

Drake University
Administrative Systems Backup and Recovery
Policy and Procedures

This document describes how backup policies and procedures are applied to the application environments.

Applications covered under this procedure are:

DUSIS which includes: SCT Banner including Self Service, Bookshelf and Online Help, SCT Banner Xtender Solutions, SCT Workflow, Eprint

Luminis which includes: SCT Luminis Content Management System, SCT Luminis Platform System

AdAstra Room Scheduling

DUSIS Production Backups

Backups are performed on the DUSIS Production Environment to mitigate the risks associated with data loss and system downtime that could result from the corruption of data, programs or operating systems.

Standby Mirror Database

The PROD database running on ODBS is mirrored by STBY running on OBACKUP. STBY is a Physical Standby database maintained by the Oracle Data Guard. Every time PROD writes an archived redo log it sends the log to STBY which duplicates all changes. The maximum time between logs is set to 15 minutes.

Disk Backups

The database instances are backed up on disk every night. Three forms of disk backup are used:

1. A full export of the database is taken and compressed. The latest nine copies are maintained in the backup directory.
2. Each database has a directory containing all of its Oracle files. Every night supporting files necessary to recreate the instance including: init.ora, control-file (.trc), tnsnames.ora, oratab, and listener.ora are copied into the directory. Then the entire directory is copied and compressed into a separate backup directory. The existing archived redo logs are also copied and compressed into the backup directory.
3. After #2, the entire contents of the backup directory for the PROD instance on the odbs server is copied to the obackup server.

Disk backups are scheduled through the Cron automated scheduler on the ODBS server. Operations is responsible for ensuring that the backups are set to run each night and ensuring that the backup has run successfully on the following morning. Should the backup procedure fail, Operations will notify the Database Administrator (DBA) in order to take corrective action.

Drake University
Administrative Systems Backup and Recovery
Policy and Procedures

Backups by Instance:

A Cron job runs between 12:30 and 2:00 AM seven days a week to copy the instances on disk. The previous night's copy is compressed and moved to a 'oneback' directory where the latest nine compressed copies are kept, and a new backup copy is created. The following is a list of the instances with their source and backup directories.

PROD:

server	odbs
database files	/udisk/u05/oradata/PROD
backup	/udisk/u05/oradata/PROD_backup
archivelogs	/udisk/u01/app/oracle/adminPROD/arch
initPROD.ora	/udisk/u01/app/oracle/adminPROD/pfile
prod_ora_NNNN.trc	/usr/u01/app/oracle/admin/PROD/udump
oraenv	/usr/local/bin/oraenv
listener init file	\$ORACLE_HOME/network/admin/listener.ora
oratab	/var/opt/oracle/oratab
tnsnames file	\$ORACLE_HOME/network/admin/tnsnames.ora

TEST:

server	obackup
database files	/udisk/u03/oradata/TEST
backup	/udisk/u03/oradata/TEST_backup
archivelogs	/udisk/u01/app/oracle/adminTEST/arch
initTEST.ora	/udisk/u01/app/oracle/adminTEST/pfile
test_ora_NNNN.trc	/usr/u01/app/oracle/admin/TEST/udump
oraenv	/usr/local/bin/oraenv

TREL:

server	obackup
database files	/udisk/u03/oradata/TREL
backup	/udisk/u03/oradata/TREL_backup
archivelogs	/udisk/u01/app/oracle/adminTREL/arch
initTEST.ora	/udisk/u01/app/oracle/adminTREL/pfile
trel_ora_NNNN.trc	/usr/u01/app/oracle/admin/TREL/udump
oraenv	/usr/local/bin/oraenv

**Drake University
Administrative Systems Backup and Recovery
Policy and Procedures**

Tape Backups

The tape backup system is programmed to make a tape copy of the entire set of DUSIS servers starting at 4:00 AM seven days a week. The tape backup will be a full backup on Sundays and an incremental backup every other day of the week. Servers backed up by the tape backup system are: ODBS, ODEV, FMX, OIAS, EPRINT, DIAL-WEBXTENDER, and OBACKUP. Note: database instances are not backed up to tape because they are unusable for recovery purposes. However, disk backups of database instances are backed up to tape. These backups can be used to recover the database in the event recovery is required.

The tape backup system is also programmed to make a 'clone' copy of the tape backup. This copy is to be taken out of the Dial Center. All clone copies are stored in Old Main.

Additionally, each month after the financial month end, the full (Sunday) backup and its clone will be pulled from the tape drive and stored. These tapes will not be recycled through the backup process and will be stored indefinitely.

Operations will be responsible for scheduling all tape backups. Additionally, they will be responsible for ensuring each backup has run successfully. Should the backup procedure fail, Operations will contact the System Administrator to assess the problems and take corrective action. Operations will also be responsible for delivery of backup tapes offsite on a daily basis.

Retention Of Backups

Type	Frequency	Retention Period
Disk - full export	Nightly	9 days minimum
Disk - files copy	Nightly	1 day
Tape	Nightly	30 days minimum
Tape Clone	Nightly	10 days minimum
Tape	Monthly	Forever

Drake University
Administrative Systems Backup and Recovery
Policy and Procedures

Special Backups or Archives of Reports and Files

Special backups or archival of reports and files may be required by various departments for regulatory purposes or audit purposes. Examples of these types of backups are the archive of official reports from the Eprint server, the save of official enrollment numbers or the save of Financial Aid files for seven year retention. Where possible, these types of backups can be performed by each department. Each department can also request this type of backup from the OIT Operations department if the backup can be performed centrally and the appropriate equipment is available. Operations will obtain the requirements and set up the backup and storage of the backup medium from the requesting department and determine whether or not a centralized back up is feasible. If OIT Operations determines the backup is feasible, the backup will be set up and added to the backup schedule by OIT Operations. Departments may be responsible for the cost of the backup medium, e.g. tape, CD-ROM and other special equipment or software when backups are performed centrally. It will be up to the discretion of the OIT CIS Director as to whether or not backups can be performed with existing media. Data Custodians must approve all requests for backup of this type. Departments can contact OIT Operations via phone by calling extension 3552 or via email at oper@drake.edu.

If the backup cannot be performed centrally, OIT Desktop Support will assist the department in determining their needs for performing the backup. In this case, each department is responsible for obtaining the equipment and software required to perform special backups. OIT Desktop Support may be contacted via phone by calling extension 3001 or via email at helpdesk@drake.edu.

Drake University
Administrative Systems Backup and Recovery
Policy and Procedures

Recovery

Recovery is the process of restoring data, programs or operating system files from the backup tape in the event of corruption. The general recovery strategy is as follows:

1. Operations will notify all affected persons. Initial notification will include OIT personnel and Data Custodians. OIT personnel will include the CIS Manager, DBA, Operations Manager and System Administrator. If deemed appropriate, a contact will be opened with the SCT Action Web.
2. The above personnel will determine the scope and type of the corruption as well as the necessity and scope of the restore. A restore may not be necessary if the scope is small. It may be easier and less risky to re-enter corrupted data. If data has changed significantly since the point of backup, restoring may result in the loss of the data. If a restore is necessary and data changes have occurred since the point of backup, Data Custodians will be responsible for determining if and how data will be brought current.
3. Determine whether or not the system will be available and if not, approximate the downtime and notify those affected.
4. Determine who is responsible for performing the restore. The type of corruption will determine who is responsible as well as who is most knowledgeable and who is available. This might be Operations, DBA or the Systems Administrator.
5. OIT will secure the hardware.
6. OIT will save the existing data if possible.
7. OIT will secure the appropriate backup.
8. OIT will load the backup to the appropriate server if the backup is a tape backup. OIT will create a RCVR database instance from the backup files if it is data that is corrupted.
9. OIT will ensure the restore has completed successfully and promote data from RCVR to the appropriate instance if it is data that is corrupted.
10. OIT and the Data Custodians will test to ensure the system is once again working properly.
11. Operations will notify those impacted that the system is once again available.
12. OIT will prevent a reoccurrence of the corruption.

Drake University
Administrative Systems Backup and Recovery
Policy and Procedures

Backup and Recovery Testing

Regular testing will occur to demonstrate the ability to recover from disruption of normal DUSIS operation. On a monthly basis:

1. Operations will retrieve selected database and application directory files from the tape backups and verify that they are correct. A log is kept to track the person who performed the restore, the date the restore was performed, what was restored, the specific tape backup media that was tested and the results of the test and any additional action that needed to be taken.
2. The DBA will emulate a complete restore of PROD by recreating the TEST instance from the PROD disk backup.

Luminis Backups

Luminis is backed on the nightly tape backup along with DUSIS.

Astra Backups

Astra is backed up on the nightly tape backup along with DUSIS. Additionally, an application specific backup is performed every Saturday at 11:00 p.m. that exports the data to d:\AstraScheduleServer6\backtemp.