Data Restore Guidelines for Database Administrators

This document provides step-by-step instructions for restoring database backups and ensuring data integrity.

1. Pre-Restoration Checklist

- Verify the backup file's location and integrity.
- Notify stakeholders about the restore operation and potential downtime.
- Backup current database state before proceeding.
- Ensure sufficient storage and permissions on destination server.

2. Restoration Procedures

1. **Stop Application Services**
    - Prevent new transactions during restore.

2. **Restore the Database from Backup**
    - For MySQL: `mysql -u user -p database_name < backup.sql`
    - For PostgreSQL: `psql -U user -d database_name -f backup.sql`
    - For MS SQL Server: Use Management Studio or `RESTORE DATABASE` command.

3. **Validate Restore**
    - Check database consistency and run integrity checks.
    - Confirm critical data is available.

4. **Restart Application Services**
5. **Notify Users**
    - Communicate restore completion and any relevant information.

3. Post-Restoration Validation

- Verify application connectivity to the database.
- Check system logs for restoration errors or warnings.
- Perform random record checks and business process simulations.

4. Common Backup File Types

Database	File Type	Extension
MySQL	SQL Dump	.sql
PostgreSQL	Custom Format	.backup
SQL Server	Backup File	.bak
Oracle	Export Dump	.dmp

5. Troubleshooting

- **Restore Fails:** Check access permissions, available storage, and backup file integrity.
- **Data Mismatch:** Review backup date/time and validate source consistency.
- **Long Restore Times:** Monitor resource usage and consider restoring during low-traffic periods.

6. Documentation

Record all steps, commands used, and issues encountered during the restore in the maintenance log for auditing and future reference.