Monitoring and Logging Policy

Policy Title	**Monitoring and Logging Policy** **Part of Information Security Policy Framework**
Responsible Party	Chief Security Officer ("CSO")
Endorsed by	Information Security Policy Committee
Contact	Chief Security Officer, Stuart Zimmerman; (918) 858-6684
Effective Date	June 1, 2015
Last Update	July 1, 2021

I. Policy Statement

Monitoring and logging of Company systems will be carried out in order to protect the safety, confidentiality, integrity and availability of information within the organization. Monitoring provides information to manage network traffic resources, user and system activity, faults and external or internal threats. Logging records these events in order to report activity and provide an audit trail.

Most importantly, on-going system monitoring and logging for audit should allow timely detection of and response to unauthorized information processing activities.

II. Policy

- **Monitoring**
- **Audit Logging**
- **Clock Synchronization**

Monitoring

Procedures for monitoring use of information processing facilities should be established and the results of monitoring activities regularly reviewed. This could include:

- Event tracking and recording as specified in the Audit logging policy
- Monitoring and review of this data, as determined by the criticality of the application/system or information involved, past experience with information security incidents, and general risk assessment.

Audit logging

Audit logs that record user and system activities, exceptions, and information security events should be produced, and kept for an agreed-upon time period, to assist in future investigations and access control monitoring. This could include recording, when relevant and within the capacity of the logging system, all key events. These will be reviewed by a member of the Information Security Policy Committee on a monthly basis. Key event data could include:

- Date/time for the event, and the event type;
- User-ID and/or system-ID associated;
- Terminal identity and/or location;
- Network addresses and protocols;
- Records of successful and unsuccessful system accesses or other resource accesses;
- Changes to system configurations;
- Use of privileges;
- Use of system utilities and applications;
- Files accessed and the kinds of access (e.g., read, modify, create, copy, delete); and
- Alarms raised by the access control or any other protection system (e.g., IDS/IPS).

Balancing audit with operational requirements: Audit controls should be implemented to allow collection of appropriate audit data on operational systems, while minimizing the risk of disruption to business processes. At a minimum, security controls will be audited and documented every three (3) years. This will be overseen by the Chief Information Officer.

Protection of log information: Logging facilities and log information should be appropriately protected against tampering and unauthorized access. This could include:

- Privacy protection measures for logged data that may be Confidential or Highly Confidential.
- Security protections of a technical, physical and administrative nature (e.g., division of responsibilities) to ensure integrity and availability of audit logs.

Retention of log information: A formal policy should specify the minimum retention periods for log data, consistent with legal-regulatory-certificatory requirements, business needs, and available storage/processing capacities.

Administrator and operator logs: System administrator and system operator activities should be appropriately logged, as part of the general audit trail process.

Fault logging: Faults should be appropriately logged, analyzed and actions taken. Action will include:

- Notification of system owner
- Notification of Chief Information Officer
- Notification of Chief Executive Officer

Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain should be appropriately synchronized with an agreed-upon time source, as part of protecting the accuracy of log information.

III. Procedure

There is no content for this section.

IV. Who is affected by this Policy

All Company employees and consultants are affected by this policy.

V. Definitions

There is no content for this section.

VI. Related Policies

- **Information Security Policy Framework**
- **Information Security Policy**
- **Information Security Plan**
- **Information Security Password Policy**
- **Information Security Incident Management**
- **Information Technology Policy**
- **Network Administrative Security Policy**
- **Data Encryption Policy**
- **Business Continuity Policy**
- **Disaster Recovery Policy and Plan**

VII. Update Log

June 1, 2015: Policy issued.
