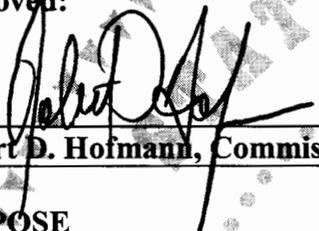


State of Vermont, Agency of Human Services Department of Corrections	Title: Security and Compliance Audits - Facilities	Page 1 of 12
Chapter: Security and Supervision	# 403.01	Supersedes # 403.01, Security & Supervision Audits, dated 7/6/1998
Attachments, Forms & Companion Documents: 1. Policy/Directive/Procedure/Post Order Checklist 2. Audit Team Assignments Checklist 3. Security Operations & Audits Review Supplementary Form		
Local Procedure(s) Required: No Applicability: All staff (including volunteers and contractors) Security Level: "B" - Anyone may have access to this document.		
Approved:  <hr/> Robert D. Hofmann, Commissioner		
<u>August 2, 2007</u> Date Signed	<u>September 4, 2007</u> Date Effective	

PURPOSE

The purpose of this administrative directive is to establish audit procedures to ensure that the confinement and security of inmates provides for basic safety, health, statutory, and constitutional standards, while at the same time ensuring the protection of staff and the public. The Director of Security Operations and Audits will ensure the completion of compliance audits of all Vermont Department of Corrections facilities and emergency procedures, including those applicable to the Department's Central Office as outlined in this directive.

POLICY

It is the policy of the Department of Corrections to support continuous improvement in the workplace and focus on positive results, to achieve a high standard of professionalism and best practice in correctional facilities. The Department will conduct regular, scheduled, audits of security and operations in facilities. An audit team will identify quality practices and areas for growth, as well as mentor staff. The focus will be on correcting problems rather than assigning blame. Results and written reports of security/compliance audits are considered confidential due to the security-sensitive information contained in them and are exempt from public inspection and copying pursuant to 1 V.S.A. section 317(c)(25) and (32).

AUTHORITY

28 V.S.A. § 102(b)(1); 28 V.S.A. § 102(c)(10). American Correctional Association Standards for Adult Correctional Institutions, 4th edition, January 2003, Standards 4-4017 and 4-4423. American Correctional Association Standards for Administration of Correctional Agencies, 2nd edition, 1993, Standard 2-CO-1A-20.

REFERENCE

Any applicable current Department of Corrections policies/administrative directives and Administrative Procedure Act rules.

DEFINITIONS

Administrative Procedure Act (APA): The State of Vermont statute that defines rulemaking to adopt rules, which, when adopted, have the effect of statute.

Audit Team (Auditors): A group of Department of Corrections' employees appointed by the Director of Security Operations and Audits to conduct security/compliance audits at all correctional facilities.

Corrective Action Plan: A plan by a facility Superintendent to address any deficiencies discovered in a security/compliance audit.

Security & Compliance Audit Manual: A manual established by the Director of Security Operations and Audits which contains audit procedures, schedules of audits, audit forms, and relative standards.

Security & Compliance Audit Program: A formal program which establishes and audits security standards and best correctional practice for a correctional facility, aimed at enhancing the security and safety of staff, the public, and inmates.

Security Manual: A manual of security standards, emergency plans, specific relevant directives, and security bulletins which is maintained at each facility based on materials provided by the Director of Security Operations and Audits.

PROCEDURAL GUIDELINES

A security audit is a process for determining the extent to which policy, procedure, standards, and practice combine to provide a safe and secure facility. In addition, the audit will evaluate areas beyond the definition of security such as the quality of life, conditions of confinement, and sanitation. The audit is designed to assist each facility's administration to evaluate current practices in comparison to established expectations in order to achieve the highest level of excellence in the performance of operations. The audit process will identify a facility's strengths and weaknesses and provide guidance to improving services. To this end, the following procedures are established.

1. Security Audit Goals

- a. To recognize a facility's adherence to a high level of security standards and best correctional practices;
- b. To determine compliance with facility and Department/Agency policy and procedure;
- c. To determine whether resources are being used in an effective and efficient manner;
- d. To identify physical plant deficiencies that could be a security concern or create a health or safety concern;
- e. To determine compliance with overall health, safety, and sanitation standards;
- f. To mentor, support, and train staff in security/compliance and audit procedures;
- g. To identify weaknesses or deficiencies in security operations.

2. Audit Responsibilities

- a. The Director of Security Operations and Audits will be responsible for the management of the Security and Compliance Audit Program and will:

- i. Establish the annual schedule of audits;
 - ii. Select and train security/compliance auditors;
 - iii. Make recommendations to the Facility Executive regarding audit standards to be included in the Department's Security Manual;
 - iv. Serve as an on-site manager of scheduled security audits;
 - v. Coordinate, prepare, and submit all audit reports.
- b. The Facility Superintendent is responsible to:
- i. Conduct facility self-audits as often as necessary to maintain compliance to audit standards;
 - ii. Establish a Security and Compliance Audit file cabinet in the Security and Operations' Supervisor's office or some other secure location. This cabinet will contain:
 - An established file folder for each current Department administrative directive relevant to facility operations, applicable APA rules, security manual standards, post orders, mandated inspection sheets, or any other communicated standard applicable to the facility operation.
 - Each folder will contain primary and secondary evidence of compliance to a respective standard or directive requirement.
 - iii. Participate in the pre-audit briefing and post-audit de-briefing;
 - iii. Ensure the completion of any corrective action plans based upon an audit;
 - iv. Complete audit preparations as outlined in sections 6 and 7 as applicable.

3. Audit Team Composition and Selection

- a. Team Composition – In addition to the Director of Security Operations and Audits, each audit team will include the following:
- i. The Department Emergency Management Service Coordinator;
 - ii. The Department Security Operations and Audits Coordinator;
 - iii. The Department Hearings Administrator;
 - iv. Minimally, three (3) team members selected from a group trained to conduct audits, to serve for an eighteen (18) month period; and
 - v. An Audit Team Leader selected on a rotating basis and who is from a correctional facility not the subject of a current audit.
- b. Team Selection
- Audit team members will be selected from a list of any facility or field staff who volunteer for this assignment provided that:
- They have more than three (3) years of correctional experience;
 - They have the endorsement of their Superintendent/District Manager;
 - They demonstrate a desire to learn and advance as a correctional professional;
 - They can demonstrate a basic knowledge of existing Department policies, directives, and APA rules.
- c. Auditor Standards
- Auditors will maintain the highest professional standards. They will:
- i. Maintain confidentiality – audit findings are confidential;

- ii. Be considerate – auditors, to the extent possible, will not interfere with ongoing facility operations;
- iii. Not affix blame to an individual – auditors will not report in a way that singles out an individual staff member for blame. However, they shall report immediately a dangerous or life-threatening situation or security breach;
- iv. Be ethical – auditors will seek legitimate opportunities to evaluate practices. They will not, for example, hide keys or unlock doors to see how long it would take to discover them, or gloss over a problem to give a facility a passing mark.

4. Audit Scheduling

Each July, the Director of Security Operations and Audits will issue a list of audits to be conducted during the next twelve (12) months. This list will include the date of each facility's scheduled audit.

- a. Each correctional facility will be audited every fifteen (15) months on a schedule that does not conflict with pre-scheduled facility lockdowns and contraband searches.
- b. The Director of Security Operations and Audits will determine the necessary size of the audit team and the length of the security/compliance audit based on:
 - i. Size of the facility;
 - ii. Complexity of facility operations;
 - iii. Anticipated concerns or issues.
- c. The Director of Security Operations and Audits will arrange for auditors to perform the audit, assigning auditors responsibilities for specific security/compliance standards.

5. Audit Inclusions

Security and compliance audits will include, but not be limited to, the following general areas, in addition to areas communicated through the Security Manual transmittal process. Compliance will be measured against current administrative policy/directives, applicable APA rules, Security Manual content, post orders, operational contracts (health and mental health), as well as physical plant maintenance, cleanliness and sanitation.

- a. Facility Management
 - i. Table of organization
 - ii. Channels of communication; e.g., schedule of staff meetings, roll call
 - iii. Policy, directive and procedure manuals
 - iv. Facility culture
- b. Perimeter Management and Security
 - i. Presence of security
 - ii. Lighting
 - iii. Maintenance of intrusion systems (fences, wire, cameras, alarms, etc.)
 - iv. Signage
 - v. Main entrance
 - vi. Secondary/emergency access
 - vii. Sallyports
 - viii. Trash/refuse removal security
 - ix. Intake and release procedures

- x. Roof access

- c. Physical Plant Management
 - i. Emergency power systems
 - ii. Building maintenance
 - iii. Grounds maintenance
 - iv. Preventive maintenance program
 - vi. American Disability Act compliance
 - vii. Lockout/tag out procedures
 - vi. Reporting/responding to maintenance requests

- d. Operational Security Management
 - i. Completeness of Security Manual inclusions
 - ii. Key control
 - iii. Security equipment: storage, accountability, issuance
 - iv. Weapons standards and control
 - v. Internal security control systems
 - Radio system
 - Camera system
 - Alarm system
 - vi. Contraband control – compliance with search procedures
 - vii. Substance testing procedures
 - viii. Staff uniform procedures
 - ix. Security inspections
 - x. Tool/sharps control
 - xi. Emergency plan implementation and training
 - xii. Log book procedures
 - xiii. Post orders
 - xiv. Mail/package procedures
 - xv. Main Control – organization, maintenance
 - xvi. Evidence control procedures
 - xvii. Information Technology/computer security
 - xviii. Transportation procedures
 - xix. Vehicle maintenance/safety records
 - xv. Visiting procedures
 - xvi. Security clearance procedures

- e. Inmate Management
 - i. Count procedures
 - ii. Restrictive status (segregation) procedures
 - iii. Intelligence gathering procedures
 - iv. Security threat group procedures
 - v. Movement procedures
 - vi. Living Unit rules
 - vii. Disciplinary procedures
 - viii. Inmate property procedures
 - ix. Special management unit procedures
 - x. Inmate telephone access
 - xii. Identification procedures
 - xiii. Communication protocols

- f. Inmate Program Services
 - i. Religious services/programs
 - ii. Volunteer services
 - iii. Recreational services
 - iii. Commissary procedures
 - iv. Inmate handbook

 - g. Incident Management
 - i. Incident reports
 - ii. Use of force procedures
 - iii. Local Emergency Response Team (LERT)
 - iv. Cell extraction procedures
 - v. Emergency plans
 - vi. Video recording procedures
 - vii. Community Alert Network (CAN) notification system
 - viii. Suicide/self harm prevention measures

 - h. Environmental Health, Safety Management
 - i. Fire prevention measures
 - ii. HAZMAT procedures
 - iii. Cleanliness/sanitation procedures
 - iv. Risk management (trip/fall) protection
 - v. Respiratory Protection Program (SCBA) compliance
 - vi. Bloodborne Pathogens Exposure Plan

 - i. Personnel Management
 - i. Roster/staffing management
 - ii. Recruitment/retention
 - iii. Training records
 - iv. Employee reward and recognition efforts
 - v. Employee wellness program
 - vi. Investigations
 - vii. Budget/overtime management
 - viii. Collective bargaining adherence

 - j. Other
 - i. Victim notification adherence
 - ii. Work opportunities/Industries
 - iii. Inmate grievance process
- 6. Pre-Audit Preparations**
- a. Pre-Audit Reference Materials – Thirty (30) days prior to the scheduled start of an audit, the facility will forward the following materials to the Director of Security Operations and Audits:
 - i. Facility schematic showing all functional facility areas;
 - ii. Complete staff roster by shift of all employees;
 - iii. Debriefing report of the last lockdown/search conducted;
 - iv. A narrative report outlining any special conditions that may exist at the time of the audit; e.g., construction, staff or inmate management problems, Buildings and Grounds (BGS) issues; and

v. Any other materials requested by the Director of Security Operations and Audits.

b. Audit Team Preparation – A pre-audit team meeting will be held prior to the scheduled audit to familiarize team members with their assignments and reporting times.

7. Conducting the Audit

- a. The audit team will assemble at the facility at 9:00 a.m.
- b. The facility liaison to the team may make introductory remarks regarding current facility status and special concerns.
- c. The audit team will meet with the facility executive staff.
- d. The audit team will tour the facility in order to become familiar with the facility geography, staff, programming, and industries, if any.
- e. After the facility tour, the auditors will informally move through the facility, assessing areas as assigned. Auditors will endeavor to ensure thorough coverage of all appropriate areas, shifts, and staff. Auditors will interview inmates as appropriate.
- f. Auditors will regularly debrief with the Audit Team Leader and Director of Security Operations and Audits, sharing observations and discussing concerns. Auditors may return to areas as necessary to follow up on issues or concerns.
- g. The audit team will set up and observe an emergency drill response.
- h. The audit team leader will monitor the ongoing progress of the audit to ensure timely completion of the audit schedule.
- i. If any critical issues or findings arise during the audit, the Director of Security Operations and Audits will coordinate with facility executive staff to ensure appropriate immediate response.

8. Audit Findings

- a. The auditors will discuss preliminary audit findings with the Audit Team Leader and the Director of Security Operations and Audits.
- b. At the conclusion of the audit, the auditors will present a general summary of audit findings to the facility executive staff. The facility Superintendent will determine what facility staff will attend this presentation.
- c. Findings Report – The audit report is formatted to include process indicators based on current Department administrative directives and best practice, process measures that define how the information was gathered, and results of measuring the specific indicators. A determination will also be made regarding any corrective action needed, based on identified deficiencies or recommendations.

- d. Corrective Action Plan – A corrective action plan will be submitted by the Superintendent within thirty (30) days to the Director of Security Operations and Audits regarding any deficiencies noted in a security audit. Should the Superintendent believe that certain unique circumstances exist to warrant an exception to any finding or recommendation, a written request may be submitted to the Facilities Executive. The request should detail the rationale for the request.
 - e. Follow-up Action – Within thirty (30) days of the submission of the corrective action plan, the Director of Security Operations and Audits will conduct a formal audit question and answer session with the Superintendent of the respective facility. The process will identify achievements and areas that require further attention. The Superintendent will have the opportunity to verbally present the facility's corrective action plan to the Deputy Commissioner, Facilities Executive, and all facility Superintendents.
 - f. Facilities in which numerous and serious deficiencies are revealed by an audit will be re-audited within three (3) months of the original audit.
 - g. The audit team will use the three attachments accompanying this directive to document findings.
 - i. *Attachment 1, Policy/Directive/Procedure/Post Order Checklist*, (a sample only) lists documents relevant to the audit standards. After auditing compliance with that document, the audit team notes whether they are “completed”, “partially completed”, “not completed”, or “not applicable.”
 - ii. *Attachment 2, Audit Team Assignments Checklist*, is a check list of what each auditor will be responsible for.
 - iii. *Attachment 3, Security Operations & Audits Review Supplementary Form*, documents both demonstrated proficiencies and deficiencies found during the audit, as well as recommendations to the facility for improvement and specific observations underlying the assessment.
9. Audit Manual Format
- a.. The content of the Security & Compliance Audit Manual will change as new directives, post orders, and standards are approved, and as new security concerns are identified. The Director of Security Operations and Audits has responsibility for maintaining updated manual content forms.
 - b. Each facility will receive an updated Security & Compliance Audit Manual, as well as updated audit sheets for inclusion in their manual. Current sample sheets are attached (*Attachments 1-3*). These forms may be revised at any time, without necessarily revising the directive, by the Director of Security Operations and Audits.

10. Post-Audit Activities

The Director of Security Operations and Audits will coordinate with audit team members to compose a preliminary draft of the audit report. This initial draft will be forwarded to the Department Facility Executive for review. Pending the need for revision, the completed report will be forwarded to the Deputy Commissioner and Commissioner for review. A completed report will be forwarded to the facility Superintendent.

TRAINING

The Facility Executive and Director of Security Operations and Audits are responsible to ensure that all audit teams are trained in order to conduct facility audits as described in this directive.

QUALITY ASSURANCE

The Facilities Executive in conjunction with the Director of Security Operations and Audits will be responsible for the quality assurance of the requirements of this directive.

- a. Quality Management Unit staff will participate in at least one (1) security/compliance audit a year.
- b. Annually, the Quality Management Unit will review the audit process and a sample of findings and corrective plans for consistency, validity, and compliance with this directive. The Quality Management Unit will make recommendations for improvement in the process to the Facilities Executive and the Director of Security Operations and Audits.

**SECURITY OPERATIONS AND AUDITS REVIEW
SUPPLEMENTARY FORM**

Correctional Facility: _____ **Date:** _____

(Use separate paper if more room needed.)

1. RECOMMENDATION(S): _____

2. DEMONSTRATED BEST PRACTICES/PROFICIENCIES: _____

3. DEFICIENCIES: _____

FURTHER COMMENTS: _____

Audit Team Leader Name and Signature:
