Veranda

LOGGING AND MONITORING POLICY

CHANGE HISTORY

Date	Version	Created by	Approved By	Description of change
08/10/2024	1.0	Bharath S	Ashwin Khosla	Basic document outline and submitted for review

1. SUMMARY

The detection of potential or actual information security incidents relies on timely and comprehensive event information being available from key security controls across Veranda Learning. These events are critical during forensic investigation in the event of a security incident. Logging from critical systems, applications, and services can provide key information and potential indicators of compromise. Computer logs are essential to the operational management of an organization. They provide a primary mechanism for automated tracking and reporting for review, audit, and compliance functions as well as a useful mechanism for tracking changes and troubleshooting.

2. PURPOSE

The purpose of this document is to establish the requirements for logging and monitoring of events across the systems of Veranda Learning for security incidents. Logging and monitoring of events help in identifying potential security vulnerabilities, configuration issues, and other anomalies within systems, applications, and network devices of Veranda Learning.

3. SCOPE

This policy applies to all employees (Full-time or Part time), contractors, visitors, third parties who access or use Veranda Learning information assets, regardless of physical location.

IT resources include all Veranda Learning owned, licensed, leased, or managed hardware and software, and use of the Veranda Learning network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

This policy also applies to information technology administered centrally, personally owned computing devices connected by wired and/or wireless network.

Mapping with Industry Standards

This policy addresses the following risks related to Logging and Monitoring and Information Security standards, frameworks:

Risk	Mapping to ISO 27001:2022
Data Loss	8.15 Logging 8.16 Monitoring Activities 8.17 Clock synchronization C 9.1 Monitoring, measurement, analysis and evaluation
Unauthorized access	8.15 Logging 8.16 Monitoring Activities C 9.1 Monitoring, measurement, analysis and evaluation C 10.1 Continual improvement
Information Leakage	8.15 Logging
Data Breach	8.15 Logging

4. POLICY

4.1 Event logging

Veranda Learning   shall log all events occurring across its systems and network. Events can be categorized as, and not limited to, any user activity, exception, security events, and anomalies. The event logs shall be stored and regularly reviewed for all scenarios where the risk of alteration of CIA parameters is high in the Risk Assessment process.

Logs shall be created when any of the following activities are performed/requested to be performed, but not limited to:

- Create, read, update, or delete any information, asset, or resource, including confidential authentication information, sensitive, critical, personal information, and proprietary information.
- Create, update, or delete information not covered in above statement
- Initiate a network connection
- Accept a network connection
- User authentication and authorization activities such as user login and logout
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes
- Application process start up, 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), failure of network services such as DHCP or DNS, or hardware fault
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.
- System Administrator and System Operator activities.
- Alerts/triggers from the Data Loss Prevention (DLP) tool and server log file.
- Access log data for cloud services.
- Attempts to access the audit logging systems and logs

Such logs shall identify or contain at least the following elements, directly or indirectly.

- **Type of action** – examples include authorize, create, read, update, delete, and accept network connection.
- **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 username, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.

- **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.

4.2 Protection of Log Information

Security event logs shall be protected from tampering, unauthorised modification, and deletion. This can be achieved by:

- **Access to Logs:**
  - that access to the log source and log destination is securely authenticated (e.g. TACACS Ensuring for network devices) and restricted (e.g. access only via separate management subnet or separate administrative control).
  - Restrict access to authorised users based on business need.
- **Protection of logs through cryptographic means:** A specialised, logging service that cryptographically signs security event logs to protect the logs from modification. The service must not have a log deletion or purge facility.
- **Integrity of the logs:**
  - Audit records shall be immutable and shall be protected against modification and deletion by anyone regardless of access privilege according to the Access Control Policy. Refer Access Control Policy.
  - Any modification/deletion detected shall trigger an alert.
  - Security tools/software such as File-integrity monitoring (or change detection software) must be implemented to detect any such modifications/deletions.
  - Note that the creation of new audit records shall not trigger an alert.Retention period

The retention period of log files depends on the statutory and regulatory requirements of the control logging. Therefore, local requirements regarding data protection the maximum retention period apply. Control and monitoring documents need to be kept for 180 days online and 1 year in backups.

4.3 Monitoring

Monitoring describes the activity of evaluating the log files and initiating necessary action. The monitoring is conducted by the IT Team. Logging of security relevant incidents are only effective as a security measure if the logged data is monitored and analysed. Therefore, Veranda Learning shall review and analyse audit records for suspicious, unusual, and inappropriate activity on an ongoing basis. When analysing data, the limitation to the purpose for which the data was collected needs to be respected.

Where possible, log monitoring must be automatic and rule-based to immediately alert on suspected security events. Automated event monitoring and alerting systems must have the capability to report devices that fail to provide logs/report, to reduce the risk of a security event going un-noticed.

- Audit records shall be reviewed and analysed for evidence of suspicious, unusual, and inappropriate activity on an ongoing basis.
- Anomalous auditable events and related security incidents shall be reported to the CISO, who shall be responsible for reporting security and compliance issues to senior leadership as appropriate.
- Procedures for monitoring the use of systems and facilities shall be established to test the effectiveness of access control and security mechanisms. The results of the monitoring activities shall be reviewed on a regular basis.
- Monitoring activities shall include execution of privileged operations, authorized access, unauthorized access attempts, and system alerts or failures.
- Veranda Learning shall meet all applicable legal requirements related to monitoring authorized access and unauthorized access attempts.
- Monitoring shall include inbound and outbound information exchanges and file integrity monitoring.

4.4 **Clock Synchronization**

Veranda Learning shall make sure that the clocks of all the infrastructure devices used by Veranda Learning are synchronized to a single time source. Veranda Learning shall synchronize system clocks with a real-time clock set to Coordinated Universal Time (UTC) to support tracing and reconstitution of activity timelines.

Veranda Learning shall restrict authorization to change system time settings to those individuals requiring access as part of their job role. Changes to system clocks on critical systems must be logged, monitored and reviewed.

External and internal requirements for time representation, synchronization and accuracy along with Veranda Learning Technology’s approach to obtaining a reference time from external source(s) and synchronizing internal clocks reliably shall be documented and implemented.

5. EXCEPTIONS AND ESCALATIONS

This policy applies to all departments unless an exception is formally requested and approved. Exceptions should be requested through the policy exception process and are subject to approval by Executive Management.

In the event an individual or department becomes aware of an exception, a request must be sent to and approved by Executive Management. In the event individuals become aware of non-compliance with this Policy, they must notify Executive Management directly or report the concern to the Information Security Committee.

Non-compliance with this policy may incur disciplinary measures and consequences including progressive discipline up to and including termination of employment.

6. VALIDITY AND DOCUMENT MANAGEMENT

The owner of this document is IT and ISMS team, who must check and, if necessary, update the document at least once in 12 months.