Data Loss Prevention Policy

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 policy is designed to ensure that the users do not send sensitive or critical information outside the corporate network. Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data.

2. Scope

Scope of the Policy shall ensure the following:

1. Network DLP
2. End Point DLP
3. Cloud DLP
4. Storage DLP

3. Objective

The objective of this policy is to ensure data protection and incident prevention for Trianz's business critical data and PII data that includes sensitive data as per applicable regulations.

4. Policy

DLP solution shall be adopted including data identification and classification so that the Trianz can meet complex and evolving compliance standards

Trianz shall ensure that DLP is adopted across Network, Endpoint, Cloud and Storage.

Trianz's **Network DLP solutions** must ensure prevention, monitoring and control the flow of information that includes PII data via the company's network, email or web.

Trianz **Endpoint DLP Solutions** must ensure solutions monitor endpoint devices, such as servers, computers, laptops and mobile devices, on which Trianz's critical information is used, moved and stored.

Trianz's **Cloud DLP solutions** must protect data stored in the cloud by encrypting sensitive data and ensuring that the data is sent to only those cloud applications that are authorized by Trianz.

Trianz's **Storage DLP Solutions** must protect data stored in unstructured form residing on a server or structured data residing on Databases.

Trianz shall also ensure that the DLP solution is fully integrated within Trianz's cybersecurity architecture.

5. Monitoring

IS operation team shall implement the required solutions, constantly monitor and analyse data to identify potential violations of security policies.

6. Compliance

InfoSec and Data Privacy Assurance Team will verify compliance of this policy through internal and external audits etc.

7. Exception(s)

Exceptions to the Data Loss Prevention shall follow the Exception handling policy. (For e.g. For Finance and HR data with adequate safeguards)

8. ISO Clause Mapping

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
Technological controls	8.11 Data Masking Control Data masking shall be used in accordance with the organization's topic specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	Data Loss Prevention Policy
Technological controls	8.12 Data Leakage Prevention Control Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	Data Loss Prevention Policy

Document Control

Owner:	CISO	Release ID:	DLP-POL-0073

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
0.1	12-Oct-2022	Shiva, Beniyel, Balu, Vijaya	Srikanth Mantena, IS Team		Initial Draft	None
1.00	12-Oct-2022	Shiva, Beniyel, Balu, Vijaya	Srikanth Mantena, IS Team	Srikanth Mantena	Approval for Baseline	Baseline
1.0	28-March-2023	Krutideepta	Vijaya R	Srikanth M	For Review	Reviewed with no changes
1.1	10-May-2023	Rama Madhavan	Vijaya		For Review	Migrated to new template Editorial changes Rephrased Purpose and Monitoring
2.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For approval	Approved and Baselined
2.1	23-Jan-2024	Beniyel S Aishee G	Balu Nair, Vijaya R		For Review	Migrated from standard ISO 27001:2013 to ISO 27001:2022 mapping updated.
3.0	23-Feb-2024	Beniyel S Aishee G	Balu Nair, Vijaya R	Srikanth M	For Approval	Approved and Baselined
3.1	17-Apr-2025	Vijaya	Balu		For Review	Migrated to a New Template and Yearly Review
4.0	14-May-2025	Vijaya	Balu	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com