Data Handling Policy (DHP)

Pillar Lead: Cygnus (Infrastructure)

I. Purpose and Principles

The Data Handling Policy outlines the procedures and controls necessary to ensure the confidentiality, integrity, and availability of all data managed by The Covenant. This policy supports the principles established in the Regulatory Compliance Policy (RCP) and the Infrastructure Security Policy (ISP).

A. Data Lifecycle

This policy governs data from its creation or acquisition, through storage and transfer, to its eventual destruction or archival.

B. Classification Mandate

All data elements must be formally classified and labeled according to the schema in Section II. This classification dictates the minimum required security controls.

II. Data Classification Schema

The Covenant utilizes a three-tiered classification schema to determine appropriate handling and encryption requirements.

Classification	Definition	Examples	Minimum Encryption Standard
P1: Public	Data intended for public consumption and distribution. Disclosure poses no risk to the project or users.	Core model output, Public documentation, Open-source code (after release).	Encryption at rest is recommended, but not mandatory.
P2: Internal	Operational or proprietary data essential to the project's internal functions. Unauthorized	Training corpus metadata, Financial records, Internal network configurations, Audit reports.	Mandatory AES-256 Encryption at rest and TLS 1.3/SSH for transfer.

	disclosure could impact performance or competitive standing.		
P3: Confidential/Secret	Highly sensitive data whose disclosure would severely compromise infrastructure security, compliance, or user privacy.	API Keys, Production database credentials, Secure Secrets Vault contents, Zero Trust access logs.	Mandatory AES-256 Encryption at rest and in transit. Strict access logging and monitoring.

III. Data Storage and Retention

A. Encryption at Rest

All data classified as P2 (Internal) or P3 (Confidential/Secret) must be encrypted using AES-256 or a superior industry-standard encryption algorithm while stored on any physical or virtual medium. Encryption keys must be managed by the Secrets Management Vault (P3).

B. Retention Limits

1. **P1 Data:** Retained indefinitely for historical and provenance purposes (e.g., training corpus sources, released model versions).
2. **P2/P3 Operational Data:** Retained for a maximum of 90 days, unless a longer period is legally mandated for regulatory compliance or active forensic investigation. After this period, data must be securely destroyed or anonymized.

IV. Data Transfer and Access

A. Data in Transit

All electronic transfer of P2 and P3 classified data, regardless of destination (internal or external), must be protected by cryptographic protocols (e.g., HTTPS with TLS 1.3, secure SFTP, or VPN tunnels). Unencrypted transfer channels are strictly prohibited for P2 and P3 data.

B. Access Logging

Access to all P3-classified data, including the reading or modification of any corresponding

configuration files, must generate an immutable log entry detailing the user, time, action taken, and system accessed. These logs are stored separately from the data itself.