Backup and Recovery Procedures

1.0 Overview

Backup and recovery methods are essential to data protection and security. Any loss of data due to file corruption, virus, security or human error is a loss of time and money. Furthermore, loss of data can severely impact the success of a project, department, or college. An effective server backup and recovery plan is crucial.

2.0 Purpose

The purpose of this plan is to provide a successful procedure for backup and recovery of critical data. These procedures are in place to assist and guide Pixel Pals CGI.

3.0 Scope

These procedures apply to Information Technology Operators. This backup and recovery plan includes, but is not limited to, backup and recovery of file and print servers, mail servers, database servers, web servers, video streaming servers and domain controllers.

4.0 Procedures

4.1 Backup Plan

- Server backups will be performed every business night, excluding holidays.
- Backups performed on Friday will be kept for a month before recycling.
- The last backup of every month will be considered the monthly backup and kept for a year before recycling.
- The last two monthly tapes will be stored off-site in a fireproof safe.
- Backups will be performed and monitored by a full-time IT staff member.
- Backups will be automated using NAS (Network Attached Storage)
- Backup failures will be reported to Information Technology and action will be taken quickly to fix the problem.
- Backups will always be performed before upgrading or modifying a server.

4.2 Loss of data

- If loss of data is discovered, evaluation and investigation by IT staff is immediately dispatched.
- In most cases, loss of data is related to file corruption, virus, security or human error.

- If loss of data is related to data corruption, IT Staff must troubleshoot and determine if the problem is hardware or software related to prevent addition file corruption.
- If the loss of data is related to a virus, IT Staff must determine the extent of the virus and remove it to prevent further loss of data.
- If the loss of data is related to security or a compromised system, IT Staff must determine the extent of the compromise and fix the vulnerability quickly to prevent further loss of data.
- If the loss of data is related to human error, IT Staff must immediately inform and train the appropriate personnel to avoid further loss of data.
- Once the problem has been determined and loss of data minimized, IT Staff should proceed to restoration of data from backup media.

4.3 Restoration of data

- Once loss of data is discovered, evaluated and minimized, IT Staff will proceed to restoration of data from backup media.
- IT Staff will determine the time and date of the lost data.
- IT Staff will determine the appropriate backup media to restore the data.
- IT Staff will insert the backup media into the appropriate server.
- IT Staff will invoke the Backup/Restore software, such as Veritas Backup Exec or Arcserve.
- IT Staff schedule the restore of the appropriate data within the Backup/Restore software.
- IT Staff monitor the restore of data.
- Upon restore, IT Staff evaluate the integrity of the restored data.
- IT Staff will contact the end-user of the data to finalize restore.
- Upon approval from the end-user, the restore is considered finished.

4.4 Disaster Recovery

- If a disaster is discovered, IT Staff will determine the extent of the problem and proceed accordingly.
- If the disaster is hardware related, IT Staff will replace the failed hardware and restore according to the steps outlined above.
- If there is a natural disaster, such as water, fire, tornado, earthquake, or other, the hardware will be replaced and the server will be restored using the offsite backup media according to the steps outlined above.
- Upon restoration of data, IT Staff will check the data for integrity and validity.
- IT Staff will contact the end-user of the data to finalize restore.
- Upon approval from the end-user, the restore is considered finished.