

1.3.A.9 Facility Security Audits

I Policy Index:



Date Signed: 02/12/2020
Distribution: Public
Replaces Policy: N/A
Supersedes Policy Dated: 07/10/2018
Affected Units: All Institutions
Effective Date: 02/12/2020
Scheduled Revision Date: May 2021
Revision Number: 16
Office of Primary Responsibility: Director of Security and DOC Administration

II Policy:

To maintain a high level of safety and control within DOC institutions, the South Dakota Department of Corrections (DOC) will ensure security audits are conducted on a regular basis at all facilities housing inmates. The purpose of a security audit is to evaluate facility compliance with security-related policies, operational memorandums, directives and standards and to protect and maintain the safety and security of the facility, staff and inmates.

III Definitions:

Corrective Action Plan:

A plan of action by the Warden or designee to address deficiencies in security practices identified by the security audit team.

Director of Security:

DOC staff member responsible for overseeing security processes and compliance at all DOC institutions. This position is supervised by the Director of Prison Operations or designee.

Lead Auditor/Coordinator:

DOC staff trained as a security auditor or those with extensive knowledge of the areas to be audited. The auditor is responsible for directing the security audit. The auditor will act as the primary contact for the security audit team during the audit and delegate duties. The auditor will draft a report of the final audit findings and forward the draft report to the Director of Security.

Security Audit:

The examination, monitoring and verification of security policies and practices.

Security Audit Instrument:

A list of accepted standards that cite related practices or procedures required to be implemented. The instrument references the standard and applicable policies, operational memorandums, directives or post orders.

Security Audit Team:

Trained and qualified staff members responsible for evaluating security policies and procedures at DOC institutions. Will include team members from a facility not the subject of the current audit.

Security Drill/Simulation:

A simulated scenario to test the adequacy of plans, procedures, training and staff knowledge and ability to appropriately respond to a particular controlled scenario and appropriate use of available equipment and resources.

Security Standard:

An operational requirement that defines the requirements and expectations of the department. Standards shall be documented in policy, post orders, directives and operational memorandums and guide the implementation of the applied process. Standards shall be consistent with correctional best practices.

IV Procedures:

1. Security Standards/Security Audit Instrument:

- A. The Director of Security shall develop and maintain a list of security standards (security audit instrument) against which various components of security operations will be measured.
- B. The standards will be reviewed annually to ensure each measures the level of acceptability for each component of security operations to which the standard applies. The contents of the security audit instrument will change as new directives, policies and procedures are developed and approved or new security concerns identified.
- C. Standards shall be consistent with and support, the mission, vision and values of the DOC. Applied security standards align with the following:
 1. Department policies;
 2. Operational Memorandums (OMs);
 3. Accepted practices, procedures, directives and post orders;
 4. Standards, rules and laws, as applicable, i.e. American Correctional Association (ACA), National Commission on Correctional Health Care (NCCHC), South Dakota Codified Law, SD Administrative Rule; and
 5. Best security practices, as identified and defined by recognized professional resources and organizations.
- D. The security audit instrument may include applicable and current standards recommended by the National Institute of Corrections (NIC).
- E. The security audit instrument includes standards for each of the approved security categories.

2. Facility Security Audit Goals:

- A. The audit will assist each facility's administration in evaluating current practices in comparison to policy and directives to help the facility achieve the highest level of security and safety in the performance of its operations.
- B. To provide each facility with a measurement of compliance/adherence to specifically targeted DOC policies, security standards, operational memorandums (OMs), directives, post orders and best correctional practices.
- C. To determine whether resources are used in an effective and efficient manner.
- D. To provide a forum for constructive, pro-active, feedback, mentorship, support and training to staff at the facility and promote discussion amongst staff to help identify best practices that promote maintaining and enhancing overall safety and security.
- E. To heighten security awareness and proficiency.
- F. To provide professional development and training for members of the security audit team.
- G. To provide consistent and standardized methods of measuring and auditing institutional security practices.
- H. To identify weaknesses and deficiencies in security operations, to include identifying broken, missing, expired, or obsolete security equipment for replacement and provide recommendations on how to remedy the weakness or deficiency.
- I. To identify significant security problems or vulnerabilities that may lead to injuries, escape, disruption, or destruction of state property because of inadequacy of policy, procedure, practices, physical plant operations or staff performance. The audit will help identify each facility's strengths and weaknesses.

3. Qualifications and Selection of the Security Audit Team:

- A. The security audit team will be experienced in the following areas:
 - 1. Knowledge of security practices and security equipment;
 - 2. Experience at a supervisory level within the DOC to affect change;
 - 3. Knowledge of DOC policies, practices and procedures;
 - 4. Knowledge of safety and security equipment, gear and hardware issued to security staff and located at the facility;
 - 5. Experience in communicating with staff on a professional level; and
 - 6. An understanding of the importance of safety and security within a correctional facility and the process of using a combination of supervision, inspection, staff accountability and clear policy and directives guide and promote safety and security best practices.

- B. Lead auditors/coordinators will have developed leadership skills, the ability to delegate duties, organization skills and experience and expertise in correctional security. Lead auditors/coordinators are selected by the Director of Security.

4. Security Audit Team Training:

- A. Because the validity and effectiveness of a security audit is in direct proportion to the knowledge and skill of the auditors, security audit team members may be required to attend audit-related training.
- B. Staff will participate in a minimum of one (1) facility security audit prior to participating in an audit as a security audit team member.
- C. Training will include information on the purpose of the security audit, roles and duties of security auditors and benefits to the facility and staff. Additional topics may include:
 - 1. An overview of the auditing protocol;
 - 2. Steps for successfully conducting a systematic review of a facility, its operations and equipment;
 - 3. Focus points and tips for engaging in professional communication with fellow staff members and administrators; and
 - 4. Knowledge, comprehension and familiarity with applicable DOC policies, facility OMs and security standards.
- D. Classroom training may be enhanced with opportunities for hands-on experience (job shadowing).
- E. Security audit team members must participate in at least one (1) audit each year to maintain their place on the team.

5. Facility Security Audit Schedule:

- A. The Department will conduct regular, scheduled audits of practices within DOC facilities. A schedule of facility security audits will be developed by the Director of Security annually. The schedule will be communicated to the Secretary of Corrections, Director of Prison Operations and Policy and Compliance Manager.
- B. The audit schedule will include the dates and location of each scheduled audit. Wardens must be notified of the audit at least thirty (30) days in advance of the audit.
- C. The duration of the audit is determined by the size of the facility, custody levels of the facility, complexity of operations, number of inmates and security standards included in the audit.
- D. The DOC may contract with trained security auditors from outside the DOC to bring additional expertise to the audit process from a broader experience base, provide a neutral and outside review of the facility security and safety processes, and to enhance the training and audit experience of SD DOC audit team members.
- E. At the direction from the Director of Prison Operations, unannounced audits of a facility may be scheduled and organized by the Director of Security.

6. Facility Security Audit Preparation:

- A. The Warden of the facility or satellite facility to be audited will be provided with a complete list of the security audit team members in advance of the audit.
- B. It is the responsibility of the Warden or designee to notify the Director of Security of any issues or events at the facility that may impact the efficiency and effectiveness of the audit.
- C. The Director of Prison Operations and/or Warden may submit a list of policies or procedures to the Director of Security to include in the list of standards to be audited during the facility security audit.
- D. The Warden or designee will ensure the security audit team members have access to:
 - 1. A designated, private work area with a computer and/or internet access.
 - 2. Access to facility staff to assist with accessing all areas of the facility.
 - 3. Access to facility OMs, post orders, the facility emergency response manual (ERM), reports and inspection results of other agencies tasked with measuring compliance of equipment or practices that are also being audited during the security audit.
- E. The audit team will schedule a “pre-audit briefing” with the Warden and staff designated by the Warden. The pre-audit will include the following:
 - 1. Introduction of audit team members;
 - 2. Introduction of facility staff who will assist with the audit and senior staff/supervisors, including the primary contact person;
 - 3. Brief overview of the audit process and goals;
 - 4. Tentative time schedule/plan;
 - 5. Opportunity for the Warden or designee to request special attention by the audit team to specific areas, processes or procedures and to ask questions;
 - 6. A pre-audit tour of the facility, as requested; and
 - 7. Identify and request access to any specific records, documents personnel and areas initially required to complete the audit.
- F. The Secretary of Corrections, Director of Prison Operations, Warden or designee may provide pre-audit input to the Director of Security regarding the development and/or inclusion of audit standards to measure specific areas, processes or procedures related to the organization of a facility.

7. Security System Checks:

- A. The Director of Security may schedule and conduct a security system check/security drill during the audit, with prior approval from the Director of Prison Operations, and if applicable, the Warden. The purpose of the security system check is to help the audit team identify areas of risk and vulnerability and suggest improvements if deficiencies are identified. The Warden will be notified in advance of a security system check.

- B. Security system checks will not be conducted in a manner that may expose staff or inmates to risk, harm, injury or directly jeopardize institutional safety and security. Checks will measure compliance with a safety and/or security procedure/policy.
- C. The following factors will be considered when scheduling a security system check:
 - 1. Pre-identification of the system(s), process(s), procedure(s), staff response(s) or equipment to be tested/audited.
 - 2. The number of staff who should participate, and the staffing posts represented or affected by the security check.
 - 3. Any staff that requires advance notice.
 - 4. Any safeguards that must in place prior to conducting the security check.
 - 5. Any specific instructions or information that will be provided to staff prior to or during the security check.
 - 6. The estimated duration of the check and how and when the check will be terminated.
 - 7. Schedule and agenda items to share with staff following the security check (debriefing) and list of staff who should attend the debriefing.

8. Facility Security Audit Results:

- A. An out-briefing will be scheduled by the security audit team/lead auditor at the conclusion of the audit. The time and location should be briefed with the Warden.
- B. The audit team will discuss preliminary audit findings.
 - 1. The out-briefing will typically include the Director of Security, members of the security audit team, the Warden and facility staff identified by the Warden.
 - 2. The out-briefing will include a summary of the significant findings of the security audit team and is not intended to be inclusive of all findings or security audit standards audited by the team. The briefing shall include standards that require corrective action and standards found to be in compliance.
 - 3. Non-compliant standards that may jeopardize safety, or security require prompt corrective action and will be included within the out-briefing or reported to the Warden directly following the audit. The Director of Prison Operations should receive a copy of those issues requiring corrective action.
- C. A full audit report containing an inclusive list of all security audit standards measured during the audit will be compiled by the lead auditor/coordinator from the security audit instruments assigned to each security audit team member and will include the observations, comments and recommended corrective action.
 - 1. The final security audit report will be completed by the Director of Security within 4 weeks of the conclusion of the audit and shall be forwarded to the DOC Policy and Compliance Manager, Director of Prison Operations and Warden by the Director of Security. The report will include staff's knowledge of the standards and responses to questions asked. The report will include documentation whether staff are following policy and procedures.

2. Within thirty (30) days of receipt of the final security audit report from the Director of Security, the Warden or designee will provide a response to the Director of Security addressing each deficiency or recommendation identified in the security audit report, to include recommended corrective action for each identified deficiency. The Director of Security shall forward the response to the Director of Prison Operations and Policy and Compliance Manager.
 3. If numerous and/or serious deficiencies are revealed by an audit, the procedures/policies may be re-audited within three (3) months of the original audit.
- D. Security audit reports/results contain information pertaining to the protection and security of the institution, staff, offenders, and public and may include unique areas of vulnerability identified through the audit process and/or specific response plans intended to prevent or mitigate criminal acts, emergency management and/or staff response to an emergency or critical incident and are considered confidential.
1. Unauthorized disclosure of security audit reports/results, in whole or in part, may compromise the security of critical systems or create a substantial likelihood of endangering public safety and is prohibited by policy.
 2. Security sensitive information is exempt from public inspection (See SDCL § [1-27-1.5](#)).
 3. The Director of Security will maintain all documents/reports relative to the security audit for three (3) years. Documentation will include the list of security audit standards measured, the security audit report and the corrective action plan from the Warden in response issues identified as requiring a corrective response.

V Related Directives:

SDCL § [1-27-1.5](#).

VI Revision Log:

May 2002: New Policy.

Removed revisions from June 2004 to May 2009.

May 2010: Revised formatting of Section 1.

July 2011: Added "Lieutenant (SDWP) to definition of Security Audit Coordinator. Deleted "the" Replaced with "designated" and "staff" Deleted "from" and Replaced with "identified in" Added "The security audit coordinator will forward the written response to the Policy and Compliance Manager and Director of Prison Operations". to Section 6. B. 2.

June 2012: Deleted "Non-Public" and Replaced with "Public" Deleted "Security Audit Coordinator" and Replaced with "Director of Security" in definitions and throughout the policy. Added operational memorandums (OMs) and directives/post orders to Section 1 B. Deleted "and remains in the this position until a replacement is appointed" in Section 2 C. Deleted "facilities" and Replaced with "the Warden" in Section 5 A. & B. Added "facility OMs" in Section 5 C. Deleted "recommendations" and Replaced with "explanation that may be required regarding a deficiency" in Section 6. B. 2.

May 2013: Deleted "A senior level DOC security staff member (normally a captain, major or lieutenant (SDWP) and Replaced with "DOC staff member under the supervision of the Director of Prison Operations" in definition of Director of Security.

May 2014: Changed title from "Facility" to "Adult Facility" Added "Director of Security" to Office of Primary Responsibility. Deleted "Security Auditor" and Replaced with "Security Audit Team". Deleted "Standards Variance" definition. Added definition of "Security Audit" Added "and application of accepted Security Standards" to Section 1 B. Added "and training" to Section 1 D. Deleted "operational" and "equipment" and Added "standards" in Section 1 F. Added G. to Section 1. Added 1-5 to Section 2 A. Deleted "security management" and Deleted "and are identified on the annual audit schedule" and Replaced with "and Warden or his/her designee" in Section 2 B. Deleted C. "The

Director of Security is appointed by the Director of Prison Operations". **Deleted** "for staff new to the process" and **Replaced** with "in the accepted methods of auditing security standards" in Section 3 A. **Added** 1-5 to Section 3 B. **Added** "and the Director of Prison Operations, Policy and Compliance Manager and" in Section 4 A. **Added** "advance" and **Added** "to the Director of Prison Operations, Policy and Compliance Manager and Wardens" in Section 4 C. **Added** "and director notification provided by the Director of Security" in Section 5 A. **Deleted** "Facilities" and **Replaced** with "the Warden or his/her designee" in Section 5 C. **Deleted** "designated facility staff will provide a written response" and **Replaced** with "lead auditor/coordinator or other staff member designated by the Warden will provide written response" **Deleted** D. in Section 5. **Added** "The response will include a status report on the deficiency and any explanation required" **Deleted** "security audit coordinator" and **Replaced** with "Director of Security" in Section 6 B. 2. **Added** "and Director of Security" and **Deleted** "an after-action plan report, which incorporates results" and **Replaced** with "all documents relative to the security audit included a list of the audit items" in Section 6 C. **Deleted** 1. and 2. in Section 6 C. regarding standard variance requests.

May 2015: Minor grammar changes.

May 2016: **Revised** policy statement. **Added** definition of "Security System Check" **Added** new Section 1. **Added** "targeted" in Section 2 b. **Added** G. to Section 2. **Added** "ability to communicate on a professional level with staff" to Section 3 A. 5. **Added** 4. to Section 3. A. **Added** 6. to Section 3 A. **Deleted** "and/or the Director of Prison Operations" in Section 3 B. **Deleted** "accomplish an audit" and **Replaced** with "conduct a systemic review of facilities, operations, and equipment" in Section 4 B. 2. **Added** "annually" to Section 5 A. **Added** "Secretary of Corrections and Added "audit team members" and **Added** "Each facility should be audited at least annually." in Section 5 A. **Added** a. to Section 5 B. 1. **Added** D. E. and F. to Section 5. **Added** "Emergency Response manual" in Section 6 C. **Added** new C. and E. F. to Section 6. **Added** new Section 7. **Added** 3. to Section 8 A. **Added** "will be compiled by the lead auditor/coordinator from the security audit instruments assigned to each facility auditor" in Section 8 B. **Added** "will be completed by the Director of Security within 2-4 weeks of the facility audit" in Section 8 B. 1. **Added** D. to Section 8.

May 2017: **Reviewed** with no changes.

May 2018: Minor language and structure changes.

May 2019: Changes to the policy.

Mike Leidholt (original signature on file)

Mike Leidholt, Secretary of Corrections

02/12/2020

Date