TRIANZ℠

Physical Access Control and Environmental 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. Purpose

The purpose of this policy is to define the requirements for protecting Trianz information and technology resources from physical and environmental threats and reduce the risk of loss, theft, damage, or unauthorized access to those resources or interference with Trianz operations.

2. Scope

This policy applies to all parties operating within the Trianz's network environment or utilizing Information Resources. It covers the data networks, LAN servers and personal computers (stand-alone or network-enabled), located at Trianz offices and company production related locations, where these systems are under the jurisdiction and/or ownership of Trianz, and any personal computers, laptops, mobile device and or servers authorized to access the Trianz's data networks. No employee is exempt from this policy

3. Policy

3.1 Physical Security Perimeter

The physical layout of Trianz's information processing facilities will be segregated into perimeter zones. Each zone will have a higher level of access restrictions and access authorization requirements.

The perimeter zones could include the following:

- Public zone and reception zone. (Limited restrictions – area under overall surveillance)
- Office zone (Limited access – registration with reception required. Area under overall surveillance)
- Restricted access zone (Limited access. Access logged. Escorted access for visitors. Area under surveillance. Eg: Secure bays)
- Highly Restricted access zone - Specifically authorized personnel only. (Highly restricted access. Logged access. Specific authorization required for employee and visitor access. Area under surveillance. Eg: server room).

3.2 Physical Entry Access

All employees, contractors, consultants, and other visitors entering Trianz premises are required to carry Trianz approved identification badges.

Physical access to Trianz information systems facilities is to be restricted to authorized persons only. Authorization to enter restricted facilities is to be granted only when there is a business or technical reason for the person to enter the premises.

All logs shall be retained for a minimum of three years.

Secure areas (restricted zones) must be protected with a combination of access control devices
(For example, physical barriers, and intrusion alarms), access-logging equipment (such as card key systems and security cameras) to ensure that only authorized personnel are allowed access.

Access to sensitive or critical information processing facilities outside normal working hours must be specifically authorized and logged.

Employees should be asked to declare their belongings like laptop computer, mobile phones, etc. before entering restricted premises. The security must verify the declarations to prevent removal of Trianz's property from the building.

3.3 Visitor Management System

Visitors must be provided supervised and controlled access to secure areas, which includes:

- Sign-in a Visitors Log that is retained and reviewed. It must be signed when first entering Trianz premises and then entering any sensitive controlled area. The logbook should record the visitor's name, company, and purpose for visiting, time of entrance, time of departure, and date.
- Wearing of a visitor badge to inform personnel that a non- associate is in the area. Visitors must produce picture identification to obtain the badge. Those visitors not wearing badges should be challenged for identification.
- Escort of the visitor by Trianz personnel or by an individual with a current Trianz company badge while the visitor is in the building.

- Visitors should be asked to declare their belongings like laptop computer, mobile phones, etc. before entering restricted premises. The security must verify the declarations to prevent removal of Trianz's property from the building.

3.4 CCTV

Surveillance Camera shall be installed, and monitoring shall be performed but limited to areas perceived as high risk unless otherwise required.

3.5 Securing Offices, Telecommunications Closets, Data Center and Facilities

Data center, equipment rooms, and telecommunications closets must be protected from unauthorized or unnecessary access.

All data centers, equipment rooms, and telecommunications closets must be locked when unattended.

Network devices such as routers, switches, and hubs must be placed in restricted access zones that provide protection from unauthorized or unnecessary access.

All source media for operating system software, applications, backup tapes/devices and license keys must be clearly labeled and stored in a software library in a restricted access zone – with access for authorized personnel only.

Adequate intrusion detection controls (e.g. burglar alarm, motion detector etc.), and safety devices (e.g. fire alarm, smoke detector, close circuit televisions etc.) must be placed in all office locations, switch rooms and data centers. Data centers shall be protected by appropriate air conditioning and very early smoke detection systems.

Support functions and equipment's such as photocopiers and fax machines should be protected from unauthorized access.

No combustible or hazardous materials should not be allowed in restricted zones.

3.6 Power Supplies

Equipment must be protected from power failures and electrical anomalies.

Electrical supply must conform to the manufacturer's specifications for each piece of equipment.

Critical equipment must be supported by uninterruptible power supply (UPS). A backup power generating equipment should also be in place where possible.

Power supply backup equipment including UPS's, backup generators etc. must be subject to regular maintenance and testing.

3.7 Equipment Maintenance

Equipment shall be maintained in accordance with manufacturers' recommendations, to ensure its availability and integrity. All faults (or suspected faults) shall be logged in the current Incident Management System and all changes shall be logged in the current Change Management System.

3.8 Wireless access points

Wireless access points should be installed at a high level to make them less exposed and more secure from theft or tampering.

3.9 Clear Desk and Clear Screen policy

Clear desk and clear screen guidelines must be written and implemented at each Trianz office location. These must include the following:

- Paper and computer media must be stored in suitable locked cabinets, offices and/or other forms of security furniture when not in use, especially outside working hours.
- Sensitive or critical business information should be locked away (ideally in a fire resistant safe or cabinet) when not required, especially when the office is vacated and unlocked.
- Personal computers and computer terminals and printers are not to be left logged on when unattended and should be protected by password protected screen savers with a minimum 15-minute time delays.
- Sensitive or classified information, when printed, is to be cleared from printers immediately.

3.10 Protection against Environmental Factors

The IT management shall ensure that sufficient measures are put in place and maintained for protection against environmental factors (e.g. fire, dust, power, excessive heat and humidity). Refer BCP policy.

4. Monitoring and Reporting

Reporting metrics and documentation templates are described in the approved and published Trianz Physical and Environmental Security Procedure. These reports shall be used to evaluate the effectiveness of the Physical and environmental security controls. These reports shall be made available to Information Security and Internal Audit upon request.

5. Compliance

Implementation and enforcement of this policy is ultimately the responsibility of IT Operations and Admin Team. Information Security and Internal Audit Team will conduct periodic audits to ensure compliance to with the policy & Procedure without notice.

6. Exception(s)

Exceptions to this policy requires formal written approval from the Information Security Assurance Team.

7. ISO Control Mapping(s)

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
7.0 Physical Controls	7.0 Physical Controls	Physical Access and Environmental Security Procedure
7.0 Physical Controls	7.2 Physical entry	Physical Access and Environmental Security Procedure

7.0 Physical Controls	7.3 Securing offices, rooms and facilities	Physical Access and Environmental Security Procedure
7.0 Physical Controls	7.4 Physical security monitoring	Physical Access and Environmental Security Procedure
7.0 Physical Controls	7.5 Protecting against physical and environmental threats	Physical Access and Environmental Security Procedure
7.0 Physical Controls	7.6 Working in secure areas	Physical Access and Environmental Security Procedure
7.0 Physical Controls	7.8 Equipment siting and protection	Physical Access and Environmental Security Procedure
7.0 Physical Controls	7.9 Security of assets off premises	Physical Access and Environmental Security Procedure
7.0 Physical Controls	7.11 Supporting utilities	Physical Access and Environmental Security Procedure
7.0 Physical Controls	7.12 Cabling security	Physical Access and Environmental Security Procedure

Document Control

Owner:	CISO	**Release ID:**	PACES-POL-0042

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Introduction/ Reason for Change	Change Description
0.01	2-Jun-17	Roshni M	Kamadev	Ganesh A	Creation of Policy	Initial Draft
1.00	14-May-18	Kamadev	Ganesh A	Ganesh A	Approved by Ganesh	Baselined
1.1	10-May-20	Balu Nair	Phani Krishna	Phani Krishna	Annual review	Template changed
2.0	14-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
2.1	21-Jan-21	Divya G	Phani Krishna	Phani Krishna	For review	Updated with new information classification
3.0	21-Jan-21	Divya G	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
3.0	11-Jan-22	Divya G	Divya	NA	For review	Reviewed and no changes

3.1	11-Jan-23	Sanjana, Shalini Kumari	Vijaya,Balu	Srikanth Mantena	For review	Log retention period is defined for three years New template change
4.0	11-Jan-23	Sanjana	Srikanth Mantena	Srikanth Mantena	For approval	Approved and baselined
4.0	28-Mar-23	Sanjana	Vijaya		For review	Reviewed with no changes
4.0	23-Feb-24	Shalini	Vijaya		For Review	Reviewed and ISO checked
4.1	06-May-25	Balu Nair	Vijaya		Yearly Review	Migrated to a new Template
5.0	14-May-25	Balu Nair	Vijaya	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com