Document Control

Organisation	Trianz Holdings Pvt. Ltd.
Title	Human Resources_ Remote working
Author	Human Resources Department
Filename	HRP_POL_IND_01_Remote working
Owner	Human Resources
Subject	Remote working/ Work From Home
Protective Marking	Public- Confidential
Review date	

Revision History

Revision Date	Reviser	Previous Version	Description of Revision
16-07-2018	**Paul Jacob**	**NA**	**Release of Policy**

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
President & CEO	Sri Manchala	
VP HR & TU	Sujit Sahoo	
VP – Chief Assurance & Data Protection officer	Ganesh Arunachala	

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
To All Employees	NA	NA
To All Contractors	NA	NA

Table of Contents

1 Policy Statement

Trianz provides users with the facilities and opportunities to work remotely as appropriate. Trianz will ensure that all users who work remotely are aware of the acceptable use of computer devices and remote working opportunities. The policy also lays emphasis on both Information security and HR Practices to be followed when the associates work remotely.

2 Purpose

- The purpose of this document is to formalise the remote working policy to enable associates who are authorised to work from home for legitimate business/personal reasons (like health, maternity, etc.).
    - If the associate is on a billable project, requisite client approvals are mandatory
- The policy is to put in place Information Security Compliance and business requirements standards that govern the use of Trianz and client IT information assets, associated relevant policies and procedures and systems in a teleworking environment.
    - To ensure that appropriate monitoring mechanisms are put in place while authorised associates work remotely.
    - To ensure suitable IT assets are provided with adequate security controls thereby enabling associates to conduct project/business work in a safe and secure environment.
    - To recognise IT information assets and any information stored on printed/storage/mobile devices/public drop boxes/one drive etc. as valuable organisational & client assets and to safeguard appropriately with requisite controls as governed by client InfoSec requirements and Trianz InfoSec standards, subject to random audit once in six months.

3 Scope

The Work from Home (WFH) Policy applies to all applicable authorised Trianz associates and client approved contract employees who use Trianz IT assets & facilities and equipment remotely from home. The scope of this policy is applicable to India only.

4 Legislation

There is no specific legislation relating to working remotely, however, the associate is bound by the aspects laid out in this document, which is corporate reference, wherever applicable.

5 Definition of Work from Home

- Working from Home is defined as the capability provided to our associates to work from a location within India apart from the designated Trianz offices or Trianz client offices (referred to as a 'remote' location subsequently), using Trianz assets and equipment, for a prolonged duration.
- To work from home, requisite approvals of manager are mandatory. However, for all the users, decision pertaining to work remotely must be on a case to case basis based on discretion and approval of the manager or Trianz management subject to meeting all statutory compliance guidelines & Policies**.**
- Whether or not an associate is permitted to work remotely is entirely at the discretion of Trianz. Working from a remote location is neither a contractual nor a statutory right and Trianz is under no obligation to approve a request by an associate to work remotely.

6 Request to work remotely

- All requests for working remotely must be in line with definition of "Remote working / Work from home "policy as described above and must comply with the criteria stated above for meeting all statutory compliance guidelines & Policies**.** All documentary evidence must be maintained pertaining to remote working / work from home .

- Associates wishing to work from a remote location must secure the agreement of their line manager prior to the actual date. Retrospective requests will not be agreed and any absence maybe considered as unauthorised, which may lead to disciplinary actions against the associate.
- If the associate is on a project requiring client approvals for work from home due to the nature of the project, approvals from the client is mandatory and should be sought by the reporting manager prior to the approval of the work from home request.
- When approving requests, the line managers are responsible for ensuring that there is a clear business requirement for the associate to work remotely rather than working from office. An example would be the associate benefiting from working on a specific task without the normal daily distractions.

7 Guidelines for approving requests for working from home

Line managers are advised to ensure that deliverables and performance are tracked even while the associate is working from a remote location. Managers should consider the below mentioned criteria when the request is initiated by an associate.

- **The nature of the associate's job:** for instance, does the associate's job require regular, face-to-face contact with other associates or members of the public, meaning that it is unsuitable for the post holder to work from home.
- **The applicant's skills, abilities and personal attributes:** The associate's performance should be considered in determining whether the associate is considered suitable to work unsupervised.
- **Associates having dependencies** on organisational IT assets and are not in the possession of the same must be excluded from the policy.
- **Impact to team:** The demands likely to be placed upon the associate's colleagues and impact upon members of other teams with whom the associate works with. In other words, the line manager needs to be confident that sufficient resources are available within the team to cover the associate's absence from work.
- **The suitability of home location:** The suitability of the associate's home location should also be considered to ensure that for associates (both critical and non-critical), a secure working environment is established as per the documented checklist and verified by the line manager before approval of Work from Home request.
- Requests for working from home which coincide with medical appointments are permitted, however line managers should approve such requests where there is a clear business benefit for associate to work at home rather than at the workplace.
- For associates on flexi-time, any hours worked at home should be recorded on attendance tracking system.
- All work from home requests will have to be reinitiated by associate on a 3 monthly basis and have to be re approved by managers unless otherwise Trianz management makes changes in the said request based on criticality. It is at the discretion of the manager to revoke the work from home at any point of time with an advance notice of 2 days.

8 Expectations of Associates who work from home

While working at home, associates must be engaged on agreed Trianz work and be contactable during regular business hours.

8.1 IT equipment

- Trianz will provide official laptops. Connectivity to Trianz network or email can happen only after IS configuration for Trianz environment is done. Any request for such equipment will need to be authorised by Project /Delivery manager and approved by InfoSec.

8.2 Work Location

- All associates are expected to work within India.
- All associates are expected to intimate managers on an e-mail in case they are not working from the location of work.

8.3 Telephone

- The associate will be required to use his/her own telephone for making occasional telephone calls while working from home.

8.4 Security Requirements

- All identified associates who qualify to work from home must clear – All mandatory trainings (POSH, INFOSEC etc.) before availing work from home.
- WFH Checklist to be filled by associate and approved by project /delivery manager & maintained for audit trail. This is the responsibility of the PM/DM to maintain the same.
- If associate is an ODC user, an approval email from the client has to be maintained for audit purposes. This is the responsibility of the PM/DM to maintain the same.
- When working from home, the associate must be aware of the increased risk of a security breach. The associate must ensure that all documentation is stored securely and that any laptop or PC is password protected and turned off when not in use.
- IT equipment provided to the associate to support working from home is for the exclusive use of that associate alone. The associate is not permitted to allow family members or friends to use IT equipment provided to them.
- The associate is also required to comply with Trianz policies that cover the use of IT equipment and applications as per **"Acceptable Usage Policy & Data Privacy Policy**." (Trinet > Corp Functions > Assurance > Blue Book > 08_Information Security Management System > 01_Policies > Acceptable Usage Policy & Data Privacy Policy)
- For accessing Trianz network / servers from remote location(s), associates are required to take access to Virtual Private Network (VPN) post approval from their manager.

8.5 Dress Code

- Associates are expected to be dressed in professional attire as per the defined Dress Code Policy while attending video conference or other client meetings over Skype or other visual media.

8.6 Background Noise

- While attending mobile calls or video calls with clients and/or Trianz stakeholders, associates are expected to ensure that background noise is avoided.

8.7 Backdrop

- In event of a planned or unplanned video call with client or Trianz stakeholders, the associate is expected to have a light coloured or plain white backdrop.

9 InfoSec Compliance requirements for Information Security Risk mitigation

Trianz recognises that there are risks associated with users accessing and handling information in order to conduct official project work/business. The mobility, technology and information that make devices so useful to associates and organisations also makes them susceptible attack surface for hackers. Securing confidential, proprietary, personal & sensitive client & Trianz data when authorized and approved

associates work remotely is of paramount importance. All work from home users are to comply with policies specified under information security management system in the Bluebook

In a ODC environment the laptop must be imaged with the right thin client profile approved by the client so that unauthorized access and unauthorized usage of Trianz or client information is prevented.

This section of the policy aims to mitigate the following risks:

- Increased risk of equipment damage, loss or theft.
- Accidental or deliberate overlooking by unauthorised individuals.
- Unauthorised access to confidential, proprietary, personal and sensitive information.
- Unauthorised introduction of malicious software and viruses.
- Potential restriction imposed by the InfoSec Assurance as a result of information loss or misuse.
- Potential HR/legal/Regulatory action against associates as a result of information loss or misuse.

Please refer to the Infosec Compliance requirements for Information Security risk mitigation at the following **Trinet location**: **Trinet > Corp Functions > Assurance > Blue Book > 08_Information Security Management System > 01_Policies**

10 Absence and sickness

- If an associate is unable to work on a particular day where he/she was expected to work from home due to sickness/injury/otherwise, he/she must follow Trianz's Absence reporting procedure and Sick Leave Policy.
- The associate is required to keep his/her line manager informed of the likely date of return to work, along with the reason for absence and progress as is done in case of working at Trianz office or Trianz client premises.

11 Disciplinary procedures

- The Disciplinary Policy and Procedures apply equally to both office-based and work from home arrangements.
- Any abuse of the work from home arrangements amounting to misconduct may be subject to disciplinary action.

12 Confidentiality Clause

While working from home, associates will remain subject to all confidentiality clauses contained within their contract of employment. A disclosure of confidential information during the course of employment may be considered by Trianz as gross misconduct and grounds for termination of employment without notice.

13 Monitoring and Review

- Line manager will be responsible for monitoring the associate's performance while working from home.
- The process for monitoring both the compliance with this policy and its effectiveness, will be through the use of audit in accordance with the Audit plan which will be done at least once in six months or earlier.
- In addition to internal, external and client audits, it is mandatory to comply with controls of security, availability, processing integrity, confidentiality & privacy. Specific technical audits may also be conducted when necessary.

- WFH audit findings, security incidents, corrective & preventive action plan is subject to management review by the Information Security Assurance Council (ISAC) comprising of members which includes management representative, Chief Assurance & Data Protection Office, HR, IS, Delivery, legal and other departments as applicable.
- The WFH policy will be reviewed on a biannual basis and any necessary amendments will be made based on the Biannual Management review findings. However, where review is necessary due to legislative or a Security Incident impacting Regulatory Compliance, the management review will happen within seven working days of the Security Incident Reporting (SIR) and corresponding Policy /procedure changes will happen within 14 days of Security Incident reporting (SIR). Action closure will happen no later than 30 days from the date of the SIR.
- For any security breaches, responsible line manager will send a notification to ISAC (Information Security Assurance Council) within 24 hours.
- The InfoSec team will assess the magnitude and impact of the breach and will provide a SIR report to ISAC
- ISAC will review the SIR and define the SIRP (Security Incident Response Plan), client communication, stakeholder communication and disciplinary action as appropriate will be invoked.

14 Variation

Trianz reserves all the rights to update this policy as required.

15 Annexure

Roles & Responsibilities

Individual Associate's Responsibilities – • All the associates who work for Trianz [permanent/contract] are responsible for the security of information/assets created/used in the course of their duties. • Associates should ensure zero breach of information security along with awareness of all relevant Information Security Policies and procedures while following their recognized Codes of Conduct. • Associates will to adhere to the Code of Conduct laid down in the Letter of Appointment along with other addendums that might have been incorporated thereafter.	**Delivery Manager's/Project Manager's/Line Manager's Responsibilities –** • Managers have overall responsibility of assessment & approval of all remote working applications and also must ensure that associates in his/her area are aware of the policies and procedures that guide the safe & secure remote working practices. • Managers are also responsible for timely assessment of the associate's performance and for capturing it in the system. • Managers must ensure that associates who have remote working approval are adequately trained in the area of work and conform to the guidelines for completion of tasks assigned. • Managers must ensure that the need for teleworking is reviewed periodically. • Managers will monitor both deliverables & discipline and any deviation in these aspects will be brought to the notice of HR.

HR Team
• HR team needs to be notified of the request on remote working.
• Associates must consult with concerned manager on any safety matters that might impact their ability to work remotely. The document must be mailed to manager and handed over to HR team prior to commencing work remotely.
• Manager must agree to employee's WFH request by sending his/her approval via email to employee while copying HR.
	IT Team
	• Trianz IT Services team is responsible for configuring IT equipment to enable smooth functioning of equipment (e.g. laptops).
	• IT Services team will ensure that all Trianz equipment is encrypted before any confidential information is processed on it.
	• IT Service team must ensure that data on network drives is backed up on a regular basis.
	• The team will also ensure appropriate access using username & password along with end point encryption and anti-virus software installation.
	• When equipment is returned, IT team is responsible for:
	  • deleting data stored locally
	  • updating the IT asset database to reflect change of user and/or
	  • storage/decommissioning of the equipment.

	• before any equipment is put into storage, IT must ensure that equipment is physically secure, end point encrypted and antivirus software is installed.
Chief Assurance & Data Protection Officer • Is accountable to ensure that every associate in Trianz is compliant with Information Security standards, Data privacy Regulations & Client Standards and Regulations etc. • Must ensure confidentiality, integrity and availability of client & Trianz information assets.	**Chief Information Officer (CIO) –** • Has the overall responsibility for security of Trianz infrastructure & information assets.