TRIANZ℠

POLICY FOR DISCIPLINARY ACTION

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 provide the management with a method to deal with non-conformances to basic work-related rules and regulations for effective functioning of Trianz in terms of Attendance, Work performance, Violation of policies, or other work-related issues and improve the conformance to the above by taking appropriate action permissible under this policy.

2. Scope

This policy applies to all our employees. The disciplinary process shall not be initiated without prior verification that an information security policy violation has occurred.

3. Objective

- Encourage all employees to achieve and maintain the Trianz standards of conduct.
- Ensure that all alleged failures of discipline are handled, fairly, reasonably, and consistently.

4. Policy

Employees who engage in any of the following activities, as well as violations of any Trianz policies, will be subject to disciplinary action, including dismissal of services. (This list is indicative and not exhaustive by any means.)

The disciplinary process shall not be initiated without prior verification that an information security policy violation has occurred.

The formal disciplinary process shall provide for a graduated response that takes into consideration factors such as:

- the nature (who, what, when, how) and gravity of the breach and its consequences;
- whether the offence was intentional (malicious) or unintentional (accidental);
- whether or not this is a first or repeated offence;
- whether or not the violator was properly trained.

The response should take into consideration relevant legal, statutory, regulatory contractual and business requirements as well as other factors as required.

The disciplinary process shall also be used as a deterrent to prevent personnel and other relevant interested parties from violating the information security policy, topic-specific policies and procedures for information security.

Deliberate information security policy violations can require immediate actions

4.1 Information Security and Data Privacy:

Noncompliance with the organization's Information Security Policy and Data Privacy Policy and Client defined Security Policy has HR consequences in the form of warnings and termination.

4.2 Attendance:

- Habitual late coming or irregular attendance or absconding.
- Absence without leave or overstaying the sanctioned leave for more than ten consecutive days without sufficient grounds or proper or satisfactory explanation.
- Absence from the employee's appointed place of work without permission or sufficient cause.

4.3 Safety & Health:

- Violating safety regulations.
- Creating or contributing to any unsanitary condition.
- Possession, consumption or being under the influence of intoxicants or narcotics on company premises is prohibited and subject to disciplinary action, up to and including termination.
- Interference or tampering with any safety devices installed in or about the premises of the company.
- Improper use of office equipment.
- Possessing firearms, weapons, explosives etc. on company premises.

4.4 Misuse of Property:

- Damage to, or improper use of, company property either willfully or through gross negligence.
- Unauthorized possession of company property.
- Disclosure of confidential company information to outsiders without proper authorization.

- Unauthorized use of bulletin boards and /or posting notices in unauthorized places.
- Stealing or committing any criminal offense on company property.
- Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.
- Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network.
- Disrupts or causes disruption of any computer, computer system or computer network.
- Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means.
- Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

4.5 Misconduct:

- Fighting, hitting, pushing, forcibly grabbing another employee, client contractor or business associate or otherwise committing an assault and /or similar physical acts or threats while on company premises or in circumstances arising out of company business relations.
- Drunkenness or riotous or disorderly or indecent behavior in the premises of the company or outside such premises where such behavior is related to or connected with the employment.
- Sleeping while on duty.
- Using abusive or threatening language.
- Any act of harassment, sexual, racial or other; telling sexist or racial-type jokes; making racial or ethnic slurs.
- Zero tolerance to indecent, disorderly, offensive, or immoral conduct.
- Commission of a felony or crime involving dishonesty while employed by the company.
- Gambling on company premises.
- Careless or willful destruction or damage to company property or the property of other employee of a company client.
- Falsification of company records, including, but not limited to, financial records, travel expense vouchers, medical bills and other employee forms and documents.
- Unauthorized dissemination of personal information form (employee filed),

or improper use of such information.

- Refusal or failure to carry out a reasonable job assignment or job request after being warned that failure to do so could result in a recommendation for termination.
- Excessive use of company telephone, email or Internet for personal use.
- Any behavior that is seriously disruptive of the normal flows of company business and is unlawful in nature.

In case the employee has a concern about any of the above-mentioned Disciplinary Incidents he or she will discuss it with his department head to mutually develop an effective solution.

However, if the problem persists and (s) he is consistently found at fault, disciplinary procedure will be followed depending on the gravity of the situation, towards maintainingthe decorum of the organization. The Head of HR after mutual discussion with head of the department will take a final call on the same. For any cases of information security &Data Privacy Violations the matter will be reported to CIO/CISO & HR Head. And will also follow the Security Incident Response procedure.

5. Disciplinary actions:

- Oral Warning

  It will describe the behavior or circumstances that made the oral warning necessary. It will be designated as an oral warning and express continued support for the employee with the knowledge that the employee will improve his or her actions or behavior.

- Written Warning

  It will include the reasons for the manager's dissatisfaction and any supporting evidence. The employee will have an opportunity to defend his/her actions and rebut the opinion of his manager at the time the warning is issued.

- Termination

  Based on the gravity of the situation and consistent breach of disciplinary processthe employee may also be terminated from the services of the company.

6. Exception(s)

There is no exception to this policy.

7. ISO Control Mapping

Category of Control	ISO 27001:2022 Control	Document Name as per ISO 27001:2022
People	6.4 Disciplinary process Control A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	Policy for Disciplinary Action

Document Control

Owner	CISO	**Release ID:**	PDA-POL-0009

For Trianz Process Improvement Group (TPIG) Purpose Only

Version History

Ver. No.	Date	Author	Reviewer	Approver	Reason for Change	Change Description
8.00	07-Dec-16	Balu Nair	GaneshA	GaneshA	Approved by CISO	Baselined
8.1	06-Feb-19	Balu Nair	GaneshA	GaneshA	Upgrade to align to InfoSec and Data PrivacyPolicy	Added section to describe consequence of noncompliance to InfoSec and Data Privacy policy
9.0	14-May-19	Balu Nair	GaneshA	GaneshA	Reviewed and Approved by Ganesh A (Chief Assurance Officer & Data Protection Officer.)	Baselined
9.1	12-May-2020	Balu Nair	Phani Krishna			Migrated to thenew template

10.0	14-May-20	Balu Nair	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
10.1	25-Jan-21	Divya G	Phani Krishna	Phani Krishna	For review	Updated with new information classification
11.0	25-Jan-21	Divya G	Phani Krishna	Phani Krishna	For Approval	Approved and Baselined
11.0	03-Jan-2022	Divya G	Balu N		For review	No changes
11.0	26-April-2023	Krutideepta	Balu N	Srikanth M	For Review	Reviewed with no changes
11.1	12-May-2023	Rama Madhavan	Vijaya		For Review	Migrated to new template
12.0	12-May-2023	Rama Madhavan	Vijaya	Srikanth M	For Approval	Approved and Baselined
12.1	23-Jan-2024	Swaroop	Vijaya	Srikanth M	For Review	Addressed requirement of ISO 27001:2022 Control 6.4 Disciplinary process And updated the ISO Control mapping section as per ISO 27001:2022
13.0	23-Feb-24	Swaroop	Vijaya	Srikanth M	For Approval	Approved and Baselined
13.1	28-May-25	Kruti	Vijaya		For Review	Migrated to new template.
14.0	29-May-25	Kruti	Vijaya	Srikanth M	For Approval	Approved and Baselined

TRIANZ℠

Contact Information

Name

Email

Phone

Thank You

infosec@trianz.com