TRIANZ℠

NETWORK SECURITY MANAGEMENT PROCEDURE

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

The purpose of this Network Security Management Procedure is to establish a structured approach to securing the organization's network infrastructure. This procedure ensures the confidentiality, integrity, and availability of network resources by implementing robust security controls, monitoring mechanisms, and incident response measures in compliance with organizational policies and regulatory requirements.

2. Objectives

Following are the objectives

Ensure Network Security – Protect the network and secured network services from unauthorized access, threats, and vulnerabilities.

Maintain Compliance – Adhere to industry standards, legal, and regulatory requirements.

Enhance Incident Detection & Response – Monitor, detect, and mitigate network security incidents.

3. Scope

This procedure is applicable to networks and networked services established at Trianz.

The procedure applies to all Trianz products and services managed.

4. Procedure

4.1 Network Security

4.1.1 Network Administration

- IS systems of Trianz will be connected through the corporate network, which serves as the backbone of Trianz data and information exchange facility. Network and telecommunication controls will be deployed at Trianz to protect critical and business sensitive information from unauthorized and illegal access through network and telecommunication links.
- Designated IS Administrator in IS Department is responsible for the administration of the corporate network
- Designated IS Administrators in IS Department will regularly review and monitor the network configurations and take adequate measures to provide physical, logical and procedural safeguards for its security
- All equipment connected to Trianz network will be monitored by IS Administrators through a tool, below are the monitoring activities done.
    - Tool is configured to identify a network device connected to Trianz network
    - Approved devices (Desktops, Laptops, Servers, Printers, Switches and Routers etc.,) can be tracked with user name, MAC address, IP address and network port
    - Tool will monitor software updates and Anti-virus updates for systems (including desktops, laptops and servers)
- Head of IS will maintain a list of designated IS Administrators from the IS team; who can access the routers and other network devices including security devices.
- Automated alert and notification system will be deployed at the critical systems to inform IS Administrator if there is any possible breach of network security like unauthorized access, hacking or virus infection or any other event that hinders the operations of the respective systems.
- Administrative privilege to all the network devices at Trianz will be provided to the designated IS Administrators in IS Department only.

4.1.2 Network Communication Security

- Designated IS Administrator in IS Department will ensure that the default passwords of all the network devices including routers are changed.
- IS Administrators should use access control lists on routers.
- Software that performs unattended file transfer to or from other systems will be used to authenticate the origin and destination file names as well as any user submitting the request.
- All system access must be logged and the log files thus generated should never be overwritten or deleted until they are backed up to off-line storage.
- Internal Network Security shall be ensured by creating different VLAN's restricting employees from accessing data residing on different VLAN's. VLAN are created based on the business risk perception by the management.
- The VLAN's shall be segregated at the core switch and the inter-VLAN communication happens through the core switch only.

4.1.3 Connectivity

- All network connection points will be marked and identified.
- All unused connections / services and network segments will be disconnected from active networks.
- IS team will assess the suitability of new hardware/ software particularly the protocol compatibility before allowing those connections to the Trianz's corporate network.
- No desktop/s or laptop/s will be allowed to connect to the LAN without approval. In case of any such requirement, the permission from the Head of IS will be taken.
- Head of Departments will request the IS Helpdesk using Service Request for network connectivity to third party laptops to any unused network terminals.
- Periodic LAN / WAN utilization report shall be generated to monitor and identify future requirement of link bandwidth. This could also be used to identify any unfavorable link utilization by systems. This is governed by Policy for Capacity Management.
- Restrictions on connection by limiting the periodicity shall be ensured to provide additional security for high-risk applications. This can be achieved

by implementing an IPS / IDS on the network segment which will reset/block connections that could lead to DoS.

4.1.4 Access Control and Security of Remote Users

- IS Administrator will monitor remote user VPN connections - Log in time and log out time through a tool, below are the activities done by the tool.
- Tool is used to monitor and generate reports for the VPN users who are connecting to Trianz network over internet
- For all users who will connect to Trianz network, authentication will be controlled by a firewall
- Trianz will provide only secured access (VPN tunnel) to its web-enabled business and /or internal applications and/or servers

4.1.5 Router Security

Routers are used at the edge of the perimeter of network as well as inside the network for routing the packets. Securing the routers is very critical for the security of the network. Compromise of a router can lead to various security problems on the network served by that router, or even other networks with which that router is communicating as trusted connection.

- All routers shall support IPSec encryption standards like 3DES/AES standards etc., if this feature is supported by the Router Manufacturer, Model and Make • All unused services and daemons will be disabled / blocked on routers.
- Access Control Lists must be configured on the router.
- Syslog (router logs) from all the routers will be directed to a centralized log server.
- Remote Access to all routers will be allowed only from the desktop of Designated System Administrators in IS Department.
- Router will be accessed via console only in worst-case scenario when the network administrator is not able to connect to the router due to network connectivity problems.
- Network management tool will be deployed to identify network traffic utilization, memory utilization, CPU utilization etc to prevent choke-ups at

the gateways (router) and take necessary actions as per Policy for Capacity Planning.

- Where possible, Authentication, Authorization & Accounting should be ensured using , AD/RADIUS / TACACS+.
- Configuration of all routers across the organization will be stored centrally at the Central Location with the Head of IS for auditing, reference and as backup purpose.
- SSH based telnet services will be used for all communication with the router.
- Any changes to the configuration of the router will be approved by the Head of IS as per Policy for Change Management.

4.1.6 Firewalls

Each firewall that is introduced into the Trianz network should adhere to following:

- Identification of network applications deemed necessary to be provided access via firewall
- Identification of TCP/UDP ports should be allowed for identified applications
- Identification of source and destination IP address ranges for identified applications Creation of firewall rule base based on applications traffic
- Firewall rules should be created to allow communication on only identified ports for identified applications between identified source and destination IP ranges. Exception may be permitted to allow all ports for technical reasons but between specific source and destination IP address range only.
- Block traffic from an infected/malicious source identified.
- All changes in firewall rule base and/or policies will be approved by Head of IS and the policy for change management will be followed. (Refer: System and Software Change Management Policy)

While assembling the rule base, following traffic will be blocked:

- Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself. This type of packet normally represents some type of probe or attack against the firewall.

- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall. This type of packet likely represents some type of spoofing attempt
- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic. Given the fact that ICMP can be used to map the networks behind certain types of firewalls, ICMP should never be passed in from the Internet, or from any un-trusted external network
- Inbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks. RFC 1918 reserves the following address ranges for private networks:
  - o 10.0.0.0 – 10.255.255.255 (Class A)
  - o 172.16.0.0 – 172.31.255.255 (Class B)
  - o 192.168.0.0 – 192.168.255.255 (Class C)

Inbound traffic with these source addresses usually indicates the beginning of a denial of-service attack

- Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic. These packets can be an indicator that an intruder is probing a network
- Inbound traffic containing IP Source Routing information. Source Routing is a mechanism that allows a system to specify the routes that a piece of network traffic will employ while traveling from the source system to the destination system. From a security standpoint, source routing has the potential to permit an attacker to construct a network packet that bypasses firewall controls
- Inbound or outbound network traffic containing a source or destination address of 127.0.0.1 (local host). Such traffic is usually some type of attack against the firewall system itself
- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0 should be blocked. Some operating systems interpret this address as either local host, or as a broadcast address, and these packets can be used for attack purposes
- Restrictions on connection times shall be used to provide additional security for high risk applications. This can be achieved by

implementing an IPS / IDS on the network segment which will reset/block connections that could lead to DoS.

- Block Inbound traffic containing directed broadcast addresses as directed broadcast is often used to initiate a broadcast propagation attack such as SMURF. Directed broadcasts allow one computer system to send out a broadcast message with a source address other than its own. In other words, a system sends out a broadcast message with a spoofed source address. Any system that responds to the directed broadcast will then send its response to the system specified by the source, rather than to the source system itself. These packets can be used to create huge "storms" of network traffic that has been used to disable some of the largest sites on the Internet

1. Testing Firewall controls
    - The first methodology is to obtain hardcopies of the firewall configurations and compare these hardcopies against the expected configuration based on defined policies.
    - The second methodology involves actual in-place configuration testing. In this methodology, the designated IS Administrator in IS Department will actually assess the configuration of a device by attempting to perform operations that are prohibited
2. Access to Firewall Platform

    The most common method for breaking into a firewall is to take advantage of the resources made available for the remote management of the firewall. This typically includes exploiting access to the operating system console, or access to a graphic management interface. The following will be followed for secure access to firewall platform

    - Access to the operating system console and any graphic management interface will be carefully controlled by use of encryption and/or strong user authentication, and restricting access by IP address

- Secure Sockets Layer will be used for graphic management interfaces that rely on the hypertext transport protocol (HTTP) for interface presentation

3. Firewall Backup

The following will be followed for firewall backups: -

- The Firewalls will be backed up immediately prior to production release
- The firewall backup will be retained for a period of at least three months

4.1.7 Intrusion Detection/Prevention System

- Network based IDS/IPS will be implemented at all gateways shall monitor all inbound and outbound network traffic at Trianz network in promiscuous mode.
- Network based IDS/IPS shall be able to generate alerts / alarms in case any unfavorable / malicious activity is identified on the network to intimate the security administrator immediately.
- Network based IDS shall be configured and managed from a common Centralized IDS Console. IDS security policies and response policies shall be stored on this console server. • Upgrades / update / Hot-fixes / patches shall be applied to IDS and documented.
- Regularly update the IDS signatures. The documentation of the same also shall done, logging the update number, time of application of the upgrade, brief on the changes to it.
- All alert logs from both network based IDS shall be forwarded from the IDS to centralized IDS Console
- The designated IS administrator must apply latest patches or attack signature updates or upgrades as and when released on all IDS sensors via the centralized IDS Console.
- The designated IS administrator must configure the security patches or updates or upgrades to the respective IDS sensors and backup the existing IDS security policy or response policy before applying the newly configured IDS policy (with patch / update / upgrade).

- Backup of IDS Policy shall be taken before performing any modification or changes in the existing security policy.
- Periodical Backup of IDS security policy, response policy and security logs shall be taken. The Frequency of periodical backup is every six months.
- Multiple backup copies shall be created and the copies must be stored in safe environment preferably at cloud.
- Reports shall be generated from the security alert logs on a periodic basis (suggest at least weekly).
- Co-relation of network based IDS shall be done to identify malicious / unfavorable activity pattern at Trianz network and take precautionary measures to block such activities in future or in case of a incidence occurrence.
- Restrictions on connection times shall be used to provide additional security for high-risk applications. This can be achieved by implementing an IPS / IDS on the network segment which will reset/block connections that could lead to DoS.
- IDS response to any illegal / hacking activity will include appropriate steps including the following: -
    - Dropping such connection
    - Reconfiguring the firewall to block connections from source IP address

4.2 Network services security & Network services access control

4.2.1 Authentication for external connections

Authentication for external connections is through SSL VPN based on authentication using Kerberos protocol,

4.2.2 Segregation of Networks

Networks are segregated using VLAN methodology based on business units.

4.2.3 Remote and Diagnostic Port Protection

Remote and Diagnostic ports are protected by blocking ICMP.

4.3 Zero Trust Principles

- Trianz shall follow a strict zero trust network architecture, so that we can prevent network security breaches and reduce blast radius in case of breach, thus not be reliant only on network perimeter security alone.
- Trianz shall implement a "never trust and always verify" approach for access to information systems by ensuring that requests to information systems are encrypted end-to-end.
- Verifying each request to an information system as if it originated from an open, external network, even if these requests originated internal to the organization (i.e. not automatically trusting anything inside or outside its perimeters).
- Trianz always follows "least privilege" and dynamic access control techniques which includes authenticating and authorizing requests for information or to systems based on contextual information such as authentication information, user identities, data about the user endpoint device, and data classification.
- By following zero trust we always authenticating requesters and always validating authorization requests to information systems based on information including authentication information and user identities, data about the user endpoint device, and data classification, for example enforcing strong authentication (e.g. multi-factor, end point agents, location based, attribute based).

5. ISO Control Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological Control	8.20 Networks security Control Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	Network Security Management Procedure

	8.21 Security of network services Control Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored. 8.22 Segregation of networks Control Groups of information services, users and information systems shall be segregated in the organization's networks.	

Document Control

Owner:	CISO	**Release ID:**	NSM-PROC-0048

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.00	26-Feb-07	Jyotessh G Nair			Initial draft	None
1.00	26-Feb-07	Jyotessh G Nair			Baseline is approved by Zulfikar Deen.	Approved Baseline.
1.01		Bharateesha B R				
2.00	03-Jun-09	Balu Nair			Approval for Baseline	Baselined
2.01	30-Dec-10	Chakravarthi			QMG review	Formatted entire Document

						Modified Properties of the document
3.0 0	30-Dec-10	Chakravarthi			Request for baseline	Baselined
3.0 1	24-May-11	Srilakshmi			QMG Review	Modified release id in header and cover page to make consistency
4.0 0	24-May-11	Srilakshmi			Approval for Baseline	Baselined
4.0 1	3-Aug-11	Sudharsana			QMG review	Replace Owner with Management Representative in place of CIO
						In Document Classification Scheme, "Retention period is 3 Years" row is removed
5.0 0	3-Aug-11	Sudharsana			Request for baseline	Approved and Baselined
6.0 0	28-Sep-12	Sudharsana			QMG review	Formatted as per latest template format
7.0 0	08-Jan-13	Gangadhar &			ISMS Surveilla nce	Modified section 4.1.1 -

		Srilakshmi			Audit Findings	Network Administration for identification and monitoring of equipment connected in network Modified section 4.1.4 - Remote User Security for Access control of remote users and monitoring of VPN / Remote users and section name from Remote user security to Access Control and Security of Remote users.
7.0 1	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	Baselined
8.1	15-May-20	Balu Nair	Phani Krishna		Annual Review	Migrated to the new template

9.0	15-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
9.1	3-May-20	Divya G	Vijaya	Phani Krishna	Annual Review	Updated with new information classification
10.0	3-May-20	Divya G	Vijaya	Phani Krishna	For Approval	Approved and Baselined
10.0	21-Dec-21	Divya G	Karthik N		Annual Review	No Change
11.1	13-Mar-2022	Sanjana	Balu N		For review	The scope has been extended to products and services
12.0	18-Mar-2022	Sanjana	Siva N	Siva N	For Approval	Approved and Baselined
12.0	10-Mar-2023	Beniyel S, Rama Madhavan	Balu N		For review	No Change Migrated to new template
12.0	10-May-2023	Beniyel S	Balu N	Srikanth M	For Approval	Approved and Baselined
12.1	02-Feb-2024	Sraveen Motupalli	Balu N & Vijaya	Srikanth M	For review	Added 4.2 Zero trust principles and removed

						CD-ROM Backups
13.0	23-Feb-24	Sraveen Motupalli	Balu N & Vijaya	Srikanth M	For Approval	Approved and Baselined
13.1	11-Mar-25	Krutideepta Barik	Balu N, Vijaya R & Beniyel S		For Yearly Review	1. Introduction section has been added. 2. Objectives and Procedures have been modified and updated. 3. Migrated to a new Template.
14.0	14-May-25	Krutideepta Barik	Balu N & Vijaya	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com