TRIANZ℠

INFORMATION SECURITY POLICY REVIEW CADENCE

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 document will detail the Control objective-wise Review Cadence of InformationSecurity Policies and Procedures

2. Policy Review Cadence Schedule

#	Control	Control Objective	Policy	Review Cadence	Triggers for Policy Review
1	5.1 Management direction for information security	Objective: To provide managementdirection and support for information security in accordance with business requirements andrelevant laws and regulations.	Information SecurityPolicy Apex Manual	Annual	• Internal Audit • External Audit • Client Audit • Client Visit feedback • Management feedback • Changes due to Technological and Environmental Factors • Compliance to anynew regulatory standards • Security Incidents • BCP Triggers • Learnings from, VA findings
2	6.1 Internal organization	Objective: To establish a management framework to initiate and control the implementation andoperation of information security within the organization	ISAC Roles and Responsibilities Access Control Policy	Annual	
3	6.2 Mobile devices and teleworking	Objective: ensure the security ofteleworking and use of mobile devices.	Policy on the useMobile computing and Communication Facilities BYOD Policy	Bi-Annual	
4	7.1 Prior to Employment	Objective: To ensure that employees and contractors understand their responsibilitiesand are suitable for the roles for which they are considered.	Background Verification Policy	Annual	
5	7.2 During Employment	Objective: To ensure that employees and contractors are aware of and fulfil their informationsecurity responsibilities.	Professional Development Policy Policy for DisciplinaryAction	Annual	
6	7.3 Terminationand changeof employm	Objective: To protect the organization's interests as part ofthe process of changing or terminating employment.	Asset Management Policy Employee Exit ProcessEmployee	Annual	

	ent		Transition Process		
7	8.1 Responsibilityfor assets	Objective: To identify organizational assets and defineappropriate protection responsibilities.	Asset management Policy Acceptable UsagePolicy	Annual	
8	8.2 Information classification	Objective: To ensure that information receives an appropriatelevel of protection in accordance with its importance to the organization.	Media Handling Policy	Bi-Annual	
	8.3 Media handling	Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	Access control Policy Password Policy	Bi-Annual	

#	Control	Control Objective	Policy	Review Cadence	Triggers for Policy Review
10	9.1 Business requirements of access control	Objective: To limit access toinformation and information processing facilities.	Access control Policy Password Policy	Bi-Annual	
11	9.2 User access management	Objective: To ensure authorizeduser access and to prevent unauthorized access to systems and services.	Access control Policy Password Policy	Bi-Annual	
12	9.3 User responsibilities	Objective: To make users accountable for safeguarding theirauthentication information	Access control Policy Password Policy	Bi-Annual	• Internal Audit • External Audit • Client Audit • Client Visit feedback • Management feedback • Changes due
13	9.4 System and applicationaccess control	Objective: To prevent unauthorizedaccess to systems and applications.	Access control Policy Password Policy	B-Annual	
14	10.1 Cryptographiccontrols	Objective: To ensure proper andeffective use of cryptography to protect the confidentiality, authenticity and/or integrity ofinformation.	Policy on the use of Cryptographic Controls	Annual	

15	11.1 Secure areas	Objective: To prevent unauthorizedphysical access, damage and interference to the organization's information and information processing facilities	Physical Access Controland Environmental Security Policy	Annual	to Technological and Environmental Factors • Compliance to any new regulatory standards • Security Incidents • BCP Triggers Learnings from, VA findings
16	11.2 Equipment	Objective: To prevent loss, damage, theft or compromise ofassets and interruption to the organization's operations.	Acceptable usage policy	Annual	
17	12.1 Operational procedures and responsibilities	Objective: To ensure correct and secure operations of information processing facilities.	System and software change management policy	Annual	
18	12.2 Protection from malware	Objective: To ensure that information and information processing facilities are protected against malware.	Antivirus Malwarepolicy	Annual	
19	12.3 Backup	Objective: To protect against lossof data	Backup and Restoration Policy Data Retention and Secure disposal policyMedia Handling Policy Password Protection Policy Personal Data Protection and privacyPolicy	Annual	
20	12.4 Logging and monitoring	Objective: To record events andgenerate evidence	Information security logging and monitoring policy	Annual	
21	12.5 Control of operational software	Objective: To ensure the integrity ofoperational systems	Patch Management Policy	Bi-Annual	

#	Control	Control Objective	Policy	Review Cadence	Triggers for Policy Review
22	12.6 Technical vulnerability management	Objective: To prevent exploitationof technical vulnerabilities.	Vulnerability Management Policy	Bi-Annual	

23	12.7 Information systems audit considerations	Objective: To minimize the impactof audit activities on operational systems.	Information SystemAudit trial Management Procedure	Annual	• Internal Audit • External Audit • Client Audit • Client Visit feedback • Management feedback • Changes due to Technological and Environmental Factors • Compliance to anynew regulatory standards • Security Incidents • BCP Triggers Learnings from, VA findings
24	13.1 Network security management	Objective: To ensure the protectionof information in networks and its supporting information processing facilities.	Email Policy Network Security Management Procedure	Bi-Annual	
25	13.2 Information transfer	Objective: To maintain the security of information transferred within an organization and with any externalentity	Email Policy Network Security Management Procedure	Bi-Annual	
26	14.1 Security requirements of information systems	Objective: To ensure that information security is an integral part of information systems acrossthe entire lifecycle. This also includes the requirements for information systems which provide services over public networks	Secure SDLC PolicyApplication security policy Group Manual ISOperations	Annual	
27	14.2 Securityin developmentand support processes	Objective: To ensure that information security is designedand implemented within the development lifecycle of information systems.	Secure SDLC PolicyApplication security policy	Annual	
28	14.3 Test data	Objective: To ensure the protectionof data used for testing	Personal data protection and privacypolicy Information SecurityPolicy	Annual	
29	15.1 Information security in supplier relationships	Objective: To ensure protection ofthe organization's assets that is accessible by suppliers	Supplier Securitypolicy	Annual	
30	15.2 Supplier service delivery management	Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements	Supplier Securitypolicy	Annual	

31	16.1 Managementof information security incidents and improvements	Objective: To ensure a consistentand effective approach to the management of information security incidents, including communication on security events and weaknesses.	Information security incident management policy	Annual	
32	17.1 Information security continuity	Objective: Information security continuity should be embedded inthe organization's business continuity management systems	Business continuitypolicy	Bi-Annual	

#	Control	Control Objective	Policy	Review Cadence	Triggers for Policy Review
33	17.2 Redundancies	Objective: To ensure availability ofinformation processing facilities.	Business continuitypolicy	Bi-Annual	• Internal Audit • External Audit • Client Audit • Client Visit feedback • Management feedback • Changes due to Technological and Environmental Factors • Compliance to anynew regulatory standards • Security Incidents • BCP Triggers
34	18.1 Compliance with legal and contractual requirements	Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related toinformation security and of any security requirements.	Intellectual propertyrights policy Risk Management Policy	Annual	
			Information SecurityPolicy	Bi-Annual	
35	18.2 Informationsecurity reviews	Objective: To ensure that information security is implementedand operated in accordance with the organizational policies and procedures	Information SecurityPolicy	Bi-Annual	

					Learnings from, VA findings

3. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Organizational Controls	5.1 Policies for information security Control Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to, and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Information Security Policy Review Cadence
Organizational Controls	5.36 Compliance with policies, rules and standards for information security Control Compliance with the organization's information security policy, topicspecific policies, rules and standards shall be regularly reviewed.	Information Security Policy Review Cadence

Document Control

Owner:	CISO	**Release ID:**	ISPR_POL_059

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	16-May-2020	Vijaya Rajeswari	Ganesh Arunachala	-	Client Risk Assessment inputs	Initial Draft
1.00	20th May2020	Ganesh Arunachala	Phani Krishna	Vivek Sambasivam	Modification to provide policy wise review cadence	For approval
1.1	1-Feb-2021	Divya G	Vijaya R	Phani	For Review	Modified as per the new template
2.00	1-Feb-2021	Divya G	Vijaya R	Phani	For Approval	Approved and Baselined
2.1	8-Nov-2021	Divya G	Vijaya R	Siva N	For Review	Modified as per the new template
3.00	8-Nov-2021	Divya G	Vijaya R	Siva N	For Approval	Approved and Baselined
3.00	3-Jan-2022	Divya G	Vijaya R	Siva N	For Review	Reviewed and no changes
3.00	07-Apr-2023	Shivateja	Vijaya R	Srikanth M	For Review	Reviewed and no changes
3.1	12-May-2023	Rama Madhavan	Vijaya		For Review	Migrated to new template
4.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined

4.1	15-feb-24	Shalini	Vijaya	Srikanth M	For Review	Mapped with ISO 27001, 2022 control 5.1 and 5.36
5.0	23-feb-24	Shalini	Vijaya	Srikanth M	For Approval	Approved and Baselined
5.1	28-May-25	Kruti	Vijaya		For Review	Migrated to new template.
6.0	29-May-25	Kruti	Vijaya	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com