

Identity and Access Policy (IAP)

Pillar Lead: Phoenix (Access & Security)

I. Policy Statement

All access to Cygnus Covenant systems, data, and models must be governed by the principle of **Least Privilege**. Access must be provisioned, maintained, and revoked based strictly on the role-based requirements of the individual.

II. User Identity and Authentication

A. Authentication Standards

- 1. **MFA Mandate:** Multi-Factor Authentication (MFA) is mandatory for all internal system access, privileged accounts, and VPN connections.
- 2. **Password Complexity:** Passwords must meet a minimum complexity standard of 12 characters, including a mix of uppercase, lowercase, numbers, and symbols. Passwords must be changed every 90 days.
- 3. **Unique Identity:** Each user must be associated with a single, unique identity (UID) tied to their employment status. Shared accounts are strictly prohibited.

B. Account Lifecycle

- 1. **Provisioning:** Access shall only be granted after formal approval from the relevant Department Head and the Phoenix Pillar Lead.
- 2. **Review:** All access privileges must be formally reviewed and recertified every six (6) months.
- 3. **Deprovisioning:** Access must be immediately revoked upon an employee's separation, role change, or extended leave. Automatic disabling of accounts is set for 24 hours after separation confirmation.

III. Access Authorization and Roles (Principle of Least Privilege)

A. Role-Based Access Control (RBAC)

Access permissions must be assigned to pre-defined roles, not to individual users. Roles are defined as follows:

Role	Core Responsibilities	Highest Data Access
System Administrator	System health,	Full control over system

(SysAdmin)	Infrastructure configuration, patching.	configurations; Restricted access to production model data.
Model Developer (Orion)	Model training, code development, experimentation.	Read/Write access to experimental and staging data; Read-Only access to production data.
Data Analyst/Curator (Cygnus)	Data cleaning, policy implementation, audit logs.	Read/Write access to raw data sets; Read-Only access to production environments.
Policy/Audit (Phoenix)	Compliance review, security logging, incident handling.	Read-Only access across all systems and logs.

B. Elevated Privileges

Temporary elevation of privileges requires:

1. Justification detailing the specific task (e.g., "Emergency patch deployment").
2. Approval from two different members of the Phoenix Pillar Lead Team.
3. Automatic revocation of privileges upon completion of the task (or after 4 hours, whichever comes first).

IV. Monitoring and Compliance

A. Logging

All system access, data transfers, configuration changes, and privilege escalations must be logged centrally and monitored by the Phoenix team.

B. Audit

The Phoenix Pillar Lead will perform automated and manual audits quarterly to detect and remediate non-compliant access permissions.