Access Control Policy — Rivermark Operations Portal (ROP) (Fictional)

> **SYNTHETIC DEMO ARTIFACT — ACADEMIC USE ONLY**

Document ID: 02_ACCESS_CONTROL_POLICY
Version: 0.1
Effective Date: 2026-02-11
Owner: Identity and Access Management (IAM) Lead (Fictional Role)
Applies To: Rivermark Operations Portal (ROP) (Fictional)

1.0 Purpose
Define account management, access provisioning, least privilege, and privileged access requirements

2.0 Scope
Applies to all users and administrators of Rivermark Operations Portal (ROP) (Fictional), including autl

3.0 Roles and Responsibilities
- **IAM Lead:** defines access roles and approves privileged access.
- **System Administrators:** provision accounts and enforce role assignments.
- **Managers:** approve user access requests.
- **Users:** protect credentials and use accounts appropriately.

4.0 Policy Statements
- Access shall be granted based on least privilege.
- Privileged accounts shall be separate from standard user accounts.
- Access requests shall be approved prior to provisioning.
- Accounts shall be disabled upon termination or role change.
- *Intentional gap:* The policy does not define the required frequency for access recertification.

5.0 Procedures
1. User submits an access request with justification.
2. Manager approves the request.
3. System Admin provisions the account and assigns a role.
4. IAM Lead approves privileged role assignments.
5. *Intentional gap:* No documented process for periodic account review / recertification.

6.0 Exceptions
Emergency access may be granted with after-the-fact approval within 24 hours.

7.0 Review Cadence
Review semi-annually. *(Intentional gap: does not specify who conducts the review.)*

8.0 Definitions
- **Least Privilege:** granting only access required to perform duties.
- **Privileged Account:** elevated permissions for administration.