TRIANZ℠

Bring Your Own Device (BOYD) 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

- To define the acceptable usage policy for the usage of employee-owned personal devices (e.g., Desktops, Laptops, Mobile phones, Smartphones, Tablets, or any such devices).
- To protect the security and privacy of Trianz's and its client's information and infrastructure assets, from the BYOD devices.

2. Objective

Allows employees to use their personally owned devices for work-related activities. Those activities include tasks such as accessing emails, connecting to the corporate network, and accessing corporate apps and data etc. with appropriate approval and adequate security control.

3. Scope

- All employee-owned personal devices must be registered with the IS department and must have supervisory approval for use within the Project.
- The policy applies to all stakeholders working for Trianz products and services.

4. Policy Statements

- In order to connect to the company network and / or access policy permitted information / infrastructure assets, employees must agree to the terms and conditions set forth in this policy and install required Mobile Application Management (MAM) software onto their mobile phones.
- In order to use Laptop, Desktop, Tablet etc. as "BYOD", employees must sign "BYOD No-Objection and Exclusivity Agreement" and ensure the validation from IS team.
- No other personal device, other than the above, is permitted inside Trianz premises and is also not permitted to access the network and computing resources of Trianz on premises / cloud / from home / from client / transit locations.

4.1Acceptable Usage of Laptops/Desktops/Tablet

For allowing associate's personal Laptop/Desktop/Tablet to be used as Trianz BYOD device, all the following shall be applicable:

- Employee's system shall be validated by IS team prior to connecting to Trianz's network.
- For any access to Client environment through Trianz VPN, BYOD shall not be allowed.
- BYOD can be allowed only with approval from CIO/CISO and explicit approval from the Client (if resource has access to client's network).
- BYOD shall be configured with all the necessary security controls as per BYOD SOP and Conditional Access (refer IS SOP).
- BYOD users shall sign-off a "No-Objection & Exclusivity Agreement" for Trianz information & deliverables on their BYOD device.

4.2 Acceptable Usage of Mobile Phone/Smart Phone

- Employees may use Personal Mobile Phone/Smartphone to access the following company-owned resources:
  - MAM managed Microsoft applications like email, calendars, documents etc.
  - Mobile service provider messages for receiving One Time Password (OTP).
  - Corporate authorized soft tokens / OTP generators.
- No other information / infrastructure assets of Trianz's or its clients should be accessed using personal Mobile /Smartphone. However, this restriction doesn't apply to the publicly accessible resources and cloud-based solutions available from anywhere.
- While personal mobile/smartphone is permitted for the above company defined purposes, associates should comply with all the government and other applicable regulations on use of mobile phones / smartphones, from as applicable in the respective countries.
- Trianz defines acceptable business use as activities that directly or indirectly support the business needs of Trianz.
- Mobile phone devices shall not be used at any time to store or transmit illicit materials, engage in outside business activities, and store or transmit proprietary information belonging Trianz or to another company.
- Users are also prohibited from:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within TRIANZ's networks.
- Posting the same or similar non-business-related messages to large numbers of UseNet newsgroups (newsgroup spam).

4.3 Security

- To prevent unauthorized access, to personal mobile phone/Smartphone or company provided mobile phone devices must be password protected as per the company's password policy.
- It is the responsibility of associate to ensure that the personal or company provided mobile phone is up to date with respect to manufacturer or network provided patches.
- Associates must not load pirated software or illegal content onto their personal devices used for official purposes.
- Associates must not store company data or client data in the personal or company provided mobile phone.
- Employee's access to company data is limited based on user profiles defined by IT and automatically enforced.
- The corporate data on the employee's BYOD device may be remotely wiped if:
  - the device is lost, or
  - the employee terminates his or her employment or
  - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

4.4 Risks/Liabilities/Disclaimers

- The company reserves the right to disconnect the personnel or company provided mobile phone devices or disable services without notification.

- Lost or stolen personal or company provided mobile phone devices must be reported to the company immediately. Employees are responsible for notifying their mobile carrier upon loss of a personal mobile device.
- If an employee suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident immediately.
- The employee is expected to use his or her personal or company provided mobile phone devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined above.
- The employee is personally liable for all costs associated with his or her mobile device.
- The employee assumes full liability for risks including, but not, limited to the partial or complete loss of the company and personal data due to an operating system crash, error, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the personal or company provided mobile device unusable.
- Trianz reserves right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

5. Roles & Responsibilities

Roles	Responsibilities	Internal/External
All Associates	• Obtain Client approval to use BYOD. • Obtain CIO/CISO's approval.	Internal
IS Operations Team	• Validate the system prior to connecting BYOD to Trianz's network.	Internal
InfoSec & Compliance Team	• Review the Security and Privacy risk. • Provide final approval.	Internal

6. Applicable standards

- ISO 27001:2013
- ISO 27701:2019

7. Reference Policies & Procedures

- Trianz-Remote-Working-Cybersecurity Guidelines
- Physical Access Control and Environmental Security Policy

8. Implementation Procedures

- IS Operation Procedure
- Physical Access Control and Environmental Security Procedure
- Admin process

9. Exceptions(s)

Exceptions to the policy for legitimate business interest need to be approved by CIO/CISO. Refer to “Exception Handling Policy”.

10. ISO Control Mapping

Category of Control	**ISO 27001:2022 Control**	**Document Name as per ISO 27001:2022**
Organizational Controls	5.10 Acceptable use of Information and other associated assets	Bring Your Own Device Policy

Document Control

Owner:	CISO	**Release ID:**	BYOD-POL-052

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	30 Apr 19	Balu Nair & Joshy			Initial Draft	Initial draft
0.2	6-May-19	Balu Nair & Joshy	Phani Krishna		Review by Phani Krishna	Policy purpose, scope, statements & exceptions modified
1.0	7-May-19	Balu Nair & Joshy		Ganesh A	Reviewed & Approved by Ganesh A	Baselined
2.0	7-Apr-20	Vijaya	Phani Krishna	CIO	Allowing Associate's Laptop/Desktop/Tablet	Conditional allowance of Associate's Laptop/Desktop/Tablet as BYOD
2.1	12-May-20	Karthik N	Balu Nair		Review	Formatting changes

3.0	14-May-20	Karthik N	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
3.0	28-Jul-20	Vijaya, Balu	Phani Krishna	Phani Krishna	Bi-Annual review	No changes incorporated
3.1	14-Jan-21	Balu Nair	Phani Krishna		Review	Updated the information classification
4.0	11-Feb-21	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
4.1	14-Jul-21	Balu Nair	Karthik/Phani	Phani Krishna	Yearly Review	Updated with the following sections 2, 5,6,7,8.
5.0	30-Jul-21	Balu Nair	Phani Krishna	Phani Krishna	Approved for Baseline	Baselined
5.0	06-Jan-22	Krutideepta	Balu Nair		For Review	No Change
5.1	12-Mar-22	Sanjana	Balu Nair	Siva N	For Review	The scope has been extended to products and services
6.0	18-Mar-22	Sanjana	Balu Nair	Siva N	For Approval	Approved and Baselined

6.1	5-Apr-2023	Sanjana, Shalini Kumari	Balu Nair		For review	Reviewed with minimal changes New template change Editorial changes
7.0	12-May-2023	Sanjana		Srikanth	For approval	Approved and Baselined
7.1	15-Feb-2024	Vijaya	Balu		For review	Updated the section ISO Control Mapping aligning to ISO 27001:2022
8.0	23-Feb-2024	Vijaya	Balu	Srikanth	For Approval	Approved and Baselined
8.1	06-May-25	Balu Nair	Vijaya		Yearly Review	Migrated to a new Template
9.0	14-May-25	Balu Nair	Vijaya	Srikanth	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com