AUDIT CERTIFICATE

STANDARD: NIST 800-171 REV 2

Source File: Acceptable_Use_Policy.pdf

SECTION 1: EXECUTIVE SUMMARY
The Acceptable Use Policy outlines the parameters for appropriate use of IT resources at [agency name], emphasizing the protection of sensitive information and the responsibility of users. Compliance with such policies is critical in maintaining the integrity of sensitive data and ensuring adherence to NIST 800-171 Rev 2 guidelines.

SECTION 2: COMPLIANCE CHECKLIST
- **Access Control (3.1.1)**: The policy mentions monitoring and password security. **[PASS]**
- **Media Protection (3.7.1)**: The policy encourages encryption for sensitive information. **[PASS]**
- **Incident Response (3.6.1)**: The policy outlines actions for unauthorized activities and violations, but lacks explicit incident response processes. **[FAIL]**
- **Awareness and Training (3.2.1)**: The policy notes user responsibility but does not reference a formal awareness or training program. **[FAIL]**

SECTION 3: CRITICAL GAPS (Citations Required)
1. The policy lacks a detailed incident response plan as required by **NIST 3.6.1**. A formal response process should be established to guide employees during security incidents.
2. There is no reference to user awareness or training initiatives as stipulated in **NIST 3.2.1**. A structured training program must be implemented to ensure that users are aware of their responsibilities and the policy's requirements.

SECTION 4: REMEDIATION PLAN
- Establish a formal incident response plan that outlines procedures for identifying, responding to, and documenting security incidents.
- Develop and implement a user awareness and training program that instructs employees on security best practices, acceptable use, and the importance of compliance with NIST 800-171 Rev 2.

SECTION 5: OFFICIAL SCORE

75

Authorized Signature