Information Security – Server Backup

Introduction

Data is one of YCCD's most important assets. In order to protect this asset from loss or destruction, it is imperative that it be safely and securely captured, copied, and stored. The goal of this document is to outline a policy that governs how and when data residing on company servers will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed up data be restored to individual systems.

What Is Backed Up

This policy refers to the backing up of data that resides on YCCD's servers. Servers and the files and/or data types on these servers that are covered by this policy do not refer to backing up of data that resides on individual PC's, laptop hard drives, notebook hard drives including any hand-held peripherals that may have the capacity for electronic storage such as iPod, mobile phones, pda's, usb drives, standalone hard drives, disc or optical media, etc. Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is strongly encouraged that end users save their data to the appropriate server in order that their data is backed up regularly in accordance with this policy.

In addition, files that are left open at the time the backup procedure is initiated may not be backed up. End users are reminded to save and close all files, as well as all related applications, prior to the backup procedure window.

It is the responsibility of server administrators to ensure that all new servers be added to this policy, and that this policy be applied to each new server's maintenance routine. Prior to deploying a new server, a full backup must be performed and the ability to perform a full restoration from that backup confirmed.

Prior to retiring a server, a full backup should be performed and placed in storage for 365 days.

Managing Tape Backups

Backups are conducted using Symantec Netbackup software.

The servers being backed up must do so according to the following procedure. This method ensures that no more than one day's working data will be missing in the event of a data loss incident:

1. All backup tapes are to be labeled using the following labeling conventions:
    - Barcodes that are recognized by the Netbackup software and the tape library robot.
2. All live full backup tapes older than 3 months are stored onsite in the Data Center.

3. All backup tapes stored offsite are to be stored at the Iron Mountain data storage facility in Tracy, CA. All full backups are to be stored for 3 months offsite before returning to the Modesto data center. This includes Weekly, Monthly and Quarterly full backup tapes. All tapes are placed in special media specific containers and are transported by Iron Mountain in a secure temperature controlled vehicle. Only authorized YCCD personnel can request or send tape containers offsite through Iron Mountain.
4. All backups will take place between the hours of 5:00 p.m. and 7:00 a.m. (there are some exceptions to this rule). This timeframe has been selected to minimize the impact of server downtime on end users that may be caused by the need to take servers offline in order to perform the backup itself. If this backup schedule in some way interferes with a critical work process, then the affected user(s) is to notify the YCCD IT Operations Department so that exceptions or alternative arrangements can be made.
5. Incremental backups (all files changed since the last full backup) will be performed daily, Monday through Thursday and twice over each weekend. These tapes will be stored onsite after the incremental backup cycle.
6. A full backup will be performed each weekend (Friday, Saturday or Sunday). These tapes will be stored offsite at the Iron Mountain location for storage. Please see offsite storage schedules from paragraphs 3 & 4 above. When this period has elapsed, the tapes will be brought back onsite for additional storage time until the retention period has ended then the tapes will be reused.
7. The following tape retention cycles are currently in place:
   Daily Incremental: 30-day retention
   Weekly Full: 90-day retention
   Monthly Full: 365-day retention
   Quarterly Full: 7-year retention

   MS-Exchange/Outlook Email (only):
   Daily Incremental: 30-day retention
   Beginning 05/27/2011 Exchange Email will have a three year retention on all Full backups:
   Weekly Full: 3-year retention (full backup done once per week in groups, Mon. – Fri.)
   Monthly Full: 3-year retention (full backup done once per month in groups, Mon. – Fri.)
   Quarterly Full: 3-year retention (full backup done once per quarter in groups, Mon. – Fri.)

   Estimated Time Line for Email Restores:
   All Email will expire three years after every week (or every Full backup) year round from 05/27/2011 forward.

8. If, for some reason the backup cannot be completed, is missed, or fails, then it will not be ran again until the next day. If a backup fails more than one day in a row, the respective server administrator(s) responsible for the server must be notified by email, phone or voicemail. It will be the responsibility of the server administrator to decide if the end users are to be notified of a failed backup, depending on the severity of the situation.
9. If a tape is discovered to be damaged or corrupt, then the tape will be destroyed to prevent further use and replaced with a new one.
10. On the last page of this document is a current list of servers being backed up. If a server administrator needs a server put on a backup schedule or removed from a backup schedule they are to email the backup administrator and copy the IT Operations manager. The same notification must be followed when retiring a server. The server administrator(s) should periodically confirm their servers are being backed up and the proper backup schedules are in place.
    (Please See Last Page For Current Server List)

Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it is essential to regularly test one's ability to restore data from its storage media.

1. Daily incremental backups/ tapes must be tested at least once every month to ensure that the data they contain can be completely restored.
2. Weekly full backups/ tapes must be tested at least once every month to ensure that the data they contain can be completely restored.
3. Monthly backups/ tapes must be tested at least once every 3 months to ensure that the data they contain can be completely restored.
4. Quarterly backups/tapes must be tested at least once every year to ensure that the data they contain can be completely restored.

Data will be restored from a backup if:

- There is an intrusion or attack.
- Files have been corrupted, deleted, or modified.
- Email has been deleted.
- Information must be accessed that is located on an archived backup.
- Email or files are needed for legal reasons.

In the event a data restore is desired or required, the following procedure will be adhered:

1. The backup administrator is responsible for overseeing backup and restores processes. If a user has a restore request, they can contact the backup administrator and/or IT Operations manager by calling 209-575-6554, sending an e-mail to the backup administrator and/or IT Operations manager, or filling out and submitting a request form, located at: http://www.yosemite.edu/it/forms/restorerequest/

   In the event of unplanned downtime, attack, or disaster, consult YCCD's Disaster Recovery Plan for full restoration procedures.

2. When requesting a restore, the requester must provide the following information:
   - Full name.
   - Contact information: Department, email, phone ext.
   - Name of server.
   - Specify if this is a Unix, Windows or other type of server.
   - Name of file(s) and/or folder(s) to be restored, include full path name.
   - Date from which file(s) and /or folder(s) are to be restored from.
   - Location in which file(s) and /or folder(s) are to be restored to.
   - Events leading to data loss, including last modified date and time (if known).
   - Urgency of restore.

3. Depending on the extent of data loss, an incremental backup tape, full backup tape, or combination of both will need to be used. The timing in the cycle will dictate whether these tapes are onsite or offsite. The backup administrator will retrieve the needed tapes. If tapes are offsite and the restore is not urgent, then the end user affected may be required to wait up to 3 business days for the tape(s) to be retrieved.