Test Plan: Data Restoration from Production to Development

# 1. Introduction

This test plan outlines the testing approach, scope, and responsibilities for validating the restoration of data from the production environment to the development environment. The goal is to ensure the data is correctly restored, sanitized (if needed), and that systems remain functional and secure post-restore.

# 2. Objectives

- Ensure data restoration from production to development completes successfully.

- Validate data completeness and integrity after restore.

- Confirm masking/anonymization of sensitive production data.

- Verify functionality of applications using restored data in dev.

- Ensure no production configurations or access tokens remain.

# 3. Scope

## In Scope

- Database and file system restore validation

- Data integrity and consistency checks

- Application-level testing post-restore

- Data masking verification

- Security/access control checks

## Out of Scope

- Performance testing

- Full application regression (unless otherwise noted)

- Live production systems

# 4. Preconditions

- A valid and restorable backup of production data is available.

- The development environment is prepared and accessible for the restoration process.

- Data masking or sanitization will be applied as required by internal policies or regulations.

- Necessary access and permissions are provided to the relevant teams for performing and validating the restoration.

- Any tools, scripts, or documentation needed for the restoration and validation are available and up to date.

# 5. Test Strategy

## 5.1 Pre-Restoration Checks

- Confirm latest production backup is complete and verified.

- Confirm availability of storage and compute in the development environment.

- Verify schema compatibility between environments.

- Backup current development environment (for rollback).

## 5.2 Restoration Execution

- Restore production DB dump/files into development environment.

- Monitor logs and error outputs during restore process.

- Log duration and success/failure status.

## 5.3 Post-Restoration Validation

### Data Validation

- Validate record counts match between production and restored DB.

- Run checksum/hash comparison on sample data tables.

- Verify referential integrity (e.g. foreign keys, constraints).

- Confirm static files (e.g. images, documents) are restored correctly.

### Data Masking Verification

- Confirm PII data is masked (e.g., emails, phone numbers, names).

- Attempt login with production credentials — should fail or be sanitized.

- Run automated queries to detect unmasked sensitive data.

### Application Functionality Checks

- Login with test user credentials.

- Access critical modules (dashboard, user profiles, transactions, etc).

- Submit test transactions/forms.

- Ensure emails/SMS are disabled or redirected in dev.

### Security Checks

- Ensure production API keys, tokens, secrets are not present.

- Ensure application points to dev services (not production).

- Access control verification — dev users only.

- Confirm audit logs are not sent to production tools.

# 6. Test Data

- Production backup (DB & files)

- Sanitization/masking scripts

- Sample test accounts for verification

- Data comparison reports or tools (optional: dbcompare, DataGrip diff, etc)

# 7. Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| QA Tester | Validate restored data and application behavior |
| DevOps/Infra | Execute the restoration, monitor performance |
| DBA | Perform pre/post-restore checks and masking |
| Security Lead | Verify sanitization and access control |
| Developer Lead | Support functional testing of features |

# 8. Risks & Mitigation

|  |  |
| --- | --- |
| Risk | Mitigation |
| Incomplete backup | Validate backup before use |
| Sensitive data leakage in dev | Enforce masking scripts and access control |
| Schema mismatch between prod and dev | Pre-check schema versioning |
| Downtime in development env | Communicate schedule and plan for rollback if needed |

# 9. Entry & Exit Criteria

## Entry

- Backup from production is verified and available.

- Development environment is ready for restore.

- All required tools and access are provided.

## Exit

- Data is restored and verified.

- Masking/sanitization is confirmed.

- Application functions as expected in dev.

- No live production credentials or references exist in dev.

# 10. Deliverables

- Test Plan (this document)

- Data validation checklist/results

- Application smoke test results

- Masking verification report

- Restoration summary log

# 11. Tools

- Database tools: pgAdmin, MySQL Workbench, or CLI

- Scripting tools: Python/SQL scripts for validation

- File integrity: md5sum, diff

- Masking: in-house scripts or open-source tools like DataMasker

- Logs/Monitoring: system logs, application logs