



# Prevention and Detection of Malicious Attack Procedure



TRIANZ INTERNAL

[trianz.com](http://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

<input type="checkbox"/>	Public
<input checked="" type="checkbox"/>	Internal
<input type="checkbox"/>	Confidential
<input type="checkbox"/>	Restricted

## Table of Contents

<b>1. OBJECTIVE</b>	<b>4</b>
<b>2. SCOPE</b>	<b>4</b>
<b>3. REFERENCE(S)</b>	<b>4</b>
<b>4. PROCEDURE</b>	<b>4</b>
4.1 Desktop / Workstation	4
4.2 Servers	4
4.3 Gateway Anti-virus	5
4.4 Users	5
4.5 Virus Detection and Prevention Tips	6
4.6 Contact with Special Interested groups	6
<b>5. ISO CONTROL MAPPING(S)</b>	<b>6</b>

## 1. Objective

The purpose of this control is to device a high performance policy-based anti-virus and content for Trianz to protect the enterprise's network and system from virus attacks, worms, Internet borne email viruses and prevent transmission of spam or non-business related contents

## 2. Scope

This control is applicable to all Trianz associates. It covers workstations/servers/devices located on TRIANZ's networks or which are connected to Trianz Infrastructure. It is applicable to all systems under the jurisdiction and/or ownership of TRIANZ, inclusive of hired systems. This control also covers all workstations and servers supplied by the customers of TRIANZ, as long as they are operated from within TRIANZ premises and all Trianz products and services.

## 3. Reference(s)

None

## 4. Procedure

### 4.1 Desktop / Workstation

Every system (i.e. PC, Laptop, etc.) must have Organization Standard corporate anti-virus software installed, which has to be regularly updated with latest patches. This will be done automatically if you are connected to the Trianz network. It is the responsibility of every employee at Trianz to ensure that his/her desktop/laptop has the latest pattern for the Anti-Virus signature files and ensures that the same is virus free.

In cases of zero-day signature update, same will be done manually by the IT team.

### 4.2 Servers

Latest anti-virus pattern file will be downloaded automatically, and updated on the Servers. In cases of zero-day signature update, same will be done manually by the IT team

### 4.3 Gateway Anti-virus

- For Internet Connection

The gateway Anti-Virus should monitor all inbound connections and accordingly filter out all malicious content which is being downloaded from the Internet.

- For E-mail

The gateway anti-virus should monitor all inbound and outgoing mail to Trianz mail server and accordingly filter out mails containing viruses.

### 4.4 Users

- Have the organization-standardized anti-virus software installed (if not installed by default) on your computer by IT Helpdesk Executive.
- Regularly scan your computer using the anti-virus software installed on your computer.
- Make sure that your anti-virus software is regularly updated to take into account new viruses and variants recently written.
- Always scan the removable storage media before accessing the files.
- In addition to saving your data files (documents, spreadsheets, etc.) to the hard drive, consider saving the critical files in centralized file server. The file server drives are scanned & backed up regularly. Having a backup of your data files may prevent data loss if a virus infects your hard drive.
- While downloading files/information from the Internet, always scan the files prior to running them.
- Do not run any Pirated programs on computer as pirated programs are a major source of viruses.
- Do not stop, remove or uninstall the Anti-Virus software from your computer.
- Do not download programs from any un-trusted or suspicious Internet site or networks. Categorized Web Filtering has been enabled to ensure this, however, the users are expected to exercise discretion while surfing the net.
- If any user feels that his/her desktop/laptop is infected with virus then it is his/her responsibility to inform the IT helpdesk about the same, through e-mail or in person

## 4.5 Virus Detection and Prevention Tips

- Do not open any files attached to an email from an unknown, suspicious or untrustworthy source
- Do not open any files attached to an email unless you know what it is, even if it appears to come from someone you know. Some viruses can replicate themselves and spread through email
- Do not open any files attached to an email if the subject line is questionable or unexpected. If the need to do so, always save the file to your hard drive before doing so
- Update the anti-virus software regularly as lots of new viruses are discovered each month.
- Back up the files on a regular basis to local file server. If a virus destroys the data files, they can be replaced with the back-up copy.
  - When in doubt, do not open, download, or execute any files or email attachments

### Symptoms of virus

- The program takes longer to load suddenly
- The program size keeps changing
- The disk keeps running out of free space
- The drive light keeps flashing when the user is not doing anything
- The files have strange names which are not recognizable
- The computer is not able to remember CMOS settings
- System memory reduces Icons change in appearance

## 4.6 Contact with Special Interested groups

Trianz can take the help of external consultant on information security in case of any support or critical decision making processes.

## 5. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
	NA	Prevention and Detection of Malicious attack Procedure

## Document Control

<b>Owner:</b>	CISO	<b>Release ID:</b>	PDMA-PROC-0050
---------------	------	--------------------	----------------

### For Trianz Process Improvement Group (TPIG) Purpose Only

#### Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.00	19-Feb-07	Jyotessh G Nair			Initial draft	•
1.00	26-Feb-07	Jyotessh G Nair			Baseline is approved by Zulfikar Deen.	• Approved Baseline.
1.01	14- May 09	Bharateesh a B R			Risk Assessment and Treatment Plan	• Consolidated the controls for preventing malicious attack.
2.00	03-Jun-09	Balu Nair			Approval for Baseline	• Baseline
2.01	30-Dec-10	Chakravarti			QMG review	• Formatted entire document and modified properties also
3.00	30-Dec-10	Chakravarti			Approval for Baseline	• Base lined

3.01	24-May-11	Srilakshmi			QMG Review	<ul style="list-style-type: none"> <li>Modified release id in header and cover page to make consistency</li> </ul>
4.00	24-May-11	Srilakshmi			Approval for Baseline	<ul style="list-style-type: none"> <li>Baselined</li> </ul>
4.01	3-Aug-11	Sudharsana			QMG review	<ul style="list-style-type: none"> <li>Replace Owner with Management Representative in place of CIO</li> <li>In Document Classification Scheme, "Retention period is 3 Years" row is removed</li> </ul>
5.00	3-Aug-11	Sudharsana			Request for baseline	Approved and Baseline
6.00	8-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	<ul style="list-style-type: none"> <li>Modified the template format</li> <li>Changed the Logo</li> </ul>
7.00	14-May-15	Sudharsana			Upgrading to ISO 27001:2013 version	<ul style="list-style-type: none"> <li>Added section 4.6 Contact with Special Interested groups</li> </ul>
7.01	29-Apr-19	Balu Nair	Joshy VM			Information classification modified Trianz logo modified
8.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	<ul style="list-style-type: none"> <li>Baselined</li> </ul>
8.1	12-May-20	Balu Nair	Phani Kraishna		Annual Review	<ul style="list-style-type: none"> <li>Migrated to the new template</li> </ul>

9.0	15-May-20	Balu Nair	Phani Kraishna		For Approval	<ul style="list-style-type: none"> <li>Approved and Baseline</li> </ul>
9.1	3-May-21	Divya G	Vijaya	Phani Kraishna	Annual Review	<ul style="list-style-type: none"> <li>Updated with new Information classification</li> </ul>
10.0	3-May-21	Divya G	Vijaya	Phani Kraishna	For Approval	<ul style="list-style-type: none"> <li>Approved and Baseline</li> </ul>
10.0	06-Jan-22	Divya G	Balu Nair		For Review	<ul style="list-style-type: none"> <li>No Changes</li> </ul>
11.1	24-Feb-2022	Kruti	Kartik		For Review	The scope has been extended to products and services
12	28-Feb-2022	Kruti	Siva N	Siva N	For Approval	Approved and baselined
12.1	28-Feb-2023	Kruti and Asha Veeramallu	Karthik N		For Review	Updated the Scope and section 4 New template change
13.0	08-May-2023	Kruti	Karthik N	Srikanth M	For Approval	Approved and baselined
14.0	23-Feb-24	Shalini	Vijaya	Srikanth M	For Approval	Reviewed and No changes.
14.1	28-May-25	Vijaya	Balu		For yearly review	Migrated to a new template
15.0	29-May-25	Vijaya	Balu	Srikanth M	For approval	Approved and Baseline



## Contact Information

Name

Email

Phone

# Thank You

[infosec@trianz.com](mailto:infosec@trianz.com)



The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.