Audit Program: Detailed Test Procedures for Compliance Verification

---

Test ID: T001

- **Related Control ID:** C001
- **Test Objective:** Verify that access controls are implemented to restrict unauthorized access to sensitive data.
- **Detailed Test Steps:**
  1. Review the access control policy document (Reference: doc_0_PI_pages_21-25.txt, Page 22).
  2. Inspect user access logs for the past 6 months to ensure only authorized personnel have accessed sensitive systems.
  3. Conduct interviews with system administrators to confirm the implementation of role-based access controls.
  4. Perform a sample test by attempting to access restricted systems with unauthorized credentials.
- **Expected Results:**
  - Access logs show no unauthorized access attempts.
  - System administrators confirm the use of role-based access controls.
  - Unauthorized access attempts are blocked.
- **Evidence Requirements:**
  - Access control policy document.
  - Access logs for the past 6 months.
  - Interview notes with system administrators.

Test ID: T002

- **Related Control ID:** C002
- **Test Objective:** Ensure that data encryption is applied to all sensitive data in transit and at rest.
- **Detailed Test Steps:**
  1. Review the data encryption policy (Reference: doc_0_PI_pages_101-105.txt, Page 102).
  2. Inspect system configurations to verify encryption protocols (e.g., TLS 1.2 or higher) are enabled.
  3. Perform a sample test by transferring sensitive data between systems and verifying encryption.
  4. Review encryption key management procedures to ensure keys are securely stored and rotated.
- **Expected Results:**
  - Encryption protocols are enabled and configured correctly.
  - Sensitive data is encrypted during transfer and storage.
  - Encryption keys are managed securely.
- **Evidence Requirements:**
  - Data encryption policy.
  - System configuration screenshots.
  - Sample test results of data transfer.
  - Encryption key management documentation.

Test ID: T003

- **Related Control ID:** C003

- **Test Objective:** Confirm that incident response procedures are documented and tested regularly.
- **Detailed Test Steps:**
  1. Review the incident response plan (Reference: doc_0_PI_pages_66-70.txt, Page 67).
  2. Inspect records of incident response drills conducted in the past 12 months.
  3. Interview the incident response team to confirm their roles and responsibilities.
  4. Verify that incident reports are documented and reviewed by management.
- **Expected Results:**
  - Incident response plan is up-to-date and comprehensive.
  - Incident response drills have been conducted as scheduled.
  - Incident reports are documented and reviewed.
- **Evidence Requirements:**
  - Incident response plan.
  - Records of incident response drills.
  - Interview notes with the incident response team.
  - Sample incident reports.

Test ID: T004

- **Related Control ID:** C004
- **Test Objective:** Validate that regular backups are performed and tested for critical systems.
- **Detailed Test Steps:**

1. Review the backup policy (Reference: doc_2_PIII_pages_1-5.txt, Page 2).
2. Inspect backup logs for the past 3 months to confirm backups are performed as scheduled.
3. Perform a sample test by restoring data from a recent backup to verify integrity.
4. Review backup storage locations to ensure they are secure and offsite.

- **Expected Results:**
  - Backup logs confirm regular backups are performed.
  - Data restoration test is successful.
  - Backup storage locations are secure and compliant with policy.
- **Evidence Requirements:**
  - Backup policy.
  - Backup logs for the past 3 months.
  - Data restoration test results.
  - Backup storage location documentation.

Test ID: T005

- **Related Control ID:** C005
- **Test Objective:** Ensure that employee training on security policies is conducted annually.
- **Detailed Test Steps:**
  1. Review the employee training policy (Reference: doc_1_PII_pages_21-25.txt, Page 22).
  2. Inspect training records for the past year to confirm attendance.

3. Conduct interviews with employees to verify understanding of security policies.

4. Review training materials to ensure they are up-to-date and comprehensive.

- **Expected Results:**
  - Training records show 100% attendance for the past year.
  - Employees demonstrate understanding of security policies.
  - Training materials are current and relevant.
- **Evidence Requirements:**
  - Employee training policy.
  - Training attendance records.
  - Interview notes with employees.
  - Training materials.

This audit program provides detailed test procedures for each control, ensuring compliance with policy requirements and traceability to source documents.