TRIANZ℠

Physical Access and Environmental Security Procedure

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

Physical access control and environmental security are one of the first lines of defense in any organization to protect its information assets by creating several physical barriers around business, processes and information processing facilities. Controls should be put in place to monitor and control physical access to the organizational premises. In a well-designed security system, there are at least 4 layers of physical access security.

- Environmental design
- Mechanical and electronic access control
- Intrusion detection
- Video monitoring

The goal is to convince potential attackers that the likely cost of attack exceeds the value of making the attack.

2. Objective(s)

The objective of this framework is to establish physical access controls to protect Trianz's information assets from unauthorized physical access, damage and interference.

3. Scope

This framework is applicable to information assets, all users (employees, consultants, contractors and third party) who have access to Trianz's information processing systems and to the premises of across Trianz.

4. Entry Criteria and Inputs:

- Physical Access control Monitoring
- Utility Services Maintenance
- Zone Identifications
- Access card and Identity card allocation

5. Process Description (Procedure)

5.1 Zones Identification

At Trianz, we have identified the following zones based on the security category of information assets within the specific area under consideration.

Zone 1: Those areas open to public, company employees, third party service providers, contractors. Areas include receptions, discussion rooms, cafeteria, lounge, company premises,

Zone 2: Those areas not open to public but open to company staff, third party service providers, and contractors. Areas include company working areas, conference rooms, employee cabins, pantry, boardrooms, and training rooms.

Zone 3: Those areas open to only those with authorized access. This is applicable to all irrespective of whether the person is a company staff, third party service provider, and contractor. Areas include server rooms, equipment rooms, file cabinets, AC control rooms, UPS Rooms. In order to identify the zones, board displaying the zone number will be displayed visibly in the zone entry point, in every case.

5.2 Perimeter Security

5.2.1 Zone 1:

Office Building

- Office building will be protected by having security guards 24/7 at various entry points
- Any employee having a visitor will accompany him/her by registering his name and employee ID at the office building

Reception

- Reception will have security guards 24/7 monitoring the movement of people, materials
- Reception area will not have any signs of display of information which is either confidential or internal use only.

5.2.2 Loading and Unloading Areas:

- Access to Loading and Unloading areas will be provided to only those who have been authorized by Trianz. This includes employees, third party service providers, contractors.
- Under no circumstances, visitors will be allowed to access the loading and unloading areas.
- Loading and unloading areas will be designed to prevent delivery personnel having access to other parts of the building.
- Avoid use of main access for movement of heavy equipment's and/or heavy Cargo, utilize loading bay facility where available.
- Hydrogen sensors shall be deployed in areas where Lead-acid batteries are used discussion Rooms.
- Discussion rooms will be designed to prevent the visitor from having access to information which is not for public consumption
- Discussion rooms will be located far from Zone 2 and Zone 3 to the extent possible.
- Discussion rooms will not have any form of display of information which is Trianz confidential or internal use only.

5.2.3 Zone 2

Cabins:

- Cabin walls will be sound proof to the extent possible to ensure confidentiality.
- Placing of Information processing equipment will be made in such a way so as to prevent disclosure of information to unauthorized sources
- Tinted glasses will be used to prevent easy access to confidential information.
- Cabins will be protected by locking the doors when in unattended state to prevent unauthorized physical access Work Areas, Conference Rooms, Training Rooms, Boardrooms
- No visitor will be allowed to enter into working areas or conference rooms or training rooms unless there is a business need and in such cases, the visitor will be always accompanied by the concerned employee
- Workstations will be designed to prevent disclosure of confidential

information.

- Conference, training rooms, and board rooms will be provided with locker facility to prevent theft of any equipment when in unattended state.
- No form of display of confidential information will be allowed in conference and training rooms and working areas.
- Conference rooms and training room walls will be sound proof to the extent possible, tinted glasses will be used to prevent leakage of confidential information to unauthorized resources.
- Display boards, projectors, will be located to prevent disclosure of confidential information to unauthorized resources.
- Record of trainings, meetings held at training and conference rooms will be maintained

5.2.4 Zone 3:

Server Rooms

- Server rooms will be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized resources
- Server rooms will be protected to prevent theft of equipment.
- Access to server rooms will be registered.
- Server rooms will be fitted with tinted glasses to prevent leakage of information to unauthorized resources
- Server rooms will be protected by locking the doors when in unattended state to prevent unauthorized physical access
- Exterior facing windows/door forced open and breakage alarm should be present for all areas.
- ZONE-3 area on Ground floor and areas susceptible for flooding shall be deployed with fluid or water sensor.

5.3 Physical Access Controls

5.3.1 Access Cards:

Physical access will be controlled using access control system which will be electronic in nature. Physical access will be provided based on the verification of access information provided at the entry points. The following information will be verified to provide the required access

- Access card number
- Employee name
- Employee ID
- Access cards will be issued to only employees and contractors.

5.3.2 Identity Cards:

- The following type of identity cards will be issued to employees, contractors, third party service providers, and visitors.
- Employee Identity Card: Employees
- Temporary Identity Card: Employees, Contractors, Third Party Service providers. Please refer Admin process for details on the procedure for issuing temporary ID cards
- Visitor Card: Visitors
- Physical access will be provided based on the display of both access and identity cards.
- Access during non-working hours: Any employee and / or contractor/ or third party service provider, who need access on any working day beyond 2100 Hours, will sign in a "Late Exit" register, provided with the security guard at reception, while leaving.
- Access during non-working days: Access during non-working days will be restricted to only employees, contractors. A separate register will be maintained for all employees and / or contractors visiting office on any off working hours (including week-ends and holidays), which should be filled in by the designated employee and / or contractors.
- Access rights to access cards
- Access to third party service providers will be allowed based on business need and approvals from relevant authority.
- Refer Admin process at Trianz QMS for more information on issuance of identity and access cards.

5.3.3 Visitor Register

Visitor register will be maintained to track the movement of visitors including third party service providers

5.3.4 Access to Server Rooms

Access to server rooms will be restricted to authorized individuals and enabled on the access control system. Access register will be maintained to track the access to server rooms.

5.3.5 Protection Against Unauthorized Access

- Admin team shall regularly monitor access points, such as doors, gates, and entryways, through security cameras, physical security systems, access logs and security alerts from all the systems logs.
- The Admin Team shall perform physical access review of access logs, in case of any discrepancy in the access logs, CCTV logs will be reviewed by the Admin team.
- Trianz shall implement a security alarm system wherever required.
- Trianz shall train the security personnel to recognize and identify suspicious or unauthorized individuals attempting to gain physical access and shall maintain visitor register and vendor register as such and shall ensure vendors and visitors shall be allowed only after verification of appropriate approval form the respective business / department heads, verifying government-issued identification (ID), such as an official identity document, driver's license, passport, etc,. Security Personnels shall update all the required details in the visitor and vendor register.
- In cases of unauthorized entry or breach, security personnel must respond immediately by approaching the intruder, verifying their identity, and taking necessary actions to secure the area.
- If an unauthorized entry is confirmed or if the situation escalates, the security supervisor should be notified to assess the severity and decide on further actions.
- Notify relevant parties, such as the facility management and law enforcement if required. Prepare incident reports for documentation and legal purposes.
- If necessary, physically restrain and escort unauthorized individuals out of the premises in a safe and controlled manner.
- Gather evidence, including security camera footage and eyewitness statements, to support any investigations or legal actions. Review

access points, entry procedures, and security measures to identify weaknesses and implement enhancements to prevent future unauthorized access.

Investigate and analyze security alerts to distinguish between false positives and actual unauthorized access attempts.

5.3.5 Data Center Personnel Training:

- Professional Development and the IS team shall develop, conduct training and awareness programs for personnels who have access to the data center.
- The training materials shall be reviewed and approved by the Professional Development in conjunction with the IS team.
- Records shall be kept and tracked to identify and confirm the personnels who have access to the data center have finished the training on a timely basis and a test shall be conducted if required.
- Maintain a constant state of vigilance by regularly patrolling and monitoring access points to deter unauthorized access attempts.
- Maintain records of all unauthorized physical access incidents, actions taken, and outcomes for future reference and compliance purposes.
- Conduct a post-incident review to identify lessons learned and areas for improvement in the physical access security process.

5.4 Work Environment Regulation

- Personnel in zone 2 and zone 3 should only be aware of existence of activities within that area on a need to know basis
- Unsupervised working in zone 2 and 3 will be avoided both for safety reasons and to prevent opportunities for malicious activities
- Vacant areas in zone 2 and zone 3 will be physically locked and periodically checked wherever possible.
- Confidential Information will not be kept in any form on work desks unless required it is absolutely required to prevent leakage of information.
- All employees, contractors, third party service provider, and visitors will be required to wear, and display, the identity cards issued to them all the time while present in the Zone 2 and 3.

- No employee of Trianz is supposed to bring any media like Floppies, CDs, DVDs, USB Drives, Tapes, portable Hard Disks, personal laptops, video cameras, etc, to Trianz premises, without written permission from the head of Administration. The media can be deposited at reception, if brought by any employee. Any Media taken inside without declaration will be considered as serious policy violation. Users will be subjected to a random check to verify this. However, Video Cameras can be used in Zone 1 areas. Mobile cameras are permitted inside with a self-restrain that employees will not use them inside areas classified as Zone 3, any misuse of mobile camera usage will be considered a serious security violation
- If an employee wants to bring any information inside the organization, which is currently stored on his/her CD, floppy, USB drive or laptop etc., he or she will take a prior approval from the Head of Department and IT manager through IT service request and handover the device to the Front desk personnel in the reception area and inform the admin department. The admin department will arrange to provide access of the data to the user. Admin department will hand over the device to the Front desk person after the activity is over

5.5 Health and Safety Regulation

- Smoking is strictly prohibited at all zones except smoking areas identified under the office premises
- Combustible and hazardous materials are strictly prohibited and if there is a business need, the same will be stored at a safe distance from zone 2 and 3.
- Beverages, food and other eatables are expressly prohibited in zone 3. Zone 2 will also be subject to this restriction except in those circumstances where there is absolute business need. e.g: client visits, board meetings, and Pantry.
- Equipment which emits electromagnetic radiations are strictly prohibited
- Bursting of firecrackers is strictly prohibited at all zones unless authorized.
- Medical Kits will be kept at reception and with the admin team.

5.6 Emergency and Safety Services

Emergency and Safety services contact list will be kept with the admin department and be displayed at selected locations on the floor. The same will be reviewed and kept current by interacting with relevant authorities

5.7 Protection against external and environmental Threats

- Admin team shall identify and document the critical equipment's and their external and environmental Threats such as chances of flooding, earthquake, damage from wind, dust, and other natural disasters. Admin team shall assess the potential impact of these hazards.
- Trianz shall ensure that an adequate risk assessment for the probability of external and environmental Threats occurrence is conducted before selecting a location.
- In case of any external and environmental threats scenarios, Admin team shall implement protective measures such as elevating equipment above flood-prone areas, securing the glass windows / doors against wind damage by implementing toughened glasses, and sealing against dust infiltration.
- Admin team shall install surge protectors and backup power sources to safeguard against electrical issues during natural disasters.
- An emergency response plan, maintenance and monitoring shall be performed as applicable by the admin team.

5.7.1 Fire protection

- Smoke detectors will be located above the false ceilings at each floor. Manual call points will be provided in each floor to raise alarms manually in case of emergencies / disasters.
- Fire extinguishers will be provided in each floor and also within the office premises. Different types of fire extinguishers will be used to extinguish fires in different situations. For e.g. in the server rooms gas based fire extinguishers will be used.
- All fire exits will be prominently marked for easy visibility. The keys to the fire exit doors will be kept in a small glass box besides the fire exit, which can be broken and keys could be retrieved in emergency situations. Duplicate keys of the fire exit will be available on request,

from the Head of Administration. At all other times, the emergency exit will be kept locked.

- To keep a check on proper working of fire safety equipment's, a periodic check will be done within the expiry time specified by the manufacturer of the equipment.
- Fire drills will be carried out (once a year) so that an employee is aware of steps to be taken in case of fire. Smoke detectors will also be checked for their proper working when fire drills are carried out
- Emergency Power off switch will be provided to prevent cascading of fire into multiple floors

5.7.2 Lightning Protection

The building power supply and distribution is made through MCB's, which are mounted in metal box. All power points are safely grounded to the earthing-pits, by flat long copper plates inserted in the building wall.

5.7.3 Telecommunication Failure

- In case of PBX communication failure, another alternate phone will be provided to the Security Personnel.

5.7.4 Water supply Failure

- The office building owner will ensure that back up water supply is available in case of primary supply failure

5.7.5 Power Failure

- Information processing equipment will be protected from power failures and other electrical anomalies including voltage surges and spikes. Information assets will be protected from damage due to power failures. All the computers and related electronic devices will be connected to power supply from UPS.
- UPS will be checked regularly to ensure that they provide adequate power output. A maintenance plan, including periodic tests and servicing, will be followed for UPS equipment. Testing of utility services, backup systems and crisis response procedures shall be performed

by the Building Management / Admin team to ensure the preparedness and effectiveness.

- Backup Generator will be put into operation in case of failure of UPS.
- Critical areas (Data centers, hub rooms, server room etc.) shall have power redundancy like multiple powers feed, stand by UPS, DG set etc.
- The Admin team / Security Personnel shall regularly monitor the temperature and humidity of the Data center / Hub, / Switch room which shall be between 18 Celsius to 24 Celsius and in case of overheating, the security personnels shall inform the admin team, and necessary actions shall be taken to maintain the temperature and humidity inside the Data center / Hub / Switch room at the required level. The Temperature and Humidity readings shall be noted down either outside the respective rooms or in a separate registry. The Temperature and Humidity readings shall be monitored manually every two hours, and the readings will be updated in the respective sheet. The records shall be maintained for at least 3 to 6 months or for an appropriate duration. Post that period, the recordings shall be disposed through shredder by admin team.
- Admin team shall monitor and refill the fire extinguisher once a year. Before taking the fire extinguisher for refill, it shall be approved by the head of Admin team and gate pass shall be provided
- Periodic testing of the utility services shall be performed as per the Master Service agreement and utility services logs are maintained and reviewed. Utility services shall be periodically tested by the Building Management / Admin team as per the Contractual Agreements.
- Monitoring of utility services shall be performed by the Building Management and the Admin team, for identification of areas for improvement, update contact information, and adjust response plans as required.

5.7.6 Emergency Lighting:

Emergency Lighting Facility is available at specific locations on the floor.

5.7.7 Emergency Evacuation Procedure:

Introduction:

The objective of emergency evacuation procedures is to familiarize all members of the Emergency Response Team (ERT) with the emergency procedures in place to facilitate safe, orderly and timely evacuation when necessary.

- General Information:
- Emergency Exits:
- Emergency exits are provided on the floor closer to the staircase entries.
- Emergency Lighting:
- Emergency Lighting facility has been provided at selected locations on the floor to facilitate safe evacuation in the case of an emergency.

Air Conditioning:
The floor's air-conditioning system will shut down automatically on the declaration of an emergency

Fire Alarms:
Fire Alarms are provided at each floor to facilitate easy determination of fire.

Fire Extinguishers:
Fire extinguishers are kept at selected locations on the floor based on the location of critical information
processing facilities.

Emergency Response Team (ERT):
At Trianz, ERT consists of ERT Lead and his deputy assisted by number ERT members appointed for each section. ERT lead will report to the Building ERT head in regard to the implementation of building evacuation plan, coordination of building evacuations, and the proper maintenance of building fire safety equipment's. The standard working day at Trianz inclusive of lunch break is 9 hours. This may be worked between 8.00 a.m. till 6.00 p.m., Monday to Friday. Outside these times, or when it may be reasonably assumed that the members of ERT are not in company premises, the duty or security officer will assume the responsibilities of ERT.

ERT Lead Responsibilities:

- The ERT lead will be responsible for maintaining an up-to-date list of their ERT. He/She will also nominate a person for the position of Deputy Building Warden who will undertake their duties in their absence
- Arranging and co-coordinating evacuation exercise
- Accurately logging the performance of, and any problems encountered during exercises
- Conducting debriefing after practice evacuations
- Continually striving to improve the effectiveness of the plan
- Ensuring an update list of the names and location of workplaces of mobility impaired persons is kept on hearing the fire alarm sounding or on being advised of an emergency situation, the ERT Lead will immediately.
- Ensure the relevant emergency service has been called.
- Proceed to the fire indicator panel.
- Inform the affected Section using the PA system or runner and initiate a search or instigate designated actions.
- Reassure staff/students that the alarm / emergency is being investigated.

If a fire / or emergency has been found, the ERT Lead will

- Evacuate the Section immediately (if not already under way)
- Inform building ERT head / security of the situation
- Consider evacuation of entire premises
- Meet the emergency services, building ERT head /security on arrival and inform them of the situation, if no fire / emergency are found, the ERT head will
- Inform staff of the false alarm
- Meet the emergency service on arrival and inform them of the situation

Equipment's:

Good Quality Torch, emergency procedures documentation, Floor plan of the entire building identifying,

- Different sections of the floor

- Section ERT members
- Location of Fire Fighting equipment
- Location of Exits
- Fire Indicator Panel
- List of All on duty staff, where applicable

Deputy ERT Lead Responsibilities:

- The Deputy ERT lead will assume the duties and responsibilities of the ERT lead whenever the ERT Lead is absent from the premises
- The ERT Lead and the deputy ERT Lead will never be simultaneously absent from the building
- The deputy ERT Lead will have the same equipment as the ERT Lead.

ERT Members Responsibilities:

- ERT members will be appointed for the purpose of directing and controlling the emergency procedures as directed by the ERT Lead
- ERT members have the authority to evacuate their area of responsibility if they consider there is any danger to staff, students or visitors
- On activation of the fire alarm or emergency actions, ERT members may receive instructions from the ERT lead. On receipt of instructions, they will either.
- Direct section staff to reassure staff whilst at the same time preparing to evacuate; and / or Initiate a search or emergency procedures of their section
- If a fire or emergency situation is found the ERT member will.
- Inform the ERT Lead
- Evacuate the section. Direct people to the fire stairs and prevent them from using lifts.
- Attempt to extinguish the fire or control emergency situation having due regard to their own safety.

  - If the fire or emergency cannot be extinguished or controlled the ERT member will,
  - Inform the ERT Lead
  - Evacuate all section staff
  - Isolate the incident by closing all possible doors: then
  - Report to the ERT Lead and act on any instructions
  - Do not allow anyone to enter the fire-affected area
  - If no fire or emergency is found the ERT member will
  - Inform the ERT Lead
  - Reassure staff the situation is under control and to resume normal operations

ERT members familiarize themselves with the area they represent, Note all means of escape from their section. Be familiar with the operation of installed firefighting equipment

- Conduct staff roll calls at assembly points and report any absences to the ERT lead (if applicable)
- Raising the alarm, by operating manual break glass alarms, or by contacting the ERT lead
- When directed, guide occupants down the fire stairs to the assembly area
- Assisting mobility impaired people
- Operating first attack firefighting equipment (eg) fire extinguishers and hose reels, or instigating emergency procedures
- Searching a floor or area to ensure nobody has been left behind. This includes checking toilets
- Searching a floor or area for suspicious articles
- Ensuring lifts are not used during the evacuation

Equipment's:

Good Quality Torch, Floor plan of entire building identifying the following features:

- Section Exits
- Section Fire Fighting Equipment

- Section Evacuation Assembly Areas
- List of all on-duty staff and emergency contacts if applicable

During evacuation, ERT Lead and members will be prepared to,

- Wait until the fire stairs are clear before entering. If congested, wait for a few moments and check again, or use an alternative exit
- Lead the occupants down the stairs, preventing running or lagging behind
- Provide assistance to any occupant falling or tripping
- Allow room for Emergency Services Personnel who may also be using the fire stairs
- Prevent any person from re-entering the floor or building, unless authorized by the ERT lead or Officer-in-Charge of the Emergency Services
- Permit only non-bulky personal items, such as purses, wallets or handbags, to be carried into the fire stairs.

Evacuation Procedures:

When an evacuation of a section is initiated by either a ERT lead or ERT member, the procedure is as follows:

- Usher staff/visitors to the nearest exit as quickly and calmly as possible
- Check toilets and other areas for stragglers
- Report to the ERT lead and act on any instructions
- As far as possible all staff/visitors should remain in the assembly area until the situation is stabilized
- ERT member conducting searches of toilets etc. must report their findings to the ERT lead. (Area clear or otherwise – mobility impaired person’s locations)
- Under no circumstances should staff members be permitted to go back into the building for any reason, until advised safe to do so
- Arrange assistance for handicapped persons
- Secure cash and valuable documents (if safe to do so)
- Evacuate with a minimum of personal material.
- Where possible close doors and windows on departure

- Prevention of panic is of paramount importance
- Obey directions given by emergency services personnel
- Keep all exists / entrances clear at all times
- Do not allow anyone except Emergency Services personnel to re-enter the building while the alarm is sounding
- Should a person refuse to comply with the directions given by a ERT Lead or ERT member,
- Ensure the person has been clearly advised they are required to evacuate the building, because of an emergency situation
- Notify the ERT Lead, who will advise the Officer-in- Charge of the Emergency Service who, at his discretion, may take the appropriate action under law to remove the person

5.8 Equipment protection

Electrical and Electronic Equipment's:

This includes Projectors, Television, and Photocopier, UPS, Air Conditioners

- Access to air conditioners at server rooms will be restricted to only admin and IT and maintenance engineer.
- Access to air conditioners at zone 2 is restricted to only authorize persons.
- All equipment's are provided with fire, peril and theft insurance

Communication Equipment's:

This includes Telephones, Blackberry, VOIP phones, Video conferencing equipment, and Fax Machines,

- Equipment's will be located in appropriate locations, such as keeping the Fax machine under Administration control, to avoid any misuse of fax machine and also reduce the risk from environmental threats and hazards.
- Shared resources like photocopiers and fax machines will be restricted to Zone 2 only.
- Fax machines will be password protected to prevent misuse.

- Fax machine for general use will be kept under the custody of Administration, at the reception, and log will be maintained in a separate register where every employee who utilizes the fax machine will make an entry in the register, specifying details of the fax done. Personal use of Fax machine will not be allowed
  - All equipment's are provided with fire, peril and theft insurance
  - Laptops, Blackberry are provided with additional insurance for accidental loss, special perils

Fire safety equipment's:

- Fire safety equipment is kept under the custody of the ERT.

Cabling Security for Electrical & Telephone:

- All network connection points will be marked and identified.
- Measures will be considered to protect network cabling within the premises of Trianz, or premises where Trianz equipment is located, from unauthorized interception or damage, for example by using conduit, or by avoiding routes through public areas.
- All cables, including power and telecommunication cables, will be protected from damage or unauthorized interception and cables shall be laid beneath the wall, floor or any other interference such that the cables are not exposed except at critical terminal points.
- Within Company premises, power and telecommunications lines will be underground, where possible, or subject to adequate alternative protection.
- Power cables shall be segregated from communication cables to prevent interference.
- Admin team shall maintain the cabling infrastructure diagram or obtain from the building management team and maintain, if required.
- Admin team shall establish a schedule for regular cable inspection and maintenance. This includes checking for signs of wear, damage, or exposure, and addressing any issues promptly. Replace damaged cables or connectors as needed. In case of a security is a concern, the

admin team shall consider additional measures such as cable locks, tamper-evident seals, or physical access controls to prevent unauthorized access to cabling infrastructure.

- Admin team shall maintain detailed records of cable installations, maintenance activities, and any changes made to the cabling infrastructure. This documentation is valuable for future reference and troubleshooting.
- Admin team in collaboration with the Building Management team shall conduct periodic risk assessment on cabling security / infrastructure and security audits to assess the overall effectiveness of your cabling security measures. Risk Assessment and the security audit shall be performed once a year or on a requirement basis. Trianz shall adjust the practices and materials as necessary to address evolving threats or changing environmental conditions.

Information processing equipment's:

This includes desktops, laptops, servers, routers, switches,

- All information processing equipment's will be protected by having a log on process to prevent un-authorized physical access
  - Inventory Information processing equipment's is maintained and reviewed on a monthly basis
  - Laptop Allotment letters will be given to laptop users and each user will be held accountable for safety of Laptop.
  - Environmental requirements
  - Temperature and Humidity for critical areas (work area, Server room, Data centers, Hub room, etc.) shall be maintained within the acceptable range (18 to 22 °C and below 65%).

5.9 Equipment Maintenance:

Electrical and Electronic Equipment:

Please refer the Admin process (\\thehub\trianzqms) for the required procedure

Communication Equipment:

Please refer the Admin process (\\thehub\trianzqms) for the required procedure

Fire safety equipment's:

Please refer Admin Process (\\thehub\trianzqms) for the required procedure

Information processing equipment:

- laptops, servers, tapes,
- IT Department will maintain list of all the critical IT hardware assets along with their maintenance schedules as prescribed by vendors/IT
- Equipment will be maintained in accordance with the supplier's recommended service intervals and specifications
- Only authorized maintenance personnel will be allowed to carry out repairs and service equipment
- Records will be kept of all suspected or actual faults and all preventive and corrective maintenance
- The maintenance personnel from vendors will be adequately monitored during maintenance operations carried out in-house
- In case the IT asset needs to be sent out for maintenance then, documentation is prepared to ensure traceability and accountability. Adequate packing and handling instructions are given to the transporter for ensuring physical safety during transit.
- Appropriate care will be taken when sending equipment off premises for maintenance

- Requirements of insurance policies relating to IT assets, if any, are complied with

Work Environment Maintenance
Please refer Admin process for the required procedure

5.10 Control of Movement of Assets:

Trianz is bounded by STPI regulations. Proper protection will be provided for equipment and information that are taken outside Trianz premises.

- The manufacturer's instruction on equipment protection will be adhered to.
- Portable computers will be carried as hand luggage.
- Magnetic media will be protected from exposure to strong magnetic radiation and heat.
- For any material going outside, gate pass will be initiated by the concerned person, specifying the details of the material going out and finally approved by administration department. The gate pass must be completely filled and will indicate whether the item is returnable or non-returnable. If item is returnable then the tentative date of return will be indicated in the gate pass and the item will be tracked for return by the security. In case the item is not returned on the tentative date of return as indicated in the gate pass, the security will inform the Administration for follow up. Exceptions to this are laptops issues by Trianz to its employees for work-related usage both within Trianz premises or external to it.

- The items, belonging to Trianz, that are to be brought inside the office premises will have the prior approval from the Administration. The inward register will be maintained by the security to maintain the status of each of the inward items. If laptop is brought inside the office premises by any third party, will indicate the name of the person, contact address, time in, contact no, person to meet, purpose of meeting and serial number and manufacturer of the laptop.

5.11 Physical Access Monitoring and Control

- CCTVs will be installed at all receptions, server rooms and entry/exit points to monitor and track the movement of assets and prevent tailgating
- Physical Access Control System will be monitored on a regular basis to detect any intrusions
- Fire Alarms will be installed at zone 2 and zone 3 to detect and signal fire
- CCTV footage shall be archived for minimum of 90 days.
- Physical access logs shall be stored for minimum of 365 days.

5.12 Re-use, Disposal and Removal of Equipment

Re-use of equipment:

- All items of equipment containing storage media will be checked for confidential information and the same will be backed up or removed or securely overwritten prior to re-use based on business requirements

- All licensed software installed on the equipment will be removed if not required while re-using the equipment.
- Record of activities performed on the equipment before issuing the same for re-use will be maintained.
- Care will be taken to ensure no compromise of security while re-using the equipment.

6. Exit Criteria and Output

- Physical Access Security Breach Identification and resolution.
- Data Centre personnel Awareness training
- Temperature monitoring.
- Utility Service Maintenance.

7. Roles and Responsibilities

Role	Responsibility	Internal/External
Admin Team / Building Management Team	• Responsible for reviewing, implementation and managing the cabling security, UPS, Server room security, Fires equipment etc,. • Co – ordinates and guide the Security personnels regarding the physical and environmental security. • Performs physical access review on a frequent basis.	Internal / External
Security Personnel	• Security Personnel is responsible for maintaining and monitoring physical and environmental security and the	Internal

	maintenance of registers, such as visitor and vendor.	
Professional Development / IS team	• The Professional Development team in collaboration with the IS team is responsible for creating, reviewing and approving the data centre Personnel training for the respective persons.	Internal

8. Prerequisites

8.1 Reference Policy, Process, Procedure, Templates, Checklist

Document Name
• User Access Management Procedure
• Media Handling Policy
• Physical Access Control and Environmental Security Policy

9. Applicable Standards:

- ISO/IEC 27001:2022
- CSA Cloud Controls Matrix v4.0.8

10. Exceptions(S):

There is no exception to this policy.

11. Review:

This Procedure shall be reviewed and approved once a year or at the time of any major change in the existing environment, whichever is earlier.

12. Appendix:

None

13.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	Release ID
CISO	PACES_PROC_0172

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	Jyotessh G Nair			Baseline is approved by Zulfikar Deen.	Approved Baseline.
1.01	9-Mar-09	Bharateesha B R			Risk Assessment Report and Risk Mitigation Plan	• Changed the Physical access control framework. • Incorporated provisions made in hardware lifecycle

						management policy • Changed the Document properties in terms of changing ownership, adding custodian • Decreased the number of Zones from 4 to 3 to simplify and increase the coverage • Added sections Introduction, definitions/acronyms/terms. • Revised the scope in line

						with current scope of the ISMS. • Revised the objectives to align with business requirements • Added Section Perimeter security to provide the controls available for perimeters having trianz information assets based on the risk assessment • Provided clarifications on Physical

						access controls. • Added sections work environment regulation, health and safety regulation, and emergency and safety services as a result of risk assessment and risk mitigation plan • Included sections water supply failure, telecommunication

						failure, and emergency evacuation procedure as part of protection against external and environmental threats • Added new sections electrical and electronic equipments, communication equipments, Fir fighting equipments, information processing equipments as part of the

						Equipment protection to provide more clarity and increase coverage • Provided more clarity on section equipment maintenance • Distinguished monitoring controls from the physical access controls • Included a new section on re-use, disposal and removal of equipments. Reviewed and removed the

						procedure for off-site equipment security
1.02	24-Mar-09	Bharateesha B R			Review by Sujit Sahoo	• Incorporated changes to Section 6.2.2, • Section 6.3.3 provided a reference to the ID card Issue process Section 6.5 Provided examples to bring in clarity
2.00	29-Apr-09	Balu Nair			Approval for baseline	Baselined
2.01	31-Dec-09	Chakravarthi			`QMG review	Formatted entire document
3.00	31-Dec-09	Chakravarthi			Request for baseline	Baselined
3.01	14-May-10	Balu Nair			QMG Review	Formatted the document, Modified cover page
4.00	20-May-10	Balu Nair			Request for baseline	Baselined
4.01	24-May-11	Srilakshmi			QMG Review	Modified release id in header and cover page to make consistency

5.00	24-May-11	Srilakshmi			Approval for Baseline	Baselined
5.01	3-Aug-11	Sudharsana			QMG review	• Replace Owner with Management Representative in place of CIO In Document Classification Scheme, "Retention period is 3 Years" row is removed
6.00	3-Aug-11	Sudharsana			Request for baseline	Approved and Baselined
7.00	17-Sep-12	Srilakshmi			ISMS Surveillance audit findings	• Modified template format of procedure as per documentation guidelines Modified section 6.12 Re-use, Disposal and Removal of Equipment and referred template

7.01	25-Jan-16	Sumanta Bhattacharya and Balu Nair			Client Audit and alignment with shared assessment checklist.	Section Removal of equipment and disposal of equipment's are moved to Media handling policy
8.00	08-Feb-16	Balu Nair			Approved by Mahesh (CISO)	Baselined
8.01	29-Apr-19	Balu Nair	Joshy VM			• Information classification modified Trianz logo modified
9.0	14-May-19	Balu Nair		Ganesh Arunachala	Approved for Release	Baselined
9.1	12-May-20	Balu Nair	Phani Krishna		For Review	Migrated to the new template
10.0	15-May-2020	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
10.1	3-May-21	Divya Gongalla	Phani Krishna	Phani Krishna	For review	Updated with new information classification
11.0	3-May-21	Divya Gongalla	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined

11.0	4-Jan-22	Divya G		Karthik	For review	No changes
11.1	11-Jan-23	Sanjana, Rama Madhavan		Karthik	For review	Reviewed with no changes Migrated to new template
12.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
12.1	30 -Oct-2023	Kishore and Vinod	Rakesh Vijendra and Balu Nair		For Review	Made Changes in line to CSA CCM v4.0 requirements
13.0	10-Nov-2023	Kishore and Vinod	Rakesh Vijendra and Balu Nair	Srikanth M	For Approval	Approved and Baselined
13.1	11-feb-24	Shalini	Vijaya	Srikanth	For Review	Mapped to ISO 27k 2022 Physical controls
14.0	23-Feb-24	Shalini	Vijaya	Srikanth	For Approval	Approved and Baselined
14.1	06-May-25	Balu Nair	Vijaya		Yearly Review	Migrated to a new Template
15.0	29-May-25	Balu Nair	Vijaya	Srikanth	Yearly Review	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com

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