TRIANZ℠

Patch 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 document describes the Information Security requirements for maintaining up-to-date Security patches on all the systems.

2. Objective

- The objective of this policy is to prevent the exploitation of vulnerabilities on computing and related systems.
- All Systems, Servers and Network Devices must be maintained, and security patches must be applied in a timely manner consistent with an assessment of risk.

3. Scope

This policy applies to all Systems, Network Devices and Servers of Trianz which are on premise, or any Cloud based infrastructure or service where Patch Management is Trianz's responsibility. This includes systems that contain company or client data owned or managed by Trianz regardless of location (On-prem or Cloud).

4. Policy Statement

4.1 Trianz Owned Assets

- Systems, Servers, and infrastructure owned and managed by Trianz shall be installed with latest security patches to protect the assets from known/Unknown vulnerabilities.
- Security Patches shall be identified, reviewed, tested and approved before implementing in the production environment.
- All Security patch updates, shall be followed through the Change control process. This is to ensure successful completion of patch updates.

4.2 Supplier Owned Assets

- Systems, Servers, and infrastructure owned by Supplier and managed by Trianz/Supplier shall be installed with latest security patches to protect the assets from known/Unknown vulnerabilities.

- In case of patches to be applied from supplier end the contract should clearly specify the same.
- Security Patches shall be identified, reviewed, tested, and approved before implementing in the production environment.
- All Security patch updates shall be followed through the Change control process. This is to ensure successful completion of patch updates.
- Trianz supplier security policy shall enforce Security patch compliance by the Suppliers/ vendors by conducting periodic vendor audits and SLA reviews.

5. Patching Schedule

IT infrastructure

Period	Activity
Monthly	Critical Security patches and Security updates and general System updates, Critical Third-party application patches and upgrades based on the security recommendations.
Quarterly	Server Updates
On-demand	High/Critical severity patches will be deployed immediately based on security recommendations

Printers, peripherals, switches, routers, firewalls, and storage

Period	Activity
Quarterly	Check for new firmware updates. Reference: OEM portals, emails, Security Blogs etc..
Vendor Update	Upgrade firmware within a week of vendor notifications. Reference: Vendor notifications,

5.1.1.1	On-demand, and emergency security patching	The IS Security team will determine the risk and the relevance of the patch, as well as when the system should be patched. All related Critical, High, and Business impact patches shall be deployed immediately upon approval.
5.1.1.2	Zero-day Vulnerabilities	**Immediate Risk Assessment:** Identify affected systems, assess the impact, and determine exposure. **Emergency Patch Deployment:** Apply vendor-released patches or hotfixes as soon as they become available. **Temporary Mitigations:** If no patch is available, implement workarounds such as disabling affected services, applying firewall rules, or restricting access. **Expedited Testing:** Conduct rapid testing of patches in a controlled environment before deployment to prevent system disruptions. **Prioritized Deployment:** Apply patches on critical systems first, followed by non-critical assets. **Monitoring & Threat Intelligence:** Continuously monitor for new threats, indicators of compromise, and vendor updates. **Incident Response Integration:** Align with the incident response process to contain, eradicate, and recover from potential exploitation. **Post-Patch Review:** Validate successful updating of patches, conduct security testing, and update documentation for future reference.
Exceptions		Systems, Network Devices, Security Appliances and applications that cannot be patched to resolve a known vulnerabilities

	will have the justification documented by the device/application owner and ensure that the necessary compensating control(s) are implemented.

Systems

- All the Systems (Desktops and laptops) must have automatic updates enabled for Security patches for Operating System.
- All the endpoints will be patched for Critical third-party applications or new version upgrades based on security recommendations.

Servers and Network/security Devices:

- Servers (Unix, Linux, Windows, etc.) must comply with the Operating Systems patches released by the vendors or as per the Trianz patch update schedule, whichever is earlier.
- Network/Security Devices must comply with the Internet Operating Systems, Firmware and patches released by the OEMs and vendors or as per the Trianz patch update schedule, whichever is earlier.
- Above patch schedule is defined to address the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Trianz asset and the data that resides on the system.

6. Monitoring and Reporting

- Patch implementation reports shall be generated and maintained by the IS Operation team, which will be used to summarize the outcome of each patching cycle.
- These reports shall be used to evaluate patch implementation, the current patching levels of all systems and to assess the current level of risk.

7. Roles and Responsibilities

Role	Responsibility	Internal/External
System Owner	They are responsible for ensuring that software they manage is maintained	Internal

	through regular software updates and patching	
CIO	CIO is accountable for ensuring that the software update and patching policy is adhered to	Internal
IS operation	IS Operation being responsible for Implementation and enforcement of this policy.	Internal
InfoSec Team	Conduct periodic/Spot audits to ensure compliance.	Internal
Product Owner / project manager	Ensure all the end points systems are patched that are being used for projects	Internal

8. Applicable Standards

- ISO 27001:2022
- ISO 27701:2019

9. ISO Controls Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological Controls	8.19 Installation of Software on Operational Systems	Patch Management Policy

10. Reference Policies & Procedures

- Information security Policy.
- IS Operations Process.
- System and Software Change Management Policy.
- System and Software Change Management Procedure.

11. Exceptions(s)

Exceptions to the Patch management policy will require formal written approval from the Information Security & Data Privacy Assurance Team.
Refer to Exception Handling Policy

Document Control

Owner:	CISO	**Release ID:**	PATM-POL-0051

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Introduction/Reason for Change	Approver	Change Description
0.01	25-May-17	Roshni Madhudhan	Shishir Kumar Singh & Kamadev	Creation of Patch Management Policy	Ganesh Arunachal	Initial Draft
0.02	12-May-18	Kamadev	Joshy VM Balu Nair	Review before final release to Blue book.	Ganesh Arunachal a	Updated as per the standard & inclusion of metrics
1.00	20-Jun-18	Kamadev Pradhan		Approval for Baseline	Ganesh AJ	Baseline
1.1	6-May-20	Vijaya Rajeswari	Karthik, Balu	For Review		Information Classification updated
2.0	15-May-20	Vijaya Rajeswari	Karthik, Balu	For Approval	Phani Krishna	Approved and Baselined
2.1	28-July-20	Anitha Ravindran	Phani Krishna	Half yearly review as per Policy		Added information

						pertaining to cloud as well and Baselined
3.0	31-July-20	Anitha Ravindran	Phani Krishna	Half yearly review as per Policy	Phani Krishna	Approved and Baselined
3.1	21-Jan-21	Divya Gongalla	Phani Krishna	For Review	Phani Krishna	Updated new information classification
4.0	21-Jan-21	Divya Gongalla	Phani Krishna	For Approval	Phani Krishna	Approved and Baselined
4.1	30-July-21	Divya Gongalla	Phani Krishna	For Review	Phani Krishna	Added Roles and Responsibilities
5.0	30-July-21	Divya Gongalla	Phani Krishna	For Approval	Phani Krishna	Approved and Baselined
5.1	8-Nov-21	Siva Krishna & Pranesh	Gangadhar Aka	For Review	Sivaramakrishnan N	Updated the policy section 5
6.0	8-Nov-21	Siva Krishna & Pranesh K	Gangadhar Aka	For Approval	Sivaramakrishnan N	Approved and Baselined
6.0	23-Jan-21	Divya G	Karthik N	For Review and Approval	Sivaramakrishnan N	Reviewed and no changes

6.1	13-Mar-22	Sanjana	Karthik N	For Review	Sivaramakrishnan N	The scope has been extended to products and services
7.0	21-Mar-22	Sanjana	Sivaramakrishnan N	For Approval	Sivaramakrishnan N	Approved and Baselined
7.1	12-May-2023	Balu Nair, Shalini Kumari	Vijaya R	Yearly Review		Format and changes done New template change
8.0	12-May-23	Balu Nair		Yearly Review	Srikanth Mantena	Approved and Baselined
8.1	15-Feb-24	Vijaya	Balu	For review	Srikanth Mantena	Updated the section ISO Control Mapping aligning to ISO 27001:2022
9.0	23-Feb-24	Vijaya	Balu	For Approval	Srikanth Mantena	Approved and Baselined
9.1	05-Mar-25	Krutideepta Barik	Vijaya R, Balu Nair & Beniyel S	For Yearly Review		Supplier Owned Assets Section & Patching

						Schedule (Zero Day Vulnerability) Section Has been modified. Migrated to a new Template.
10.0	14-May-25	Krutideepta Barik	Vijaya R, Balu Nair & Beniyel S	For Approval	Srikanth Mantena	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com