



# Information Security and Data Privacy Apex Manual



TRIANZ INTERNAL

[trianz.com](http://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

<b>1. SCOPE</b>	<b>5</b>
<b>2. NORMATIVE REFERENCE</b>	<b>7</b>
<b>3. DEFINITIONS/ABBREVIATIONS/ACRONYMS</b>	<b>7</b>
<b>4. CONTEXT OF ORGANIZATION</b>	<b>8</b>
4.1 Understanding the organization and its context	11
4.2 Understanding the needs and expectations of interested parties	12
4.3 Determining the scope of the Information Security and Privacy management system	17
4.4 Information Security & Privacy Management System	19
<b>5. LEADERSHIP</b>	<b>22</b>
5.1 Leadership and commitment	22
5.2 Policy	22
5.3 Organizational roles, responsibilities and authorities	23
<b>6. PLANNING</b>	<b>23</b>
6.1 Actions to address risks and opportunities	23
6.1.1 General	23
6.1.2 Information security and Privacy risk assessment	25
6.1.3 Information security risk treatment	25
6.1.4 Information security and Privacy objectives and planning to achieve them	26
6.1.5 Review of Information Security and Privacy Management System	26
6.2 Planning for changes-	26
<b>REFER TO SYSTEM AND SOFTWARE CHANGE MANAGEMENT PROCEDURE</b>	<b>27</b>
<b>7. SUPPORT</b>	<b>27</b>
7.1 Resource	27
7.2 Competence	28

7.3 Awareness	28
7.4 Communication	29
7.5 Documented information	30
7.5.1 General	30
7.5.2 Creating and updating	30
7.5.3 Control of Documented information	30
<b>8. OPERATION</b>	<b>32</b>
8.1 Operational planning and control	32
8.2 Information security and Privacy risk assessment	32
8.3 Information security and Privacy risk treatment	33
<b>9. PERFORMANCE EVALUATIONS</b>	<b>33</b>
9.1 Monitoring, measurement, analysis and evaluation	33
9.2 Internal Audit	35
9.2.1 General	35
9.2.2 Internal Audit Program	35
9.3 Joint Controller	37
9.4 Management review	37
<b>10. IMPROVEMENT</b>	<b>38</b>
10.1 Nonconformity and Corrective Action	38
10.2 Continual Improvement	39
<b>11. ISO CONTROL MAPPING(S)</b>	<b>40</b>

## 1. Scope

The purpose of this ISMS Manual is to provide an outline of the Information Security Management System implemented at Trianz, which complies with the requirements of ISO 27001:2022 and ISO 27701:2019 Standards.

Internally the manual is used to help all the Associates to understand the management system and refer various processes that must be met and maintained to ensure customer satisfaction and continual improvement

Externally the manual is used to introduce our Management System to our customers and auditors. The manual is also used to familiarize them with the controls that have been implemented and to assure them that the integrity of the Management System called "Blue Book" is maintained

**Note:** Our Management System is called as "Blue Book"

### Scope of ISO 27001:2022 Certification

ISMS Apex Manual is applicable for all Trianz associates, all Trianz establishments at all onshore and offshore locations.

#### Bangalore

Software Development, Testing services, Maintenance and Support services for customized applications along with Support functions

#### Concierto platform: -

The Information Security Management System that covers the requirements, design, development, testing, deployment, release, support and enhancements of Concierto SaaS platform enabled by associated corporate functions.

#### Hyderabad

Software Development, Testing services, Maintenance and Support services for customized applications along with Support functions

**Chennai**

Software Development, Testing services, Maintenance and Support services for customized applications along with Support functions

**TCI- Virginia**

Software Development, Testing services, Maintenance and Support services for customized applications along with Support functions

**Scope of ISO 27701: 2019 Certification**

ISMS Apex Manual is applicable for all Trianz associates, all Trianz establishments at all onshore and offshore locations.

**Bangalore**

Software Development, Testing services, Maintenance and Support services for customized applications along with Support functions

**Hyderabad**

Software Development, Testing services, Maintenance and Support services for customized applications along with Support functions

**Chennai**

Software Development, Testing services, Maintenance and Support services for customized applications along with Support functions

**TCI- Virginia**

Software Development, Testing services, Maintenance and Support services for customized applications along with Support functions

## Information Security Policy and Objectives

### Information Security Policy

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

Data Protection & Privacy Policy

Please refer to Data Privacy and Protection Policy Document

### Information Security & Privacy Objectives:

Information Security and Privacy objectives are to be defined at each function and at each level that relates to risk assessment which is tracked at regular intervals. MR will be discussing the objectives.

Refer Information Security and Privacy Objectives

## 2. Normative Reference

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

## 3. Definitions/Abbreviations/Acronyms

Acronym/Abbreviation/Word	Expansion/Definition
---------------------------	----------------------

<b>BCP</b>	Business Continuity Plan
<b>CIO</b>	Chief Information Officer
<b>CEO</b>	Chief Executive officer
<b>CISO</b>	Chief Information Security Officer
<b>CMT</b>	Crisis Management Team
<b>CRO</b>	Chief Recovery Officer
<b>ISMS</b>	Information Security Management Systems
<b>ISO</b>	International Organization for Standardization
<b>ISAC</b>	Information Security Assurance Council
<b>ITSM</b>	Information Technology Security Manager
<b>NDA</b>	Non-Disclosure Agreement
<b>PIMS</b>	Privacy Information Management System
<b>SOA</b>	Statement of Applicability
<b>TMR</b>	Top Management Review
<b>Top Management</b>	VPs, President and CEO

[Refer Appendix A ISMS Definitions](#)

## 4. Context of Organization

### Security Context

**Purpose:** Trianz is a Business Advisory and Technology Services company having its offices in 3 countries. Trianz offers integrated portfolio of services such as Custom Application Development, Application Maintenance, IT Service Management, Packaged Application, Testing, Remote Infrastructure Maintenance, Monitoring services and Cloud consulting services. Trianz leverages its extensive global infrastructure and network of offices to provide holistic, multi-service delivery in key industry verticals including high tech, insurance, financial services, retail, life sciences, public sector, healthcare, and logistics industries.

Our overall strategic mission is to provide our clients with:

A Secure environment and best practice that conforms to ISO 27001:2022, , ISO 27701:2019 , ISO 9001:2015 and ISO 20000-1:2018.

- Drive execution of strategic initiatives and deliver measurable business impact as envisioned by Sr. Management.
- Business continuity, so ensuring the availability of data and to continue business operations with minimal impact in case of any disruptions.
- Appropriate information security measures to protect the confidentiality of information we retain and provide
- Assurance that our own outsourced providers operate with integrity, professionalism and have appropriate information security measures in place.
- Supporting and enhancing the client IT infrastructure with cloud service offering to provide scalability elasticity along with security to meet growing business demands.

Below are the external and internal issues that are relevant to Trianz purpose, in order to achieve the intended outcomes of its Information Security and Privacy Management System.

**External Issues:**

- Legal and regulatory
- Power and Connectivity
- High expectation (state of the art technology) of client
- Location
- Competition
- Economic pressures
- Increased Regulation and Compliance
- Supply chain disruption
- Competitive pressure
- Technology advancement
- Product Demos to Compliance

**Internal Issues:**

- Information systems
- Organization's culture
- Organization structure
- Roles and responsibilities within the organization
- Availability of reliable and skilled manpower
- Contractual agreements with customers
- SLAs with customers
- Values of internal stakeholders
- Human resource capabilities
- Standard working procedures and guidelines
- Policy and Procedure Updation in alignment with Trianz Products
- SIEM -Managed Threat Detection and response
- Information Security and Privacy Risk Assessment for Third Parties initiated
- Critical associates falling sick
- VAPT Assessments
- Training session for Concierto
- Relationship with investors

Trianz ISMS shall encompass all the services mentioned below:

## Technology Services Portfolio:

We bring digital visions to life with end-to-end tech capabilities



1

### 4.1 Understanding the organization and its context

Trianz started in the Silicon Valley in 2001, we now cater to several Fortune 1000 companies across different industry verticals and have a presence across the Silicon Valley, Washington DC Metro, New York, Bengaluru, Chennai, Hyderabad,

Trianz offers services in technology and functional industry. The services include Big data, Information management & Data Warehouse, Business Intelligence & Analytics, Enterprise Mobility, Remote Infrastructure Management, Enterprise Content & Portals, Custom Application Development, Information Security, Enterprise Software, IT service management, Independent Verification & Validation, Sales CRM, Customer Service CRM and Cloud consulting Services.

Acceliant is a healthcare division of Trianz. It provides integrated eClinical Trial Data Management suite developed to handle large end-to-end clinical trials.

Trianz provides services across high-tech, insurance, financial services, retail, life sciences, and public sector, healthcare, and logistics industries with clients from Fortune 1000 to startup companies worldwide.

## 4.2 Understanding the needs and expectations of interested parties

At Trianz the following needs and expectations were identified by interested parties:

- a) Interested parties that are relevant to the information security management system include: The Management team, Trianz customers, Trianz IS team, HR team, Admin team, Learning and Support and maintenance team. Etc.

Interested Party	Expectations	Addressed by	Responsibility
<b>Management</b>	<p>Ensure C, I, A and P of the Information assets,</p> <p>Ensure transparency in operations,</p> <p>Ensure customer IS needs are meet,</p> <p>BCP strategies are made and maintained.</p>	<p>1. Management addresses the Information Security Management through various interested parties inputs and also the direction for Implementing ISMS</p> <p>2. ISDPA shall address implementation of ISMS with the help of Direction from Management and other Interested Parties Inputs</p>	<p>1.CIO and CISO</p> <p>2. ISDPA</p>
<b>HR , Learning</b>	<p>Ensure C,I A and P of the Human</p>	<p>1. HR and Training ensures compliance to</p>	<p>1. Global HR Head</p> <p>2. ISDPA</p>

	<p>resource assets, To ensure Personal records of Employee &amp; NDA's are maintained, Ensure Salary information, Training records, Leave records, Appraisal Documents are made and maintained. To ensure completion of mandatory courses with respect to Information security and Privacy, also to support in scaling the competence level of resources.</p>	<p>People's Controls as per ISO 27001:2022</p> <p>2.ISDPA Ensures the implementation of HR and Learning compliance to ISO 27001:2022</p>	
<b>IS Operations</b>	<p>Ensure C, I , A and P of the Infrastructure assets.</p>	<p>Ensure Technical Controls, and applicable Organizational and</p>	<p>1.CIO and CISO and IS Team 2. ISDPA Team</p>

		<p>Physical Controls compliance as per ISO 27001:2022</p> <p>2.ISDPA Ensures the implementation of IS Operations compliance to ISO 27001:2022</p>	
<b>Employees</b>	Adherence to ISMS Policies and Procedures	<p>Ensure complying with Organization defined Information Security Policies and Procedures</p> <p>2.ISDPA Ensures the implementation of Employees compliance to ISO 27001:2022</p>	<p>1. Employees 2. ISDPA Team</p>
<b>Contract Employees</b>	Comply with information security policies and procedures and contractual requirements	<p>Ensure complying with Organization defined Information Security Policies and Procedures</p>	<p>1. Contract Employees 2. ISDPA Team</p>

- b) The requirements of these interested parties relevant to information security are given below:

External Interested Parties	Expectations	Addressed by	Responsibility
<b>Customers/ Clients</b>	<p>Specify the ISMS and PIMS Requirements in MSA</p> <p>Conduct Third Party Audits</p>	<p>ISDPA team ensures Compliance to ISMS/PIMS Requirements as per MSA (Contract Obligations Tracker)</p> <p>Ensuring compliance to feedback from Third party audits as applicable</p>	CIO / CISO, Trianz ISDPA and IS team
<b>Vendors</b>	<p>Meeting compliance to the standards such as ISO 27001:2013 and ISO 27701:2019</p> <p>In addition, ISO 27017:2015 and ISO 27018:19(as applicable)</p> <p>Third party audit (right to audit)</p> <p>And other applicable agreements such as NDA and DPA</p>	<p>Purchase team</p> <p>Ensuring Vendors compliance to ISMS Requirements</p> <p>ISDPA team ensuring vendors compliance to ISMS requirements as applicable</p>	Purchase Team ISDPA Team
<b>Trainers/External Faculty</b>	Meeting compliance to the standards such as	Professional Development team Ensuring	Professional Development Team

External Interested Parties	Expectations	Addressed by	Responsibility
	ISO 27001:2013 and ISO 27701:2019 In addition, ISO 27017:2015 and ISO 27018:19 (as applicable)	Trainers compliance to ISMS Requirements ISDPA team ensuring vendors compliance to ISMS requirements	ISDPA Team
<b>Government agencies/regulators</b>	Government Agencies/ Regulators Publish the and release the applicable information security/business continuity laws and regulations,	ISDPA team ensuring the compliance to necessary and applicable laws and regulations	ISDPA Team
<b>Utility organizations(auditing bodies)</b>	Auditing the Organization to ensure Organizations compliance to the standards such as ISO 27001:2013, 27017:2015, 27018:2019, 27701:2019	ISDPA team ensuring the compliance to necessary and applicable laws and regulations	ISDPA Team
<b>Authorities(Legal, All Constitutional bodies(as applicable)</b>	Provide inputs to the organization to safeguard and Comply with information	ISDPA team ensuring the compliance to necessary and	ISDPA Team

External Interested Parties	Expectations	Addressed by	Responsibility
	<p>security/business continuity laws and regulations,</p> <p>Also provides a legal framework for critical information infrastructure in India. For example, in Section 43A of the IT Act, Indian businesses and organizations must have “reasonable security practices and procedures” to protect sensitive information from being compromised, damaged, exposed, or misused</p>	<p>applicable laws and regulations</p>	

The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

### 4.3 Determining the scope of the Information Security and Privacy management system

Trianz offers services in technology and functional industry. The services include Big data, Information management & Data Warehouse, Business Intelligence & Analytics, Enterprise Mobility, Remote Infrastructure Management, Enterprise Content & Portals, Custom Application Development, Information Security, Enterprise Software, IT service

management, Independent Verification & Validation, Sales CRM, Customer Service CRM and Cloud consulting Services.

Security Infrastructure is established at Trianz to achieve information security organizational goals addressing the following:

- Personnel security: Is maintained to reduce risks of human error, theft, fraud or misuse of facilities and to ensure that all the employees are aware of Information Security threats and concerns.
- Employee conduct: All employees are expected to conduct in line with the ISMS policy of Trianz
- Information classification: Trianz has classified its data into various types depending on the sensitivity such as Public, Internal, Confidential, Restricted.
- Data labeling: All assets of the Trianz should be labeled.
- Data transmission: Is securely transferred and protected with latest technologies.
- Data encryption: Data is protected with Passwords and access permissions. • .
- Access control: Strict Controls are followed; Entry to the premises is for authorized personnel only. (Access control list shall be maintained by Admin and IT team)
- Firewall rule: Periodic Monitoring and necessary precautions are being followed by Firewall Microsoft Essential.
- Network application: Required controls are being in place.
- Logging of Systems: System Logs are generated and regularly monitored.
- Information Asset management: Is done by IS Team.
- Physical security: Is maintained and controlled at all secured and unsecured areas
- Security maintenance: Information security is periodically monitored and controlled. Refer to IS Operation Process
- Cloud Infra access: All customers cloud infrastructure access is controlled through secure SSO

- Asset Risk Register :- Asset Risk Register is reviewed once in a year
- Note:** All goals shall be reviewed once in a year (in the form of objectives).

## 4.4 Information Security & Privacy Management System

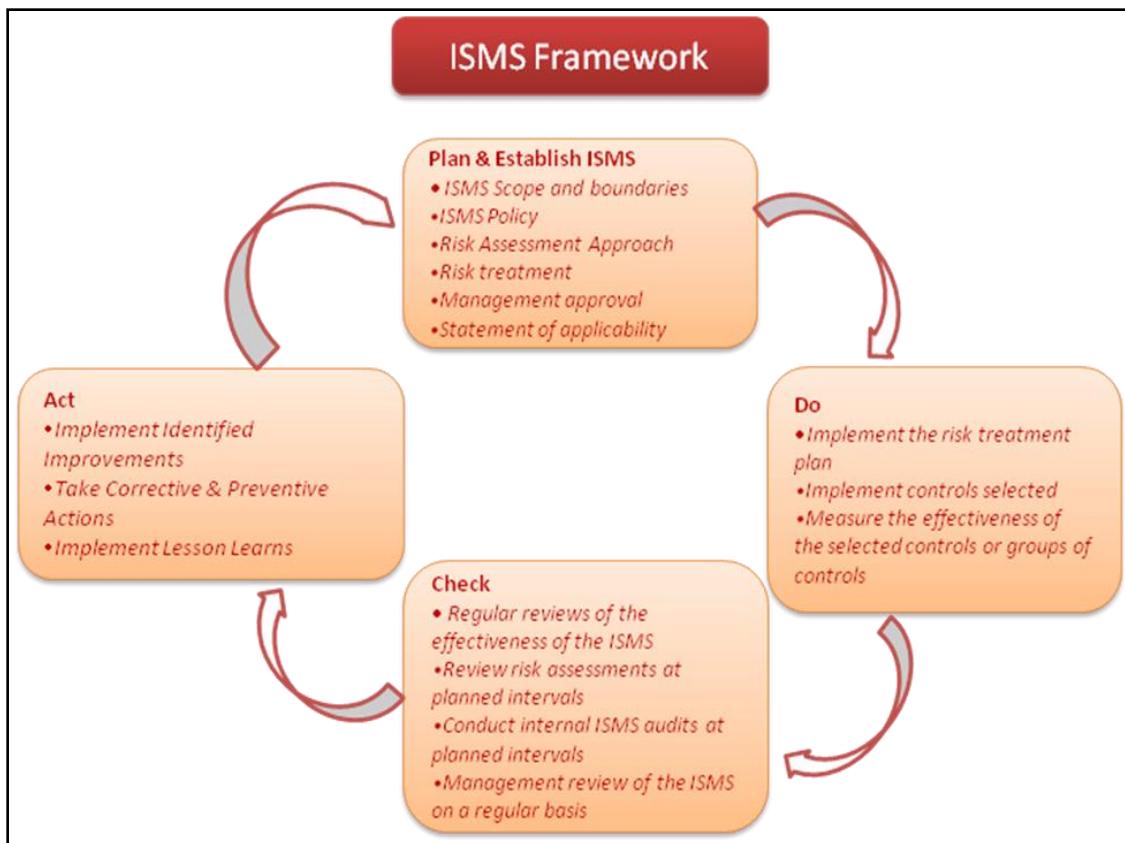
The organization shall establish, implement maintain and continually improve an Information Security Management System including the processing needed and their interactions in accordance with the requirements of the document.

The organization shall establish, implement, maintain, and continually improve an information security management system, in accordance with the requirements of this International Standard

At Trianz,ISDPA team is responsible for developing, implementing, maintaining and continually improving the Information Security and Privacy within the context of the organization's overall business activities.

Information Security and Privacy frame work shown below describes the frame work of Information Security and Privacy adopted in accomplishing this goal. The following block diagram gives the view of the Organization. (PDCA Model)

The Information Security and Privacy framework described at Trianz follows a continuous cycle of activities: Plan, Do, Check, and Act and ensures the Information Security controls are implemented with interaction of the processes defined in ISMS- Organizational Controls, People Controls, Technological Controls and Physical Controls with the necessary Interested Parties involved.



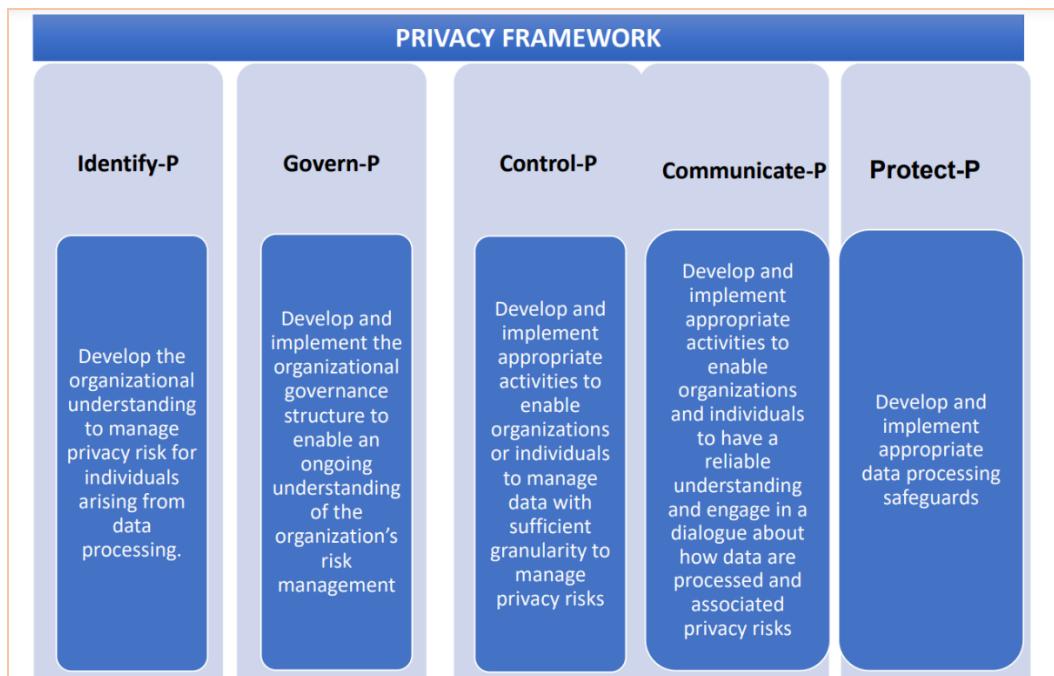
ISDPA team ensures

The five Privacy Framework Functions are defined as follows:

- **Identify-P** – Develop the organizational understanding to manage privacy risk for individuals arising from data processing. The activities in the Identify-P Function are foundational for effective use of the Privacy Framework. Inventorying the circumstances under which data are processed, understanding the privacy interests of individuals directly or indirectly served or affected by an organization, and conducting risk assessments enable an organization to understand the business environment in which it is operating and identify and prioritize privacy risks.
- **Govern-P** – Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk. The Govern-P Function is similarly foundational, but focuses on organizational-level activities such as establishing organizational privacy values and policies, identifying legal/regulatory

requirements, and understanding organizational risk tolerance that enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs

- **Control-P** – Develop and implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage privacy risks. The Control-P Function considers data processing management from the standpoint of both organizations and individuals.
- **Communicate-P** – Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks. The Communicate-P Function recognizes that both organizations and individuals may need to know how data are processed in order to manage privacy risk effectively.
- **Protect-P** – Develop and implement appropriate data processing safeguards. The Protect-P Function covers data protection to prevent cybersecurity-related privacy events, the overlap between privacy and cybersecurity risk management



## 5. Leadership

### 5.1 Leadership and commitment

- Top Management is committed to establish, implement, operate, monitor, review, maintain and improve the Information Security and Privacy by:
  - Establishing an ISMS policy & Data Privacy and Protection Policy
  - Ensuring that Information Security and Privacy objectives and plans are established
  - Establishing roles and responsibilities for information security
  - Communicating to the organization the importance of meeting Information Security and Privacy objectives and conforming to the information security & Data Privacy and Protection policy, its responsibilities under the law and the need for continual improvement
  - Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the Information Security and Privacy
  - Deciding the criteria for accepting risks and for acceptable risk levels
  - Ensuring that internal Information Security and Privacy audits are conducted
- Conducting management reviews of the Information Security and Privacy
- CISO will present the status and effectiveness of Information Security and Privacy to CIO at least once in year
- The review will include assessing opportunities for improvement and the need for changes to the Information Security and Privacy System policies and procedures

[Refer Management Review Procedure in Common Support Folder](#)

### 5.2 Policy

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

Please refer to Data Protection and Privacy Policy document for "Data Protection and Privacy Policy "

Objectives, Scope and Security Context are identified in the policy

[Refer Information Security Policy](#)

### **5.3 Organizational roles, responsibilities and authorities**

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.

Trianz Management has established the Infosec and Data Privacy Organization's roles and responsibilities and authorities to ensure the success and sustainability of the enterprise wide Information security deployment and management including the communication to all stakeholders in the organization.

ISAC consists of representatives from various corporate functions and business units and is headed by CIO/CISO

ISDPA function is responsible for implementation, maintenance, operation and improvement of ISMS at Trianz.

[Refer ISAC Roles and Responsibilities](#)

## **6. Planning**

### **6.1 Actions to address risks and opportunities**

#### **6.1.1 General**

When planning for the information security management system, the organization shall consider the issues and determine the risks and opportunities that need to be addressed to:

Trianz ensures the information security management system can achieve its intended outcomes such as C, I,A and P of the Information assets, Ensure transparency in operations

Ensure customer Information security needs are meet, BCP strategies are made and maintained.

Proven, or reduce, undesired effects such as breach of Information security requirements by any employee or process, loss of data or integrity of the data or systems; and

To achieve continual improvement. The Trianz shall plan: Feedback from stakeholders, customer feedback, Internal Audit results, accomplishment of objectives are reviewed from time to time.

The risk mitigations are handled to counter the negative effect. This is determined through risk assessment Action to address these risks assessment methodology and opportunities; and Information Security and Privacy effective evaluation to be developed.

Refer Risk & Opportunity Management Procedure

Refer Business continuity and disaster procedure

### **Evaluate risk:**

All the risks are analyzed and evaluated for applying possible controls from ISO 27001:2022, and ISO 27701:2019 recommended and any additional if required. The business impacts are analyzed for each threat to information asset that might result in loss of confidentiality, integrity or availability.

The security failures are analyzed, taking into account the consequences of Assets the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities and impacts associated with these assets, and the controls currently implemented.

### 6.1.2 Information security and Privacy risk assessment

During risk assessment, the risk value of the asset is calculated as product of (Business Impact \* Probability of occurrence).

The "C", "I", "A" and "P" values are rated on a scale of 1, 3 and 9, and the business impact is calculated on scale of 1, 3 and 9, the probability of occurrence on a scale of 1, 3 and 9.

Asset identification is carried out for the assets, which contain information value in each department. Risk assessment methodology process is developed to identify a unified method of conducting the risk assessment.

The risk owners are to be identified in risk assessment. All the threats for an Asset are identified and all the applicable threats are documented

Vulnerabilities are identified for each information asset followed by associated threats

Risk assessment methodology will be used to perform risk assessment on all identified assets

Refer Risk and Opportunity Management Procedure in ISMS Procedure folder

### 6.1.3 Information security risk treatment

Based on the Risk Assessment, Delivery, Corporate Functions/Support Functions shall develop Risk treatment plan, CIO/CISO has authority to recognize and accept the risk where the management feels that no risk treatment plan is feasible/ cost effective and hence not being implemented

The risk treatment plan is implemented in order to achieve the identified control objectives, which includes consideration for funding and allocation of roles and responsibilities.

For more information, Refer Risk and Assessment and Opportunity Management Procedure in ISMS Procedure folder

#### **6.1.4 Information security and Privacy objectives and planning to achieve them**

Top Management shall establish and direct ISDPA team to ensure information security objectives at relevant functions and levels are defined in line with the information security policy. These Objectives are measurable ensuring infosec requirements are met considering the results from risk assessment and risk treatment history.

Information Security Objectives shall be documented detailing the plan to achieve the objectives, responsibilities, resources required and evaluation mechanism etc.

ISDPA ensures communication to all relevant stake holders and reviewing and monitoring the Information Security Objectives.

#### **6.1.5 Review of Information Security and Privacy Management System**

Information Security and Privacy Management System consists of Policies, Procedures, Guidelines, Templates and Checklists. All the Policies, Procedures, Guidelines, Templates and Checklist shall be reviewed at least once a year to ensure suitability, effectiveness, and alignment with existing business environment. All revised ISMS process assets shall be approved by CIO/CISO before releasing to ISMS in Blue Book.

Information Security and Privacy Objectives:

Information Security and Privacy objectives are to be defined at each function and level and are to be connected with risk assessment which is tracked at regular intervals. MR will be discussing the objectives.

Refer Information Security and Privacy Objectives

### **6.2 Planning for changes-**

Trianz shall plan for changes in Information Security Management System. They shall be recorded in a controlled manner and the changes are planned, evaluated, authorized, prioritized, tested, implemented, and documented.

## Refer to System and Software Change Management Procedure

# 7. Support

## 7.1 Resource

At Trianz management will determine and provide the resources needed to:

- Ensure that right information is available only to the right people at the right time.
- Protect Information Assets
- Protect critical information from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional
- The confidentiality, integrity and availability of critical information, is ensured at all times
- Initiate corrective and preventive actions on reported, actual or suspected security incidents by the designated Chief Information Security Officer after investigation
- Ensure that awareness programs on Information Security are available to all employees, wherever applicable and also to third parties viz. Subcontractors, Vendors, Consultants etc.
- Ensure compliance to all legal and contractual requirements – Master Service Agreement between client and Trianz, agreements between vendor/supplier and Trianz, Non-disclosure agreements with client, suppliers and employees, Data Processing Agreements with clients and vendors (wherever applicable).
- Review the policy at periodic intervals – to check for its effectiveness, changes in technology, legal and contractual requirements and business efficiency
- Ensure that all employees adhere to the information security policies and procedures to take appropriate action in case of its violation are established.
- Increase confidence of business partners in exchanging critical information with Trianz

- Enhance Trianz's reputation as a reliable partner for executing key initiatives

## 7.2 Competence

ISAC group ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

At Trianz, ISAC group will also ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

Providing competent training

Based on the feedback, evaluating the effectiveness of the training provided and actions taken

Maintaining records of education, training, skills, experience and qualifications

At Trianz, ISAC group will also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

Refer Professional Development Procedure

Refer ISMS Objectives

## 7.3 Awareness

Trianz will ensure that all personnel assigned responsibilities defined in the ISMS are competent to perform the required tasks.

This is ensured by several processes including the following:

- Providing competent training and certification to deployed personnel
- The organization's learning and development will maintain records of education, training, skills, experience & qualification of all personnel pertaining to the training held related to Information Security and Privacy Management System.

- Trianz will also ensure that all concerned personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the Information Security and Privacy objectives, by means of various user education activities
- Learning & Development will plan, conduct, measure effectiveness of information security related trainings.

[Refer Professional Development Procedure](#)

## 7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

- a) on what to communicate;
- b) when to communicate;
- c) with whom to communicate;
- d) how to communicate

The Trianz communicates the need of information security and Privacy management system and Specific training is given to the employees at the time of induction. It team will be orienting on Information Security and Privacy policies. ISMS policy is published intranet portal.

Communicates on Information Security and Privacy policies at the induction program.

Communication is done among the employees as part of internal review meetings.

Communicate the Information Security and Privacy polices on Bluebook

Specific needs of customer are communicated to the project team and internal audit team.

[Refer Project Management planning process](#)

[Refer Professional Development Procedure](#)

## 7.5 Documented information

### 7.5.1 General

There are 2 types of documents at a high level

Blue Book Documents – Policies, Manuals, Group Manuals, Procedures, Guidelines, Checklists and Templates

Documents related to Projects and Corporate Functions

- a) Documents prepared related to project during project execution such as PM Workbooks, SRS, Design, Test Plan, Test Cases etc.,
- b) Documents related to Corporate Functions (InfoSec and Compliance, HR, Recruitment, L&D, Admin, Purchase and IS Operations)

### 7.5.2 Creating and updating

At Trianz Records are identified in each procedure at the end. All records are identified in the procedures are maintained by the process owners for the purpose of ISMS.

These records are used as source of evidence for implementing the ISMS and also for checking the effectiveness from time to time.

Internal audit team will verify these records and compare with the procedures to check the adequacy. Most of the records are maintained in the soft copy format or in the hard copy format.

In case of copies the backup process will ensure that they are available and the access control policy will ensure its Confidentiality.

### 7.5.3 Control of Documented information

- It is ensured that all the Bluebook documents are controlled through proper reviews and approvals
- Changes to the controlled documents are reviewed and approved by appropriate authority before release for use

- All evolving documents are version controlled and only the relevant approved versions of documents are available for use
- All documents are available online for reference by authorized personnel at a common database
- All controlled documents are identified through unique Release Identification (Release ID)
- All documents of external origin are suitably identified and made available only for intended purposes and users
- Any Blue Book process document used for the purpose of proposals or customer's offsite usage or any other distribution outside the premises of the organization will be considered as uncontrolled and change control will not be applicable for the same once it leaves the premises of Trianz
- Blue Book Process Artifacts, which are no longer in use, are moved to obsolete folder
- All records identified by the projects and corporate functions are generated and stored as records specific to projects and corporate functions
- All records related to projects and corporate functions are retained until 7 years (as applicable) from the date of creation of the record. The records older than 7 years will be disposed off at the discretion of the PM / Corporate Function Manager

[Refer Documented Information Procedure](#)

[Refer Configuration Management Process](#)

- All ISMS documents and records will be protected and controlled as per Documented Information Procedure which is available in Common Support Process Folder in Blue Book.

[Refer Documented Information Procedure.](#)

## 8. Operation

### 8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements is as follows

All information security and privacy risk points are identified and a risk treatment plan is formulated that identifies the appropriate management action, responsibilities and priorities for managing information security risks.

- Control objectives are achieved through implementation of controls selected.
- Awareness programs are conducted across Trianz to bring awareness.
- Operations are managed with respect to ISMS resource.
- Procedures will be in place to enable prompt detection of and response to security incidents.
- Manage operations of Information Security and Privacy
- Manage resources for the Information Security and Privacy
- Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents.
- Implement training and awareness program

Refer Information Security and Privacy Objectives

### 8.2 Information security and Privacy risk assessment

Risk assessment methodology will be used to perform risk assessment on all identified assets

Refer Risk and Opportunity Management Procedure in ISMS Procedure folder

Based on the Risk Assessment, ISAC will develop Risk treatment plan, CIO/CISO has authority to recognize and accept the risk where the management feels that no risk treatment plan is feasible/ cost effective and hence not being implemented

## 8.3 Information security and Privacy risk treatment

At Trianz all information risk points are identified and a risk treatment plan is formulated that identifies the appropriate management action, responsibilities and priorities for managing information security risks.

The risk treatment plan is implemented in order to achieve the identified control objectives, which includes consideration for funding and allocation of roles and responsibilities.

The documented treatment plan, residual risk, monitoring documents pertain to ISMS are retailed for internal Information Security reviews.

Refer Risk and Opportunity Management Procedure in ISMS Procedure folder

## 9. Performance evaluations

### 9.1 Monitoring, measurement, analysis and evaluation

At Trianz following activities are done to ensure proper review of Information Security and Privacy

#### Review of Risk Assessment

Review of risk assessment will be performed once in a year by CISO, additional risk assessments will be performed based on business and operational environment requirements

Upon review of a risk assessment, the ISAC makes a determination as to whether the identified risk is acceptable, or requires treatment using the criteria for accepting risks as defined in the risk assessment methodology

Refer Risk and Opportunity Management Procedure in ISMS Procedure folder

#### Vulnerability Assessment and Penetration Testing (VA/PT)

Vulnerability Assessment and Penetration Testing will be conducted on a periodic basis at least once a year by IS team. Frequency of testing will be increased if required by the business or the operating environment

Vulnerability Assessment and Penetration Testing will be conducted to gain more comprehensive assessment of the overall Network security posture

## Compliance

Trianz will comply with the following requirements:

- Legal Requirements (Statutory and Regulatory Requirements)
- Contractual Requirements
- Compliance with Blue Book information security policies and procedures
- Technical compliance review

### Legal Requirements

Representatives from corporate functions (Finance, HR, Admin , Infosec and Data Privacy Assurance and IT) form a team called 'Compliance team'

Compliance team will identify legal requirements related to their function

Legal requirements will be reviewed and updated annually once and also on event driven basis whenever any ACTs are amended or new ACTs come into force

The compliance team is responsible for maintaining and complying with the identified legal requirements

Refer 'Legal Requirements' in Compliance folder of Organization Publications

### Contractual Requirements

Concerned Project Managers and Delivery Center Heads are responsible for complying with contractual requirements, identified in their contracts with customers

### Compliance with Information Security Policies and Procedures

Information Security and Privacy Policies will be implemented to maintain the confidentiality, integrity and availability of the information processing facilities maintained by Trianz

Compliance with Information Security and Privacy Policies at Trianz is mandatory for all the employees. These policies will apply to all personnel,

outside consultants, contractors, temporary employees, clients or third parties accessing Trianz information assets

If an individual violates the provisions in Information Security Policies, either by negligence or intent, Trianz reserves the right to take disciplinary action including dismissal, legal prosecution, claims for compensatory damages etc.

Any exceptions to the policy will be approved by the Information Security Assurance Council (ISAC), which may decide to seek higher-level management authorization

Compliance with policies and procedures will be reviewed by CISO, once in year

### **Technical Compliance Review**

Auditor will Information systems are regularly checked for compliance with security implementation procedure like updating virus and security patches

## **9.2 Internal Audit**

### **9.2.1 General**

The Organization shall conduct Internal Audits at planned intervals to provide information on whether the information Security management System

- a) conforms to
  - 1) The organizations own requirements for its ISMS
  - 2) The requirements of the document
- b) is effectively implemented and maintained

### **9.2.2 Internal Audit Program**

The organization shall plan establish implement and maintain an audit programme, including the frequency methods responsibilities planning requirements and reporting

When establishing the internal audit program the organization shall consider the importance of the processes concerned and the results of previous audits

The Organization shall

Define the audit criteria and scope of for each audit

Select auditors and conduct audits that ensure objectivity and impartiality of the audit process

Ensure that the results of the audits are reported to the relevant management

Documented Information shall be available as evidence of the implementation of the audit program and the audit results

Audit is a systematic and independent examination of various activities intended to determine compliance with Blue Book and the applicable standards

An audit is planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits

The audit criteria, scope, frequency and methods are defined

The selection of auditors and conduct of audits will ensure objectivity and impartiality of the audit process. Auditors will not audit their own work

#### **Refer to Internal and External Audit Procedure**

### 9.3 Joint Controller

Please refer to Joint Controller and Information Sharing Framework For Trianz group of companies

### 9.4 Management review

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

- a) the status of actions from previous management reviews;
- b) changes in external and internal issues that are relevant to the information security management system;
- c) Changes in Needs and expectations of the Interested parties that are relevant to ISMS
- d) feedback on the information security performance, including trends in
  - 1) nonconformities and corrective actions;
  - 2) monitoring and measurement results;
  - 3) audit results.
  - 4) fulfilment of information security objectives;
- e) feedback from interested parties; f) results of risk assessment and status of risk treatment plan;
- and g) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system. The organization shall retain documented information as evidence of the results of management review

Top management shall review the Trianz information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

ISMS effectiveness is reviewed for its effectiveness from time to time, typically the risk assessment review is carried out once in six months and the

Management review is carried out once in a year. This would include the inputs coming from Security audits, interested parties, customer inputs, incidents and ISMS objectives trends.

The effectiveness of the controls is measured from various sources such as, IS incidents, breaches, objectives tracking.

- a) At Trianz reviews are done to assess the level of residual risk and acceptable risk, taking into account changes to:
  - o The organization connected changes such as change in processes, IT infrastructure etc.
  - o Technology adopted for service delivery.
  - o Business objectives and processes required for service delivery.
  - o Identified threats during ISMS operation at Trianz over period to check the effectiveness of implementation.
  - o External events, such as changes to the legal or regulatory environment and changes in social climate, contractual obligations connected with information security are monitored from time to time. Any need for conducting the reassessment of risks is evaluated in the management review.

The management review shall include consideration of:

- o The status of actions from previous management reviews;
- o Changes in external and internal issues that are relevant to the information security management system;
- o Feedback on the information security performance, including trends in:
- o Nonconformities and corrective actions, monitoring and measurement results and audit results

## 10. Improvement

### 10.1 Nonconformity and Corrective Action

At Trianz ISAC team will take action to eliminate the cause of nonconformities associated with the implementation and operation of the ISMS in order to

prevent recurrence. The documented procedures for corrective action will define requirements for:

- Identifying nonconformities of the implementation and/or operation of the ISMS
- Determining the causes of nonconformities and potential impacts associated and damage to the ISMS.
- Evaluating the need for actions to ensure that nonconformities are not repeated.
- Determining and implementing the corrective action needed
- Recording results of action taken
- Reviewing of corrective action taken.
- Potential NC's are identified and eliminate them from occurrence,

## 10.2 Continual Improvement

- The organization has defined and documented Information Security policy and Objectives. The ISMS Measurement Framework is designed keeping the policy and objectives in view.
- Top Management Review will be conducted to assess the ISMS implementation and effectiveness in the organization and to come up with required corrective or preventive actions in the areas where improvements are identified for continual improvement
- Internal Audits, customer audits and certification body audits are conducted periodically to check adherence to Blue Book and also for continual improvement of Blue Book
- Corrective and Preventive actions are taken to prevent the recurrence and occurrence of the nonconformities
- Apply the lessons learnt from the security experiences of other organizations, such as clients, vendors, suppliers, partners and advisories.
- We encourage employees to initiate process improvement by submitting 'process change request' to TPIG

Infosec team evaluates process change requests and implements in Blue Book if found feasible

[Refer Continual Improvement Process](#)

[Refer Corrective and Preventive Action process](#)

[Refer Management Review Procedure](#)

### **Corrective Action**

The organization takes action to eliminate the causes of nonconformities in order to prevent recurrence.

After identifying the nonconformities RCA is conducted to identify root causes and corrective actions. The identified corrective actions are implemented and the effectiveness is verified.

If any corrective action requires a process change, the appropriate Blue Book process artifact will be modified.

[Refer Corrective and Preventive Action Process in Common Support Process folder](#)

### **Preventive Action**

The organization takes action to eliminate the causes of potential non-conformities in order to prevent their occurrence.

The priority of preventive action is determined by the ISAC based upon the inputs from security reviews and concerned departments.

The implemented preventive actions are verified for effectiveness.

[Refer Corrective and Preventive Action Process in Common Support Process folder](#)

## **II. ISO Control Mapping(s)**

<b>Category of Control</b>	<b>ISO 27001:2022 Control</b>	<b>Document Name as per ISO 27001:2022</b>
----------------------------	-------------------------------	--

All Controls	All Controls	Information Security and Data Privacy Apex Manual
--------------	--------------	---

## Document Control

<b>Owner:</b>	CISO	<b>Release ID:</b>	IAM-POL-0006
---------------	------	--------------------	--------------

**For Trianz Process Improvement Group (TPIG) Purpose Only**

## Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
<b>0.00</b>	27-Apr-07	Jyotessh Nair			NA	Draft
<b>1.00</b>	07-May-07	Jyotessh Nair			ISO 27001:2013 Stage 1 Audit from BVQI	Incorporated the Feedback of the Stage 1 Audit and Baseline.
<b>1.01</b>	07-May-08	Bharateesha B R			Internal ISMS Review/Audit	Revised the policies and procedures of all sub domains, their control objectives and controls including the sections addressing the ISO-27001 standard requirements

<b>1.02</b>	04-Aug-09	Bharateesha B R			2 <sup>nd</sup> Surveillance audit	<ul style="list-style-type: none"> <li>• Included terms/definitions/acronyms/abbreviations in section 2.5</li> <li>• Included a ISMS strategy and methodology to establish and maintain ISMS at Section 4</li> <li>• Added few more reasons for having ISMS at Trianz under sub section "Purpose" at Section 5.1</li> <li>• Included Section on ISWG at 5.2.6</li> </ul> <p>Removed all sections pertaining to policies and procedures as they are being addressed in the SOA</p>
<b>2.00</b>	06-Aug-09	Balu Nair			Approval for Baseline	Baselined
<b>2.01</b>	08-Oct-09	Bharateesha B R			Acquisition of Blue Ally by Trianz	<ul style="list-style-type: none"> <li>• Changed the scope of ISMS</li> <li>• Re arranged the sections to bring in alignment with PDCA framework</li> </ul>
<b>3.00</b>	08-Oct-09	Balu Nair			Approved for Baseline	Approved

<b>3.01</b>	17-May-10	Bharateesha B R			Annual Review	<ul style="list-style-type: none"> <li>• Formatting Changes</li> <li>• Changed the release IDs as per the Trianz Blue Book</li> <li>• Provided clarity on Information Security policy review frequency</li> <li>Provided hyperlinks to appendices`</li> </ul>
<b>4.00</b>	18-May-10	Bharateesha B R			Approval for Baseline	Baselined
<b>4.01</b>	31-Dec-10	Balu Nair			QMG Review	Formatting done
<b>5.00</b>	04-Jan-10	Balu Nair			Reviewed and approved	Baselined
<b>5.01</b>	24-May-11	Srilakshmi			QMG Review	Modified ReleaseID in cover page and header
<b>6.00</b>	24-May-11	Srilakshmi			Reviewed and approved	Baselined
<b>6.01</b>	27-Jun-11	Balu Nair			Input from SAI	<ul style="list-style-type: none"> <li>• Added Scope of certification</li> <li>Remove ISMC from section 5.2 Management commitment</li> </ul>

<b>7.00</b>	29-June-11	G. D. Venkateswar Reddy			Reviewed the above changes and approved.	Baselined
<b>7.01</b>	3-Aug-11	Sudharsana			QMG review	<ul style="list-style-type: none"> <li>Replace Owner with Management Representative in place of CIO</li> <li>In Document Classification Scheme, "Retention period is 3 Years" row is removed</li> </ul>
<b>8.00</b>	3-Aug-11	Sudharsana			Request for baseline	Approved and Baselined
<b>9.00</b>	08-May-12	Srilakshmi			QMG Review	<ul style="list-style-type: none"> <li>Modified the template format as per the standard format</li> <li>Included sections <ul style="list-style-type: none"> <li>– Overview of organization, organization chart, SOA sections</li> </ul> </li> <li>Modified Introduction, control of documents and records, internal audits, ISMS improvements section</li> <li>Modified PDCA</li> </ul>

						<ul style="list-style-type: none"> <li>Removed Scope diagram and ISMC related process</li> </ul> <p>Aligned all sections for clarity</p>
<b>10.00</b>	08-Nov-12	Balu Nair			Standardization of Blue Book Process Assets	<ul style="list-style-type: none"> <li>Modified the template format</li> </ul> <p>Changed the Logo</p>
<b>11.00</b>	29-Apr-13	Srilakshmi			PCR raised by GD	Modified section 4.4 Information security policy and objectives from CIO to CEO for review of policy
<b>12.00</b>	17-Apr-14	Srilakshmi			Review of Information Security Policy	<ul style="list-style-type: none"> <li>No change in policy statement</li> <li>Modified Logo</li> </ul> <p>Modified section 1.1 Organization overview and service portfolio as per changes in the organization</p>
<b>13.00</b>	16-May-15	Sudharsana			Updated based on new version ISO 27001:2013	<ul style="list-style-type: none"> <li>Updated ISMS Scope</li> <li>Added Technical compliance review</li> </ul> <p>Reviewed and approved</p>
<b>14.00</b>	26-May-15	Sudharsana			Updated based on new	Reviewed and baseline

					version ISO 27001:2013	
<b>14.01</b>	16-Oct-16	Balu Nair			Addition of Cloud services as scope of Certification.	<ul style="list-style-type: none"> <li>Apex Manual is modified to include Cloud services</li> </ul> <p>Cloud Services added under Scope of ISO 27001:2013 Certification</p>
<b>15.00</b>	07-Dec-16	Balu Nair			Approved by CISO	Baselined
<b>15.1</b>	29-Apr-19	Balu Nair	Joshy VM			<ul style="list-style-type: none"> <li>Information classification modified</li> </ul> <p>Trianz logo modified</p>
<b>16.0</b>	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
<b>16.2</b>	06-May-20	Balu Nair	Phani Krishna			<ul style="list-style-type: none"> <li>Added CISO as additional approval authority</li> </ul> <p>Added Apex manual applicability to all the locations under Scope of ISO 27001:2013 Certification</p>
<b>17.0</b>	14-May-20	Balu Nair	Phani Krishna	Vivek Sambasivam	For Approval	Approved and Baselined

<b>17.1</b>	9-Feb-21	Balu Nair	Phani Krishna		Review	<ul style="list-style-type: none"> <li>• Updated the information classification</li> <li>• Modified Scope of ISO 27001:2013 Certification as stated in the current "Certificate" for all the three locations</li> <li>• Changed responsibility</li> <li>• of CISO to Delivery and Corporate Function/Support Functions under section 6.1.3</li> </ul>
<b>18.0</b>	12-Feb-21	Balu Nair	Phani Krishna	Phani Krishna	Approved for Baseline	Approved and Baseline
<b>18.1</b>	25-Mar-2022	Vijaya	Balu Nair	Siva N	For review	<ul style="list-style-type: none"> <li>• Scope of Certifications added to all locations – 27017:2015, 27018:2019, 27701:2019</li> <li>• And ISMS Manual updated as Information Security and Privacy Manual</li> </ul>

<b>19.0</b>	25-Mar-2022	Vijaya	Balu	Siva	Approved for Baseline	Approved and Baseline
<b>18.1</b>	25-Mar-2022	Vijaya	Balu Nair	Siva N	For review	<ul style="list-style-type: none"> <li>• Scope of Certifications added to all locations – 27017:2015, 27018:2019, 27701:2019</li> <li>• And ISMS Manual updated as Information Security and Privacy Manual</li> </ul>
<b>19.0</b>	25-Mar-2022	Vijaya	Balu	Siva	Approved for Baseline	Approved and Baseline
<b>19.1</b>	06-05-2022	Divya	Balu Nair	Siva N	For review	Scope of Certifications is updated to all locations and updated the risk rating
<b>20.0</b>	11-05-2022	Divya	Balu Nair	Siva N	Approved for Baseline	Approved and Baseline
<b>20.1</b>	15-July-2022	Divya	Balu N		For Review	Updated Footer from Trianz Confidential to Trianz Internal
21.0	15-July-2022	Divya	Balu N	Siva N	For Approval	<ul style="list-style-type: none"> <li>• Approved and Baseline</li> </ul>

21.1	10-Mar-2023	Beniyel S, Rama Madhavan	Balu N		For Review	Added Infosec Mandatory training in HR Learning .  Migrated to new template
22.0	09-May-2023	Beniyel S	Balu N	Srikant h M	For Approval	Approved and Baseline
22.1	15-Feb-2024	Vijaya, Balu	Srikanth		For Review	Section 4, 6, 7, 8, 9, 10 are updated in alignment to ISO 27001:2022
23.0	23-Feb-2024	Vijaya, Balu	Srikanth	Srikant h M	For Approval	Approved and Baseline
23.1	30-Apr-2025	Vijaya	Balu		For Review	Scope Section modified for current scope, Removed scope of California location, ISO 27017 and ISO 27018 Certifications
24.0	14-May-25	Vijaya	Balu	Srikant h M	For Approval	Approved and Baseline



## Contact Information

Name

Email

Phone

# Thank You

[infosec@trianz.com](mailto: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.