COMPLIANCE AI

Date: 2026-01-16

AUDIT CERTIFICATE

STANDARD: ISO 27001

Source File: Acceptable_Use_Policy.pdf

SECTION 1: EXECUTIVE SUMMARY
This Acceptable Use Policy is designed to safeguard [agency name] from unauthorized access and illegal activities, thereby aligning with best practices for data protection and information security management as outlined in ISO 27001. Compliance with this policy helps ensure a secure and reliable operational environment for all users accessing the agency's information systems.

SECTION 2: COMPLIANCE CHECKLIST
- **Requirement 1:** Clearly defined acceptable and unacceptable use of IT resources - [PASS]
- **Requirement 2:** Regular auditing and monitoring of IT resources - [PASS]
- **Requirement 3:** Implementation of incident management procedures - [FAIL]
- **Requirement 4:** Employee training and awareness regarding information security policies - [FAIL]

SECTION 3: CRITICAL GAPS (Citations Required)
1. **CFR 164.308(a)(5)(ii)(B)** ? Absence of a clear incident management procedure is identified as a deficiency, as there is no detailed process for reporting and responding to security incidents mentioned.
2. **ISO 27001: A.7.2.2** ? The policy lacks a comprehensive employee training plan to ensure all employees are aware of the policy and its implications, which is critical for compliance.

SECTION 4: REMEDIATION PLAN
- Develop and implement a detailed incident management procedure, outlining the steps to be taken when a security incident occurs, including reporting protocols.
- Establish an employee training program that covers information security policies, including the Acceptable Use Policy and incident response, to ensure understanding and compliance among all staff.
- Include regular reviews and refresher training sessions in the training program to keep employees updated on changes in policies and threats.

SECTION 5: OFFICIAL SCORE

75

Authorized Signature