TRIANZ℠

Information 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. Introduction

This Information Security Policy (Policy) promotes an effective balance between information security practices and business needs. The Policy helps Trianz Inc., (hereinafter "Trianz") meet our legal obligations and our clients' expectations. From time to time, Trianz may implement different levels of security controls for different information assets, based on risk and other considerations.

2. Purpose

Trianz handles sensitive information of clients. Protection of client information is vital to the Trianz.

To fulfil this strategic objective Trianz has implemented information security management system.

3. Objectives

Top Management will provide commitment and direction to establish and maintain information security.

- To ensure confidentiality, integrity and availability of critical information at all times
- To protect information assets
- To protect critical information from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional
- Ensuring Identification of the Information Security Objectives
- Ensuring a commitment to continually improve the Information Security Management System based on Information Security Objectives

4. Trianz Information Security Policy Statement

Trianz Is committed to implement processes and systems to protect and safeguard the Confidentiality, Integrity and Availability (CIA) of all critical information and information processing assets from internal and external threats sources in order to ensure secure provision of business operations."

All associates are expected to read, understand, and follow this, Policy. However, no single policy can cover all the possible information security issues Organization

may face. You must seek guidance from your manager or other designated Trianz resource before taking any actions that create information security risks or otherwise deviating from this Policy's requirements. Trianz may treat any failure to seek and follow such guidance as a violation of this Policy. This Policy is applicable for all On Premise and Cloud environments as well. For specific Security and Privacy related Policy information for Cloud computing environments, please refer to **Cloud Security and Privacy Policy**.

Our clients, employees, and others rely on us to protect their information. An information security breach could severely damage our credibility. Security events can also cause loss of business, Reputation, revenue etc.to Trianz. Strong information security requires diligence by all workforce members, including employees, contractor employees, third party vendors, volunteers, and any others accessing or using our information assets. It is the responsibility of everyone.

Please refer to **Data Protection and Privacy Policy** for organizational commitment on how Trianz is committed to protecting Personally Identifiable Information(PII) or Personal Data.

4.1 Guiding Principles

Trianz follows these guiding principles when developing and implementing information security controls:

a) Trianz strives to protect the confidentiality, integrity, and availability of its information assets and those of its clients.

b) Trianz will comply with applicable privacy and data protection laws.

c) Trianz will balance the need for business efficiency with the need to protect sensitive, proprietary, or other confidential information from undue risk.

d) Trianz will grant access to sensitive, proprietary, or other confidential information only to those with a need to know and at the least level of privilege necessary to perform their assigned functions.

e) Recognizing that an astute workforce is the best line of defence, Trianz will provide security training opportunities and expert resources to help individuals understand and meet their information security obligations.

f) Trianz will define Information Security Objectives against Information Security Controls for better control effectiveness and continual improvement.

4.2 Scope

This Policy applies across the entire Trianz enterprise including External vendors, Service Providers, Clients, Business Partners that may have access to Trianz's Organizational information.

This Policy provides detailed information security guidance to employees must be followed in addition to any obligations listed in applicable code of conduct or employee handbook.

This Policy states Trianz' s information security policy. In many cases, you are personally responsible for taking or avoiding specific actions as the Policy states. In some situations, The Infosec & Data Privacy Assurance Team, or another Trianz resource takes or avoids the stated actions.

From time to time, Trianz may approve and make available more detailed or location or business unit specific policies, procedures, standards, and processes to address specific information security issues. Those additional policies, procedures, standards, and processes are extensions to this Policy. You must comply with them, where applicable, unless you obtain an approved exception.

4.3 Resources

No single document can cover all the possible information security issues you may face. Balancing our need to protect Trianz's information assets with getting work done can also be challenging. Many effective Organizational, People , Physical, and Technical Controls are available. Do not make assumptions about the cost or time required to implement them. Ask for help.

You must seek guidance before taking any actions that create information security risks. Contact your manager.

4.4 No Exception of Privacy and Monitoring

Except where applicable law provides otherwise, you should have no exception of privacy when using Trianz's network or systems, including, but not limited to, transmitting and storing files, data, and messages.

To enforce compliance with Trianz's policies and protect Trianz's interests, Trianz reserves the right to monitor any and all use of its network and systems to the extent permitted by applicable law. By using.

Trianz's systems, you agree to such monitoring. Monitoring may include (but is not necessarily limited to) intercepting and reviewing network traffic, emails, or other messages or data sent or received and inspecting data stored on individual file directories, hard disks, or other printed or electronic media.

4.5 Regulatory Compliance

Various information Security and Data protection or Privacy laws, regulations, and industry standards apply to Trianz and the data we handle that includes Personally Identifiable Information or Personal Data or Personal Sensitive Data. Trianz is committed to complying with all such applicable laws, regulations, and standards. Our clients expect nothing less from us.

This section lists the obligations that you are the most likely to encounter. Do not assume that these are the only laws that may apply. To identify specific obligations, you must seek guidance from Legal and the Infosec & Data Privacy Assurance Team when collecting, creating, or using new or different types of information or Personal Data.

(a) **Personal Information: Data Protection and Breach Notification Laws**: State laws protect individuals' personal information, such as Social Security numbers, driver's license numbers, financial account information, and other sensitive data. Most states have enacted breach notification laws that require organizations to notify affected individuals if personal information is lost or accessed by unauthorized parties. Some states have enacted data protection laws that require organizations to protect personal information using reasonable data

security measures or more specific means. These laws may apply to personal information for Trianz's employees, clients, business partners, External Vendors, Service Providers and others.

Before collecting, creating, using or Processing personal information for any purpose, contact Data Privacy team via email: Privacy@trianz.com

5. Responsibilities: Security Organization, Authority, and Obligations

Trianz and its leadership recognize the need for a strong information security program.

5.1 The Infosec & Data Privacy Assurance Team

Trianz has designated Chief Information officer (CIO) and Chief Information Security Officer (CISO) to head the Information Security and Data Privacy Assurance and accountable for all aspects of its information security program. Contact the team via email: InfoSec@trianz.com for any guidance/clarifications/support needed.

5.2 Policy Authority and Maintenance

Trianz has granted the Information Security and Data Privacy Assurance team the authority to develop, maintain, and enforce this Policy and any additional policies, procedures, standards, and processes, as deemed necessary and appropriate.

5.3 Policy Review

On at least annual basis, Information Security and Data Privacy Assurance team will initiate a review of this Policy, engaging stakeholders such as individual business units, Human Resources, Legal, and other Trianz organizations, as appropriate.

5.4 Exceptions

Trianz recognizes that specific business needs and local situations may occasionally call for an exception to this Policy. Exception requests must be logged in the exception handling tool in the control doc tool by IS Team with necessary approvals from CISO with reference to the exception handling policy. The Information Security and Data Privacy Assurance team must periodically review all the exceptions.

Information Security and Data Privacy Assurance team will not approve any exception simply because the same was previously approved in a similar situation. Each noncompliant situation requires a review of the specific facts and risks to Trianz's information assets and those of our clients.

5.5 Workforce Obligation to Comply

Employees and contractors are obligated to comply with all aspects of this Policy that apply to them. This Policy is not intended to restrict communications or actions protected or required by federal, state, or local law.

Trianz may treat any attempt to bypass or circumvent security controls as a violation of this Policy. For example, sharing passwords, deactivating anti-virus software, removing or modifying secure configurations, or creating unauthorized network connections are prohibited.

Trianz takes steps to help employees and contractors understand this, Policy. Employees and Contractors are responsible for their own actions and compliance with this Policy. Employees and Contractors should question and report any situation to manager or Infosec & Data Privacy Assurance Team that appears to violate this Policy or creates any undue information security risk.

5.6 Sanctions

Any violation of this Policy may result in disciplinary action or other sanctions. Sanctions may include (in accordance with applicable law) suspension, access restrictions, work assignment limitations, or more severe penalties up to and including termination. If Trianz suspects illegal

activities, it may report them to the applicable authorities and aid in any investigation or prosecution of the individuals involved.

5.7 Acknowledgment

All employees and contractors must acknowledge that they have read, understood, and agree to comply with this Policy either in writing or through an approved online process. Acknowledgment must be completed on a timely basis following a new hire or as otherwise designated by Information Security and Data Privacy Assurance team. Material changes to this Policy may require additional acknowledgment. Trianz will retain acknowledgment records.

5.8 Information Security Awareness, Education and Training

AWARNESS:

Trianz's information security awareness programme shall aim to make personnel aware of their responsibilities for information security and the means by which those responsibilities are discharged.

The awareness programme shall be planned to take into consideration the roles of personnel in the organization, including internal and external personnel (e.g. external consultants, supplier personnel). The activities in the awareness programme shall be in the form of mailers.

Information security awareness shall cover general aspects such as:

- Management's commitment to information security throughout the organization.
- Familiarity and compliance needs concerning applicable information security rules and obligations, taking into account information security policy and topic-specific policies, standards, laws, statutes, regulations, contracts and agreements.
- personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and interested parties.
- basic information security procedures [e.g. information security event reporting and baseline controls [e.g. password security

- contact points and resources for additional information and advice on information security matters, including further information security awareness materials.

EDUCATION & TRAINING:

Trianz shall identify, prepare and implement an appropriate training plan for technical teams whose roles require specific skill sets and expertise. Technical teams should have the skills for configuring and maintaining the required security level for devices, systems, applications and services. If there are missing skills, the organization should take action and acquire them.

The education and training program shall consider different forms [e.g. mentored by expert staff or consultants (on-the-job training), rotating staff members to follow different activities, recruiting already skilled people and hiring consultants.

Trianz recognizes that an astute workforce is the best line of defense. Trianz will provide security training opportunities and expert resources to help employees and contractors understand their obligations under this Policy and avoid creating undue risks. Employees must complete information security training within a reasonable time after initial hire. All workforce members must complete information security training on at least an annual basis. Managers must ensure that their employees complete all required training.

Trianz may deem failure to participate in required training a violation of this Policy.

Trianz will retain attendance records and copies of security training materials delivered.

5.9 Client Policies

Trianz may handle sensitive client information. In some cases, Trianz may agree to comply with specific client information security policies or standards. To minimize special cases, Trianz has developed this Policy to include the requirements common to most of our clients.

If Trianz agrees to comply with additional client-specific information security policies or standards, Trianz will notify affected workforce members. Trianz's Workforce must comply with any such policies or standards, including any related training or additional background screening requirements.

Legal and the Information Security and Data Privacy Assurance team must review and approve any client agreements that require compliance with specific information security policies or standards.

5.10 Data: Information Classification and Risk-Based Controls

Trianz has established a three-tier classification scheme to protect information according to risk levels. The information classification scheme allows Trianz to select appropriate security controls and balance protection needs with costs and business efficiencies.

All Trianz information may be classified as Public, Internal, Confidential and Restricted.

Unless it is marked otherwise or clearly intended to be Public Information, treat all Trianz and client information as if it is Confidential Information, regardless of its source or form, including electronic, paper, verbal, or other information.

You must apply security controls appropriate for the assigned information classification level to all information you store, transmit, or otherwise handle. Use classification level markings, where feasible.

5.11 Public

Public Information is information that Trianz has made available to the general public. Information received from another party (including a client) that is covered under a current, signed non-disclosure agreement must not be classified or treated as Public Information.

(a) **Public Information Examples**: Some Public Information examples include, but are not limited to:

i. press releases; ii. Trianz marketing materials; iii. job announcements; and iv. any information that Trianz makes available on its publicly accessible website.

Do not assume that any information you obtain from Trianz's internal network or systems is publicly available. For example, draft marketing materials are typically Confidential Information until their release. Consider all information to be at least Confidential Information, and not available for public disclosure without authorization, until you verify it is Public Information.

5.12 Internal

Internal classification is for all organization assets that are owned by Trianz and meant only for internal circulation.

Internal – Internal use only - information will be made available to all the employees of the organization and would be made available only to authorized persons outside the organization (for example, a client or a third-party service provider).

Adequate security measures shall be taken to prevent unauthorized access and/or modifications within the organization.

Some examples are operating procedure manuals, internal announcements, process assets etc.

5.13 Confidential

Confidential Information is information that may cause harm to Trianz, its clients, employees, or other entities or individuals if improperly disclosed, or that is not otherwise publicly available. Harms may relate to an individual's privacy, Business Confidential information, Trianz's marketplace position or that of its clients, or legal or regulatory liabilities.

Mark Confidential Information to denote its status when technically feasible.

Applications or databases that contain Confidential Information may be marked with an initial banner shown upon system access.

You must have authorization to disclose Confidential Information to an external party.

Seek guidance from your manager or Legal prior to disclosing Confidential Information and verify that an appropriate nondisclosure or other agreement is in effect.

(a) **Confidential Information Examples:** Some Confidential Information examples include, but are not limited to:

i. Trianz financial data, client lists, revenue forecasts, program or project plans, and intellectual property;

ii. client-provided data, information, and intellectual property;

iii. client contracts and contracts with other external parties, including vendors;

iv. communications or records regarding internal Trianz matters and assets,

Including operational details and audits;

v. Trianz policies, procedures, standards, and processes (for example, this Policy is Confidential

Information and should not be shared without authorization from the Infosec & Data Privacy Assurance Team);

vi. any information designated as "confidential" or some other protected information classification by an external party and subject to a current non-disclosure or other agreement;

vii. information regarding employees

viii. any summaries, reports, or other documents that contain Confidential Information; and

ix. Drafts, summaries, or other working versions of any of the above.

(b) **Safeguards:** You must protect Confidential Information with specific administrative, physical, and technical safeguards implemented according to risks, including (but not necessarily limited to):

i. **Authentication**: Electronically stored Confidential Information must only be accessible to an individual after logging in to Trianz's network.

ii. **Discussions**: Only discuss Confidential Information in non-public places, or if a discussion in a public place is absolutely necessary, take reasonable steps to avoid being overheard.

iii. **Copying/Printing/Faxing/Scanning**: Only scan, make copies, and distribute Confidential Information to the extent necessary or allowed under any applicable non-disclosure agreement or other applicable agreement. Take reasonable steps to ensure that others who do not have a business need to know do not view the information.

When faxing Confidential Information, use a cover sheet that informs the recipient that the information is Trianz's Confidential Information. Set fax machines to print a confirmation page after sending a fax. Locate copiers, fax machines, scanners, and other office equipment in physically secured areas and configure them to avoid storing Confidential Information.

iv. **Encryption**: Encrypt Confidential Information when storing it on a laptop, smartphone, or other mobile device, including mobile storage devices. Consider encrypting Confidential Information when processing or transmitting / transporting it externally, based on specific risks. Seek assistance from IS Team or Information Security and Data Privacy Assurance Team, if needed.

v. **Mailing**: Use a service that requires a signature for receipt of the information when sending Confidential Information outside Trianz. When sending Confidential Information inside Trianz, use a sealed security envelope marked "Confidential Information."

vi. **Meeting Rooms**: You should only share Confidential Information in meeting rooms that are physically secured. Erase or remove any Confidential Information that you write on a whiteboard or other presentation tool upon the meeting's conclusion.

vii. **Need to know**: Only access, share, or include Confidential Information in documents, presentations, or other resources when there is a business need to know.

viii. **Physical Security**: Only house systems that contain Confidential Information, or store Confidential Information in paper or other forms, in physically secured areas.

5.14 Restricted

Restricted Information is information that may cause serious and potentially irreparable harm to Trianz, its clients, employees, or other entities or individuals if disclosed or used in an unauthorized manner resulting in legal liabilities. Restricted Information is a subset of Confidential Information that requires additional Protection as it contains personal or Sensitive Data .

Mark Restricted Information to denote its status when technically feasible. Applications or databases that contain Restricted Information may be marked with an initial banner shown upon system access.

You may not remove Restricted Information from Trianz's environment without authorization.

You must have authorization to disclose Restricted Information to an external party. Seek guidance from Legal and the the Infosec & Data Privacy Assurance Team prior to disclosing Restricted Information externally to ensure Trianz meets its legal obligations.

(a) **Restricted Information Examples: Some Restricted** Information examples include, but are not limited to:

i. Personal information for employees, clients, business partners, or others; and ii. Sensitive Trianz business information, such as budgets, financial results, or strategic plans.

(b) **Safeguards:** You must protect Restricted Information with specific administrative, physical, and technical safeguards implemented according to risks and as prescribed by applicable laws, regulations, and standards, both at rest and in transit including (but not necessarily limited to):

ii. **Authentication**: Electronically stored Restricted Information must only be accessible to an individual after logging in to Trianz's network and with specific authorization.

iii. **Discussions**: Restricted Information can only be discussed in non-public places, after ensuring that there is no eavesdropping.

iv. **Copying/ Printing/Faxing/Scanning**: Do not scan, copy, or distribute Restricted Information unless absolutely necessary. Take reasonable steps to ensure that others who do not have a specific business need to know do not view the information.

i. When faxing Restricted Information, use a cover sheet that informs the recipient that the information is Trianz's Restricted Information. Set fax machines to print a confirmation page after sending a fax. Locate copiers, fax machines, scanners, and other office equipment in physically secured areas and configure them to avoid storing Restricted Information.

ii. **Encryption**: You must encrypt Restricted Information when transmitting it, whether externally or internally, or when storing it on a laptop, smartphone, or other mobile device, including mobile storage devices such as USB drives. You should also encrypt Restricted Information when storing it on a server, database, or other stationary device.

iii. **Mailing**: Do not mail Restricted Information unless absolutely necessary. Use a service that requires a signature for receipt of the information when sending Restricted Information outside Trianz. When sending Restricted Information inside Trianz, use a sealed security envelope marked "Restricted Information." If you use electronic media to mail Restricted Information, you must encrypt, and password protect it.

iv. **Meeting Rooms**: You must only share Restricted Information in meeting rooms that are physically secured. Erase any Restricted Information that you write on a whiteboard or other presentation tool upon the meeting's conclusion.

v. **Need to know**: Only access, share, or include Restricted Information in documents, presentations, or other resources when there is a specific business need to know.

vi. **Network Segmentation**: You may only make Restricted Information available to areas of Trianz's network where there is a specific business need. Restricted Information must be segmented from the rest of Trianz's network through the use of controls such as firewalls, access control, or other security mechanisms.

vii. **Physical Security**: Only house systems that contain Restricted Information, or store Restricted Information in paper or other forms, in physically secured areas, accessible only to those with a specific business need to know.

Data Retention: Data is retained securely only as-long-as it is necessary to meet legitimate business requirements and applicable law or any other legal / contractual requirements.

6. People: Roles, Access Control, and Acceptable Use

People are the best defense in information security. They are also the weakest link. Trianz grants access to its systems and data based on business roles. Trianz

places limits on how you may use and interact with its information assets. These restrictions help lower risks and protect you and Trianz.

6.1 Roles

Business roles and role-based access are based on the individual's stake with Trianz and assigned activities.

a) **Employees**: Human Resources provides employee screening and background investigations. Trianz may require employees who handle Restricted Information to undergo additional background screening and testing where permitted by applicable laws.

   Supervising managers may request access for their employees only to those Trianz systems and data required to meet business needs.

b) **External Parties**: Trianz grants systems access to approved external parties, such as contractors, vendors, service providers, business partners, or others with a demonstrated business need that cannot be reasonably met through other means. Trianz may support different access levels for different business situations.

   A sponsoring employee must be designated for any external party before Trianz grants access to its systems or data. The sponsoring employee is responsible for supervising the external party, including compliance with this Policy.

   The sponsoring employee may request access only to those Trianz resources necessary to meet business needs. The sponsoring employee must also request that any access granted be terminated when the business need ends.

6.2 Identity and Access Management.

Trianz uses identity and access management controls to provide user accounts with appropriate privileges to employees and others. Trianz will assign each individual a unique identifier using a standard algorithm (the individual's "primary ID"). Trianz should only create device or application-specific identifiers if the primary ID cannot be used. Device or application-specific identifiers must be linked to an accountable individual.

a) **Unique User Accounts**: Trianz assigns unique user accounts and passwords to individuals, using their primary ID. You must not share your account or password with others. If system or other administrative accounts cannot be uniquely assigned to specific individuals, Trianz should use mediated access, audit logs, or other technical controls to provide individual accountability.

b) **Add, Change, Terminate Access**: Trianz restricts access to specific resources to those with a business need to know. Responsible managers should direct requests to add or change access levels to Information Systems (IS team). System and application administrators must periodically review user accounts and access levels to confirm that a legitimate business need for the access still exists.

   When an employee leaves the business, Human Resources must immediately notify Information Systems (IS team). . Information Systems (IS team) will timely deactivate the individual's account(s). Managers should seek guidance from Human Resources and Infosec & Data Privacy Assurance Team regarding access for employees on extended leaves.

c) **Authorization Levels and Least Privilege:** Proper authorization levels ensure that Trianz only grants individuals the privileges they need to perform their assigned activities and no more. Known as least privilege access, this method minimizes risks. Least privilege applies to user and administrative access. You must not grant administrative privileges unless there is a specific business need and limit them to the extent feasible.

d) **Role-Based Access Controls:** Use role-based access control methods wherever feasible to assign authorization levels according to business functions, rather than uniquely for each individual. This method supports the least privilege mechanism by standardizing access. It also simplifies periodic access reviews.

6.3 Acceptable Use Policy

Trianz provides employees and others with network resources and systems to support its business requirements and functions. This section limits how you may use Trianz's information assets and explains the steps you must take to protect them.

If you have any questions regarding acceptable use of Trianz's resources, please discuss them with your manager or contact The Infosec & Data Privacy Assurance Team for additional guidance.

General Use of Information Technology Resources: Trianz provides network resources and systems for business purposes. Any incidental non-business use of Trianz's resources must be for personal purposes only. Do not use Trianz's resources for commercial purposes, personal gain, or any purpose that may create a real or perceived conflict of interest with Trianz.

Do not use Trianz's resources in a manner that negatively impacts your job performance or impairs others' abilities to do their jobs.

Do not use Trianz's network or systems for activities that may be deemed illegal under applicable federal, state, local, or international law. If Trianz suspects illegal activities, it may report them to the appropriate authorities and aid in any investigation or prosecution of the individuals involved.

Prohibited Activities: Trianz prohibits using its resources to engage in activities such as (but not necessarily limited to) the following:

hacking, spoofing, or launching denial of service attacks;

gaining or attempting to gain unauthorized access to others' networks or systems;

sending fraudulent email messages;

Forwarding emails from the personal email id's to Trianz official email id's without verifying the sender's identity and authenticity.

Forwarding emails from Trianz official Id's to personal Id's without verifying the sender's identity and authenticity.

distributing or attempting to distribute malicious software (malware);

spying or attempting to install spyware or other unauthorized monitoring or surveillance tools;

committing criminal acts such as terrorism, fraud, or identity theft;

downloading, storing, or distributing child pornography or other obscene materials;

downloading, storing, or distributing materials in violation of another's copyright;

creating undue security risks or negatively impacting the performance of Trianz's network and systems;

causing embarrassment, loss of reputation, or other harm to Trianz;

uploading, downloading, or disseminating defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene, or otherwise inappropriate or offensive messages or media;

distributing joke, chain letter, commercial solicitations, or hoax emails or other messages (spamming);

disrupting the workplace environment, creating a hostile workplace, or invading the privacy of others;

using encryption or other technologies in an attempt to hide illegal, unethical, or otherwise inappropriate activities; and

installing or distributing unlicensed or pirated software.

Desktop, Laptop, and End-User Controls: You may only access Trianz's network using approved end user devices that support our current minimum information security standards. Standards for end user devices may include protective controls and specific configurations, such as anti-virus software, patching levels, and required operating system or other software versions. Trianz-owned machines may be configured to automatically receive upgrades. You may be denied remote access using non Trianz owned devices that do not meet current standards.

Use your own Trianz-provided account(s) to access Trianz's network and systems, unless you have been specifically authorized to use a device-specific, administrative, or other account .

Screen saver passwords, also known as "workstation timeouts" or "lock screens," secure Confidential Information by protecting active computer sessions when you step away. Locking screen savers must activate after a maximum inactivity time of 15 minutes. If you handle Restricted Information, lock your screen any time you leave it unattended.

Information Handling and Storage : You must properly handle, store, and securely dispose of Trianz's information in accordance with Trianz's Records Retention Schedule. You are responsible for any Confidential or Restricted Information that you access or store. Do not allow others to view, access, or otherwise use any Confidential or Restricted Information you control unless they have a specific business need to know.

Store files or other data critical to Trianz's operations on regularly maintained (backed up) servers or other storage resources. Do not store business critical data only on end-user devices such as desktops, laptops, smartphones, or other mobile devices.

Physically secure any media containing Trianz information, including hard drives, CDs, disks, paper, voice recordings, removable drives (such as thumb drives, flash drives, USB drives), or other media.

Media containing Confidential or Restricted Information must be stored in a locked area when not in use.

Shred or otherwise destroy paper that contains Confidential or Restricted Information prior to disposal. Return all electronic, magnetic, or optical media to IT for secure disposal when it is no longer required to meet business needs.

Internet Use: Email, Messaging, Social Media, and Cloud Computing. The internet offers a variety of services that Trianz employees and contractors depend on to work effectively. However, some technologies create undue risks to Trianz's assets. Some uses are not appropriate in the workplace.

Trianz may block or limit access to particular services, websites, or other internet-based functions according to risks and business value. Recognize that inappropriate or offensive websites may still be reachable and do not access them using Trianz resources.

General Internet Use: Limit your web browsing and access to streaming media (such as videos, audio streams or recordings, and webcasts) to business purposes or as otherwise permitted by this Policy. Internet use must comply with this Policy.

Never use internet peer-to-peer file sharing services, given the risks to Trianz's information assets they create.

Do not use internet-based remote access services to access Trianz's network or systems, including desktop computers. If you need remote access, use Trianz-provided or authorized software..

Email and Social Media. Do not disclose Confidential or Restricted Information to unauthorized parties on blogs or social media or transmit it in unsecured emails or instant messages. Do not make postings or send messages that speak for Trianz or imply that you speak for Trianz unless you have been authorized to do so.

Use good professional judgment when drafting and sending any communications. Remember that messages may be forwarded or distributed outside your control, and your professional reputation is at stake. Email signatures should be professional, appropriate for your business role, and not unreasonably long or complex.

Never open an email attachment that you did not expect to receive, click on links, or otherwise interact with unexpected email content. Attackers frequently use these methods to transport viruses and other malware. Be cautious, even if messages appear to come from someone you know, since attackers can easily falsify (spoof) email senders. Trianz may block some attachments or emails, based on risk.

Do not respond to an email or other message that requests Confidential or Restricted Information unless you have separately verified and are certain of its origin and purpose. Even then, always protect Confidential or Restricted Information as described, Data: Information Classification and Risk-Based Controls.

If you have any doubts regarding the authenticity or risks associated with an email or other message you receive, contact IT immediately and before interacting with the message. Do not reply to suspicious messages, including clicking links or making unsubscribe requests. Taking those actions may simply validate your address and lead to more unwanted or risky messages.

Cloud Computing Trianz may use internet-based, outsourced services for some computing and data storage activities based on business needs. Cloud computing services store data and provide services in internet accessible data centers that may be located almost anywhere. Cloud services vary significantly in service levels and security provided.

While cloud services may offer an attractive cost model, they also present significant risks. Using them may also affect Trianz's ability to comply with some laws. Before using any cloud computing services to collect, create, store, or otherwise manage Trianz's Confidential or Restricted Information, you must obtain approval from Legal and the The Infosec & Data Privacy Assurance Team .

This Policy applies to any document sharing or other internet-based services, if Trianz Confidential or Restricted Information is stored.

Mobile Devices and Bring Your Own Device (BYOD) to Work:

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, so you must take appropriate steps to protect them.

Trianz may permit employees and others to use their own equipment to connect to its network and systems, as per BYOD Policy. If you choose to do so, you agree that your use of those devices is subject to this Policy and any additional policies, procedures, standards, and processes Trianz implements. You may be required to install specific security controls on your device (for example, device management software, access controls, encryption, remote wiping in case your device is lost or stolen, or other security controls).

You must allow IT to review your device and remove any Trianz data, if your relationship with Trianz terminates, you change devices or services, or in other similar situations. You must also promptly provide Trianz with access to your device when requested for Trianz's legitimate business purposes, including any security incident or investigation.

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 Restricted Information. Mobile devices, including those that provide access to Trianz email, must be protected using a password or other approved authentication method.

Physically secure any mobile devices you use to access or store Trianz information. Never leave laptops or other devices unattended unless locked or otherwise secured. Do not leave mobile devices or the bags containing them visible in a parked car or check them as baggage on airlines or other public transportation.

Do not connect a 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.

a) **Remote Access:** If you have a business need to access Trianz's network and systems from home, while traveling, or at another location, Trianz may grant you remote access.

   Use two-factor authentication to access Trianz's network remotely. Configure remote access capabilities to limit access to only those assets and functions for which Infosec & Data Privacy Assurance Team approves. You may only use Trianz-provided means for remote access (for example, VPN connections, dial-up modems, Trianz portal). Do not install or setup any other remote connections, including remote desktop software, without the Infosec & Data Privacy Assurance Team 's authorization.

   Remote access connections should timeout (be disconnected) after a maximum of one hour of inactivity. Trianz does not permit split tunnelling or other mechanisms that bridge unsecure networks with Trianz's network.

b) **External Network Connections:** Some business situations may require creating a secure connection from Trianz's network to an external party's network (extranet). Examples include working extensively with client systems, outsourcing, or partnering with another organization for an extended period of time. Extranet connections allow the organizations to share information and technical resources in a secure manner by connecting the two networks at their respective perimeters.

   The Infosec & Data Privacy Assurance Team must review and approve all extranets and any other external connections to Trianz's network before implementation. A signed business agreement between the two organizations must accompany any extranet connection. Limit connectivity to only those assets required to perform the specified functions for the specified time period as contractually agreed between two parties. Trianz monitors extranet connections and may deactivate them if unusual or inappropriate traffic is detected.

c) **Wireless Network Connections**: Do not connect any wireless access points, routers, or other similar devices to Trianz's network unless Infosec & Data Privacy Assurance Team has reviewed and approved them.

   Secure and maintain approved wireless network (WiFi) connections according to current Trianz technical and physical security standards. Do not connect wireless access points (WAPs) directly to Trianz's trusted network without going through a firewall or other protective controls. Deactivate WAPs when they are not in use, including during non-business hours.

Only transmit, receive, or make available Restricted Information through WiFi connections using appropriate protective controls, including encryption. If you have questions regarding appropriate WiFi security measures to take when handling Restricted Information, contact Infosec & Data Privacy Assurance Team

End-user devices that access wireless networks, such as laptops, must have personal firewalls installed and maintained according to current Trianz standards. Deactivate your computer's wireless networking interface when it is not in use.

7. Information Security Objectives

Top Management will provide commitment and direction to Identify the Information Security Objectives at relevant functions and levels and responsibilities will be assigned on how and when to achieve them.

8. Information Assets

Protecting and Managing Trianz's Information Technology Environment:

This section describes key safeguards that Trianz uses to protect and manage its information technology (IT) environment. You must support their use to the extent that they apply to you.

8.1 Protecting Information Assets

Install and configure Trianz-owned computers according to current technical standards and procedures, including anti-virus software, other standard security controls, and approved operating system version and software patches. Trianz supports preventive controls to avoid unauthorized activities or access to data, based on risk levels. Trianz supports detective controls to timely discover unauthorized activities or access to data, including continuous system monitoring and event management.

a) **End-User Computers and Access**: Configure end-user computers to request authentication from Trianz's domain at startup and user login. End-user computers may be denied network access if installed software versions do

not match current standards. Users may not access Trianz's network unless they have been properly authenticated.

Configure user accounts to require strong passwords. To protect against password guessing and other brute force attacks, Trianz will deactivate user accounts after five failed login attempts. Reactivation may be based on a timeout or manual reset according to risk and technical feasibility.

Secure remote access points via VPN or Secure Private Access require two-factor authentication or single sign on (SSO). Encrypt authentication credentials during transmission across any network, either internal or external.

b) **Passwords and User Credentials**: Select strong passwords and protect all user credentials, including passwords, tokens, badges, smart cards, or other means of identification and authentication. Implement password rules so that users select and use strong passwords, as per Password Policy. Automate password rule enforcement to the extent technically feasible.

i. Minimum Password Rules. At minimum passwords must:

A. User-specified number of characters between 0 and 14 , be at least 8 characters;(mandatory)

B. be comprised of a mix of letters (upper and lower case), numbers, and special characters (punctuation marks and symbols);

C. not be comprised of or use words that can be found in a dictionary;

D. not be comprised of an obvious keyboard sequence or common term (i.e., "qwerty," "12345678," or "password"); and

E. Not include easily guessed data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Several techniques can help you create a strong password. Substituting numbers for words is common. For example, you can use the numerals two or four with capitalization and symbols to create a memorable phrase. Another way to create an easy to remember strong password is to think of a sentence and use the first letter of each word as a password.

Treat passwords as Restricted Information. You may be required to change your password periodically according to current Trianz standards. Change

your password immediately and report the incident ,if you have reason to believe that it has been compromised.

ii. **Password Protection**: Protect your passwords at all times by:

A. Not disclosing your passwords to anyone, including anyone who claims to be from IT;

B. Not sharing your passwords with others (including coworkers, managers, clients, or family);

C. Not writing down your passwords or otherwise recording them in an unsecure manner;

D. Not using save password features for applications, unless provided or authorized by Trianz;

E. Not using the same password for different systems or accounts, except where single sign on features are automated; and

F. Not reusing passwords.

IT procedures and technical standards define additional steps to protect passwords for administrative or device-specific accounts.

c) **Perimeter Controls**: Perimeter controls secure Trianz's network against external attacks. Use firewalls with UTM (Unified Threat Management) features, configured according to current technical standards and procedures, to separate Trianz's trusted network from the internet or internet-facing environments.

Trianz may implement additional perimeter controls including intrusion detection and prevention services, data loss prevention software, specific router or other network configurations, or various forms of network monitoring according to risks. Do not create internet connections outside perimeter controls.

d) **Data and Network Segmentation**: Trianz may use technical controls, such as firewalls, access control lists, or other mechanisms, to segment some data or areas of its network according to risks. Segment Restricted Information from the rest of Trianz's network, to the extent technically feasible and reasonable Do not alter network segmentation plans without approval from the Infosec & Data Privacy Assurance Team.

e) **Encryption**: Trianz uses encryption to protect Confidential and Restricted Information according to risks. Encryption may be applied to stored data

(data-atrest) and transmitted data (data in-transit). Encrypting personal information may lower Trianz's liability in the event of a data breach.

Only use generally accepted encryption algorithms and products approved by the The Infosec & Data Privacy Assurance Team Periodically review encryption products and algorithms for any known risks.

Laws may limit exporting some encryption technologies. Seek guidance from Legal prior to exporting or making any encryption technologies available to individuals outside the US.

i. **Encryption Key Management**: Encryption algorithms use keys to transform and secure data. Because they allow decryption of the protected data, proper key management is critical. Select encryption keys to maximize protection levels, to the extent feasible and reasonable. Treat them as Restricted Information.

   Ensure that keys are available when needed to support data decryption by using secure storage methods and creating and maintaining secure backups. Track access to keys. Keys should never be known or available to only a single individual. Change encryption keys on a periodic basis according to risks.

f) **Data and Media Disposal**: When Trianz retires or otherwise removes computing, network, or office equipment (such as copiers or fax machines) or other information assets that may contain Confidential or Restricted Information from the business, specific steps must be taken to scrub or otherwise.

   render the media unreadable. Degaussing machine

   Simply deleting files or reformatting disks is not sufficient to prevent data recovery. Either physically destroy media, according to applicable waste disposal regulations, or scrub it using data wiping software that meets generally accepted data destruction standards. For example, see the National Institute of Standards and Technology's Special Publication 800-88, Guidelines for Media Destruction.

g) **Log Management and Retention**: Trianz logs system and user activities on network, computing, or other information assets according to risks. Security controls or other network elements may also produce logs.

Secure log data and files to prevent tampering and retain them according to Trianz's Records Retention Schedule. Regularly review logs, using automated means where feasible, to identify any anomalous activities that may indicate a security incident.

ICT Readiness for Business Continuity

8.2 Managing Information Assets

IT manages IT operations and related activities at Trianz.

Only Trianz-supplied or approved software, hardware, and information systems, whether procured or developed, may be installed in Trianz's IT environment or connected to Trianz's network.

CISO must approve and manage all changes to Trianz's production IT environment to avoid unexpected business impacts. Direct questions regarding IT operations to IS@trianz.com / itservicedesk@trianz.com Development environments must comply with this Policy and current IT standards to minimize information security risks.

a) **Procurement**: Only those authorized by IT, may procure information assets for use in or connection to Trianz's network. This Policy applies whether software or other assets are purchased, open source, or made available to Trianz at no cost. Seek guidance from Infosec & Data Privacy Assurance Team early in the software development process to identify and manage information security risks prior to implementation. Before using cloud computing services to access, store, or manage Confidential or Restricted Information, you must obtain authorization from Legal and Infosec & Data Privacy Assurance Team (Cloud Computing).

b) **Asset Management**: Track and document all information assets, including hardware, software, and other equipment, using Trianz's asset management system(s). This inventory tracking should include operating system levels and all installed software and software versions to support vulnerability identification and mitigation. Update the asset inventory as assets are removed from the business. Confidential or Restricted Information must have an assigned data owner who is responsible for tracking its location, uses, and any disclosures. Properly dispose of all data and media to help avoid a breach of Confidential or Restricted Information .

c) **Authorized Environments and Authorities**: Only authorized IT personnel, may install and connect hardware or software in Trianz's IT environment. Do not convert end-user computers to servers or other shared resources without assistance from IT. Limit administrative, or privileged, systems access to those individuals with a business need to know. IT must distribute administrative access and information regarding administrative processes to more than one individual to minimize risks.

Internet connections and internet-facing environments present significant information security risks to Trianz. Head of IS Operations must approve any new or changed internet connections or internet-facing environments.

d) **Change Management**: IT maintains a change management process to minimize business impact or disruptions when changes are made in Trianz's production IT environment. Change requests must be accompanied by an action plan that includes assigned roles and responsibilities, implementation milestones, testing procedures, and a rollback plan, in the event the change fails.

Implement and maintain a change management process to track identified problems, fixes, and releases during software development. Design these processes to include code archiving (versioning) tools so that earlier versions can be recovered and rebuilt, if necessary.

e) **Application and Software Development**: To avoid any undue or unexpected impact to Trianz's production IT environment, application and software development activities, including system testing, must take place in reasonably segmented environments. Maintain segregation of duties between development and operations. Developers may be granted limited access to production environments where personnel and expertise availability is limited, but only for specific troubleshooting or support purposes. Software development must take place in authorized environments.

Use security-by-design principles to identify potential information security risks and

resolve them early in the development process. Seek guidance from Infosec & Data Privacy Assurance Team, critical vendors, industry experts, and best

practices to identify and avoid application-level security risks. Pay particular attention to protecting Restricted Information through encryption or other appropriate means. Use defensive coding techniques and regular code review and application-level scanning to identify and remediate any information security issues before releasing software.

8.3 Mobile Device Management & Mobile Application Management

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and their use is supported to achieve business goals.

However mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

Trianz has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. To accomplish this objective all mobile devices, whether owned by Trianz or owned by employees, that have access to corporate networks, data and systems, not including corporate IT managed laptops will be monitored as below:

Mobile Device Management (MDM) for Trianz Company own devices:

1. All devices will have to be mandatorily enrolled for MDM.
2. All the information present on the device will be owned by Trianz.
3. Trianz may, at its discretion or based on certain incidents like theft of device, compromised device etc., may remotely wipe the entire data on the device.

Mobile Application Management (MAM) for Bring Your Own Device (BYOD):

1. All BYOD devices need to be enrolled for MAM, before being allowed for accessing BYOD policy permitted information or tools.
2. All the MAM managed application information will be owned by Trianz, and all other information will be owned by the BYOD device owner.

3. Trianz may, at its discretion or based on certain incidents like theft of device, compromised device etc., may remote wipe only the MAM managed data on the device such as Corporate Email data, One Drive data etc.
4. Trianz MAM solution will not have access to user's personal information or any other applications. Also, MAM solution will not wipe any other information other than MAM managed applications data.

9. Threat Intelligence

Trianz is committed to ensuring that effective methods are employed to ensure the accuracy, completeness and timeliness of the threat intelligence it uses. This Process sets out the major steps involved in collecting and processing intelligence about threats at the strategic, tactical and operational levels.

Please refer to Threat Intelligence Procedure

10. Physical Security, Monitoring and Protecting against physical and environmental threats.

a) **Physical (Environmental) Security**: Trianz uses physical safeguards to avoid theft, intrusions, unauthorized use, or other abuses of its information assets. You must comply with Trianz's current physical security policies and procedures and:

Trianz uses physical safeguards information assets such as Unauthorized entry.

b) ensuring buildings are unobtrusive, IT and give minimum indication of their purpose or inside the building, identifying the presence of information processing activities;

Ensures that display of Confidential and Restricted Information is not being visible and audible for unauthorized individuals and outside the organization.

Trianz ensures continuous monitoring as follows.

c) Installed CC TV Cameras to view, record and to monitor accessing to sensitive areas within and outside an organization's premises;

CCTV equipment configuration and data protected from unauthorized access in order to prevent surveillance information, such as video feeds, from being

accessed by unauthorized persons or systems being disabled remotely and compliance to applicable regulations.

All Data Centres are equipped with Alarm Systems for any….(Need to ask Chandra)

d) Risk assessments to identify the potential consequences of physical and environmental threats shall be performed prior to beginning critical operations at a physical site, and at regular intervals. Necessary safeguards/Controls shall be implemented and changes to threats shall be monitored. Specialist advice shall be obtained on how to manage risks arising from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions and other forms of natural disaster or disaster caused by human.

11. Configuration Management

Trianz has established Configuration Management Framework that includes software, Hardware and Services, networks etc., For all applicable Configuration Changes templates are defined, ,implemented and logs shall be maintained for all Configuration changes. Configurations shall be monitored with a comprehensive set of system management and shall be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed.

12. Information Deletion

a) "Data Retention and Secure Disposal Policy " ensures deletion method (e.g. electronic overwriting or cryptographic erasure) in accordance with business requirements and taking into consideration relevant laws and regulations; recording the results of deletion as evidence; and obtaining evidence of information deletion from suppliers etc.

Refer to Data Retention and Secure Disposal Policy and Procedure.

13. Data Masking

Sensitive data is encrypted at rest and in transit and complies with applicable legal, statutory, regulatory and contractual requirements. Various techniques such

as Pseudonymization, Anonymization, Data Obsufication etc (Data Masking) are followed.

Refer to Privacy By Design Procedure, Policy on the usage of Cryptographic Controls, Encryption Key Management Policy

14. Data Leakage Prevention

The policy is designed to ensure that the users do not send sensitive or critical information outside the

corporate network. Data Loss Prevention (DLP) is the practice of detecting and preventing data.

breaches, exfiltration, or unwanted destruction of sensitive data which includes Network DLP,

End Point DLP, Cloud DLP & Storage DLP

Please refer to DLP Policy

15. Supplier Monitoring Activities

Trianz shall monitor regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

conduct audits of suppliers and sub-suppliers, in conjunction with review of independent auditor's reports, if available and follow-up on issues identified; Please ensure Supplier Security Policy

conduct audits of suppliers and sub-suppliers, in conjunction with review of independent auditor's reports, if available and follow-up on issues identified;

16. Web Filtering

Trianz ensures secure networking methods that includes Web filtering.This Policy is to protect systems from malware compromise and prevent access to unauthorized web resources.

This enables Trianz to eliminate security risks such as malware infection that may arise because of access to external websites with malicious content.

Please refer to Web Filtering Policy

17. Secure Coding

Secure coding practices are integral part of Application Security followed by Trianz. All applications that pass or store data owned by Trianz are subject to this policy. This policy applies to all.

applications within Trianz's production environment, as well as administrators and users of these applications.

Please refer to Secure SDLC Policy, Secure SDLC Procedure and Dev SEC Ops Procedure

18. Incident Reporting and Response

The Infosec & Data Privacy Assurance Team maintains a security incident reporting and response process that ensures management notifications are made based on the seriousness of the incident. The Infosec & Data Privacy Assurance Team investigates all reported or detected incidents and documents the outcome, including any mitigation activities or other remediation steps taken.

18.1 Incident Reporting

Immediately notify IS@trianz.com and/or log an incident ticket in the ~~control doc tool~~ Concierto tool if you discover a security incident or suspect a breach in Trianz's information security controls. Trianz maintains various forms of monitoring and surveillance to detect security incidents, but you may be the first to become aware of a problem. Early detection and response can mitigate damages and minimize further risk to Trianz.

All Information Security Incidents shall be managed in accordance with the Information Security Incident Management Response Policy and Procedure. The severity of the incident shall be assessed, and the management response shall be proportionate to the threat.

Treat any information regarding security incidents as Restricted Information and do not share it, either internally or externally, without specific authorization.

Security Incident Examples: Security incidents vary widely and include physical and technical issues. Some examples of security incidents that you should report include, but are not limited to:

loss or suspected compromise of user credentials or physical access devices (including passwords, tokens, keys, badges, smart cards, or other means of identification and authentication);

suspected malware infections, including viruses, Trojans, spyware, worms, or any anomalous reports or messages from anti-virus software or personal firewalls;

loss or theft of any device that contains Trianz information (other than Public Information), including computers, laptops, tablet computers, smartphones, USB drives, disks, or other storage media;

suspected entry (hacking) into Trianz's network or systems by unauthorized persons;

any breach or suspected breach of Confidential or Restricted

Information;

any attempt by any person to obtain passwords or other Confidential or Restricted Information in person or by phone, email, or other means.

(sometimes called social engineering, or in the case of email, phishing); and

any other any situation that appears to violate this Policy or otherwise create undue risks to Trianz's information assets.

Phishing

Compromised Devices: If you become aware of a compromised computer or

another device:

immediately deactivate (unplug) any network connections, but do not power down the equipment as valuable information regarding the incident may be lost if the device is turned off; and

immediately notify IS@trianz.com , itservicedesk@trianz.com

18.2 Event Management

The Infosec & Data Privacy Assurance Team defines and maintains a security incident response plan to manage information security incidents. Report all suspected incidents, as described in this Policy, and then defer to the incident response process. Do not impede the incident response process or conduct your own investigation unless the Infosec & Data Privacy Assurance Team specifically requests or authorizes it.

18.3 Breach Notification

The law may require Trianz to report security incidents that result in the exposure or loss of certain kinds of information or that affect certain services or infrastructure to various authorities, affected individuals or organizations whose data was compromised, or both. Breaches of Restricted Information (and especially personal information) are the most likely to carry these obligations . The Infosec & Data Privacy Assurance Team 's incident response plan includes a step to review all incidents for any required breach notifications. Coordinate all external notifications with Legal and The Infosec & Data Privacy Assurance Team. Do not act on your own or make any external notifications without prior guidance and authorization.

19.Service Providers: Risks and Governance

The Infosec & Data Privacy Assurance Team maintains a service provider governance program to oversee service providers that interact with Trianz's systems or Confidential or Restricted Information. The service provider governance program includes processes to track service providers, evaluate service provider capabilities, and periodically assess service provider risks and compliance with this Policy.

19.1 Service Provider Approval Required

Obtain approval from Legal and the Infosec & Data Privacy Assurance Team before engaging a service provider to perform functions that involve access to Trianz's systems or Confidential or Restricted Information.

19.2 Contract Obligations

Service providers that access Trianz's systems or Confidential or Restricted Information must agree by contract to comply with applicable laws and this Policy or equivalent information security measures. Trianz may require service providers to demonstrate their compliance with applicable laws and this Policy or agreed equivalent Information Security measures by submitting to independent audits or other forms of review or certification based on risks.

20. Client Information: Managing Intake, Maintenance, and client Requests.

Trianz frequently creates, receives, and manages data on behalf of our clients. With guidance from the Infosec & Data Privacy Assurance Team, each business unit develops, implements, and maintains an appropriate process and procedures to manage client data intake and protection.

Business unit-specific client data intake and protection processes may vary but must include, at minimum, means for (1) identifying client data and any pertinent requirements prior to data intake or creation; (2) maintaining an inventory of client data created or received; and (3) ensuring Trianz implements and maintains appropriate information security measures, including proper data and media disposal when Trianz no longer has a business need to retain the client data (or is no longer permitted to do so by client agreement).

20.1 Requirements Identification

Identify any pertinent client data requirements prior to data intake or creation according to your business unit's client data intake and protection process. Requirements may be contractual, the result of applicable law or regulations, or both.

20.2 Intake Management

Business unit-specific client data intake processes and procedures must provide for secure data transfer. Maintain an inventory of client data that includes, at a minimum:

a) a description of the client data;

b) the location(s) where the data is stored;

c) who is authorized to access the data (by category or role, if appropriate);

d) whether the data is Confidential or Restricted Information;

e) how long the data is to be retained (using criteria, if appropriate); and

f) any specific contractual or regulatory obligations or other identified data protection or management requirements.

Treat any client-provided personal information as Restricted Information To minimize risks for clients and Trianz, engage clients in an ongoing dialogue to determine whether business objectives can be met without transferring personal information to Trianz.

20.3 Client Data Protection

Protect all client data Trianz creates or receives in accordance with this Policy and the data's information classification level, whether Confidential or Restricted Information, in addition to any specific client identified requirements.

20.4 Client Data and Media Disposal

Ensure that any client data, or media containing client data, is securely disposed of when it is no longer required for Trianz business purposes, or as

required by client agreement .Update the applicable business unit client data inventory accordingly.

21. Risk and Compliance Management

Trianz supports an ongoing risk management action cycle to

- ✓ enforce this policy;
- ✓ identify information security risks;
- ✓ develop procedures, safeguards, and controls; and
- ✓ verify that safeguards and controls are in place and working properly.

21.1 Risk Assessment and Analysis

Trianz maintains a risk assessment program to identify information security risks across its IT environment, including application software, databases, operating systems, servers, and other equipment, such as network components. The The Infosec & Data Privacy Assurance Team coordinates risk assessment activities that may take several.

forms, including analyses, audits, reviews, scans, and penetration testing. **Do not take any actions to avoid, impact, or otherwise impede risk assessments.**

Only the The Infosec & Data Privacy Assurance Team is authorized to coordinate risk assessments. Seek approval from Legal and the Information Security Coordinator prior to engaging in any risk assessment activities or disclosing any assessment reports outside Trianz.

21.2 Remediation and Mitigation Plans

The Infosec & Data Privacy Assurance Team maintains and oversees remediation and mitigation plans to address risk assessment findings according to risk levels.

21.3 Vulnerability and Penetration Tests

Manufacturers, security researchers, and others regularly identify security vulnerabilities in hardware, software, and other equipment. In most cases, the manufacturer or developer provides a patch or other fix to remediate the vulnerability. In some situations, the vulnerability cannot be fully remediated, but configurations can be changed, or other steps taken to mitigate the risk created.

The Infosec & Data Privacy Assurance Team maintains a process to identify and track applicable vulnerabilities, scan devices for current patch status, and advise system administrators. Schedule any necessary updates using standard change management processes and according to risk level. Make all Trianz-owned devices available to IT for timely patching and related activities.

21.4 Compliance Management

Trianz maintains compliance management processes to enforce this, Policy. Trianz may automate some monitoring and enforcement processes. If compliance management processes indicate that you may have acted contrary to this Policy, you may receive an automated notification or be contacted by the Information Security Coordinator to explain. In some cases, the Information Security Coordinator may contact your supervising manager or Human Resources to resolve the issue.

22. Effective Date

This Information Security Policy is effective from the date of notification.

23. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational Control	5.1 Policies for information security Control Information security policy and topic-specific policies shall be defined, approved	Information Security Policy

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
	by management, published, communicated to, and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	

Document Control

Owner:	CISO	Release ID:	IS-POL-0005

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
0.01	26-Feb-07	Jyotessh G Nair			Review	Review feedback incorporated
1.00	26-Feb-07	Balu Nair			Approved by Zulfikar Deen	Baselined
1.01	30-Jul-08	Bharateesha B R			Revised the policies in accordance with the revised ISMS frame work	Changed the Policy template
2.00	29-Apr-09	Balu Nair			Approval for Baseline	Baselined
2.01	04-Jan-10	Balu Nair			QMG review	Formatted entire document
3.00	04-Jan-10	Balu Nair			Request for Baseline	Baselined
3.01	14-May-10	Balu Nair			QMG Review	Formatted the document, Modified cover page

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
4.00	20-May-10	Balu Nair			Request for baseline	Baselined
4.01	06-May-11	Srilakshmi			To maintain common release id allocation for bluebook documents	Modified ReleaseID in cover page and header
5.00	06-May-11	Srilakshmi			Request for baseline	Baselined
6.00	21-May-12	Srilakshmi			QMG Review	Modified this policy format to template format of policy as per the standard format Modified purpose statement No change in policy statement
7.00	08-Nov-12	Balu Nair			Standardizationof Blue Book Process Assets	Modified the template format. Changed the Logo No change. in policy statement
8.00	19-May-15	Sudharsana.			Reviewed Information Security Policy and approved	Included Security Statement and context

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
8.01	16-Oct-16	Balu Nair			Addition of Cloud services as scope of Certification.	Inclusion of the Cloud Services wherever applicable
9.00	09-Dec-16	Balu Nair			Approved	Baselined
9.00	08-Nov-17	Balu Nair	Joshy VM	Ganesh A	Reviewed	No changes
9.00	17-Oct-18	Balu Nair	Joshy VM	Ganesh A	Reviewed	No changes
9.01	16-Jan-19	Joshy VM	Balu Nair			Added Policy clauses
10.00	15-Mar-19	Balu Nair		Ganesh A	Approved	Baselined
10.1	29-May-19	Balu Nair	Phani Krishna		Addition of MDM Policy	Added MDM Policy
11.0	31-May- 19	Balu Nair		Ganesh A	Approved for Release	Baselined
11.1	12-Nov-19	Anitha Ravindran		Vivek Sambasivam	Reference to Data Protection and Cloud Policy	
11.2	20-Nov-19	Karthik Narasimha	Phani Krishna, Balu and Anita		Review	
11.3	19-Dec-19	Karthik N	Phani	Vivek S	Approved for release	Baselined
11.4	14-Apr-20	Anitha Ravindran	Phani Krishna		Made it generic for	

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
					all Trianz entities. Removed references to particular Trianz entity	
12.0	15-Apr-20	Anitha Ravindran	Phani Krishna	Vivek S	Approved for Release	Baselines
12.1	11-May-20	Karthik N	Balu Nair		Review	Roles modified with CISO/CIO. Incident reporting modified.
13.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
13.1	29-Jul-20	Anitha Ravindran	Phani Krishna		Half yearly review as per review Cadence report	Formatting and table of contents has been changed
14.0	31-July-20	Anitha Ravindran	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
14.1	14-Jan-21	Balu Nair		Phani Krishna	For Review	Updated the information classification, Replaced Information Systems Coordinator with Infosec & Data Privacy Assurance Team and updated section 12 – Risks and Compliance Management
15.0	02-Feb-21	Balu Nair	Vijaya Rajeswari	Phani Krishna	For Approval	Approved and Baselined

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
15.1	08-Nov-21	Karthik Narasimha	Karthik N	Sivaramakrishnan N	For Review	Updated the sections 2, 4, 5 and 7.3
16.0	08-Nov-21	Karthik Narasimha	Karthik N	Sivaramakrishnan N	For Approval	Approved and Baselined
16.0	12-Aug-22	Sanjana,	Karthik N		For review	Reviewed with no changes.
16.1	12-May-23	Rama Madhavan	Vijaya		For Review	Migrated to new template
17.0	12-May-23	Beniyel S	Balu N	Srikanth M	For approval	Baselined
17.1	19-Jan-24	Balu, Beniyel, Vijaya	Srikanth M	Srikanth M	For Review	Policy is updated – Migration from ISO 27001:2013 to ISO 27001:2022, Updated all sections, added Sections Web filtering, Information Deletion, Configuration Managment, Data Masking, Data Leakage Prevention ,Threat Modeling etc.
18.0	23-Feb-24	Balu, Beniyel, Vijaya	Srikanth M	Srikanth M	For approval	Approved and Baselined
18.1	6-May-25	Balu Nair	Vijaya		Year Review	Migrated to a new Template
19.0	14-May-25	Balu Nair	Vijaya	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com