Company SOP – MySQL Database Backup Using DigitalOcean Web Console

Document Purpose
This Standard Operating Procedure (SOP) describes the approved method for performing a MySQL database backup using **mysqldump** via the DigitalOcean Droplet Web Console. This SOP applies to production, staging, and disaster recovery scenarios.

1. Scope & Applicability

This SOP applies to all engineers, system administrators, and support personnel responsible for database operations on systems hosted in DigitalOcean. It is designed specifically for DigitalOcean Managed MySQL databases.

2. Prerequisites

- Access to DigitalOcean Droplet Web Console
- Valid database connection details (host, port, username, database name)
- Sufficient disk space on the Droplet
- Non-root or root user with sudo privileges

3. Access DigitalOcean Web Console

1. Log in to DigitalOcean dashboard.
2. Navigate to **Droplets**.
3. Select the target Droplet.
4. Click **Launch Droplet Console**.
5. Log in using root or a sudo-enabled user.

4. Install MySQL Client (One-Time Setup)

Run the following commands in the Web Console:

```
apt update
apt install mysql-client -y
```

5. Perform Production-Safe Database Backup

Use the following approved mysqldump command. This command ensures minimal impact on production systems and avoids GTID-related restore issues:

```
mysqldump --single-transaction --quick --set-gtid-purged=OFF -h <DB_HOST> -P 25060 -u <DB_USER> -p <DB_NAME> > db_backup.sql
```

When prompted, enter the database password. Password input will not be visible on screen.

6. Compress Backup File

```
gzip db_backup.sql
```

7. Verify Backup Integrity

```
ls -lh db_backup.sql.gz
zcat db_backup.sql.gz | head
```

8. Transfer Backup to Local Machine

Move the compressed backup to a non-root user directory and download it using SCP from your local machine.

9. Cleanup (Mandatory)

After confirming successful download, remove the backup file from the production server to avoid security risks.

10. Security & Compliance Notes

- Never store database backups permanently on production servers.
- Never transmit database backups via email or unsecured channels.
- Always run backups during low-traffic periods.
- Use non-root users wherever possible.

End of Document