

9400-P167: Information Technology Resource Monitoring

I. PURPOSE

This policy provides authorization to agencies to monitor the information technology (IT) resources they own, control, or manage. . Monitoring under this policy is not intended to be a formal IT security audit.

II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as “agency” or “agencies”) and any non-State entity that connects an electronic device to the State network.

III. POLICY

- A. The State and its agencies have the right to monitor and log all activities on the IT resources and/or network infrastructure they own, control, or manage.
- B. The State and its agencies have the right to filter and block any inbound and outbound traffic (reference Policy 1200-P143: Internet Acceptable Use Policy). Agencies shall not intentionally impede access to resources that are required for official business.
- C. The State and agencies shall provide notice of system monitoring in the form of security warning banners in accordance with Policy 9400-P173: Logical Access Controls on IT Resources and Standard 9400-S173: Security Warning Banner.
- D. Host and network-based security sensors shall be placed at strategic locations within State and agency network infrastructures. These systems shall alert security administrators of possible security incidents.
- E. Use of security monitoring tools.
 1. Security monitoring tools such as protocol analyzers, password crackers, network mapping, and packet sniffers can be employed with the approval of the appropriate security authority within the agency. The State Chief Information Officer shall designate the approval authority for the State Wide Area Network (WAN).
 2. The potential risks of operational disruptions caused by the use of monitoring tools shall be made known to the resource owners and approving authority prior to use.
 3. Unless specifically authorized to the contrary (see G below), monitoring tools shall not target a specific user. When there is suspicious activity that can be

9400-P167: Information Technology Resource Monitoring

attributed to an individual, notifications shall be conducted per State and/or agency personnel rules.

4. For the purpose of accurate event, audit, and log reporting, all IT network resources, to the extent possible, shall be synchronized to a common time source.

F. Protection of security audit logs.

1. Security audit logs shall be configured for read only, when possible.
2. Administrator access to these audit logs shall be granted on a tightly controlled, need-to-know basis.
3. State and agency personnel who have a security role, as appropriate, shall create, use, review, protect, and retain security audit logs and security tool data. Security incidents discovered during audit log review shall be reported in accordance with Policy 9400-P190: Reporting Security Events and Vulnerabilities.
4. Retention of security audit logs.
5. Agencies shall determine the appropriate retention and purging period for their security audit logs consistent with standard State record management policies.
6. Longer retention periods shall be prescribed on a case-by-case basis or if the security audit logs are evidence in a legal matter.

G. Expectations of personnel assigned with system monitoring duties.

1. Personnel assigned the duties of system security monitoring, shall be specifically appointed and designated in writing.
2. Personnel permitted to monitor system activity shall be bound by all State and agency policies and non-disclosure agreements. Violations of State or agency policies and agreements may result in disciplinary actions in accordance with State personnel rules.
3. Personnel permitted to monitor system activity shall not focus on a specific employee's activities unless they have proper agency authorization, are actively working on a documented trouble ticket, or are actively pursuing a potential security incident that requires them to do so. If it is determined in the course of performance and/or maintenance monitoring that specific

9400-P167: Information Technology Resource Monitoring

employee monitoring is required, proper authorization shall be obtained in order to proceed.

CIO Approved Date: 3/22/12