TRIANZ℠

Anti-Virus Malware 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 is designed to protect the organizational resources against intrusion by viruses and other malware. This document establishes the corporate policy and standards for antimalware protection on any system owned by Trianz and all other system resources, both internally and externally, that interact with these systems.

2. Objective

The objective of the policy and applicable procedure is to provide Trianz with a documented and formalized process to ensure the implementation of antivirus and anti-malware technical controls on all applicable systems. Compliance with stated policy and supporting procedure also contributes to the confidentiality, integrity, and availability of the Trianz systems.

3. Scope

This policy covers all system resources that are owned, operated, maintained, and controlled by Trianz and all other system resources, both internally and externally, cloud service provisioning, cloud service consumption that interact with these systems including products.

4. Policy Statements

The anti-virus product shall be operated in real time on all servers and individual computers/Laptops. The product shall be implemented to cater for the following threats as minimum:

- The anti-virus library definitions shall be updated within 1 day of their release.

- Anti-virus scans shall be done a minimum of once per week on all user-controlled workstations and servers.
- All personal computers and servers that are connected to the Trianz's network or otherwise using the IT facilities must run an approved and up-to-date anti-virus product that continually monitors for malicious software (viruses, worms, Trojan horse, rootkits, adware, spyware, logic bombs, etc.).
- Do not try to uninstall or disable anti-virus software. Any messages suggesting that anti-virus protection has been disabled should be investigated immediately.
- No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.
- All personal computers, devices and servers connected to Trianz's network must run the latest available patches applied on the operating system as well as on the applications.
- Removable devices such as USB Drives, CDs, etc. shall be scanned before being connected to Trianz's network.
- Trianz's IS policy prohibits any activity intended to create and / or distribute malicious code (viruses, worms, etc.) on the network or IT facilities.
- Trianz reserves the right to disconnect any device from the network if an infection is found or suspected. The device will be disconnected until the infection is removed and suitable preventative tools have been installed on the device.
- If a device is infected with a virus, the incident to be reported to the Helpdesk staff who shall follow the standard incident handling procedures.
- Email attachments must be scanned by an anti-virus product before delivery.
- Check the authenticity of attachments / software to be installed from internet sources. Do not install applications that arrive on unsolicited media.
- Reports shall be generated to identify the systems that have not received the latest anti-virus updates. The updates shall run either remotely or on site for such systems.
- Awareness and training sessions on malware protection systems shall be held to report and recover from malware attacks.
- Regular reviews of the software and data content of systems supporting critical business processes shall be conducted to ensure reduction of vulnerabilities that could be exploited by malware, e.g., through technical

vulnerability management (as per the Vulnerability Management Procedure).

- Appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup and recovery arrangements, implementing procedures to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware implementing procedures to verify information relating to malware shall be implemented.

5. Roles & Responsibilities

Sl. No	Item	Roles	Responsibility
1	Anti-Virus/Malware	Associate	• Check whether Anti-virus software is installed and updated.
2	Anti-Virus/Malware	IS Operations/, Cloud Service Customer	• Check all the Desktops, Laptops; Servers are installed with Anti-virus/malware software. • Check all the endpoint devices and servers updating with Anti-virus signatures.
3	Anti-Virus/Malware	IS Operations	• Continuous Monitoring- (24x7x365 Days). • Immediate reporting of unauthorized activities.
4	Audit & Compliance	InfoSec Assurance	• Spot Audit. • Annual Policy & Compliance Review.

6. Measurement and Review

- What percentage of systems have anti-virus tools installed and enabled on them?
- What percentage of systems have up-to-date anti-malware signatures?
- What percentage of systems have specific anti-malware tools or features installed and are active (e.g., anti-spyware, browser protection, etc.)?

7. Compliance and Monitoring

The InfoSec Assurance team will verify compliance with this policy through various methods, including but not limited to business tool reports, internal and external audits etc.

8. Exceptions(s)

None as of now. Exceptions to the Anti Malware Policy shall follow the Exception handling policy.

9. ISO Control Mapping(s)

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological Controls	8.16 Monitoring activities Control Networks, systems and applications shall be Monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Anti-virus Malware policy
Technological Controls	8.7 Protection against malware	Anti-virus Malware policy

Document Control

Owner:	CISO	Release ID:	AVM-POL-047

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.01	14 Apr 2018	Kamadeva Pradhan	Balu Nair		Initial Draft	**None**
1.00	20-Jun-2018	Kamadeva Pradhan		Ganesh AJ	Approval for Baseline	Baseline
2.00	22-Nov-2019	Vijaya Rajeswari	Phani Krishna	Vivek Sambasivam	Updated to align to ISO 27017 and ISO 27018 Standard	Roles and responsibilities for Cloud Provider and Cloud Customer updated
2.1	11-May-2020	Karthik N	Balu Nair		Review	Formatting changes Integrated with new template

3.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
3.1	1-Feb-2021	Vijaya Rajeswari	Phani Krishna		For Review	Information Classification updated
4.0	1-Feb-2021	Vijaya Rajeswari	Phani Krishna	Phani Krishna	For approval	Approved and Baselined
4.0	3-Jan-22	Divya	Balu Nair		Annual review	No changes
4.1	15-03-22	Sanjana	Balu Nair		For review	The scope has been extended to products and services
5.0	18-03-22	Sanjana	Balu Nair	Siva N	For approval	Approved and baselined
5.1	14-03-23	Krutideepta, Shalini Kumari	Karthik N		For Review	New template change Editorial changes Objective added
6.0	12-05-2023	Krutideepta	Karthik N	Srikanth M	For Approval	Approved & Baselined
6.1	15-Feb-24	Shalini	Vijaya		For Review	Mapped with ISO 27001,2022 control 8.16

7.0	23-Feb-24	Shalini	Vijaya	Srikanth	For Approval	Approved and Baselined
7.1	30-Apr-25	Krutideepta Barik	Vijaya R		For Yearly Review	Migrated to a new Template.
8.0	14-May-25	Krutideepta Barik	Vijaya R	Srikanth	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com