Guidelines on Intranet Usage

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. Objective

The company utilizes Intranet as a critical resource to carry on the business processes. Therefore, Trianz has developed systems & procedures to ensure that security is maintained for Intranet at all times, with a uniform code of conduct.

2. Scope

To stipulate a framework for ensuring all legitimate use of intranet for business needs of TRIANZ are met and the utilization of organizational intranet resources is optimal.

These guidelines are applicable to all the users of TRIANZ. It covers Local Area

Network (LAN) and Wide Area Network (WAN) connected with Trianz's workstations and servers including applications and system software. It is applicable to all systems under the jurisdiction and/or ownership of TRIANZ, inclusive of hired systems. This policy also covers all workstations and servers supplied by the customers of TRIANZ, as long as they are operated from within TRIANZ premises.

3. Reference(s)

Information Security Code of Conduct

4. Rules on Intranet Usage

All services on the Intranet of Trianz LAN and WAN network are for the purpose of the information update and dissemination among the employees and selected third party vendors. All information posted to the Intranet must have a designated owner and all postings or modification of posted information shall be by approval.

- Default Access:
  Default Intranet access shall be given to all employees based on the department in which an employee joins, and accordingly the default username and password for Intranet access would also be communicated to the user.

Default Intranet access shall be given to all employees with private protected VLAN / Isolated Wi-Fi connection based on their Project requirements. All intranet access will be protected with Zscaler webproxy to ensure the security of the sites.

- Access to other resources of Intranet:
  For any access more than the default access, the users shall have to raise a Service Request to the IS Department with an approval from their respective Head of Department. The access shall then be given as per the approval for the specified duration.

- Authentication & Authorization:
  All Intranet access is governed by proper authorization and all intranet servers access will be protected and managed through PAM.

- Information Dissemination:

Intranet information is for dissemination only to authorized people. Users must not forward this information to others without seeking approval through appropriate channel.

5. Roles and Responsibilities

- Any user, as defined in the "Scope section", is responsible for using the TRIANZ's intranet resources in compliance with this policy.
- The IS Manager is responsible for reviewing these guidelines once in a year.
- The designated Information Security Officer/Designated member of the Security Forum along with the Human Resources group shall be responsible for distributing these guidelines.

Document Control

Owner:	Management Representative	Release ID:	INTR-GUID-0059

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Author	Reviewer	Approver	Date	Reason for Change	Change Description
0.00	Jyotessh G Nair			19-Feb-07	Draft	•
1.00	Jyotessh G Nair			26-Feb-07	Baseline is approved by Zulfikar Deen.	• Approved Baseline.
1.01	Bharateesha B R			24- Feb -09	New Asset Management Framework	• Changed the Title to Rules Intranet usage • Removed the Sections Documentation Framework, Enforcement, • • Added document classification scheme
2.00	Balu Nair			29-Apr-09	Approval for Baseline	• Baselined
2.01	Chakravarthi			30-Dec-10	QMG review	• Formatted entire document
3.00	Chakravarthi			31-Dec-10	Request for baseline	• Baselined
3.01	Srilakshmi			24-May-11	QMG Review	• Modified release id in header and cover page
4.00	Srilakshmi			24-May-11	Approval for Baseline	• Baselined

Ver. No.	Author	Reviewer	Approver	Date	Reason for Change	Change Description
4.01	Sudharsana			3-Aug-11	QMG review	• Replace Owner with Management Representative in place of CIO • In Document Classification Scheme, "Retention period is 3 Years" row is removed
5.00	Sudharsana			3-Aug-11	Request for baseline	• Approved and Baselined
6.00	Sudharsana			28-Sep-12	QMG review	• Formatted as per latest template format
6.1	Pranesh Kulkarni	Pranesh Kulkarni	Gangadhar	30-July-2021	review and update	• IT name replaced with IS. • Updated Rules on Intranet Usage with VLAN information.
7.0	Pranesh Kulkarni	Pranesh Kulkarni	Gangadhar	30-July-2021	For Approval	• Baseline
7.0	Kruti	Vijaya R		03-June-2024	Annual Review	No Changes
7.1	Vijaya	Balu		26-May-2025	For Annual Review	Migrated to a new template
7.2	Vijaya	Siva		28-May-2025	Reviewed	Rules updated by Siva
8.0	Vijaya	Siva	Srikanth M	29-May-2025	For Approval	Approved and Baselined

TRIANZᔆᴹ

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com