Logging and Security Monitoring Policy

Purpose

This policy establishes the uniform policy within Milestone for the auditing, logging, measurement, and monitoring of networks and automated information systems (AIS). This policy establishes minimum practices to ensure Milestone systems and networks are audited to maintain awareness of the operating environment, to detect indications of security problems, and to ensure Milestone AIS systems and networks are used for authorized purposes.

Scope

The provisions of this policy apply to all Milestone employees and contractor employees using or operating Milestone computer systems, as well as the systems and networks, and to contractor employees providing services to the Milestone by using Milestone AIS and networks. This policy applies to production AIS, servers, and server applications only.

Policy

General Policy

It is Milestone's policy that audit trails shall be used for the following:

- Individual Accountability. Audit trails shall be used to support accountability by providing a trace of user actions.
- Reconstruction of Events. Audit trails shall be used to support after-the fact investigations of how, when, and why normal operations ceased.
- Intrusion Detection. Audit trails shall be designed and implemented to record appropriate information to assist in in intrusion detection.
- Problem Identification. Audit trails shall be used as online tools to help identify problems other than intrusions as they occur.

All Milestone operational information technology (IT) systems shall enable audit and normal logging processes within the scope previously defined.

A. *Contents of Audit Trail Records*

An audit trail shall include sufficient information to establish what activity occurred and who (or what) caused it. Given the diversity of IT systems' capabilities and missions, the scope and contents of the audit trail shall balance security needs with performance needs, privacy, and costs.

The following list is representative of events that would provide an acceptable audit trail and is included in this policy as guidance.

- User login – unsuccessful, successful if feasible
- Server startup and shutdown
- Service startup and shutdown -- unsuccessful and successful, if feasible
- User account permission modifications -- unsuccessful and successful
- User account additions and deletions -- unsuccessful and successful
- IP address or hostname associated with a given event, if feasible
- Firewall rule base modification, if applicable -- unsuccessful and successful
- Software installation or removal -- unsuccessful and successful, if feasible

Audited events shall be documented in the appropriate system security plan or baseline configuration document of that operating system, network device, or application.

B. *Audit Trail Security*

Audit trails shall be protected from unauthorized access. The following precautions shall be taken:

- Control online audit logs. Access to online audit logs shall be strictly controlled.
- Separation of duties. Separation of duties between security personnel who administer the access control function and those who administer the audit trail shall be ensured.
- Protect confidentiality. Confidentiality of audit trail information shall be ensured.
- Audit logs shall be protected from accidental or malicious deletion and modification.
- Paper copies of audit logs shall have employed and distributed on a strictly need-to- know basis, shall be destroyed when no longer needed.

C. *Audit Trail Reviews*

Audit trails shall be reviewed as follows:

- For medium/highly critical servers on internal protected networks, on a weekly basis.
- For perimeter security intrusion detection systems on a daily basis, including firewall and IDS applications, daily.
- Following a known system or application software problem, a known violation of
- Existing policy by a user, or anomalous or suspicious system activity.

D. *Monitoring of Milestone Network and AIS Activity*

- Milestone networks and AIS shall be monitored for unauthorized or improper use.
- Unauthorized or improper use of the systems shall be investigated and, when appropriate, official sanctions shall be imposed as a result of such use. If criminal activity is discovered, system logs shall be provided to the appropriate law enforcement officials.
- The focus of network and AIS monitoring or auditing shall be predicated on identification and confirmation of behavior in violation of Milestone policy or federal law.
- Only authorized local network and system administrators, auditors, and/or investigators for diagnostic and troubleshooting purposes and monitoring of misuse or malicious network activity will use network packet analyzers, or devices that operate in promiscuous mode.

E. *Employee Investigations*

- Requests for an employee investigation can be made by: 1) the supervisor, or a superior in the management chain of the employee to be audited with the approval of Executive Management, 2) the Office of Human Resources, 4) Director of IT and 5) Milestone Executives (CEO, President & VP of Technology)

- A record shall be maintained of user investigation requests and results.

- Auditing can take place for any and all traffic on the network and AIS activity. All requests for log records related to employee misconduct (including Supervisors) shall be coordinated with VP of Operation & Technology approved by the President and/or CEO.

F. *Uniform Monitoring*

- Network and AIS monitoring shall only be used to monitor activity on a system-wide level without the targeting of any specific person(s) until any suspected unauthorized activity has been identified. To ensure the integrity and objectivity of the network monitoring function, segregation of duties shall be maintained.
- A user investigation report record shall be maintained for each individual investigation.
- Precautions shall be taken to prevent or decrease the risk of errors or irregularities with regard to data collection; identifying problems; and ensuring that the chain of evidence is preserved.
- No single individual shall have control over all phases of network monitoring.
- Approval for the collection, analysis, or use of the information gathered and the disclosure to law enforcement agencies, or other agencies outside the Milestone, shall be coordinated with VP of Technology and approved by the President and/or CEO.

G. *Employee Notification and Privacy Expectations.*

- Milestone employees and contractor employees shall be notified on logical access to a Milestone IT system through a warning message that must be agreed to or state that further use indicates consent to monitoring. This warning message will state that all IT systems may be monitored, and that unauthorized use will be grounds for disciplinary, civil or criminal proceedings.
- Milestone employees and contractor employees do not have a right, nor should they have an expectation, of privacy while using any Milestone IT system at any time, including accessing the Internet or using e-mail. To the extent that Milestone employees and contractor employees wish that their private activities remain private, they should avoid using Milestone IT systems, the Internet or e-mail. By using Milestone IT systems, Milestone employees and contractor employees give their consent to disclosing the contents of any files or information maintained using Milestone IT systems to authorized Milestone staff. In addition to access by authorized Milestone staff, data maintained on Milestone IT systems may be subject to the legal process of discovery and Freedom of Information Act (FOIA) requests.
- Milestone employees and contractor employees, by using Milestone IT systems, give implied consent to monitoring and recording with or without cause, including (but not limited to) their accessing the Internet or using e-mail. Any use of Milestone IT systems

is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

- Milestone employees and contractor employees shall not receive additional notification of specific monitoring actions of their usage unless the appropriate authority determines disciplinary action or criminal investigation is appropriate.

H. Implementation

Specific implementation details for this policy may be in the appropriate system security plan of a given AIS or documented in the operating system baseline configuration document.

I. Compliance

- Prohibited uses of Milestone AIS resources can result in administrative, judicial, or non- judicial punishment in accordance with federal law and civilian employee regulations.
- User Accounts shall be randomly audited to ensure compliance with established Milestone IT security standards. Milestone employee and contractor employee accounts shall be audited upon termination of employment and/or completion/termination of a contract.
- Audit trail information is subject to the Freedom of Information Act (FOIA).
- Milestone AIS, systems or applications that cannot meet established IT security standards shall be modified to remedy any deficiencies, where feasible. If compliance is not technically feasible then the System Owner of the AIS may defer compliance via a Plan of Action and an expected date of compliance or a waiver of this policy may be requested. For waiver details please refer to the Milestone IT Security Handbook or similar policy instruction.

Responsibilities

All Milestone employees and contractor employees shall be aware of and observe the Milestone policy regarding network and AIS audit, logging, measurement, monitoring. All Milestone employees and contractor employees shall adhere to this policy and refrain from any activity that might circumvent this policy.

System Owners, Information System Security Officers, and System Administrators shall implement the mandatory practices of this policy for all Milestone AIS, systems, or applications they are responsible for.

The Milestone IT Department shall:

- Log, monitor, and investigate possible security violations from activity involving access to and modification of sensitive or critical files.
- Review audit logs weekly for e-mail servers, medium and high criticality servers and hosts on the internal, protected network.
- Review audit logs from the perimeter security systems daily.
- Ensure the protection of system event logs with file-level permissions, segregation of duties, and all other safeguards commensurate with the highest level of sensitivity of the information resident on the system that the logs record data.
- When required, implement additional monitoring tools on critical servers as a supplement to the activity logging process provided by the operating system.

The Milestone IT Department shall ensure that all systems have current and effective IT security plans that accurately reflect system status.

The Milestone Information Technology Department shall:

- Maintain and update this policy and monitor compliance through the conduct of annual compliance reviews.
- Ensure communication of the policy to all Milestone employees and contractor employees and will ensure that IT security awareness and training programs address network and AIS audit, logging, measurement, and monitoring.
- Be responsible for monitoring of system user compliance with this policy as part of the periodic IT security self-assessment program or automated system audits.