COMPLIANCE AUDIT CERTIFICATE

Generated by Compliance AI | Date: 2026-01-16

Source Document: Acceptable_Use_Policy.pdf

Standard: NIST SP 800-171 Rev 2

NIST 800-171 COMPLIANCE AUDIT REPORT

1. EXECUTIVE SUMMARY
This audit report evaluates the Acceptable Use Policy (AUP) of [Agency Name] against the standards set forth by NIST SP 800-171. The review focuses on areas such as the purpose, scope, policy declarations, user responsibilities, and any accompanying guidelines. Ultimately, this compliance audit aims to identify both compliant areas and any gaps requiring remediation to enhance the organization's security posture and ensure protection of Controlled Unclassified Information (CUI).

2. COMPLIANT AREAS (Pass)
- **Policy Overview and Purpose**: The policy includes a clearly defined overview and purpose that addresses the need for protecting both the employees and organization from damaging actions. It emphasizes the importance of an open culture built on trust and integrity.
- **Scope**: The policy scope is comprehensive, covering all employees, contractors, consultants, and any personnel interacting with agency systems. This includes mention of third parties accessing sensitive information, aligning with NIST guidance.
- **General Use and Ownership**: Clear ownership statements and user responsibilities are outlined, emphasizing that all data created on agency systems remain the property of [Agency Name].
- **User Accountability**: The policy mandates employees to exercise good judgement and provides mechanisms for monitoring and auditing, which support due diligence in protecting agency data.
- **Unacceptable Use Section**: A detailed list of unacceptable activities helps set clear boundaries on acceptable and unauthorized actions, including strong stipulations against illegal behavior.

3. GAPS DETECTED (Fail)
- **Lack of Training Requirement**: The AUP does not require formal training or acknowledgment from users regarding the policy. Regular training on acceptable use and security best practices should be included.
- **Insufficient Encryption Guidelines**: While the policy mentions encryption for sensitive information, it lacks detailed guidelines on how and when to apply encryption across all data classifications.
- **Password Security Details**: The policy refers to a separate Password Policy but lacks specific requirements applicable to this acceptable use context. There should be explicit rules governing password

complexity, expiration, and management.
- **Inadequate Incident Response**: There are no detailed provisions for reporting policy violations or security incidents. A clear incident response plan should be integrated into the AUP.
- **Not Mentioning Remote Work Security**: Given the increase in remote work, the policy does not address the acceptable use of agency systems in a remote work environment or requirements for secure connections.

4. REMEDIATION STEPS
1. **Implement Mandatory User Training**: Require all employees to undergo training on the Acceptable Use Policy and security best practices annually, with records of completion.
2. **Develop Detailed Encryption Guidelines**: Create specific guidelines and procedures for encryption based on data sensitivity levels, ensuring all employees understand when and how to encrypt data.
3. **Update Password Security Requirements**: Integrate explicit password management requirements directly within the AUP, including complexity, refresh cycles, and storage.
4. **Establish Incident Response Procedures**: Add a section outlining the steps for reporting violations and an internal response strategy for addressing security incidents or breaches.
5. **Include Remote Work Policies**: Formulate and append remote work protocols, specifying acceptable use of agency resources and required security measures for remote access.

5. FINAL SCORE (0-100)
Score: 70/100

This score reflects strong compliance in several foundational areas, but identifies significant gaps that necessitate immediate action for enhancing security and compliance with NIST 800-171. Addressing these gaps will enhance the effectiveness of the Acceptable Use Policy and fulfill the organization?s responsibility for safeguarding sensitive information.