TRIANZ℠

WIRELESS SECURITY 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. Glossary

Word/Abbreviation	Description
WLANs	wireless local area networks
SSID	Service Set Identifier
WPA	Wi-Fi Protected Access
Wi-Fi	Wireless Fidelity

2. Purpose

The Wireless devices or networks used to access, store, process, or transmit Trianz's information or access must be implemented in a secure manner. This document describes the Information Security requirements for maintaining up-to-date Security patches.

3. Objectives

This policy applies to all wireless devices, networks, services, and technologies used to access, store, process or transmit Trianz's information. The term "wireless" refers to any technology that does not use cables.

Wireless includes radio frequency (i.e., satellite, microwave, radio) and optical (i.e. infrared) technologies.

Wireless networks include both wireless local area networks (WLANs) and wireless wide area networks.

Wireless devices are any end-user device that uses wireless technology to communicate.

4. Scope

The scope of this Policy is to secure and protect Trianz's Wi-Fi assets from wireless security threats.

5. Policy

5.1 Access Control

All wireless infrastructure devices that reside at Trianz's network, or provide access shall:

- Use Industry Standards for Wireless Security
- Use Industry Standard authentication protocols and infrastructure
- Use industry Standard encryption protocols
- Maintain a hardware address (MAC address) that can be registered and tracked.

5.2 Risk Assessment

Trianz's Security Team shall employ security measures commensurate with the risk associated with the wireless network.

Due to the ever-changing threats and vulnerabilities, risk assessments shall be conducted on a periodic basis no less than annually to provide an accurate picture of the total risk to the organization.

A risk assessment shall be performed to ensure the capabilities of protection for the technologies utilized.

A risk assessment shall include but not limited to; identifying data sensitivity, network vulnerabilities, and critical services. The focus is to identify potential threats and vulnerabilities.

5.3 Securing Wireless Networks and Devices:

- **Change default passwords.:** Changing default passwords makes it harder for attackers to access a device. Use and periodic changing of complex passwords shall be your first line of defense in protecting your device
- **Restrict access:** Only authorized users shall be allowed to access Wi-Fi network. Each piece of hardware connected to a network has a media access control (MAC) address. Restrict access Wi-fi network by filtering these MAC addresses.

- **Encrypt the data on your network:** Encrypting Trianz's wireless data prevents anyone who might be able to access network from viewing it. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices.
- WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.
- **Protect Service Set Identifier (SSID):** To prevent outsiders from easily accessing Trianz's network, avoid publicizing your SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer's default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.
- **Install a firewall:** Consider installing a firewall directly on your wireless devices (a hostbased firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer.
- **Maintain antivirus software:** Install antivirus software and keep your virus definitions up to date. Many antivirus programs also have additional features that detect or protect against spyware and adware.
- **Keep your access point software patched and up to date:** The manufacturer of wireless access point will periodically release updates to and patches for a device's software and firmware. Be sure to check the manufacturer's website regularly for any updates or patches for your device.
- **Check internet provider's or router manufacturer's wireless security options:** Internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions. **This shall be applicable for work from home users.**

6. Patching Schedule:

Period	Activity
Monthly	Critical Security patches and Security updates and general System updates, OEM released patches and upgrades based on the security recommendations.
Quarterly	Release Updates and upgrades
On-demand	High severity critical patches will be deployed immediately based on s recommendations

7. Monitoring and Reporting:

Wireless strength: Monitor and manage factors like total number of access points, number of users, rogue access point signal strength.

Wireless network traffic: Monitor the total bytes received by wireless client systems, total bytes received by access points and more

Wireless network utilization: Monitor the various parameters that helps to keep a tab on the utilization of wireless networks such as CPU utilization, memory utilization, total bytes sent to the station, disk utilization, client total bytes transmitted etc.

MIS Reports must generate based on monitoring factors and alert must be generated as and when modifications happen at the wireless networks.

8. Roles & Responsibilities

Role	Responsibility	Internal/External
IS Administrators	IS team are responsible for ensuring that Wireless network connection is managed and maintained through regular best practices and software updated regularly.	Internal

CISO	CISO is accountable for ensuring that the wireless security compliance 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

9. Applicable standards

IEEE/ISO Standards

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)

NA

12. ISO Control Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological Controls	8.20 Networks Security- Networks shall be secured managed and controlled to protect information in applications and systems	Wireless Security Policy

Document Control

Owner:	CISO	**Release ID:**	WS_POL_0072

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	22-Nov-2021	Pranesh K	Pranesh K/Gangadhar Aka	Gangadhar Aka	Procedure Creation of Security for Wireless Networks and Devices	Initial Draft
1.0	22-Nov-2021	Pranesh K	Pranesh K/Gangadhar Aka	Gangadhar Aka	For Approval	Approved and Baselined
1.0	12-Aug-22	Krutideepta	Karthik N	Karthik N	For Review	Reviewed with No Change
1.1	24-April-2023	Krutideepta, Rama Madhavan	Karthik N	Srikanth M	For Review	Reviewed with No Change

						Migrated to new template
2.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
2.1	15-Feb-2024	Vijaya	Balu	Srikanth M	For Review	Updated the section ISO Control Mapping aligning to ISO 27001:2022
3.0	23-Feb-2024	Vijaya	Balu	Srikanth M	For Approval	Approved and Baselined
3.1	29-Apr-25	Krutideepta Barik	Balu		For Yearly Review	Migrated to a new Template.
4.0	14-May-25	Krutideepta Barik	Balu	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com