State of Iowa Department of Corrections

Policy and Procedures

Policy Number: IO-SC-26
Applicability: Instituions
Policy Code: Public Access
Iowa Code Reference: N/A
Chapter 3: ADMINISTRATION & MANAGEMENT
Sub Chapter: SECURITY & CONTROL
Related Doc Policies: N/A
Administrative Code Reference: N/A
Subject: INSTITUTIONAL SECURITY AUDITS
PREA Standards: N/A
Responsibility: Nick Lamb
Effective Date: February 2024
Authority:

1. PURPOSE

To establish a framework for and provide guidelines for the development of an Iowa Department of Corrections (IDOC) security audit program.

2. POLICY

It is the policy of the IDOC to maintain a high level of safety and control by achieving compliance with security standards. This policy sets guidelines for auditing institutional operations against security standards that comply with IDOC policy.

CONTENTS

3. DEFINITIONS – As used in this document:

A. Security Audit – Review of institutional security operations by a Security Audit Team to ensure that the IDOC institutions are safe and secure and comply with established security standards.

B. Security Audit Coordinator – A member of the audit team designated by a Deputy Director to coordinate auditing activities.

C. Security Audit Instrument – A document that assists Security Auditors during an audit by setting expectations and standards, relating issues to specific policy statements, measuring sound correctional practices, and allows for documentation of findings.

D. Security Auditor – An IDOC employee trained in conducting security audits who participates in an IDOC security audit.

E. Audit – An examination of institution policies, records, accounts, and practices to determine compliance with standards. It is conducted by a team of Security Auditors.

F. Security Standard – An operating requirement that establishes required security practices. Standards are derived from policy and procedures or mutually accepted practices in the profession.

G. Standard Variance – Exemption from a specific standard or policy required by IDOC.

H. Internal Audit – An internal examination of institution policies, records, accounts and practices to check their accuracy and offer corrective plans to meet the audit standards. The make-up should be internal persons assigned to the institution.

4. PROCEDURES

A. Audit Philosophy and Goals are intended to:

1. Develop consistent standard security and operating practices, equipment, policies and procedures.

2. Provide a structured process to continuously improve security at each institution.

3. Provide operating standards at each institution to improve compliance with IDOC policy.

4. Provide a forum for constructive peer interaction among corrections professionals searching for more effective and efficient operating security programs.

5. Provide a pathway for the expression of ideas that improve security operations and IDOC policy and procedures.

B. Audit Schedule

1. The Security Audit Coordinator shall notify institutions and auditors in advance of the audit schedule and provide a published audit schedule. Institutions shall conduct an internal audit prior to the formal audit.

2. A room shall be made available to the team at the audit site. Staff shall be assigned to facilitate audit team access to any/all areas of the institution and to answer specific operational questions. The audit team shall be at the institution site for a period of time required to conduct the audit.

3. Institutions shall be audited once annually by an external security audit team.

4. At least annually, the Audit Team shall review the auditing guidelines taking into consideration input from institutional administrators, policy changes, and any recently accepted practices in the profession and make recommendations for revision to the Deputy Director of Institution Operations.

C. Audit Areas

The following areas focus on the development of a standard security program:

1. Incarcerated Indvidual Count

2. Key Control

3. Tool Control

4. Armory/Arsenal and Security Equipment

5. Post Orders

6. Perimeter Security
7. Incarcerated Indvidual Visiting
8. Entrance Procedures/Operations
9. Control Movement
10. Use of Force
11. Incarcerated Indvidual Transport
12. Segregation (Special Management/Housing)
13. Admission and Discharge
14. Control Center(s)
15. Searches
16. Contraband Control
17. Physical Plant
18. Blood Borne Pathogen Precautions
19. Audit of the General Emergency Plan
20. Security Inspections
21. Fire Safety
22. Hazardous Material Management

D. Audit Reporting

1. Initial Audit Report – The audit report shall be compiled from the audit instrument and observations of the audit team. All audit findings shall be communicated to the administration during the exit briefing at the conclusion of the site visit. The written audit report shall be submitted to the Deputy Director of Institution Operations, Warden, and Associate Warden/Security within 45 days of the site visit.

2. Institution Action Plan – Within 60 days of receipt of the audit report, the institution shall evaluate discrepancies, recommend corrective action, and complete the IDOC action plan form provided by the Audit Team Coordinator. Should any issue be brought forward as a guideline variance, the report should indicate this in the final action plan.

3. Guideline variance requests are to be submitted to the respective Deputy Director of Institution Operations by the Warden for approval.

4. Follow-Up Review – The institution shall conduct a follow-up assessment to determine if corrective action taken for each discrepancy is achieving compliance with the applicable guideline. The Deputy Director of Institution Operations/designee shall follow-up on the final Security Audit Report/Summary Corrective Action Plan.

E. Qualifications of Audit Team Members

1. Generally, auditors shall be trained in security audit procedures by the National Institute of Corrections (NIC). The Director may authorize an exception for individuals with sufficient experience.

2. Auditors shall be experienced in security operations.

3. The Audit Team Leader shall be responsible for guidance and training for audit team members to ensure that auditors have the knowledge, skills and training in security audit philosophy, goals, the role of Security Auditors, the benefits of security auditing, and the overall process.

4. During the audit process new audit team members will be paired with an experienced audit team member.