Acceptable Usage 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 this policy is to define the acceptable use of equipment and computing services.

2. Objective

The objective of this policy is to describe the acceptable use of information technology equipment and services at Trianz.

3. Scope

The scope of this policy is applicable to all Trianz managed business systems, Trianz provided Client Services & Trianz developed products.

4. Policy Statement

- The following activities are considered unacceptable with no exception. Under no circumstances, an employee of TRIANZ or contractor or third-party service provider authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing TRIANZ owned resources.
- The policy applies to all mentioned stakeholders working for Trianz products and services.

5. Acceptable Use

- Associates can install necessary utilities like software, application, only after receiving an approval from IS and InfoSec & Data privacy assurance.
- All associates must respect and protect the confidentiality, integrity, availability, and privacy of Trianz information & resources.
- All associates/users must respect and protect the intellectual property rights of others by following the copyright laws.
- Users must take ownership and report all security related incidents in the tool.
- Users must use Trianz assets for official purposes only.
- Associates can use their mobile phones for accessing the outlook, VPN tokens etc. in a secure manner and adhering to MDM policy.

- Associates can use personal laptops for their official use by adhering to BYOD policy.
- Associates can browse internet sites that are safe by adhering to internet user policy.

6. Unacceptable Use

6.1 System and Network Activities

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by TRIANZ.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which TRIANZ or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan Horses, e-mail bombs, etc.)
- Revealing/sharing your account/access credentials to others or allowing use of your account by others.
- Using a TRIANZ computing asset to actively engage in procuring offensive content or transmitting material that is in violation of POSH or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any TRIANZ account.
- Making statements about warranty/commitment, expressly or implied, unless it is a part of normal job duties.

- Any action causing disruptions to network communication, allows/causes unauthorized access, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to is made to the IT department.
- Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, TRIANZ employees to parties outside TRIANZ.
- Use of cloud computing services for work purposes must be formally authorized by the IT Manager/CIO. The IT Manager/CIO shall ensure that security, privacy, and all other IT management requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the CISO/CIO.
- The use of such cloud services must comply with the cloud security and data privacy controls governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by Trianz.
- Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

6.2 Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within TRIANZ's networks of other Internet/Intranet/Extranet

  service providers on behalf of, or to advertise, any service hosted by TRIANZ or connected via TRIANZ's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

7. Exceptions(s)

No Exceptions.

8. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational controls	5.10 Acceptable use of information and other associated assets Control Rules for the acceptable use and procedures for handling in formation and other associated assets shall be identified, documented and implemented.	Acceptable Usage Policy

Document Control

Owner:	CISO	**Release ID:**	AU-POL-0003

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	
1.00	26-Feb-07	Jyotessh G Nair			Baseline is approved by Zulfikar Deen.	Approved
1.01	30-Jul-08	Bharateesha B R			Revised the policies in accordance with the revised ISMS Framework	Changed the Policy statements, Changed the template Added Document Classification Scheme
2.00	28-Apr-09	Balu Nair			Approval for Baseline	Baselined
2.01	30-Dec-10	Chakravarthi			QMG review	Formatted entire document
3.00	31-Dec-10	Chakravarthi			Request for Baseline	Baselined
3.01	06-May-11	Srilakshmi			To maintain common release id allocation for bluebook documents	Modified Release ID in cover page and header

4.00	06-May-11	Srilakshmi			Request for Baseline	Baselined
4.01	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
5.00	3-Aug-11	Sudharsana			Request for baseline	Approved and Baselined
5.01	14-Oct-11	Venkateswar Reddy GD			QMG Review	Used new template as per documentation guidelines ‘Shall’ word is replaced by ‘Will’ throughout policy Reviewed for continued suitability
6.00	14-Oct-11	Venkateswar Reddy GD			Approval for Baseline	Baselined
7.00	08-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	Modified the template format Changed the Logo

7.01	14-Oct-16	Shishir and Balu			Addition of Cloud services as scope of Certification.	Modified Emergency Access of Password section TRIANZ Logo modified
8.00	07-Dec-16	Balu Nair			Approved by CISO	Baselined
8.01	29-Apr-19	Balu Nair	Joshy VM			Minor changes to the contents, Information classification modified
9.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
9.0	22-Apr-20	Balu Nair	Karthik N		Review	Reviewed and no changes observed
9.1	11 -May -20	Karthik N	Balu Nair		Review	Roles modified with CISO/CIO Integrated with new template
9.2	12-May-20	Karthik N	Balu Nair		Review	Added Acceptable use after Phani review
10.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined

10.1	14-Jan-21	Balu Nair	Phani Krishna		Review	Updated the information classification
11.0	11-Feb-21	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
11.0	23-Dec-21	Balu Nair	Karthik N		Annual Review	No Changes
11.1	24-Feb-22	Sanjana	Karthik N	Sivaramakrishnan N	For Review	The scope has been extended to products and services
12.0	24-Feb-22	Sanjana	Karthik N	Sivaramakrishnan N	For Approval	Approved and baselined
12.1	25-Feb-23	Krutideepta, Shalini	Karthik N		For Review	Exception Details has been changed. New template change. Editorial changes. Objective and Scope added.
13.0	12-May-23	Krutideepta	Karthik N	Srikanth M	For Approval	Approved and Baselined.

13.1	15-Feb-24	Beniyel S	Vijaya R		For Review	ISO Control Mapping(s) has been added.
14.0	23-Feb-24	Beniyel S	Vijaya R	Srikanth M	For Approval	Approved and Baselined
14.1	16-Apr-2025	Vijaya R	Balu		For Review	Migrated to a new Template and yearly review
15.0	14-May-25	Vijaya R	Balu	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com