TRIANZ℠

Trianz-Remote-Working-Cybersecurity Guidelines

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

IMPORTANT:

Working remotely or working from home you continue to be responsible for protection of Trianz' s, it's clients, suppliers or other third parties' confidential and sensitive information and are responsible for Trianz' s devices. Keep the devices, infrastructure, and information safe and secure. You continue to be bound by all the agreements, policies and declarations signed during your course of employment with Trianz, including but not limited to, Confidentiality, IP Assignment Agreement, Information Security policy etc. You will comply with client confidentiality agreements, Information security, Data Privacy or Data Protection and any other policies, documents and requirements as required by client/s from time to time.

In addition, you agree to adhere to below 'Remote Working Cybersecurity Guidelines':

Cybersecurity

- Ensure laptops/devices have hardware encryption.
- Make sure that shoulder-surfing (someone else looking onto the screen, over the shoulder) becomes harder by ensuring no one is standing behind or right next to you, especially while working on sensitive information.
- Make two factor authentication (2FA) mandatory for remote access of all systems and applications, wherever feasible.
- Ensure to follow the below mentioned password best practices
  - ➢ Do not share passwords with anyone
  - ➢ Do not send passwords through emails, etc.
  - ➢ Do not store passwords in browsers
  - ➢ Use different passwords for different applications wherever required
  - ➢ Configure password lockouts and timeouts to avoid password attacks, etc.
- Do not open links or documents with Coronavirus information, without validating the source of information.
- Always protect the confidentiality of information.
- Ensure critical updates (patches) to software, firmware etc.
- Do not browse websites that are out of scope of work and reach out to is@trianz.com, in case of doubt.
- Do not use illegal movie websites as they pose a risk of ransomware and malware infections.

- Do not lend Trianz systems to children or other members of the family.
- Intentionally or accidentally laptop screens must not be part of any pictures taken by self or family members.
- Do not share full desktop while sharing the screen, and just share the required program (like presentation, excel, etc.) unless it is absolutely essential to share the full desktop.
- Take utmost care to protect Trianz assets from thefts, damages, water spillover, etc.
- Ensure all system updates are installed on timely basis.

Reference: Refer and comply with **Information Security Policy** in the Bluebook and Information Security Training on the LMS portal.

Privileged Users

- All IT and business privileged users
  - Be cognizant of your security responsibilities while using high privilege access.
  - Refrain from using high privilege logins, unless it is an absolute necessity to do so .
  - Report all errors and issues immediately to is@trianz.com, while using high privilege access.

Reference: Refer and comply with **User Access Control Policy** and procedure in the Bluebook.

Phishing Emails

- Immediately report to is@trianz.com, if you have:
  - Accidentally clicked on a suspicious file and or link.
  - Opened a suspicious PDF or Word, excel file with a macro.
  - If any malware/ransomware infection messages are appearing, etc.

Reference: Refer and comply with **Phishing Awareness** Training on the LMS portal

Online Meetings and Calls

- Ensure to keep the microphone on mute when you are not speaking in a conference call.
- Ensure webcams are not switched on by default.
- Do not leave the system unlocked, especially during a call or while moving away from the system.
- Do not work from coffee shops or public places – especially if you are on confidential

calls or working on confidential documents, etc.

Reference: Refer and comply with **Work From Home Policy** in the Bluebook.

Exceptions

- Exception is a condition that is not aligned with formal security expectations as defined by the policy, standard, and/or procedure. For e.g. Access to specific sites, installing a new software etc.
- All exceptions should be routed through is@trianz.com.
- All risks arising out of the exception should be thoroughly analyzed.

Reference: Refer and comply with **Exception Handling Policy** in the Bluebook.

Privacy

- Protecting the privacy of our associates, clients, etc. is our primary responsibility.
- All online activities could be monitored for potential breach of various IT, Security and Privacy regulations.
- Do not share personal information via email or store personal information in non-approved locations.
- Obtain necessary consent if you are recording a video or an audio call of the participant.

Reference: Refer and comply with **Data Protection Policy** in the Bluebook.

Backup

- Ensure that all critical documents are backed up regularly onto the approved backup locations.
- Do not use any un-approved external cloud storage services for backup, etc.
- Please reach out to is@trianz.com for any cloud storage or cloud service related issues.

Reference: Refer and comply with **Backup and Restoration Policy** and procedure.

Cyber-attack & Incident Response

- Be alert for phishing emails and other attempts to compromise/steal account details.
- Report phishing emails and malicious activity, if any, to is@trianz.com.
- Double-check before acting on any critical or non-BAU (Business as Usual) directions from managers etc. and preferably use out of band (such as phone calls etc.) communication to reconfirm the actions to be performed.
- Always keep the copies of Policy, Procedure and SOPs ready for quick reference and reach out to the concerned stakeholders when in doubt.
- Please make sure to report any technical errors, configurations mistakes etc. immediately to is@trianz.com so that appropriate remedial actions can be initiated and contain any unwanted repercussions.

Reference: Refer and comply with **Anti-Malware Policy** and **Incident Management Policy** and procedure in the Bluebook.

Document Reference

Owner:	Management Representative	Release ID:	RWCS-GUID-0073

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Version	Author	Reviewer	Approver	Date	Reason for Change	Change Description
0.01	Karthik	Balu & Anitha		27-Mar-2020	Initial Version	None
1.00	Karthik	Balu & Anitha	Phani Krishna	27-Mar-2020	Approved	Review feedback incorporated and baseline
1.1	Karthik	Balu & Anitha		28-Apr-2020	Review	Incorporated changes suggested by Latha
2.0	Karthik	Balu & Anitha	Phani Krishna	28-Apr-2020	Updated document reviewed and approved	Reviewed and Approved
2.1	Sanjana	Balu Nair		24-Dec-21	For Review	Updated with new information classification
3.0	Sanjana	Balu Nair	Siva N	24-Dec-21	For Approval	Approved and Baselined
3.0	Sanjana	Balu Nair	Balu Nair	12-Aug-22	For review	Reviewed with no changes
3.0	Shalini	Balu Nair	Balu Nair	12-May-23	For Review	Reviewed with no changes
3.0	Aishee	Vijaya		8th June 24		Reviewed with no changes

3.1	Kruti	Vijaya		28-May-25	For Review	Migrated to New Template
4.0	Kruti	Vijaya	Srikanth M	29-May-25	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com