Vulnerability Management 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 shall ensure managing risks related to technical vulnerabilities in an effective, systematic, and repeatable way, and to confirm the effectiveness of actions.

2. Scope

This policy applies to all information assets connected to the Trianz network infrastructure including but not limited to computer workstations, laptops, tablets, smartphones, servers, appliances, network switches and routers, etc. The Chief Information Officer (CIO) and Chief Information Security Officer (CISO) shall ensure vulnerability assessments on any information asset, product, or service within Trianz.

3. Roles and Responsibilities

Sl. No	Item	Roles	Responsibility
1	Vulnerability assessment	CISO/CIO	• Responsible for overseeing the vulnerability assessment
2	Vulnerability assessment	IS Operations	• Applying all applicable fixes, patches and updates in a timely manner • Routinely reviewing vendor sites, bulletins, and notifications • Implementing vulnerability mitigation strategies in accordance with the organizational vulnerability management program • Responsible for tracking likely vulnerabilities in and patches available for their assets.
3	Vulnerability assessment	IS Operations	• Responsible for conducting vulnerability assessment as per the schedule.

4	Vulnerability assessment	IS Operations	• Responsible for review the vulnerability assessments reports for Management reporting.

4. Policy Statement

Processes to identify, classify and remediate vulnerabilities across all technology environments and platforms to reduce the Trianz's exposure to cyber threats must be documented.

Establish a vulnerability and patch management process to:

- Ensure information systems are patched in a timely manner.
- Ensure that the patch management process and cadence is consistent with the recommendation of patch providers.
- Reduce the number of service disruptions, incidents and problems caused by vulnerabilities.
- Provide a defined, repeatable method for ensuring consistent execution of associated patch management activities and tasks.
- Provide clarity around stakeholder/participant roles and responsibilities.
- Enable key performance metrics to be captured for performance monitoring and improvement.
- Define roles and responsibilities associated with vulnerability management.

- In support and consistent with the Asset Management policy, perform asset discovery scans on the internal network; update asset inventories as necessary.

- Monitor security-related email alerts and/or vendor notification sites for vulnerabilities that may affect systems or applications.

- Perform credentialed vulnerability scans. Where technically feasible, include endpoints (i.e., desktops and laptops).

- Conduct automated vulnerability scans, at a minimum quarterly, on internal and external networks.

- For PCI-specific environments, perform vulnerability scans on externally facing IP addresses; use an Approved Scanning Vendor (ASV) and track findings through remediation.

- Perform ad hoc vulnerability assessments after any significant change to the PCI environment (e.g., new system component installations, changes in network topology, firewall rule modification, major version upgrade).

- Perform vulnerability scanning before any significant infrastructure or application upgrade or modification (e.g., new system component installations, changes in network topology, firewall rule modifications) is implemented into production.

- Perform manual vulnerability assessments on a periodic basis to identify difficult to detect vulnerabilities.

- Test for the presence of unauthorized wireless access points on Commonwealth networks on a quarterly basis.

- Review public-facing web applications via manual or automated application vulnerability security assessment tools or methods at least quarterly.

- For PCI specific environments, perform reviews on public-facing web applications after any change to the PCI environment, or install a web application firewall in front of a public-facing web application as a mitigating control.

- Conduct internal and third-party network-layer and application-layer penetration testing at least annually or collect evidence to attest that the third party has had a vulnerability assessment performed.

- Perform timely reviews of vulnerability information received from internal and external sources (e.g., software suppliers) and report to the Trianz Chief Assurance Office. The report shall include:

    - Vulnerability description
    - Hosts affected
    - Current status at the time of reporting
    - Recommendations for remediation
    - Supporting information

- Vulnerabilities shall be prioritized using a risk-based approach

Severity	Level	Description	Remediation timeframe
🟨🟨🟨🟨⬜	Critical	Threat actor may gain control of the host, or there may be potential leakage of confidential information.	01 day
🟧🟧🟧⬜⬜	High	Threat actor may gain access to sensitive information stored on the host, including security settings resulting in potential misuse.	03 days

🟨🟨⬜⬜⬜	Medium	Threat actor may be able to collect sensitive information from the host, such as the precise version of software installed.	07 days
🟦⬜⬜⬜⬜	Low	Limited risk to host.	14 days

- Perform necessary actions to ensure that the likelihood and impact of threats, which can potentially exploit vulnerabilities are minimized by implementing security controls within the established timeframes.

- Remediate vulnerabilities by deploying patches or making configuration changes as a mitigation strategy. Appropriate testing must be conducted prior to patch deployment.

- In the event that a patch or mitigation strategy is not available to remediate the vulnerability, a mitigating control shall be enacted or an approval for security deviation from the CIO / CISO is required.

- Report through the various stages of the vulnerability and patch management process using established performance metrics. Summary reports shall be used to inform management of the current status and effectiveness of the vulnerability and patch management program.

- IS Operations must report vulnerabilities on a monthly basis to the CIO/CISO Office:

    - ❖ Vulnerabilities by severity and aging
    - ❖ Vulnerabilities with deviations in place
    - ❖ Open and closed vulnerabilities

- Periodic Vulnerability assessment of its information assets, network equipment’s and applications have to be conducted and fix all gaps found during the assessment.

- On a quarterly basis Vulnerability assessment to be conducted enterprises wise or as per Client requirements. Assessments are repeated until “clean results” are obtained.

- Any major change in the IT environment has to be followed by vulnerability assessment and penetration testing to the setup. These penetration tests conducted on Annual basis. Application Layer and Network Layer Penetration Tests (including components that support network functions as well as operating systems)

- The Penetration tests must be carried out either by Third party organization specialized in Security Testing or by specialized internal resource. It shall be ensured that penetration test.

    - Includes coverage for the entire Trianz Network perimeter and critical systems
    - Includes testing from both inside and outside the network
    - Includes testing to validate any segmentation and scope-reduction controls
    - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
    - Specifies retention of penetration testing results and remediation activities results.

- Wireless Network scans are performed using Wireless Analyzer on quarterly basis.

- System File Integrity Monitoring must be done on all critical servers in production environment and servers storing Cardholder information.

- All function owners to follow the timeline requirements for reacting to notifications of relevant vulnerabilities.

5. Measurement and Review

- Mean time interval taken to remediate / patch vulnerabilities after identification by the Vulnerability Assessment (VA) tool. (i.e. post detection)

- This measures the ratio of known assets (e.g.: from Asset Management solution) to those which actually get scanned and an be split by Internal Assets & External assets.
- Based on Risk based Prioritization of vulnerability, considering a number of factors (e.g.: CVSS, Asset Criticality, Exploit Availability, Asset Accessibility (Internet vs Intranet), Asset Owner etc.)

- Based on Risk based Prioritization of vulnerabilities (outlined above), the average risk exposure can be calculated based on different groupings.

- What % of systems are fully patched and have no high severity vulnerability present and can be reported by asset groups.
- Inputs for above measurements are obtained from Vulnerability assessment tool and for more details; you can refer to Vulnerability Assessment and Penetration Testing (VAPT) procedure

6. Compliance and Monitoring

- Users Access right: Periodic review of the entire user identity, provisioning and access rights lifecycle, with findings, analysis, and recommendations reported to senior management within timeline.

- Configuration Standards: Periodic review of critical system resources for ensuring the applicable hardening reported to senior management within timeline.
- Network Architecture and Topology: Periodic review of the entire Resolver security architecture for ensure a layered, Défense in Depth approach is being utilized, with findings, analysis, and recommendations reported to senior management within Resolver.

7. Exception(s)

None

8. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological Control	8.8 Management of technical vulnerabilities	Vulnerability Management Policy

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Author	Date	Reviewer	Introduction/Reason for Change	Approver	Change Description
0.01	Kamadev Pradhan	14-May-18	Balu Nair			Initial Draft
1.00	Kamadev Pradhan	20-Jun-2018		Approval for Baseline	Ganesh AJ	Baseline
1.1	Karthik N	6-May-2020	Balu Nair	For Review	-	Updated information classification n and modified with CISO/CIO roles
2.0	Karthik N	15-May-2020	Balu Nair	For Approval	Phani Krishna	Approved and Baselined
2.1	Karthik N	19th May 20	Anitha Ravindran	Review comments from DA		Changes made in Measurement and review
3.0	Karthik N	19th May 20	Phani Krishna	For Approval	Phani Krishna	Approved and Baselined
3.1	Balu, Vijaya	28 Jul 2020	Phani Krishna	Fore Review		Modified Purpose of the document, CISO and CIO Responsibilities

						Formatted the document to ensure the readability/legibility
4.0	Balu, Vijaya	28 Jul 2020	Phani Krishna	For Approval	Phani Krishna	Approved and Baselined
4.1	Balu Nair	14-Jan-21	Vijaya and Bala	Review	Phani Krishna	Updated the information classification
4.2	Shalini	11-Feb-24	Vijaya and Bala	Review	Srikanth	Mapped with new ISO 27k 2022 Controls
5.0	Shalini	23-Feb-24	Vijaya and Bala	For Approval	Srikanth	Approved and Baseline
5.1	Krutideepta Barik	30-Apr-25	Vijaya and Bala	For Yearly Review		Migrated to a new Template.
6.0	Kruti	14-May-25	Vijaya and Bala	For Approval	Srikanth	Approved and Baseline

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com