TRIANZ℠

USER ENDPOINT 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

The purpose of User endpoint policy is to protect information against the risks introduced by using user endpoint devices, mobile computing and communication facilities policy is as defined below:

- Prevent misuse of electronic communications and computing resources
- Ensure employees are not exposed to unethical behavior such as error, fraud, defamation, breach of copyright, unlawful discrimination, illegal activity, privacy violations and computing resource service interruptions

1.1 Mobile Computing

Mobile Computing facilities include, but are not restricted to, the following items:

- Laptops, mobile phones and other portable computing devices
- Media, CD-ROMs, DVDs, disks, pen drives and memory storage devices etc.
- Video conferencing

1.2 Communication Facilities

Communication facilities include, but are not restricted to, the following items:

- E-mail
- Internet
- Mobile phones, VOIP phones, Skype, Microsoft Teams, Kaizala,
- Forums, blogs and other internet-based communications tools etc.

2. Objectives

The objectives of this Policy are to:

- To facilitate the efficient, effective, responsible and lawful use of the Trianz computing and communication facilities.

- Safeguard the interests of the Trianz and all authorized users of its computing and communication facilities; and provide guidelines and instructions to authorized users in the appropriate use of the Trianz's computing and communication facilities.

3. Scope

All Trianz Associates and contractors having access to Trianz Mobile computing and communication facilities.

4. Policy Statements

Trianz shall ensure that effective measures are in place to protect confidential information in respect of the use of mobile computing and communication facilities.

Protection is in place to avoid the unauthorized access to, or disclosure of confidential data stored and processed by these mobile computing and communication facilities.

- Mobile devices, including laptops, smartphones, and tablet computers, can provide substantial productivity benefits. Mobile storage devices may simplify information exchange and support business needs. However, all these mobile devices also present significant risks to Trianz's information assets.
- Trianz may permit employees and others to use their own equipment (BYOD- refer to BYOD Policy) to connect to its network and systems. It is required to install specific security controls on the devices (as per BYOD Policy).
- IT shall review the devices and remove any Trianz data, if any relationship with Trianz terminates, change devices or services, or in other similar situations.

- It is recommended to use encryption, other protection strategies (for example, device management software, access controls, remote wiping in case your device is lost or stolen, or other security controls), or both on any mobile device that contains Confidential or Highly Confidential Information. Mobile devices, including those that provide access to Trianz email, must be protected using MFA (a password and/or other approved authentication methods).
- Physically secure any mobile devices you use to access or store Trianz information. Laptops shall be never left unattended.
- Associates shall not take pictures from mobile phones/cameras inside any ODC's provided to the Customers as part of the MSA/SOW.
- It is recommended not to connect mobile device containing Trianz information to any unsecured network without an up-to-date firewall configured (or other security controls in place).
- Unsecured networks include home networks, hotel networks, open or for-pay wireless hotspots, convention networks, or any other network that Trianz has not approved or does not control. Refer to BYOD policy for more details on associate owned devices.
- Remote geolocation capabilities shall be maintained for all mobile devices.
- Remove wipe to be enabled in all the Trianz managed mobile devices to securely wipe the data if the devices is lost.
- Ensure all endpoints are updated with latest version periodically with definitions UpToDate.
- Use of removable devices, including removable memory devices, Physical ports to be disabled (e.g. USB ports, SD cards).

5. Roles & Responsibilities

Role	Responsibilities	Internal/External
All Associates	• Associates are responsible for all the activity on mobile computing and communication facilities which is initiated by their ID. • If user suspects that the security of their computing & Communication facilities has been breached or compromised, it should be reported to the IS Team.	Internal
IS Team	• Respond and investigate the breach reported.	Internal
InfoSec Team	• Bi-Annual review of Policy on the use of mobile computing and communication facility	Internal

6. Applicable standards

ISO 27001:2013
ISO 27001:2022
ISO 27701:2019

7. Reference Policies & Procedures

BYOD Policy

Access Control Policy

Antivirus Malware policy

Asset Management Policy

Data Loss Prevention Policy

Email Security Policy

System and Software Change procedure

Encryption Key management Policy

Password Policy

Media Handling Policy

8. Exceptions(s)

Exceptions to the Change management policy will require formal written approval from the Information Security Assurance Team.

Refer to Exception Handling Policy.

9. ISO Control Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Technological	8.1 User end point devices Control Information stored on, processed by or accessible via user end point devices shall be protected.	User Endpoint Policy

Document Control

Owner:	CISO	**Release ID:**	MCCF-POL-0023

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
1.00	09-Jan-14	Srilakshmi			None	Initial release to Blue Book
1.01	14-Oct-16	Sriharsha			Addition of Cloud services as scope of Certification.	Modified the policy section 3
2.00	07-Dec-16	Balu Nair			Approved by CISO	Baselined
2.1	12-May-20	Balu Nair	Phani Krishna		For review	Migrated to the new template
3.0	15-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
3.1	19-May-20	Karthik N	Srilakshmi		Review comments from DA	Updated the policy section. Added more details on Mobile computing.

4.0	19-May-20	Karthik N	Anitha Ravindran	Phani Krishna	For Approval	Approved and Baselined
4.1	28-Jul-20	Balu Nair, Vijaya Rajeswari	Phani Krishna	Phani Krishna	For Review	Formatted the document for legibility, updated communication facilities and referred BYOD policy wherever applicable
5.0	31-Jul-20	Balu Nair	Phani Krishna	Phani Krishna	Approved for Baseline	Baselined
5.1	11-Feb-21	Balu Nair	Phani Krishna		Review	Updated the information classification Formatted and made few minor changes
6.0	11-Feb-21	Balu Nair	Phani Krishna	Phani Krishna	Approved for Baseline	Baselined
6.1	30-July-21	Divya G	Phani Krishna	Phani Krishna	Review	Updated the objectives and roles and responsibilities
7.0	30-July-21	Divya G	Phani Krishna	Phani Krishna	Approved for Baseline	Baselined
8.0	04-01-2022	Divya G	Balu N	Siva N	Annual Review	Reviewed and no changes
8.1	15-Mar-22	Sanjana	Divya G	Siva N	For Review	The scope has been extended to products and services

9.0	15-Mar-22	Sanjana	Divya G	Siva N	For Review	Approved and Baselined
9.0	05-Apr-23	Sanjana	Balu N		For review	Reviewed with no changes
9.1	12-May-2023	Rama Madhavan	Vijaya		For Review	Migrated to new template
10.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
10.1	11-Feb-23	Vijaya	Vijaya and Bala	Srikanth M	For Review	Mapped with ISO 27k 2022 new controls
11.0	23-feb-23	Vijaya	Vijaya and Bala	Srikanth M	For Approval	Approved and Baselined
11.0	24-Feb-24	Vijaya	Vijaya and Bala		For Review	Reviewed with no changes
11.1	28-May-25	Kruti	Vijaya		For Review	Migrated to new template
12.0	29-May-25	Kruti	Vijaya	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com