TRIANZ℠

WEB FILTERING 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. Introduction

Web filtering enables Trianz to monitor, manage, and regulate users' web activity. By allowing access to approved websites (green sites) and blocking malicious or non-compliant content, web filtering helps protect against cybersecurity threats, enforce corporate policies, and enhance overall network security. This ensures a secure and productive browsing environment while mitigating risks such as malware, phishing, and unauthorized data access.

2. Objectives

- The objective of this policy is to establish controls to ensure authorized network traffic and prevent unauthorized access to the Internet.
- Enhance Cybersecurity – Prevent access to malicious websites that may contain malware, phishing attempts, or other cybersecurity threats.
- Ensure Compliance – Enforce regulatory, legal, and organizational policies by restricting access to unauthorized or non-compliant web content.
- Mitigate Insider Threats – Monitor and control employee web activity to identify and prevent potential security risks from within the organization.

3. Purpose

- This Policy is to protect systems from malware compromise and prevent access to unauthorized web resources.
- This enables Trianz to eliminate security risks such as malware infection that may arise because of access to external websites with malicious content.

4. Policy

Trianz shall establish and implement necessary controls to prevent employees from accessing external websites that may contain viruses, phishing materials, or other types of illegal information.

Infosec and IS Team shall determine or decide on which websites shall not be accessed by employees and IS team shall implement the same in the security controls.

In particular, the following types of websites shall be blocked:

- Websites with information upload functionality – Access shall be restricted and only permitted upon approval for legitimate business needs.
- Websites containing malicious content – Sites known or suspected to host malware, phishing, or other cyber threats shall be blocked.
- Command and Control (C2) servers – Access to known C2 infrastructure shall be denied preventing cyberattacks.
- Threat intelligence-based malicious websites – Malicious domains identified through threat intelligence sources shall be restricted, in alignment with the Threat Management Policy.
- Websites distributing illegal content and materials – Any website hosting illegal or unethical content shall be blocked.

5. Implementation Guidelines

Trianz shall ensure effective techniques to prevent access to dangerous external websites by blocking the IP addresses or domain of websites identified as dangerous. For instance, some browsers and anti-malware tools enable Trianz to do this automatically with effective implementation.

a) Trianz shall ensure the web filtering practices as defined below:

URL Categorization:

- Blacklists and Whitelists are compared against predefined lists of known malicious or safe websites.
- Human reviewers assess URLs and assign them to appropriate categories based on their content.

- Contextual Analysis of URLs are categorized based on the context in which they are shared or accessed, such as within a specific application or communication channel.

Web Content Filtering:

Maintain log details of each access attempt, including the user, time, URL, and action taken (allowed or blocked).

These logs can be used for auditing, compliance, and troubleshooting purposes. Additionally, reporting features provide insights into web usage patterns and policy violations.

SSL Inspection:

Decrypt and inspect encrypted HTTPS traffic to enforce content filtering policies on secure connections.

b) Trianz shall consider blocking access to the following types of categories:

Blocked Categories:

- Adult Content: Internet Websites containing explicit sexual material, nudity, or pornography.
- Gambling: Internet Websites related to online betting, casinos, or gambling.
- Malware and Phishing: Websites known for distributing malicious software or phishing attacks.
- Illegal Activities: Internet Websites promoting illegal drugs, hacking, or other unlawful activities.
- Violence and Hate Speech: Web Content advocating violence, hate speech, or discrimination.
- Social Networking (if restricted): Internet Websites like Facebook, Twitter, or Instagram, which can be distracting during work hours.
- Streaming Media (if restricted): Web Video and audio streaming platforms like YouTube, Netflix, or Spotify.
- Gaming (if restricted): Web Online gaming sites that may impact productivity.
- Peer to Peer File Sharing: Includes file sharing sites such as Google Docs and Dropbox

- Personals and Dating: Includes online dating sites.
- Dead/Obsolete: Websites that are no longer maintained.
- Anonymous Pop-ups, advertisement: Includes specific sites who serve ads to websites.

c) Trianz shall consider Allowing access to the following types of categories:

Allowed Categories:

- Education and Learning: Educational resources, e-learning platforms, and research articles.
- Health and Wellness: Health-related Internet Websites, medical information, and wellness blogs.
- Technology and Science: Technology blogs, scientific research, and software development resources.
- Travel and Tourism: Travel guides, booking platforms, and destination information.
- Business and Economy: Internet Websites related to business news, stock markets, and financial information.
- News and Media: Reliable news sources, journalism, and current events.

d) Trianz shall take necessary action on False positives cases.

- Prior to deploying this control, Trianz shall establish rules for safe and appropriate use of online resources, including any restriction to undesirable or inappropriate websites and web-based applications. The rules shall be kept up to date.
- Training shall be given to personnel on the secure and appropriate use of online resources.
- including access to the web. The training shall include Trianz rules, contact points for raising security concerns, and exceptional processes when restricted web resources need to be accessed for legitimate business reasons. Training shall also be given to personnel to ensure that they do not overrule any browser advisory that reports that a website is not secure but allows the user to proceed.
- Web filtering can include a range of techniques including signatures, heuristics, list of acceptable websites or domains, list of prohibited websites or domains and bespoke configuration to help prevent malicious software and other malicious activity from attacking the Trianz network and systems.

6. ISO Control Mapping

Category of Control	ISO 27001:2022 Control	Document name as per ISO 27001:2022
Technological Control	8.23 Web filtering Control Access to external websites shall be managed to reduce exposure to malicious content	Web Filtering Policy

Document Control

Owner:	CISO	**Release ID:**	WEB-POL-0075

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	09-FEB-2024	Aishee Ghosh	Vijaya		Initial draft	Initial release to Blue Book
1.0	23-FEB-2024	Shalini	Vijaya	Srikanth	For Review and Approval	Approved and baselined
1.1	20-MAY-2024	Nagarathinam	Vijaya and Balu		For Review	Updated the contents on section. 6Guidance. (Web filtering practices, categorization, and False positive)
2.0	06-JUNE-2024	Nagarathinam	Vijaya and Balu	Srikanth	For Approval	Approved and baselined
2.1	07-Mar-25	Krutideepta Barik	Vijaya R, Balu Nair & Beniyel S		For Yearly Review	Introduction, Objectives, Policy Statement

						Section have been Modified. Ownership of the Control Section has been removed. Migrated to a new Template.
3.0	14-May-25	Krutideepta Barik	Vijaya R, Balu Nair & Beniyel S	Srikanth	For Approval	Approved and baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com