**Logging and Monitoring Policy**

**Paradigm Software Technologies, Inc. DBA Nexelus**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Purpose**

The purpose of this policy is to outline requirements for audit logging and monitoring of system activity at Paradigm Software Technologies, Inc. DBA Nexelus. Frequent monitoring and maintenance of audit trails are required to effectively assess information system controls, operations, and general security.

**Scope**

This policy applies to all Paradigm Software Technologies, Inc. DBA Nexelus system components including applications, infrastructure (including cloud infrastructure), network, security tools and utilities, or any other components that could impact the security of Paradigm Software Technologies, Inc. DBA Nexelus and the data it manages and processes.

**Roles & Responsibilities**

* **General Manager(GM)** – Is responsible for managing and overseeing Logging and Monitoring procedures and ensures compliance with company policies.
* **Support Team** – Members from support will coordinate and notify relevant stakeholders if any event or activity violates the Logging and Monitoring Policy.
* **System Admin Team** – Will establish logging and monitoring processes, controls and monitoring/notification system.

**Section**

**Event Logs**

All Paradigm Software Technologies, Inc. DBA Nexelus systems that may access or handle sensitive information, accept network connections, manage access control (authentication and authorization), or that may affect the security of the environment (e.g., anti malware utilities, firewalls, etc.) will record and retain audit-logging information sufficient to answer: What activity was performed? Who performed it? Where, when, and how (with what tools) was it performed? And, what was the status, outcome, or result of the activity?

**Logged Activities**

Log records will be created for the following activities:

* Attempts to create, read, update, or delete sensitive information, confidential authentication information such as passwords.
* Attempts to create, update, or delete information not covered in above;
* Initiating a network connection;
* Accepting a network connection;
* User authentication and authorization for activities covered above such as user login and logout;
* All invalid logical access attempts;
* All actions taken by any individual with administrative access, including any interactive use of application or system accounts.
* Attempts to grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, elevation of privileges, modifications of administrative access, firewall rules changes, and user password changes;
* All access to audit logs
* initialization of new audit logs, all starting, stopping, or pausing of the existing audit logs.
* Creation and deletion of system-level objects;
* System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
* Application process startup, shutdown, or restart;
* Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
* Detection of suspicious/malicious activity such as from an intrusion detection or prevention system (IDS/IPS), web application firewalls, anti-malware system, or anti-spyware system.

[If a Cloud Service Customer], Paradigm Software Technologies, Inc. DBA Nexelus to assess whether the logging capabilities provided by the cloud service provider are sufficient, or if additional logging capabilities need to be implemented.

**Log Elements**

Each log will identify or contain at least the following elements, directly or indirectly (unambiguously inferred):

* Type of action - examples include authorize, create, read, update, delete, and accept network connection, including whether it was a successful or failed action.
* Subsystem performing the action - examples include process or transaction name, process or transaction identifier.
* Identifiers (as many as available) for the subject requesting the action - examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
  + In the case of sharing logs with third parties (including auditors), the use of identifiers containing PII will be limited to:
* Identifiers (as many as available) for the object the action was performed on - examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address.

Note that such identifiers should be standardized in order to facilitate log correlation.

* Before and after values when action involves updating a data element, if feasible.
* Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
* Whether the action was allowed or denied by access-control mechanisms.
* Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

**Clock Synchronization**

• To ensure the accuracy of system logs, system clocks and time will be synchronized using time-

synchronization technology.

* The system will also ensure clock synchronization for the accuracy of audit logs. Time received from external sources will be based on International Atomic Time or Coordinated Universal Time (UTC). A network time protocol will be used to keep all of the servers in synchronization with a central time server.
* Time synchronization settings and data will be restricted to only personnel with a business need. Any changes to time settings on critical systems will be logged, monitored, and reviewed.

**Protection of Audit Logs**

To safeguard and prevent manipulation of logs by individuals with elevated access or unauthorized users, the following will be implemented where appropriate and possible:

* Read access to audit logs files will be limited to those with a job-related need.
* Audit log files will be protected to prevent modifications by individuals.
* System administrators will be restricted from erasing or deactivating logs of their own activities.
* Audit log files, including those for external facing technologies, will be backed up to a secure, central, internal log server or other media outside of the control of a system administrator or operator.
* Monitoring system and network administration activities will be performed by using an intrusion detection system managed outside of the control of system and network administrators.
* File integrity monitoring or change-detection mechanisms will be used on audit logs to ensure that existing log data cannot be changed without generating alerts.
* Frequent review of logs to maintain accountability of privileged users.
* All activities carried out by system administrators and operators will be logged. These logs will be safeguarded and subjected to routine reviews.
* In instances where Paradigm Software Technologies, Inc. DBA Nexelus has been delegated privileged operations, the performance of these operations will be logged.

**Monitoring**

* Failures of critical security control systems will be detected, alerted, and addressed promptly through the monitoring of logs and alerting mechanisms. Critical security control systems include:
  + Network security controls.
  + IDS/IPS.
  + Change-detection mechanisms.
  + Anti-malware solutions.
  + Physical access controls.
  + Logical access controls.
  + Audit logging mechanisms.
  + Segmentation controls.
  + Audit log review mechanisms.
  + Automated security testing tools.
* Failures of any critical security controls systems identified through log monitoring will be responded to promptly in accordance with incident response policies and procedures, including but not limited to:
  + Restoring security functions.
* Identifying and documenting the duration (date and time from start to end) of the security failure.
* Identifying and documenting the cause(s) of failure and documenting required remediation.
* Identifying and addressing any security issues that arose during the failure.
* Determining whether further actions are required as a result of the security failure.
* Implementing controls to prevent the cause of failure from reoccurring.
* Resuming monitoring of security controls.

**Revision History**



**Version Date Editor Approver Description of Changes** **Format**

