Langslide

HR Disciplinary Policy & Procedure

Version 1.0

PURPOSE

This disciplinary Policy and Procedure establish a clear, fair, and consistent approach to addressing any breaches of the rules and regulations of Rudramsa Systems Pvt. Ltd..(hereby referred to as organization). This policy outlines the steps to be taken when an employee's conduct is considered unsatisfactory or in violation of organizational standards, with the aim of correcting behavior rather than simply imposing sanctions.

SCOPE

This policy applies to all employees of the organization, including third parties, consultants, contractors, and others acting on the organization's behalf. It is global in nature and covers all departments, business units, and functions within the organization.

DEFINITIONS

- **Confidentiality:** The principle of safeguarding sensitive information from unauthorized access, use, or disclosure, ensuring that personal, financial, and organizational data is protected by company policies and legal requirements.
- **Employee Access Control:** A system of policies and procedures designed to regulate and monitor employee access to sensitive information, systems, and physical spaces within the organization, ensuring that individuals can only access what is necessary for their job function.
- **Incident Response:** The structured approach to addressing and managing security breaches or threats, including steps to detect, respond to, and recover from security incidents that may impact HR systems, employee data, or overall organizational security.
- **Background Checks:** Reviewing an individual's criminal, financial, and employment history before hiring or promoting within an organization to ensure a secure and trustworthy workforce.

RESPONSIBILITY

HR Head

- Primary responsibility for implementing this policy.
- Coordinates with the ISG (Information Security Group) and department heads to ensure consistency and compliance.

Department Heads

- Provide oversight for their teams, ensure job descriptions include any necessary security responsibilities, and work with HR to enforce policy requirements.

ISG (Information Security Group)

- Guides policy content, assists with security training and ensures alignment with broader information security objectives.

POLICY

- **Informal Action First:** Wherever appropriate, informal action will be considered before initiating a formal disciplinary procedure.
- **Progressive Approach:** The formal procedure may apply at any stage if the employee's alleged misconduct warrants it.

- **Evidence Disclosure:** The employee will be provided with written copies of evidence and relevant witness statements (if available) before a disciplinary hearing.
- **Right to Appeal:** An employee may appeal against any formal disciplinary action.
- **Confidentiality:** All information arising from disciplinary processes will be retained confidentially and accessible only to those who need it for legitimate purposes.
- **Gross Misconduct:** Acts considered gross misconduct may result in dismissal without notice. Gross misconduct indicates a fundamental breach of contract or policies that makes it impossible for the organization to continue the employment relationship.
  Examples of Gross Misconduct
  While not exhaustive, these examples illustrate acts that may constitute gross misconduct:
  - Physical violence or intimidation.
  - Deliberate and severe damage to property or information.
  - Theft, fraud, corruption, and intentional falsification of records.
  - Consumption of alcohol while on duty.
  - Policy on Sexual Harassment (POSH)-related serious offenses.

PROCEDURE

Informal Action

- **Minor Misconduct:** If the alleged misconduct is minor, the line manager will initiate a private, informal discussion with the employee to highlight the unsatisfactory behavior.
- **Discussion and Feedback:**
    - The manager clarifies the expected standards of conduct and why the current behavior is unacceptable.
    - The employee has an opportunity to present their viewpoint.
    - An agreed timeframe is set for the employee to improve or correct their conduct.
- **Follow-up:** If the required improvements are not met or maintained, the organization will proceed with formal disciplinary procedures.
- **Record-keeping:** The manager keeps confidential notes of any informal action for reference.

Investigation

- **Objective:** Before taking formal disciplinary action, an investigation must be conducted to establish whether sufficient evidence exists to proceed.
- **Responsibility:** The investigation team typically comprises the employee's line manager and HR manager.
- **Process:**
    - Interview relevant witnesses, gather statements, and collect evidence.
    - Maintain confidentiality throughout.
    - The employee is informed of the outcome within five working days (or notified of any justified delay).

Formal Disciplinary Actions

Written Warning

- **Criteria:** Issued for misconduct that was too serious for informal action but not severe enough to warrant dismissal.
- **Content:**
  - Specifies the complaint and the required improvement, including timescales.
  - Warns that a final written warning may follow if improvement does not occur.
- **Record:** A copy of the written warning is kept on file but may be disregarded for disciplinary purposes after six months of satisfactory conduct.

Final Written Warning

- **Criteria:** If no improvement follows a previous written warning or the misconduct is sufficiently serious to justify an immediate final warning.
- **Consequence:** Further misconduct or lack of improvement may lead to termination.
- **Record:** A copy is kept on file but may be disregarded if the employee's conduct remains satisfactory over the agreed period.

Dismissal for Gross Misconduct

- **Basis:** Certain actions (e.g., theft, fraud, serious security breaches) may constitute gross misconduct, resulting in dismissal without notice.
- **Process:**
  - The employee receives a formal letter detailing the reasons for dismissal.
  - Dismissal takes effect immediately unless there is a pending appeal.

Appeals Against Dismissal

- **Right to Appeal:** The employee may appeal in writing to the board of directors or designated appeal authority within ten working days.
- **Outcome:**
  - The dismissal does not become final until the appeal decision is communicated.
  - The board of directors may review the case and, if necessary, conduct a hearing to make a final determination.

Suspension

- **Purpose:**
  - Suspension may be used while misconduct is being investigated or if the misconduct is potentially gross.
  - It is not in itself a disciplinary action.
- **Authority:** Written approval must be obtained from management to suspend an employee.
- **Process:**
  - The employee receives written notification of suspension, including the reason and duration if known.

- Suspension is typically on full pay unless the employment contract states otherwise.

S. NO.	Annexure - Infromation Security Breaches
1.	Not using the access cards provided to individual employees but using other employee access cards while on the organization premises (tailgating)
2.	Unauthorized use of pen drives/external hard disks/any storage media
3.	Sharing of system/mail passwords
4.	Unauthorized disclosure of internal processes in public places like cafeterias, canteens, etc.
5.	Unauthorized access to computers
6.	Damage to information systems such as laptops, desktops, printers, etc.
7.	Unauthorized modification to confidential data
8.	Disclosure of any confidential information to external parties/vendors, etc.
9.	Disclosure of controlled information without approval, even within the organization
10.	Unauthorized entry into critical computing facilities like server rooms, UPS rooms, etc.
11.	Unauthorized use of desktops and laptops for personal uses like IMs, chats, free downloads, and printing personal information
12.	Printing of confidential information and leaving it at the printers
13.	Usage of official mail for personal purposes
14.	Visitors access unauthorized areas without proper approvals
15.	Leaving confidential papers on individual desks/conference/meeting rooms
16.	Absconding from duties without information
17.	Disclosure of confidential information to competitors
18.	Carrying or taking official equipment home/for personal use without prior approvals
19.	Accessing social media sites
20.	Not reporting security breaches and befriending employees who have breached information/physical security.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya