TRIANZ℠

Information Security Logging and Monitoring Policy

TRIANZ INTERNAL

trianz.com

Statement of Confidentiality

The information contained in this document is internal to Trianz. It shall not be disclosed, duplicated, or used for any purpose other than that stated herein, in whole or in part, without the express written consent of Trianz.

Information Classification

☐	Public
☒	Internal
☐	Confidential
☐	Restricted

Table of Contents

1. Purpose

This policy establishes requirements for the collection, maintenance and review of audit logs for Trianz applications and related network resources, in support of identity management and threat monitoring. Audit logs consist of information trails that are used to track and associate user and system activity to events.

2. Scope

This policy covers all Trianz assets which is available currently, or which may be created, used in the future. All Trianz employees, contractors and other stakeholders are responsible for understanding and complying with this policy.

3. Policy Statement

Trianz shall identify the systems, applications, or processes that make data vulnerable to unauthorized or inappropriate tampering, uses or disclosures. For each identified system, application, or process. Trianz shall identify user activities (e.g. Create, Read, Update, and Delete) that needs to be tracked and audited.

Logging shall include system, application, and database & file activity whenever available or deemed necessary.

- Logging shall include creation, access, modification and deletion activities.
- Log files shall be regularly examined for access control discrepancies, breaches, and policy violations.
- Data custodians or device managers are responsible for developing appropriate processes for monitoring and analyzing their logs.
- Individuals shall not be assigned to be the sole reviewers of their own user activity.
- System activity review cycles shall include review of audit logs minimally every 30 days and may include daily exception reporting.
- The Information Systems team shall be responsible for monitoring and reviewing audit logs to identify and respond to inappropriate or unusual activity.
- Browser Weakness and Updates

4 Measurement and Review

Audit logging records system and user activities used for system performance tuning, detecting unauthorized access and to investigate incidents.

4.1 Log Reporting

Configure logs to be of sufficient size to reporting key events such as:

- Individual access to private data (e.g., file system, application)
- Actions taken by an individual with root or administrative privileges
- Access to audit trails
- Invalid logical access attempts (e.g., authentication, ACL, missing web page, web server error)
- Use of identification and authentication mechanism
- Initialization of audit logs
- Use of privileges (e.g., sudo, UAC, elevated use of privileges)
- Activation and de-activation of protection systems, such as anti-virus and intrusion detection systems
- Configure log report key entries to include:
    - user identification
    - type of event
    - date and time
    - success and failure indication
    - origination of the event
    - identity or name of affected private data, or system
    - network addresses and protocols
- Synchronize the clock to the Trianz NTP servers.

4.2 Logging Security-Related Events

Security-related events/incidents must be logged in the control dock tool. Also, the Information Security Compliance team will review these events and prescribe corrective measures as needed.

Security-related events include, but are not limited to:

- Brute force attempts

- Accounts that have been automatically locked due to failed attempts
- Multiple simultaneous login events from any geo-locations
- Port scan attacks
- Evidence of unauthorized access
- Anomalous occurrences that are not related to specific applications on the host
- Theft of computing equipment

4.3 Log Review and Retention

- Review logs and security events for all system components to identify anomalies or suspicious activity.
- Review the following at least daily:
  - All security events
  - Logs of all system components that store, process, or transmit CHD and/or SAD
  - Logs of all critical system components
  - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)
- Review logs from all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
- Automation can improve the review and analysis of logs. However, log reduction, review, and reporting tools should support log analysis without altering original log records
- All physical and logical access logs, audit trails etc. shall be retained for a minimum of five years.

5 Compliance and Monitoring

- Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)
- Write logs for external-facing technologies onto a secure, centralized, internal log server or media device
- Promptly back up audit trail files to a centralized log server or media that is difficult to alter
- Set proper permissions on log files and use a separate server (Central Syslogger) to store all log files
- Make regular backups of the log files and encrypt log files.

6 References

NIST Special Publication 800-92 Guide to Computer Security Log Management

7 Standards Addressed

ISO 27001	
Clause/Annexure	**Description**
A12.4	Logging and monitoring

8 Exception(s)

Any requests for exceptions to this policy must be submitted in writing and will be reviewed on a case-by-case basis. Exceptions shall be permitted only after documented approval from the ISAC.

9 ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological Control	8.15 Logging Control Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analyzed. 8.16 Monitoring activities Control Networks, systems and applications shall be Monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.	Information Security and Monitoring Policy
Organizational Controls	5.28 Collection of evidence Control The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	Information Security Logging and Monitoring Policy

Appendix A: Source and Contents of Log

System/Software	Event/Activity to be Recorded
Anti-malware software (such as anti-virus, anti-	Instances of detected malware File and information system disinfection attempts File quarantines

spyware and root kit detectors	Malware scans Signature or software update	
Intrusion detection and intrusion prevention systems	Suspicious behavior Detected attacks Actions performed to stop malicious activity	
Remote access and wireless access systems	Login attempts Amount of data sent and received during session	
Web proxies	URLs accessed	
Vulnerability Management software (includes patch management and vulnerability assessment software)	Patch installation history Vulnerability status Known vulnerabilities Missing software update	
Authentication Servers (includes directory servers and single sign-on servers	Authentication attempt	
Routers and switches	Blocked activity	
Firewalls	Detailed logs of network activity	
Network Quarantine Servers	Status of host security checks Quarantined hosts and reason	
Operating Systems (—such as those for servers, workstations and networking	System Events • System shut down • Service starting	Security Events • File accesses • Policy changes

devices (e.g., routers, switches))		• Account changes
Applications (e.g., e-mail servers and clients, Web servers and browsers, file servers and file sharing clients, database servers etc.)	• Client requests and server response • Authentication attempts • Account changes • Use of privileges • Number and size of transactions • Operational events (Startup and shutdown)	• Configuration changes • Application-specific events such as: • Email sends and receipts • File access • Service request • System level transactions • Function performed (such as read, write, modify, delete)

Document Control

Owner:	CISO	**Release ID:**	ISLM-POL-0040

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.01	19 Oct 17	Kamadev Pradhan	Balu Nair		Creation of Policy	Initial Draft
1.00	23-Jun-2018	Kamadev Pradhan		Ganesh Arunachala	Approved by Ganesh	Baselined
1.01	29-Apr-19	Balu Nair	Joshy VM		Review	Information classification modified
2.0	14-May-19	Balu Nair	Ganesh Arunachala	Approved for Release		Baselined
2.1	11-May-2020	Karthik N	Balu Nair		Review	Modified the incident reporting
3.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and baselined

3.1	14-Jan-21	Balu Nair	Phani Krishna/ Rajesh B	Phani Krishna	Review	Updated the information classification
4.0	11-Feb-21	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and baselined
4.1	06-Oct-21		Karthik N		Review	Updated section 4.2 and format level changes. Added section 7
5.0	11-Oct-21		Karthik N	Sivaramakrishnan N	For Approval	Approved and baselined
6.0	30th Oct 2021	Pranesh K	Pranesh K	Gangadhar Aka	Review and updates	Document review and updates.
6.0	21-12-2021	Karthik N	Karthik N		Annual Review	No changes
6.1	06-01-2023	Sanjana,	ISDP Team		As per client feedback	Updated log retention period
7.0	06-01-2023	Sanjana	ISDP Team	Srikanth Mantena	For Approval	Approved and Baselined

7.0	30-04-2023	Sanjana	ISDP Team		For review	Reviewed with no changes
7.1	12-May-2023	Rama Madhavan	Vijaya		For Review	Migrated to new template
8.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
8.1	15-Feb-24	Shalini	Vijaya		For Review	Mapped with New ISO control 27k, 2022 8.15 and 8.16
9.0	23-Feb-24	Shalini	Vijaya	Srikanth	For Approval	Approved and Baselined
9.1	17-Apr-2025	Vijaya	Balu		For Yearly Review	Migrated to a new template
10.0	14-May-2025	Vijaya	Balu	Srikanth	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com