

Environment Separation Policy

Document Title: Environment Separation Policy

Version: 1.0

Prepared by: Navas Shereef

Next Review Date:

1. Purpose

To define controls and requirements for the segregation of Development, Testing, and Production environments to reduce the risk of unauthorized access, unintended changes, or misuse of operational data, and to ensure compliance with ISO/IEC 27001 control A.12.1.4.

2. Scope

This policy applies to:

- All environments involved in software development and deployment.
- All personnel (employees, contractors, vendors) involved in the development, testing, or maintenance of systems.

It covers:

- On-premise, cloud, and hybrid infrastructure.
- Applications, databases, configurations, and CI/CD pipelines.

3. Policy Requirements

3.1 Environment Separation (ISO 27001: A.12.1.4)

Development, Testing, and Production environments must be **logically and/or physically separated**.

Data, applications, and services must not **cross environments** without defined approval and security controls.

3.2 Access Control (ISO 27001: A.9.1, A.9.2)

Dev/Test access is limited to developers and testers.

Prod access is limited to authorized operations and support staff.

Privileged access to Production must be **justified, time-bound, and logged**.

3.3 Code and Data Promotion (ISO 27001: A.14.2.9)

Code must flow from Dev → Test → Prod through **automated pipelines**.

Promotion requires successful testing and **multi-party approval**.

Production deployments must be logged and traceable.

3.4 Data Usage and Protection (ISO 27001: A.18.1.4)

Production data must not be used in lower environments unless **anonymized or masked**.

Use of real data in non-prod environments must undergo **risk assessment** and **Data Protection Officer (DPO)** approval (where applicable).

3.5 Configuration and Secrets Management (ISO 27001: A.9.2.1, A.14.1.2)

Environment-specific configurations (e.g., connection strings, API keys) must be **isolated** and stored securely using tools like **Key Vaults or Secrets Managers**.

No hard-coded secrets are allowed in code repositories.

3.6 Monitoring and Logging (ISO 27001: A.12.4.1, A.12.4.3)

All environments must implement **separate logging systems**.

Production logs must be retained per retention policy and stored securely.

Dev/Test logs may be consolidated for QA purposes but must be access-controlled.

3.7 Change Management (ISO 27001: A.12.1.2, A.14.2.2)

Changes to Production must follow the **formal change control process**.

Emergency fixes must be documented and reviewed retrospectively.

4. Non-Compliance

Violation of this policy may result in disciplinary action, up to and including termination of employment or contract.

5. Roles and Responsibilities

Role	Responsibility
Developers	Work in Dev/Test; follow promotion procedures
Test Engineers	Conduct UAT and regression in Test environment.
DevOps Engineers	Maintain deployment pipelines and



	environment integrity.
Security Team	Enforce policy, monitor access and segregation.
Management	Approve access rights and ensure compliance

6. Review and Maintenance

This policy must be reviewed at least annually or when significant changes to systems or business processes occur.

Approval

Name	Position	Date	Signature
Sherry George	Technical Director		_____

--End of Document--