TRIANZ℠

REMOTE WORKING 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 ensure that Remote working is undertaken safely from an informationsecurity perspective. It is therefore required that information security risks, related to each specific Remote working scheme, are identified assessed and managed.

2. Scope

- Trianz employees authorized for Remote working, having remote access to Trianz IT Infrastructure and Information systems wherever is applicable.
- Trianz IT Infrastructure and Information systems to which remote access is permitted for business purpose.

3. Policy Statements

3.1 Applicability

This standard applies to remote access users who have access to Trianz IT infrastructure and information assets through public networks. In addition to remote working users, this standard is applicable to security, system, and network engineers and administrators, as well as computer security program managers, who are responsible for the technical aspects of preparing, operating, and securing remote access solutions and client Networks.

3.2 Management Requirements

Before reporting managers and/or supervisors authorize work to be performed under a remote working arrangement, they must do the following:

- Identify the type of work to be performed through the remote working arrangement.
- Only authorize Remote working user access to resources which are necessary to carry out the remote working arrangement safely and securely. Reporting Managers

and/or supervisors shall consider whether the needs to support the remote working arrangement can be met with less access and connectivity than provided at the Trianz office.

- Work to be performed during an on demand / emergency situation to maintain essential operations may not warrant the remote working user to have the same access or connectivity as they do at the Trianz office. In many cases, a VOIP, MS –Lync, telephone and email access through a secure connection may be all that is required.

3.3 IT Administrator Requirements

Before connections are made, Trianz IT Administrators shall ensure that the following requirements are met:

3.3.1 General Requirements:

- Trianz IT Administrator to ensure that all Remote working arrangements must be approved by the IT Manager.
- Remote working users are provided with Trianz owned Laptop with System Image and Internet Data Card to establish secure connectivity to Trianz IT Infrastructure wherever applicable with supported business need.

3.3.2 Technical Requirements:

- **Standard Build Requirements:**

  Laptop issued to users under telecommuting arrangements must be supported by IT personnel and actively standards such as: security patches, anti-virus, removal of administrative rights, authentication, auditing, disabling unnecessaryservices, password complexity, user privileges, local security policies, etc

- **Security Update Requirements:**
  All systems used to remote connectivity must be kept up to date with the most current security patches for the operating system as well as any applications such as Anti-virus software, Microsoft Office, Google

Chrome and Microsoft Edge eetc

- **Anti-Virus Requirements:**
  - All systems used to Remotely connect have Windows Defender anti-virus software installed and properly configured with latest update.
  - The anti-virus software must be configured to scan files in real-time.
  - The anti-virus software must be configured to scan the entire system.
  - The anti-virus software must be configured to alert upon the discovery of a virus.
- **Network Security Requirements:**
  - All systems used to remote connect must be protected with a Trianz FortiGate UTM firewall or web gateway proxy server.
  - The firewall/proxy server must be configured to block all unsolicited inbound connections.
- **Authentication/Authorization Requirements:**
  - All systems used to remote connect must require users to login before using the system.
  - Administrative rights shall be restricted.

3.3.3 User Requirements:

- **General Security Requirements:**
  Remote working users should connect to an internet and utilize Trianz SSL VPN to connect with Trianz IT wherever is needed.
- **Authentication Requirements:**
  Passwords for all user accounts on the system must meet the minimum complexity requirements defined as per Trianz Password Security Policy.
- **Attack Prevention:**
  - Remote working users shall ensure that a combination of software and software features are installed and operating on their information assets in order to prevent attacks, including antivirus and antispyware software.
  - Personal firewalls that deny all types of communications that users have not specifically approved as being permitted.

3.4 Security Maintenance and Monitoring

Remote working users shall maintain their information assets' security on an ongoing basis including:

- Confirming periodically that the operating system and primary applications are up-to-date.
- Checking the status of security software periodically to ensure that it is still enabled,configured properly, and up-to-date.
- Periodically checking for potential security issues on the information asset (e.g.,running utilities that check the computer for potential problems).
- Investigating any cases in which the information asset begins to display unusual behavior using Security Event Viewer.

4.Exceptions(s)

There is no exception to this policy.

5. ISO Control Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
People Control	6.7 Remote working Control Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Remote Working Policy

Document Control

Owner:	CISO	**Release ID:**	TELE-POL-0028

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.01	16-May-15	Sudharsana .CV			Initial Draft	None
1.00	19-May-15	Sudharsana .CV			Reviewed	Baselined
1.01	14-Oct-16	Sriharsha			Addition of Cloud services as scope of Certification.	Modified the scope Trianz logo modified
2.00	07-Dec-16	Balu Nair			Approved byCISO	Baselined
2.1	13-May-20	Balu Nair	Phani Krishna			Migrated to thenew template
3.0	14-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved andBaselined
3.1	22-Jan-21	Karthik N	Phani Krishna		For Review	Updated the Information classification. No other changes

4.0	22-Jan-21	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved andBaselined
4.0	23-Dec-21	Karthik N	Sivaramakrishnan N		Annual Review	No Changes
4.1	25-Feb-23	Kruti, Pallavi Chakrabarty	Karthik N & Pranesh K		For Review	Antivirus changed to Symantec antivirus to Windows Defender anti-virus. Network Security Requirements has been modified. New template change
5.0	12-May-23	Kruti	Karthik N & Pranesh K	Srikanth M	For Approval	Approved and Baselined.
5.1	28-Jan-24	Vijaya & Beniyel	Pranesh Kulkarni	Srikanth M	For Review	Policy updated to Remote Working aligning to ISO 27001:2022.
6.0	23-Feb-24	Vijaya & Beniyel and Bala	Vijaya and Bala	Srikanth M	For Approval	Approved and Baselined.
6.1	30-Apr-25	Kruti	Vijaya and Bala		For Yearly Review	Migrated to a new

						Template.
7.0	14-May-2025	Kruti	Vijaya and Bala	Srikanth M	For Approval	Approved and Baselined.

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com