Backup System Policy

1. Purpose

The purpose of this policy is to establish clear guidelines for backing up DevEngineers' critical data and systems to ensure business continuity in the event of data loss or system failure. This policy outlines the requirements for secure, consistent, and effective backups, as well as the procedures for managing and verifying those backups.

2. Scope

This policy applies to all data and systems deemed critical to DevEngineers' operations, including financial records, customer data, employee information, and business applications. It also extends to third-party systems or services used by DevEngineers. Exclusions include non-critical data and systems that do not require regular backups, such as test or development environments, which are specified by the IT Security Team.

3. Policy

3.1 Backup Schedule and Retention

- All critical systems and data must be backed up daily, with full backups conducted weekly and incremental backups occurring daily.
- Backup retention periods are as follows:
  - [redacted]**Standard data:** 90 days
  - [redacted]**Compliance-related data (e.g., financial records, PII):** Retention must align with industry-specific regulations (e.g., GDPR, HIPAA, PCI-DSS), which may require retention periods that exceed 90 days.

3.2 Backup Storage and Encryption

- Backups must be stored in geographically separated locations, with both on-premises and cloud solutions utilized to minimize risk.
- All backups must be encrypted using AES-256 encryption or an equivalent industry-standard encryption algorithm.
- Encryption methods will be audited **annually** to ensure they remain compliant with current security standards and are free from vulnerabilities.

3.3 Testing and Backup Verification

- Backup restorations must be tested at least **quarterly** to ensure that the backup and recovery processes meet established recovery time objectives (RTOs) and recovery point objectives (RPOs). The results of these tests must be documented and reviewed by the IT Security Team.

3.4 Vendor Management and Responsibilities

- Third-party vendors responsible for managing backups must comply with DevEngineers' backup policies and security standards. Regular vendor performance audits will be conducted to ensure adherence to security protocols, with a particular focus on encryption, backup frequency, and disaster recovery capabilities.
- All third-party vendors must undergo a **risk assessment** and provide assurances (e.g., SOC 2 compliance, ISO 27001 certification) that their backup management practices align with industry standards.

3.5 Disaster Recovery Integration

- In the event of a disaster, critical system backups will be prioritized for restoration based on the recovery time objectives (RTOs) outlined in DevEngineers' disaster recovery plan.
- Regular disaster recovery drills will include scenarios where backup systems are utilized to ensure that the restoration process works seamlessly with other disaster recovery protocols.

3.6 Compliance and Legal Audits

- The IT Security Team must conduct **annual compliance audits** of the backup systems to ensure adherence to this policy and all external regulatory requirements. These audits will focus on backup retention, encryption, vendor management, and testing procedures.
- Backup systems must comply with data protection and privacy laws, including but not limited to the **General Data Protection Regulation (GDPR)**.

3.7 Incident Response and Escalation

- In the event of a high-severity incident, such as a backup failure or corruption affecting critical systems, the issue must be **escalated to the Chief Information Officer (CIO)** within 24 hours for immediate investigation and resolution.
- A post-incident review will be conducted to assess the root cause of the failure and update the policy as necessary to prevent future incidents.

3.8 Employee Training and Awareness

- All employees involved in managing backups must undergo annual training on backup procedures and security protocols.
- Training effectiveness will be measured through **annual assessments** and simulated recovery exercises to ensure that all personnel are proficient in backup and recovery processes. These assessments will include mock incidents to verify that employees can respond to backup-related failures effectively.

4. Record Management

- Backup logs, restoration test results, and audit reports must be maintained for a minimum of one year and made available for review during compliance audits.
- The CMS administrators, in collaboration with the IT Security Team, are responsible for maintaining records of all backup activities and ensuring that records are periodically reviewed to ensure compliance with this policy.

5. Revision History

Date of Change	Responsible	Summary of Change	Next Review
July 2024	Chief Information Officer	Initial creation of policy	January 2025

Glossary of Terms

- **AES-256 Encryption:** A widely used encryption algorithm that provides strong protection for data.
- **RTO (Recovery Time Objective):** The target amount of time within which a system or process must be restored after a disaster.
- **RPO (Recovery Point Objective):** The maximum acceptable amount of data loss measured in time, such as minutes or hours.
- **Compliance Audits:** Evaluations conducted to ensure that backup systems and processes comply with external regulatory requirements.