Minnesota Department of Corrections

Policy:	**600.600**	**Title: Security/Compliance Audit**
Issue Date:	**8/5/14**	
Effective Date:	**8/19/14**	

AUTHORITY: Minn. Stat. §241.021

PURPOSE: To ensure compliance with department policies and procedures, and ensure that confinement and security of offenders housed provide for basic safety, health, statutory, and constitutional standards while ensuring the protection of the public.

APPLICABILITY: Minnesota Department of Corrections (DOC); all Minnesota correctional facilities (MCFs)

POLICY: The department security audit coordinator ensures regular security/compliance audits of all MCFs as outlined below. Security/compliance audit reports are for internal department use only, and are not released to the public or used as the foundation for employee discipline. Results and written reports of security/compliance audits are considered confidential due to the security-sensitive information contained in them, see Position Statement – Security Audits (attached).

Security/compliance audits are conducted by experienced staff to ensure public safety and to maintain safe and secure living and work environments for staff and offenders. The goal of security/compliance audits and subsequent follow up is to proactively enhance security practices, institute sound correctional practices, and consistently integrate department-wide security issues.

DEFINITIONS:

Security/compliance audit standards - a list of expected MCFs conditions/outcomes which security auditors examine during the security/compliance audit process. Security/compliance audit standards cover the following topics:

1. Incident command
   - 1.01 Incident command system (ICS)
   - 1.02 Use of force
   - 1.03 Emergency plans
   - 1.04 Emergency response teams
   - 1.05 Canine

2. Physical plant management
   - 2.01 Emergency power
   - 2.02 Physical plant
   - 2.03 Vehicle maintenance
   - 2.04 Maintenance/grounds maintenance

3. Facility management
   - 3.01 Facility atmosphere
   - 3.01a Staff/offender communication
   - 3.02 Mailroom
   - 3.03 Electronic/computer security
   - 3.04 Property control

3.04b Canteen
3.05 Food services
3.06 Post orders
3.07 Logs
3.08 Training
3.09 Administrative inspections
3.10 Office of special investigations (OSI)/security threat groups (STG)
3.11 Facility intake/reception

4. Perimeter management
4.01 Perimeter security
4.02 Lighting
4.03a Access points - main entrances
4.03b Access points - secondary/emergency
4.03c Access points - vehicle gates
4.04 Tunnels
4.05 Master control/control centers
4.06 Transportation - offenders
4.07 Trash/refuse removal

5. Operational security management
5.01 Tool control
5.02 Access control devices (key control)
5.03 Weapons control/security equipment
5.04 Electronic communication equipment
5.05 Contraband control/searches and shakedowns/offender drug testing
5.05a Discipline/due process
5.06 Uniforms
5.07 Medical services/pharmacy
5.08 Security inspections
5.09 Camera systems

6. Offender management
6.01 Counts
6.02 Living units
6.02a Special management
6.02b Segregation
6.03 Telephone security
6.04 Visiting
6.05 Recreation/gym/recreation yard
6.06 Offender movement
6.07 Religious resource/volunteers
6.08 Offender work assignment

7. Environmental, health, safety management
7.01 General employee safety
7.02 Safety - fire prevention
7.03 Safety - PPE
7.04 Safety - respiratory protection
7.05 Safety - lockout/tagout

7.06 Safety - fall prevention
7.07 Safety - confined spaces
7.08 Safety - hazardous waste management
7.09 Training

8. Health services

9. Administration and management
9.01 General administration
9.02 Fiscal management
9.03 Personnel management
9.04 Information systems
9.05 Offender programming and case management
9.06 Records and case records

Security audit coordinator – DOC staff member that coordinates all security audit activities for the department.

PROCEDURES:

A. The department security audit coordinator:
1. Maintains, reviews, and updates security/compliance audit standards;
2. Selects, trains, and schedules security/compliance auditors;
3. Schedules MCF security/compliance audits;
4. Serves as on-site manager of MCF security/compliance audits;
5. Coordinates preparation/submission of security/compliance audit final reports;
6. Records, files, maintains, and distributes all security/compliance audit reports to appropriate department authorities; and
7. Maintains and reviews prior facility audits to ensure previously cited deficiencies have been resolved, and documents any recurring issues.

B. Auditor selection/training - the department security audit coordinator, in cooperation with facility wardens, selects appropriate personnel to serve as security/compliance auditors. The security audit coordinator pairs a new security/compliance auditor with an experienced security/compliance auditor for his/her first audit.

C. Audit scheduling
1. The department security audit coordinator maintains a schedule for regular MCF security/compliance audits so that each MCF undergoes a security/compliance audit at least once every four years.

2. The department security audit coordinator, in conjunction with the facility warden, must set the date(s) for the security/compliance audit to occur.

3. The department security audit coordinator determines the necessary size of the audit team and the length of the security/compliance audit based on:
a) Size of facility;
b) Complexity of facility operations/industries/programming;
c) Facility security level; and
d) Any anticipated concerns/issues.

4. The department security audit coordinator arranges for auditors to perform the audit, assigning auditors responsibility for specific security/compliance standard chapters.

D. Pre-audit preparations

1. Based on the make-up of the audit team for any particular facility audit, the department security audit coordinator conducts a pre-audit meeting with the audit team, performs introductions, and briefs the auditors on the upcoming audit, including audit schedule and any special considerations related to the facility being audited. The meeting may include an informational presentation by a representative from the facility being audited.

2. Audit team members must become familiarized with assigned chapter(s) of security/compliance audit standards and all relevant policy/directives/instructions.

E. Conducting the audit

1. The audit team and the department security audit coordinator assemble at the facility to be audited.

2. The facility must provide a room for auditors to use as a base of operations during the audit. The room must include a phone and computer(s) with access to the network. The department security audit coordinator must meet with the team and discuss any pertinent information before the audit. The facility liaison to the team may make introductory remarks regarding current facility status and special concerns.

3. The audit team must meet with the facility executive staff and perform introductions.

4. The audit team must tour the facility in order to become familiarized with the facility geography, staff, programming, and industries.

5. After the facility tour, the auditors informally move through the facility, assessing areas as assigned. Auditors inspect all appropriate areas, shifts, and staff. Auditors interview offenders as needed.

6. Auditors review findings and corrective actions from the previous audit, and re-check during the current audit to ensure previous recommendations were implemented.

7. Auditors must regularly debrief with the audit team and department security audit coordinator, sharing observations and discussing concerns. Auditors may return to areas as necessary to follow up on issues or concerns. The audit team sets up/observes several ICS drill responses.

8. The department security audit coordinator monitors the ongoing progress of the audit to ensure timely completion of the audit schedule.

9. If any critical issues or findings arise during the audit, the department security audit coordinator must coordinate with facility executive staff to ensure appropriate immediate response.

10. The auditors must discuss preliminary audit findings with team members and the department security audit coordinator.

11. At the conclusion of the audit, the auditors present a general summary of audit findings to the facility executive staff. The facility warden must determine what facility staff may attend this presentation.

F. Post-audit activities

1. The department security audit coordinator must coordinate with audit team members to compose a preliminary final draft of the audit report.

2. The department security audit coordinator must prepare a final draft of the facility security/compliance audit report and forwards this report to the warden, deputy commissioner - facility services, and assistant commissioner - facility services for review within 21 days of receipt of the auditor reports.

3. The security audit coordinator receives the facility's responses to the audit report, typically within 45-60 days of receipt of the final report. Dates are specified in the cover letter to the facility warden. The security audit coordinator then prepares responses for review by the assistant commissioner-facility services and the deputy commissioner-facility services within 21 days of receipt of the facility response.

G. Follow-up audit

1. Approximately six months after the facility's security/compliance audit, the department security audit coordinator must review compliance and response documents and schedule a one-day follow-up audit of the facility, if deemed necessary. The audit team reviews the audit report, tours the facility, and examines areas of concern, noting the current condition of issues identified in the audit report. The audit team must meet with the facility executive staff and present the latest findings.

2. The department security audit coordinator must report findings from the follow-up audit to the deputy commissioner - facility services and assistant commissioner - facility services for review.

INTERNAL CONTROLS:

A. The security audit coordinator collects and electronically maintains the official documentation of the security audit schedule, and all reports that are generated for the security audit program.

B. Security audits are completed at least once every four years at each MCF.

C. Unresolved issues from previous audits are documented in all future audits.

REVIEW: Annually

REFERENCES: Policy 100.200, "Accreditation."
ACA Standards 2-CO-1A-20, 4-4017, 3-JTS-1A-23, 1-ABC-1A-16.

SUPERSESSION: Policy 600.600, "Security/Compliance Audit," 3/5/12.
All facility policies, memorandums, or other communications whether verbal, written or transmitted by electronic means regarding this topic.

ATTACHMENTS: Position Statement - Security Audits (600.600A)

/s/
Deputy Commissioner, Community Services

Deputy Commissioner, Facility Services