

<Company Name>

Infrastructure Service Documents

A Sample Oracle database backup Policy

Purpose

This document describes the Oracle database backup policy. This policy is used to determine the appropriate implementation for procedures, hardware and software required to backup production databases.

Responsibilities

1. Oracle database backup policy is determined by IT in conjunction with business partners, compliance leads and IT infrastructure .
2. IT Infrastructure database team is responsible for ensuring the implementation of the oracle database backup policy.
3. IT infrastructure database team is responsible for the day to day management of the technical environment used for the backups.
4. IT infrastructure server admin team is responsible for running the backup, changing tapes, ensuring tapes are transferred to storage, storing tapes and observing tape retention requirements etc.

Maximum Permissible Data Loss

1. In the event of a catastrophic machine loss or other disaster the maximum permissible data loss for production corporate applications data is 1 working day.
2. In the event of a single disk failure, the database should be recoverable to the last committed transaction.
3. In the event of a data corruption, the database or, if appropriate, the object(s) affected should be recoverable to a point in time prior to that corruption.
4. In the event of a database object, e.g. a table being deleted in error, the object should be recoverable to either the night before or the whole database to a point in time prior to the object being deleted.

Maximum Recovery Times

1. In the event of a failure requiring database recovery IT infrastructure will ensure that the recovery activity is assigned critical priority. Whilst no specific recovery time guarantees have been agreed guideline recovery times for most common scenarios are published as part of the backup and recovery documentation set.

2. In the event of a catastrophic machine loss or other major disaster all production databases identified for priority recovery in the IT infrastructure disaster recovery plan must be recovered within three working days.

Database Availability

1. Disruption to database availability due to backups must be minimized, i.e. backup techniques which do not require database downtime will be used as far as possible for all production databases.

Backup Storage And Retention Periods

1. Tape storage media must not be stored beside servers. A fire safe, or other secure storage location must be used for long term storage of media.
2. Daily backups sets for production corporate applications will be retained for a period of six (6) weeks from the date of the backup unless otherwise agreed with the respective IT infrastructure business partners.
3. The final backup set each month for production corporate applications will be retained for a period of 1 year from the date of the backup unless otherwise agreed with the relevant IT infrastructure business partners.

Actions In The Event Of Backup Failure

1. Should a backup fail to complete on a production database EUCS Unix/FM must be contacted to establish the cause of failure and to advise on whether a manual hot backup should be taken.
2. Should a backup fail to complete on a production database on two consecutive nights a manual hot backup must be performed immediately.
3. All backup failures must be logged by IT infrastructure server admin staff in the backup failure log.

Current Backup Procedures (Overview)

1. A full hot backup, i.e. a backup where the database remains online, is taken every night, 7 days a week on all production databases. These backups take place typically between 9pm and 9am.
2. Full database exports are taken each night on all production databases. These are taken prior to the backup and the export files are included in the main backup.
3. Tape storage media is removed from the machine room each morning after the backups complete and stored in a fire safe in the same building.
4. Each Friday media for the previous day's backup is removed to an off site fire safe for longer term storage.

5. A full cold backup of the relevant database, i.e. a backup where the database is shutdown until completion, is taken before major database or system upgrade.
6. Full cold backups may also be taken from time to time on an ad hoc basis when requested by MIS business partners, e.g. to provide a snapshot of the database at a specific point in time.
7. Each week day media for the previous day's backup is removed for temporary off site storage.