



INFORMATION SECURITY CODE OF CONDUCT

DOCUMENT

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

| | |
|-------------------------------------|--------------|
| <input type="checkbox"/> | Public |
| <input checked="" type="checkbox"/> | Internal |
| <input type="checkbox"/> | Confidential |
| <input type="checkbox"/> | Restricted |

Table of Contents

| | |
|--|----------|
| 1. OBJECTIVE | 4 |
| 2. SCOPE | 4 |
| 3. INFORMATION SECURITY CODE OF CONDUCT | 4 |
| 4. ISO CONTROL MAPPING(S) | 8 |

1. Objective

- The purpose of this document is to ensure effective and secure access to the Trianz information assets.

2. Scope

- This code of conduct shall be applicable to all employees, consultants, third party service providers and contractors of Trianz and third parties who have access to Trianz Information Assets.
- All Trianz products and services

3. Information security code of conduct

- Employees, contractors, and third-party service providers shall sign a non-disclosure agreement prior to be given access to Trianz information assets
- Employees, contractors, and third-party service providers shall sign confidentiality and intellectual property Agreement making them aware of copyright and data protection laws applicable to them.
- Employees and contractors during the course of company work shall classify all the information assets produced in accordance with the Asset Classification policy of Trianz. They shall handle the information assets in accordance with Guidelines for information labeling and handling.
- No employee of Trianz shall bring to Trianz office premise, any media, including but not limited to, Floppies, CDs, DVDs, USB Drives, Tapes, portable Hard Disks, laptops, camera, video cameras, etc.

- Users shall be responsible for protecting their computer/user account given/created to execute their work towards the company and are accountable for any action carried out by the assigned user-ids.
- Users shall keep their password confidential and shall not reveal passwords to others or share their account with others. Temporary password shall be changed at first logon as defined in password management policy or whenever there is any indication of possible system or password compromise.
- Computers (Desktop & Laptops) shall not be kept logged on if not used and unattended for an extended period of time. The computer shall be locked or should have password protected screen saver. At the end of the day, before leaving for the day, users shall shutdown the computer systems and peripheral devices.
- Computers shall be provided by the company for official use and should run only company authorized applications and programs.
- Users shall not download and install any program on the computers unless prior approval has been obtained from the respective Director and the same has been registered with the IT helpdesk for further approval. Any screen saver running on the user's machine shall not contain anything which violates copyrights, is obscene or contains anything objectionable or illegal.
- All users directly connected to the Trianz central network shall ensure that their computers always have the latest versions of Antivirus programs. Though the Antivirus programs get updated automatically through the central server, users shall ensure that they are updated regularly otherwise he/she shall report the same to IT helpdesk if the antivirus software is not installed or it is not being updated.
- Data stored on individual computer shall not be backed up in regular working conditions. Users shall store all business critical data on specific servers or request IT helpdesk to take a backup of data with Director approval
- Data which is private to a user may be stored on computers, provided users undertake risk of loss to Trianz and own the responsibility for such data which is not related to the business of Trianz. The storage of such data shall be limited and not hamper the normal office productivity of the user. However, users shall not install any applications (software, screen-savers etc.) or additional hardware (modems, printers etc.) on their machines. Any kind of configuration change on Trianz computers is strictly prohibited, and if required, shall be requested to the IT helpdesk to perform the changes.

- Users shall collect their printouts from the printing device immediately once it has been printed.
- Users shall not share their user id and password with anyone else. In case, it has to be shared due to some emergencies password shall be changed immediately after the emergency is over.
- Employees shall make sure that working on portable computers in public places is avoided. If required to work on portable computers in public places it shall be ensured that there is no risk of overlooking.
- In case of an audit, if any unauthorized software (which is not part of an approved Software list) is found on their system then, the employee shall be held responsible for that and subjected to disciplinary process.
- Company e-mail accounts shall be used primarily for business communications purposes. Users are prohibited from leaking confidential and internal information through mails and shall be solely responsible to Trianz for unauthorized disclosures.
- Users shall not use company account to initiate or forward junk mails, chain mails, jokes etc. Company e-mail account must not be used for "Spam" or unsolicited mails.
- Users shall not transmit any unlawful, harassing, libelous, abusive, threatening, harmful, vulgar, obscene, or otherwise objectionable material of any kind or nature.
- Attachments in e-mail are routinely used to spread computer viruses. Users shall never open mails attachments from unknown or un-trusted sender. It is advisable to delete mails with attachment that has been sent unsolicited and appear suspicious due to mail content or attachment name
- All personal emails shall be kept in a separate folder. The emails in this folder must be deleted periodically, preferably weekly, so as not to clog up the system.
- All outgoing mail shall have the Trianz Email disclaimer.
- Use of Trianz information systems to access Internet for personal purpose is not allowed and will be considered cause for disciplinary action.
- IP phones and soft phones installed on your system should be used only for official purpose between Trianz India and across USA.
- Users are encouraged to use Internet to assist them in the performance of their jobs. Authorized uses include but are not limited to the following: Client and customer services, education and research, electronic communication

for professional purposes and procurement of information from external sources.

- Internet chat groups and newsgroups are public forums where it is not appropriate to discuss or reveal confidential information, customer data, trade secrets, and any other material described or referred in this policy. User must identify them honestly, accurately and completely when participating in chat groups, newsgroups and setting up account on outside computer systems.
- Trianz is not responsible for material viewed or downloaded by users from Internet. The Internet is worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with the material while using the Internet. Even innocuous search request may lead to sites with highly offensive contents. Users accessing the Internet do so at their own risk.
- Information is a key asset for the company. Users shall not reveal confidential or internal company information to outsiders (Third party, family members, press or public) unless authorized to do so.
- Users shall protect their documents which contain company's confidential information. It is the user's responsibility to restrict the distribution of classified documents to authorized persons only and prevent unauthorized access by keeping the documents under lock.
- Any event of inappropriate use of Trianz Information systems and breaches of security and any suspected security weakness, malfunction related to Trianz IT infrastructure at all locations that is observed by the user shall immediately be reported to ISWG
- The company has installed a variety of security technologies to assure the safety and security of the company's infrastructure. Any attempt to circumvent or subvert any such security measures is strictly prohibited.
- It is prohibited to run programs or tools without authority against any system or application of Trianz that can result in compromise of its security.
- Users are to comply with the security policies and processes of Trianz. Non-compliance can result in punitive action ranging from reprimand to suspension/termination, and/or legal action.
- Violation of any point/points published in this document will be subjected to Disciplinary action as per our Disciplinary action policy.

4. ISO Control Mapping(s)

| Category of Control | ISO 27001:2022 Control | Document Name as per ISO 27001:2022 |
|----------------------------|---|--|
| Organizational Controls | 5.15 Access control Control Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements. | Information Security Code of Conduct |

Document Control

| | | | |
|---------------|------|--------------------|----------------|
| Owner: | CISO | Release ID: | ISCC-PROC-0042 |
|---------------|------|--------------------|----------------|

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

| Ver. No. | Date | Author | Reviewer | Approver | Reason for Change | Change Description |
|----------|-----------|-----------------|----------|----------|---|--|
| 0.0 | 26-Feb-07 | Jyotessh G Nair | | | Initial draft | None |
| 0.1 | 26-Feb-07 | Jyotessh G Nair | | | Review | Review feedback incorporated |
| 1.0 | 26-Feb-07 | Jyotessh G Nair | | | Baseline is approved by ZulfikarDeen. | ApprovedBaseline. |
| 1.1 | 15 Mar-09 | Bharateesh aB R | | | Revised to include the changes due to New Asset management framework and risk assessment and treatment plan | <ul style="list-style-type: none"> • Include clauses related to information classification and handling • Included a clause on NDA and confidentiality and intellectual property agreement |
| 2.0 | 29-Apr-09 | Balu Nair | | | Approval for Baseline | Baselined |

| | | | | | | |
|-----|-----------|-------------|--|--|-----------------------|---|
| 2.1 | 30-Dec-09 | Aswari | | | QMG review | Formatted |
| 3.0 | 30-Dec-09 | Chakravarti | | | Approval for baseline | Baselined |
| 3.1 | 12-May-10 | Balu Nair | | | QMG Review | Document formatted |
| 4.0 | 21-May-10 | Balu Nair | | | Approval for baseline | Baselined |
| 4.1 | 24-May-11 | Srilakshmi | | | QMG Review | <ul style="list-style-type: none"> Modified release id in header and cover page to make consistency |
| 5.0 | 24-May-11 | Srilakshmi | | | Approval for Baseline | Baselined |
| 5.1 | 3-Aug-11 | Sudharsana | | | QMG review | <ul style="list-style-type: none"> Replace Owner with Management Representative in place of CIO. In Document Classification Scheme, "Retention period is 3 Years" row is removed. |
| 6.0 | 3-Aug-11 | Sudharsana | | | Request for baseline | Approved and Baselined |
| 7.0 | 28-Sep-12 | Sudharsana | | | QMG review | <ul style="list-style-type: none"> Formatted as per latest template format |

| | | | | | | |
|------|-----------|-----------------|---------------|-------------------|----------------------|---|
| 7.1 | 29-Apr-19 | Balu Nair | Josh VM | | | Information classification modified |
| 8.0 | 14-May-19 | Balu Nair | | Ganesh Arunachala | Approved for Release | Baselined |
| 8.1 | 11-May-20 | Karthik N | Balu Nair | | Review | Integrated to new template |
| 9.0 | 14-May-20 | Karthik N | Phani Krishna | Phani Krishna | For approval | Approved and Baselined |
| 9.1 | 3-May-21 | Divya G | Vijaya R | Phani Krishna | Review | Updated with new information classification |
| 10.0 | 3-May-21 | Divya G | Vijaya R | Phani Krishna | For approval | Approved and Baselined |
| 10.0 | 3-Jan-22 | Divya G | Vijaya R | | Review | No changes |
| 10.1 | 24-Feb-22 | Kruti, | Karthik | | For Review | The scope has been extended to products and services. |
| 11.0 | 28-Feb-22 | Kruti | Siva N | Siva N | For approval | Approved and baselined |
| 11.0 | 05-Apr-23 | Shivateja | Srikanth M | Srikanth M | For Review | Reviewed No Changes |
| 11.1 | 12-May-23 | Asha Veeramallu | Vijaya | | For Review | Migrated to New template |
| 12.0 | 12-May-23 | Asha Veeramallu | Vijaya | Srikanth M | For approval | Approved and Baselined |

| | | | | | | |
|------|---------------|---------|--------|---------------|--------------|--|
| 12.1 | 15-Feb-24 | Shalini | Vijaya | Srikanth M | For Review | Mapped with new ISO 27001, 2022 control 5.15 |
| 13.0 | 23-Feb-24 | Shalini | Vijaya | Srikanth M | For Approval | Approved and Baselined |
| 13.1 | 28-May- 25 | Kruti | Vijaya | | For Review | Migrated to New template |
| 14.0 | 28-May- 25 | Kruti | Vijaya | Srikanth M | For Approval | Approved and Baselined |



Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com



The content in this document is copyrighted; any unauthorized use – in part or full – may violate the copyright, trademark, and other laws. This document may not be modified, reproduced, or publicly displayed, performed, or distributed, or used for any public or commercial purposes. The Trianz name and its products are subject to trademark and copyright protections, regardless of how and where referenced.