COMPLIANCE AI

Date: 2026-01-16

AUDIT CERTIFICATE

STANDARD: OSHA GENERAL INDUSTRY

Source File: Acceptable_Use_Policy.pdf

SECTION 1: EXECUTIVE SUMMARY
The Acceptable Use Policy aligns with fundamental compliance principles intended to safeguard workplace security and integrity at [agency name]. It is essential for preventing illegal or damaging actions that could compromise employee and organizational safety.

SECTION 2: COMPLIANCE CHECKLIST
- Requirement 1: Ensure all electronic resources are monitored for security and compliance. [PASS]
- Requirement 2: Prohibit unauthorized access to sensitive information. [PASS]
- Requirement 3: Clearly outline penalties for violation of computer usage policies. [PASS]
- Requirement 4: Implement proper training for employees on acceptable use of IT resources. [FAIL]

SECTION 3: CRITICAL GAPS (Citations Required)
- Lack of specific training requirements for employees on acceptable use of IT resources. This is a violation of *OSHA 1910.132(f)*, which mandates that employers provide training to their employees on personal protective equipment and safety practices, extending to cybersecurity training to avoid workplace hazards.
- Absence of a clear incident reporting mechanism for breaches or misuse of network systems, as suggested by *OSHA 1910.1030(c)* on exposure control plans, which should include protocols for addressing potential breaches.

SECTION 4: REMEDIATION PLAN
- Develop and implement mandatory training programs focusing on acceptable use, emphasizing employee roles and responsibilities.
- Establish a clear incident reporting procedure for employees to report cybersecurity incidents or violations of the Acceptable Use Policy.
- Periodically review and update the policy to ensure continued compliance with OSHA requirements and advancements in cybersecurity practices.
- Ensure documentation of training sessions and attendance is maintained for compliance

verification.

SECTION 5: OFFICIAL SCORE

85

Authorized Signature