

# 7100-P211 – Policy and Technical Compliance

## I. PURPOSE

For the continued protection of State information, it is essential that agencies verify their compliance with information security policies. This policy sets the requirements for State and agency-directed compliance, maintenance and monitoring activities relevant to information security.

## II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as “agencies”).

## III. POLICY

Agencies shall ensure they comply with information security policies, standards, and procedures on a continuous basis by implementing a monitoring process that employs internal compliance reviews and independent reviews to include the following:

### A. Continuous policy, standard, and procedure compliance.

1. Agency heads shall be aware of the degree of information security compliance within their agency.
2. Information technology resource owners shall ensure continuous compliance with information security policies, standards, and procedures that are applicable to their area of responsibility. Compliance activities can include but are not limited to the routine review of intrusion detection sensors, firewalls, and/or system logs; the use of password strength tools; the reconciliation of authorized users to active system accounts; and the verification that unneeded accounts are properly disabled or removed.

### B. Internal compliance reviews.

1. Agencies shall develop a process to assess their degree of compliance to policies, standards, and procedures on a regular basis appropriate to the risk.
2. Technical and non-technical risks associated with non-compliance shall be identified and reported to the Agency head.
3. Detailed assessment findings shall be marked as “Restricted”, distributed on a strict need-to-know basis, and backed up to unalterable media as soon as possible.
4. Compliance gaps and vulnerabilities (weak or nonexistent technical or non-technical information security controls) identified during internal compliance

reviews shall be remediated in accordance with Policy 9400-P183 – Vulnerability Management.

### **C. Independent compliance reviews.**

1. Agencies are encouraged to obtain the services of an independent entity, internal or external to the agency, to assist with a review of their technical and non-technical security controls to test compliance with a set of specified policies, standards, or procedures.
2. Compliance gaps and vulnerabilities (weak or nonexistent technical or non-technical information security controls) identified during independent compliance reviews shall be remediated in accordance with Policy 9400-P183 – Vulnerability Management.

### **D. Technology considerations during compliance reviews.**

During internal or independent compliance reviews, automated compliance testing tools shall be used in such a way to minimize the risks to the production environment. If automated security tools are used to measure system compliance, the following shall apply:

1. Personnel responsible for systems to be tested (Information Resource Owners) shall be briefed on the tests to be performed, possible risks to their systems while the tests are being performed, and emergency back-out procedures. They must concur with the entire process and procedure prior to testing.
2. All tests shall have a responsible party who is in the position to stop the running of automated tools. Tests designed to measure State, agency, or third party provider's response to a particular security event shall have a "trusted agent" in the loop.
3. Tests shall be minimally intrusive. For example, test tools may be configured to inspect system files for vulnerabilities but not modify them.
4. "Denial of Service" tests, or tests that produce DOS effects, by any State entity, shall not be performed unless approved by the Agency head.
5. Access to the automated security tools shall be strictly limited.

**CIO Approved Date: 1/5/2011**