

System Logging and Monitoring Policy

# Overview/Purpose

Monitoring and logging is an essential information security control that is used to identify, respond to, and prevent operational problems, security incidents, policy violations, and fraudulent activity.

The purpose of this policy is to establish requirements and parameters for creating, maintaining, storing, and accessing <**Utility Name**> computer and communication device logs. The logs shall be used to assist in troubleshooting, monitoring changes to system performance, recording the actions of users when necessary to properly maintain security, track and investigate security incidents, and provide data useful for investigating malicious activity. Additionally, logs may be used to assist in business recovery activities, and to comply with federal, state, and local laws and regulations.

# Scope

All employees, contractors, consultants, temporary and other workers and its subsidiaries must adhere to this policy. This policy applies to technology, as defined in the Introduction herein, that is owned, operated, or leased by <**Utility Name**> or registered under a <**Utility Name**>-owned internal network domain.

# Policy

## General Requirements

### The time settings of all systems generating log files will be synchronized to an authoritative time source, using an application such as the Network Time Protocol (NTP) Service. Synchronizing time stamps for log events will help to facilitate the investigation of issues involving more than one system.

### <**Utility Name**> will use a centralized system for log collection and correlation. All network devices, servers, workstations shall provide log data to the centralized logging system. This system should also collect data from wireless access points and intrusion detection devices.

The level of information detail contained in a log will be determined by the IT Manager based on the risks to the relevant technology and underlying data, and shall be determined in accordance with the risk management policy.

### Log files must be examined on a regular basis in order to protect technology. The frequency and nature of log monitoring and review depends on the risks to the relevant technology and underlying data and shall be commensurate with the risk management policy. To satisfy PCI DSS requirements, logs will be review on daily basis when collecting data from protective devices and applications such as IDS, IPS (standalone or built into firewall), and antivirus consoles.

### The following list of events shall be logged for PCI DSS compliance:

* Directory Service Access Attempts
* Directory Service Access - Success/Failure
* Logon Failures – Active Directory
* Logon Failures – Local Logons
* Object Access Attempts – Success/Failure
* Object Deletions
* Password Reset Attempts by Administrators or Account Operators
* Process (Program) Usage
* User Activity in Auditing Categories
* Successful Network Logons – Workstations and Servers
* Policy Change - Success/Failure
* Account Management – Success/Failure
* Directory Service Access - Success/Failure
* System Events - Success/Failure

(This list of logged information needs to be verified periodically against the current PCI DSS standard.)

### Log files may contain confidential data, and thus must be handled in a manner that is consistent with the **<Utility Name>**’s policy for such data. Logging facilities and log information should be protected against tampering, modification, destruction, and unauthorized access. When technically feasible, system administrators should not have permission to erase, deactivate, or modify logs of their own activities.

### Log files will be maintained only as necessary to comply with the record retention policy or as required to support analysis of misuse, incident reconstruction, or other investigations. To satisfy PCI DSS requirements, logs need to be maintained for one year, with logs for three years readily available.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy>** will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* Adapted from “Cyber Security Policy Framework”

(<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.

* See also, “Maintenance, Monitoring, and Analysis of Audit Logs” (<http://www.sans.org/critical-security-controls/control/14>) and “Account Monitoring and Control” (<http://www.sans.org/critical-security-controls/control/16>)
* PCI DSS Requirements  
  <https://www.pcisecuritystandards.org/document_library>

# Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **System Admin**  **Network Admin** | **IT Department** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |