Post-Migration Testing Strategy Document

Project: [Project Name]

Date: [YYYY-MM-DD]

Version: [1.0]

1. Objective

The purpose of this document is to define the strategy for validating the successful migration of systems, data, and processes as part of the [Project Name] post-migration phase.

2. Scope

- Applications involved in migration
- Data sets and integrations
- Environments: Production, UAT, etc.

3. Testing Types

- **Smoke Testing**: Basic validation of system accessibility and core features.
- **Functional Testing**: Validation of business functionalities.
- **Data Integrity Testing**: Ensures data consistency, correctness, and completeness post-migration.
- **Integration Testing**: Validates interfaces with external and internal systems.
- **Performance Testing**: Confirms response times and throughput are within acceptable limits.
- **Security Testing**: Verifies access controls and data privacy.

4. Test Approach

- Identify critical business processes and applications for validation.
- Prepare baseline data for comparison.
- Create test cases mapping old vs. new environment behavior.
- Define entry and exit criteria for each test phase.

5. Roles & Responsibilities

Role	Responsibility
Test Lead	Test planning, coordination, and reporting
Testers	Execute test cases, log defects
Business Analyst	Review test coverage, validate requirements
Technical Lead	Environment setup, migration support

6. Entry & Exit Criteria

Entry Criteria

- Migration completed and environments available

- Test data loaded and available
- Test scripts and documentation ready

Exit Criteria

- All critical defects fixed
- Test cases executed with 100% pass rate for critical features
- Test summary report completed

7. Defect Management

- All defects to be logged in [Defect Tracking Tool]
- Prioritization and resolution tracked daily

8. Reporting & Communication

- Daily status updates to stakeholders
- Final test summary report post completion
- Defect summary reports as required

9. Risks & Mitigation

- **Risk:** Test environment instability
  Mitigation: Early validation and monitoring
- **Risk:** Data loss or corruption
  Mitigation: Data backup and dry runs

10. Approval

Signature: _____

Date: _____