Time	-		

Requester Details Edit

Requester Name	Desmond Grant	**Email Address**	desmond.grant@pueblolibrary.org
Contact number	719-562-5622	**Mobile number**	-
Department	Information Technology, Rawlings Library - IT		
Assets belonging to the User			

Asset Name	Product Name	Product Type	Resource Type	Manufacturer Name	Warranty Expiry
No Asset(s) found for the User					

Time Elapsed Add Work Log

		Technician	Description	Executed Time	Time Elapsed	Charges ($)
No worklog present for this request						