Title: Master Information Security Policy
Owner: Replenit sp. z o.o.
Version: 2.1
Effective Date: November 28, 2025

Document 1: Information Security Policy (ISP)

1. Purpose and Scope

The purpose of this Information Security Policy (ISP) is to protect the confidentiality, integrity, and availability (CIA) of the information assets of Replenit sp. z o.o. ("Replenit") and its clients. This policy applies to all employees, contractors, and third-party vendors who access Replenit's systems.

2. Access Control Policy

- **Principle of Least Privilege:** Access rights are granted strictly on a "need-to-know" basis.
- **Authentication:** Multi-Factor Authentication (MFA) is mandatory for all access to production environments (e.g., AWS, Azure, Google Cloud, Databricks) and corporate identity providers (Google Workspace).
- **Access Reviews:** User access rights are reviewed quarterly. Access is immediately revoked within 24 hours of employee termination.

3. Cryptography and Encryption

- **Data in Transit:** All data transmitted over public networks must be encrypted using TLS 1.2 or higher.
- **Data at Rest:** All sensitive data stored in databases, object storage, or backups must be encrypted using strong standard algorithms (e.g., AES-256).
- **Key Management:** Encryption keys are managed via centralized Key Management Services (KMS) with restricted access logs.

4. Operations Security

- **Vulnerability Management:** Automated scans are performed weekly on all production infrastructure. Critical patches must be applied within 14 days of release.
- **Logging & Monitoring:** System logs (audit trails) are retained for a minimum of 1 year. Logs must capture: User IDs, timestamps, success/failure of access, and files accessed.

5. Supplier Relationships

- Replenit ensures that all sub-processors (e.g., Databricks, Microsoft) are subject to a security review prior to onboarding.
- Replenit maintains Standard Contractual Clauses (SCCs) and Data Processing Agreements (DPAs) with all vendors processing personal data outside the EEA.

6. Remote Work & Endpoint Security

- All company-issued laptops must have full-disk encryption (BitLocker/FileVault) enabled.
- Antivirus/EDR software must be active and updated automatically.
