AUDIT CERTIFICATE

STANDARD: NIST 800-171 REV 2

Source File: Acceptable_Use_Policy.pdf

SECTION 1: EXECUTIVE SUMMARY
The Acceptable Use Policy (AUP) serves as a critical guide for maintaining security and proper usage of agency-owned systems. It outlines the responsibilities of employees and the agency's commitment to safeguarding information assets against misuse.

SECTION 2: COMPLIANCE CHECKLIST
1. **Access Control**: Ensure that access to information systems is limited to authorized users only. [PASS]
2. **Incident Response**: Define procedures for detecting, reporting, and responding to security incidents. [FAIL]
3. **Media Protection**: Use encryption to protect sensitive information from unauthorized access. [PASS]
4. **User Training**: Ensure all employees receive security awareness training on acceptable usage. [FAIL]

SECTION 3: CRITICAL GAPS (Citations Required)
1. **Incident Response**: The policy lacks explicit procedures for incident detection, reporting, and responses as required under **NIST 800-171 Rev 2, 3.6.1**.
2. **User Training**: There is no mention of mandatory security training for employees regarding acceptable use and associated policies as outlined in **NIST 800-171 Rev 2, 3.2.2**.

SECTION 4: REMEDIATION PLAN
- Develop and implement a comprehensive incident response plan that includes detection, reporting, and mitigation procedures.
- Include mandatory security awareness training for all employees, focusing on acceptable use and the specific policies that pertain to data security and user responsibilities.

SECTION 5: OFFICIAL SCORE
75

Authorized Signature