Disciplinary Governance Policy

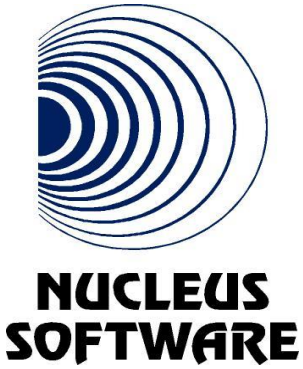

Table of Contents

1. Objective

Nucleus' Disciplinary Governance Policy explains how we address an employee's misconduct or inadequate performance. Employees must be aware of the consequences of their actions. We use this policy to outline our disciplinary procedure.

2. Scope

All employees of Nucleus Software Exports Limited & its group of companies are covered under this policy.

3. Definitions

Service Rules and Regulations are all policies, processes, standards and guidelines under which all employees in the organization will be governed. These include:

- HR Policies
- Administration Policies
- Code of Conduct
- ISMS Policy
- Acceptable Usage Policy
- Electronic Communication Policy
- Criminal Verification Form
- Undertaking
- Declaration
- Finance Policies

Conduct is the behavior and/or actions displayed by an employee in the course of:

- being associated with their job at the workplace
- communicating with colleagues, clients, customers or any other person at the workplace

Misconduct is conduct that is inconsistent with the ethical principles and standards as defined by the service rules and regulations of the organization

Serious Misconduct is misconduct of such an extreme nature that it would be grounds for immediate termination of employment basis a disciplinary process.

Negligence is the deliberate failure to satisfactorily complete job requirements despite having the necessary skills and knowledge and the opportunity to do so. Negligence, particularly if the intention is to cause harm or economic loss to the organization or its customers.

Disciplinary Action Process (DAP) is a formal mechanism to ensure correct and fair treatment for employees who are suspected of committing breaches. The formal disciplinary process should provide for a graduated response that takes into consideration the following factors:

- Nature and gravity of the breach and its impact on business,

- Whether or not this is a first or repeat offence
- Whether or not the violator was properly trained
- Relevant legislation
- Business contracts and other factors as required.

In serious cases of misconduct the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.

The person alleged to have caused the grievance.

4. Categorization

Categorization of breach of service rules and regulations:

I. General Misconduct
II. Poor Performance
III. Long-term absence
IV. Information security breach
V. Network marketing

I. General Misconduct

In case of **misconduct**, a meeting will be conducted with the employee to explain the disciplinary procedure and reasons for initiating it. Suitable disciplinary action will be taken basis the degree of severity of the breach committed.

The procedure will be in line with the Disciplinary Action Process (DAP) as defined in this policy.

- **Corrective Action:** Verbal warning to be issued to the employee by respective BU head and BHR

- **Preventive Action**: Sensitize employees through e-mail communication about the consequences of this act.

In case of repeat/offence of similar nature – Written warning will be issued by HR Head and same to be filed in employee records.

Further repetition shall lead to termination – In case it is a proven offence, committed knowingly.

II. Poor Performance:

Individual Development Plan will be initiated for the employees who are not able to perform.

III. **Long-Term absence**

In case of long-term absence or in case an employee absconds from employment, a separate disciplinary process will be initiated. Process details are mentioned below:

a. Absconding Process

- For an absconding case, the rehire option is 'NO'
- There will be zero notice period served by the absconding employee
- The IBU coordinator, IO of the employee or BHR is required to send the employee, at least 2 enquiry mails for his/her absence, with a time gap of 3 days with reference to the 1st enquiry mail (with all date/time details mentioned & HR Ops team member in loop of the same)
- If there is no response from the employee or employee is not traceable, closure waiver is to be given for maximum of 1 month from the last day when attendance was recorded.
- Notice period liability in this case is automatically waived off on either side.
- Experience / relieving letter will be given to the employee only on receiving the recovery amount
- Status of absconding employee to be communicated to any prospect employer in case reference check is conducted.
- If the employee is traceable within 1 month from the last day (when attendance was recorded) or responds back to HR, then with proper resignation mail/letter (mailer to HR, IO and BU Head) and initiation on NPP, employee will be considered as a normal resignation case.

IV. Breach of Information Security

This includes any form of breach in information security, communication policy or acceptable usage policy including web sense. As soon as an incident is detected or reported, the security manager along with responsible authority will gather the necessary information to define whether the incident requires "disciplinary" action or not.

It is the duty of the security manager to define the scale of disciplinary action on a 4-point rating (4 – Extreme, 3 – High, 2 – Medium, 1 – low) based on the specific incident. Depending on the nature of misconduct/breach, necessary help from external authorities such as police, cyber-crime cells, forensics experts, and/or any other relevant authorities may be sought.

The security manager shall submit the incident related information to the organization, which would in turn, then would decide the fate of employee/service provider on final disciplinary action. It is required that the security manager collect and present evidence for the purposes of disciplinary action in liaison with the HR department.

Desired procedure in case of information security breach is as below:

a) **Preventive Action**: Sensitize employees through e-mail communication about the consequences of this act
b) **Corrective Action**: Verbal warning to be issued to the employee by respective BU Head and BHR
    a. In case of repetition of offence of same/similar nature, written warning to be issued by HR Head and same to be filed in employee records. Further repeats shall lead to termination.

c) In case of a serious breach, related to proprietary / copyright information of the organization, decision will be taken by the Security Manger and HR head and shall amount to dismissal of services as well.

a. Guidelines for Information Security Breach

In general, the rules for evidence cover:

I. **Admissibility of evidence**: whether or not the evidence can be used in court;
To achieve admissibility of the evidence, the organization shall ensure that their information systems comply with any published standard or code of practice for the production of admissible evidence.

II. **Weight of evidence:** the quality and completeness of the evidence.
The weight of evidence provided should comply with any applicable requirements. To achieve weight of evidence, the quality and completeness of the controls used to correctly and consistently protect the evidence (i.e. process control evidence) throughout the period that the evidence to be recovered was stored and processed will be demonstrated by a strong evidence trail. In general, such a strong trail can be established under the following conditions:

a) **For hard copies of documents:** the original is kept securely with a record of the individual who found the document, where the document was found, when the document was found and who witnessed the discovery; any investigation should ensure that originals are not tampered with;

b) **For information on computer media**: mirror images or copies (depending on applicable requirements) of any removable media, information on hard disks or in memory will be taken to ensure availability; the log of all actions during the copying process will be kept and the process will be witnessed; the original media and the log (if this is not possible, at least one mirror image or copy) will be kept securely and untouched.

Any forensics work shall only be performed on copies of the evidential material. The integrity of all evidential material will be protected. Copying of evidential material will be supervised by trustworthy personnel and information on when and where the copying process was executed, who performed the copying activities and which tools and programs have been utilized will be logged.

Laptop Usage Guidelines

Laptop usage guidelines establish best practices for users who are using Nucleus Software owned laptops. The following guidelines must be kept in mind by all the laptop users.

It is the user's responsibility to take appropriate precautions to prevent loss, theft, and/or damage to their laptop and information stored on their laptop

No employee is permitted to carry other employee's laptop without transfer/allocation process

a) Personal laptops are not allowed inside Nucleus Software premises
b) Security is not authorized to keep laptop during office or non-office hours
c) Frisking of bags will be conducted at sign-in/sign-out areas. Disciplinary action will be initiated against an employee found carrying other employee's laptop
d) Do not install any unauthorized software/application on your laptop
e) Do not leave your assigned laptops unattended, including at Workstations/Meeting rooms/Vehicles.
f) Display of Laptop Authorization card is mandatory while carrying the allocated laptop from one unit to another

In case of other queries regarding laptop allocation/ de-allocation, please contact ISS (Extn.1717)

Protection of Evidence

When an information security event is first detected, it is advised to involve a lawyer/police early in any contemplated legal action and take advice on the evidence required. Before the consequences of any indiscipline are identified, it is imperative to secure the evidence.

Evidence may transcend organizational and/or jurisdictional boundaries. In such cases, it will be ensured that the organization is entitled to collect the required information as evidence. The requirements of different jurisdictions will also be considered to maximize chances of admission across the relevant jurisdictions.

V. Network Marketing

It is a business model that depends on person-to-person sales by independent representatives, often working from home. It is also known as **multi-level marketing** (MLM), which is a direct selling method that uses a **network** of people to sell a product or a service.

Desired procedure in case of Network Marketing either practiced in any form or reported by any Nucleite shall involve the following steps:

1. **Report** to BHR / HR Head:
   - The complaint shall be made in writing, inside or outside the office premises during or after office hours using the following listed mechanism to report the matter:
     a. By email
     b. By letter
     c. By phone
     d. By personally meeting BHR/HR Head

   The complaint should cover the following details:
     a. Employee name practicing the same
     b. Brief of complaint
     c. Any witness
     d. Any supporting document, email etc.

2. **Disciplinary Action:**

- Verbal warning to be issued to the employee by respective BU Head and BHR.
- In case of repetition of offence of same/similar nature, written warning to be issued by HR Head and same to be filed in employee records.
- Further repeats shall lead to termination.

3. **Preventive Action:** Creating awareness about Network Marketing & sensitization through e-mail communication about the consequences of such practices.

5. Disciplinary Action Committee

The disciplinary action process as defined in **Section 8**, will be driven a committee, basis the severity of breach.

1. Minor/ BU specific misconduct : BU head along with Business HR and Supervisor
2. Severe or organization level misconduct : HR Head along with BU Head and Global Functional Heads
3. Serious Misconduct : MD, Global Delivery Head HR Head along with BU Head and Global Functional Heads (if required)

6. Types of Disciplinary Action

After a disciplinary hearing, disciplinary actions can be any one of the following:

- Complaint dropped/closed immediately
- Issue a verbal/written/final warning
- Provide counseling or training to help resolve the issue
- Apply a disciplinary penalty, such as demotion or dismissal

Employee's previous records and/or any other special circumstances will be considered while taking any decision.

Disciplinary action other than dismissal: BU head along with Business HR and Supervisor.

If an employee's misconduct is not very high on severity then action, other than disciplinary, shall be taken:

- Transfer employee to another job
- Demote an employee
- Penalty by submitting fine (E.g. not paying their eligible bonus)
- Suspend the employee on full pay during the ongoing investigation where necessary
- Suspend them without pay (May result in loss of employee's services for some time)

The most severe disciplinary penalty is dismissal. This case might arise when:

- Issued warnings, either formal or informal
- In gross misconduct cases, an employee may be able to dismiss without giving notice or pay in lieu of notice. This is called summary dismissal and is generally not recommended.

7. Guidelines:

- This Policy must observe procedural fairness and comply with the laws of natural justice.
- Disciplinary outcomes will be fair and appropriate.
- The rights of staff members must be respected and they will be given the opportunity to exercise these right.
- Investigations into misconduct, and all information related to an investigation are to be kept strictly confidential and should not be disclosed to any person not involved in the investigation process.

8. Changes & Modifications

This policy can only be altered or modified at the sole discretion of the HR Head.

9. Policy Violation

Any violation to any part of this policy shall lead to disciplinary action by the concerned authority.