# Disciplinary Policy

HR-PO726, Ver. 1.4

# Table of Contents

## 1. INTRODUCTION

One of the important guiding principles in Tech Mahindra is responsible corporate citizenship, which expects each associate to align himself/ herself with Tech Mahindra's value system. This document highlights the disciplinary actions that can be initiated against associates for any willful act of commission or omission, which is detrimental to the interest of the Company or if one's behavior is not in alignment with Tech Mahindra values. The organization, despite its pro people practices, would choose to deal sternly with cases of indiscipline or misconduct.

## 2. OBJECTIVE

Formal disciplinary action is warranted when non-compliance takes place. The purpose of this document is to lay down the disciplinary process to be followed in the organization in order to deal with instance/s of indiscipline including non-compliance to information security policies and procedures, by users.

## 3. SCOPE

This policy is applicable to all associates who are on permanent rolls of Tech Mahindra on Indian terms and conditions of employment. It is also applicable to direct and indirect contractors of Tech Mahindra who are on Indian terms and conditions of contract.

## 4. DEFINITIONS

1. "Discipline" means ethical behavior, living by the values of the organization and fairness in dealing. The definition of 'misconduct' is enumerated below:

2. Misconduct means:
   - Failure to obey orders, rules, or instructions, or failure to discharge the duties for which an individual was employed; or
   - substantial disregard of the employer's interests or of the associate's duties and obligations to the employer; or
   - Evincing such willful or wanton disregard of an employer's interests as is found in deliberate violations or disregard of standards of behavior which the employer has the right to expect of an associate; or
   - Carelessness or negligence of such degree or recurrence as to manifest equal culpability or wrongful intent.
   - Failure to comply with the Information Security policies and procedures enforced from time to time.

However, mere inefficiency, unsatisfactory conduct, failure to perform as the result of inability or incapacity, a good faith error in judgment or discretion is not termed as misconduct.

## 5. LEVELS OF MISCONDUCT AND DISCIPLINARY MEASURES

| Level | Definition | Probable disciplinary |
|---|---|---|

| | | measures |
|---|---|---|
| Level 1 | Any act that is not in line with the general conduct that constitutes good corporate behavior including violation of security policy or procedure. | Written warning |
| Level II | Misconducts that has serious consequences but done unintentionally or one of incident or the frequent occurrences of incidents which do not have serious consequences, but does not comply with the expectations of Tech Mahindra from its associates and/or Failure to take corrective action on level 1 warning and/or serious policy violations | Written warning and any or combination of the following:<br>- Penalty (monetary)<br>- Withholding promotion<br>- Withholding of certificates, monetary dues from company's side<br>- Withholding onsite opportunity |
| Level III | Serious misconduct wherein the delinquent associate has been found to have compromised with the values of Tech Mahindra / commitment to customers, internal and external / commitment to investors / reputation of the company and/or failure to take corrective action on written reprimand and/or serious violations of policy and procedures resulting into financial / reputation loss to Tech Mahindra or posing serious security concerns/ affecting Tech Mahindra's market image or having major financial / legal implications. | - Termination of services by way of dismissal |

.

## 6. NATURE OF MISCONDUCT AND DISCIPLINARY ACTIONS

### 6.1 MISCONDUCT - INFORMATION SECURITY GUIDELINES

| Sr. No | Violation Category | Description | Violation Examples | Action |
|---|---|---|---|---|
| 1 | Policy Violation | General violation of Tech Mahindra or Customer or Project Security Policy or Procedure or Guidelines or Requirements. | Bringing or using personal or unauthorized diskettes / CD / DVD / USB Drives / USB Disks / Camera or other unauthorized or personal devices | L I / L II / L III (Depending on Intent / Impact / Extent of Misuse / Possible Impact) |
| | | | Unauthorized photography within or of restricted areas, or information | |
| | | | Retaining unauthorized copies of information without approval (e.g. after project change or closure or after business purpose has ended) or having such information in custody without approval and authorization. | |
| | | | Breach of tolerance policy of customer/s of the Company | Depending upon the |

| | | | | |
|---|---|---|---|---|
| | | | by any employee working on the project of such customer/s | gravity of misconduct . |
| | | | Accessing or providing access to unauthorized persons to restricted areas/ premises without authorization or approvals. | |
| | | Not complying or following customer and Tech Mahindra security processes and policies in management roles. | Not informing the client about user de-allocation in time | |
| | | | Allowing access to information or work area without allocation or customer approval or before fulfillment of security requirements as per contract. | |
| 2 | Misuse of Privileged Access or Rights | Misuse of privileged access or rights or assets or resources. | Accessing for non-business purpose internet sites that are restricted/ hold a security risk as per TechM categories, or accessing the same for non-business purpose if access is provided to the sites as an exception for business purpose or are accessible due to a system/ service error or accessible through other means (e.g. Data Card, Wi-Fi, etc.), or using TechM or customer provided assets or network resources (e.g. customer VPN or internet) for accessing such sites | L II / L III (Depending on Intent / Impact / Extent of Misuse / Possible Impact) |
| | | | Sharing or unauthorized use of individual passwords or credentials or devices (example Security Tokens, ID or Access Cards, etc.) used for authentication or authorization for maintain information security or data privacy | |
| 3 | Violation Leading to Low / Medium Security Impact | Any action or attempt that impacts or could impact TechM or its customers or vendors or other parties information security, business continuity, data privacy or lead to Contractual, Legal, Financial or other business issues. | Bypassing TechM or customer or project or default security controls or restrictions (logical or physical) | L II / L III (Depending on Intent / Impact / Extent of Misuse / Possible Impact) |
| | | | Changing default proxy or system or network or other security related settings without approval | |
| | | | Unauthorized download/ copying/ sharing/ installation/ use of software (freeware / shareware / licensed) including client provided software | |
| | | | Accessing any network/ services/ software/ information within TechM/ customer/ project network by unlawful or unauthorized means | |
| | | | Making unauthorized copy of licensed software or confidential/ copyrighted information (TechM or other parties - external or internal) | |
| | | | Using unauthorized or unapproved means for data transmission or sharing or storage or exchange that could lead to information being leaked (e.g. using Dropbox for storing project data without approval, using personal pen drive for sharing data) | |
| 4 | Violation Leading to Serious Implications or High Security Impact | Any action or attempt that could or that seriously impacts TechM or its customers or vendors or other parties information security, business continuity, data privacy or lead | Accessing illegal sites such as hacking, wares, pornography, software cracks, etc. | L III |
| | | | Downloading/ installing/ storing/ mailing/ printing software cracks or unauthorized license keys or serial numbers, hacking or cracking or illegal or similar software, etc. | |
| | | | Downloading/ sharing/ viewing/ printing/ mailing pornographic or other objectionable material | |
| | | | Violation of Client IPR or Code of Conduct | |

| | | | | |
|---|---|---|---|---|
| | | to Contractual, Legal, Financial or other business issues. | Sharing with unauthorized persons or parties, information that is protected as per law or is critical to customer business (e.g. Personal Information of client's customers) | |
| | | | Gain access to confidential or proprietary information by unlawful or unauthorized means | |
| 5 | Unauthorized Information Disclosure or Extrusion | Data disclosure or movement or copying without approval or authorization. | Disclosing confidential or proprietary information (which includes but is not limited to financial information, new business or product ideas, marketing strategies or plans, employee information or information regarding clients of our customer or vendor, customer list, technical product information, source code or test scripts, application executables, computer or network access credentials or codes, business relationships, etc.) to any unauthorized person or making unauthorized copies of the same or sharing / uploading the same outside TechM or customer domain (e.g. to personal mail, personal storage, internet data sharing sites) without approval. | L III |
| 6 | Malicious Activity | Any malicious activity or action or attempt | Unauthorized scanning of network or hacking or causing denial of service or any malicious activity (example performing an action that leads to malicious software or applications installing or spreading). | L III |
| | | | Implanting logic bombs / malicious code into software or other actions that can impact normal service or business or cause harm or other impact | |
| | | | Spreading virus or malware or unapproved actions causing these to spread | |
| | | | Unauthorised deletion or manipulation of information or actions causing information or assets or services to be lost/ inaccessible/ impacted | |

## 6.2 MISCONDUCT – OTHERS

Given below are some of the misconducts and the suggested disciplinary action to be taken. However the list is not exhaustive and the punitive measures are suggestive under normal circumstances.

| No | Nature of Misconduct | Level of Disciplinary Measure |
|---|---|---|
| 1 | Habitual late attendance, habitual leave, absence without leave | L I |
| 2 | Overstaying leave without obtaining consent for the same from appropriate authority. | L II |
| 3 | Repeatedly forgetting to carry the swipe card/ forgetting to swipe/ not swiping despite carrying the card | LI |
| 4 | Going on leave without proper authorization as per process<br>• Written warning + loss of salary + leave debits | L II |
| 5 | Preaching religious practices within the premises/ through the use of company's facilities or resources/ Sending messages/communication against any caste, religion or race<br>• Warning letter + monetary penalty (Rs.1000/-) | L II |
| 6 | Violating the dress code | L I |
| 7 | Using Company's resources for personal requirements/ Using Company resources or facilities without authorization. | L II / LIII (depending on |

| | | |
|---|---|---|
| | • Use of the printer for printing personal docs – warning letter + Actual cost or Rs.5000 whichever is higher, as penalty.<br>• Use of the telephone/ Auth. Code facility – Warning letter + Actual cost/ Rs.5000/- whichever is higher, as penalty.<br>• Use of bus facilities without approval – Warning letter + Rs.2000/- as penalty<br>• Misuse of email – esp. forwarding chain mails which are not of official nature – Warning Letter + Penalty of Rs.2000/- | impact/ extent of misuse) |
| 8 | Habitual neglect of work<br>• Warning letter + withholding of variable pay and / or increment | L II |
| 9 | • Smoking within TechM campus/premises Warning letter + penalty of Rs.5000/- | L II |
| 10 | Causing willful damage to Tech Mahindra's property<br>• Warning letter + actual costs/ Rs.10,000/- whichever is higher. | L II |
| 11 | Failure to take corrective action post level 1 disciplinary measure.<br><br>Violation of Company Dress Code (2nd instance) – Warning letter + Penalty of Rs.250/- | L II |
| 12 | Copying during internal assessments<br>• ITPians copying in the ITP exams - termination | LII/ LIII |
| 13 | Being under the influence of alcoholic beverages/ banned drugs while on duty. | L III |
| 14 | Willful insubordination or disobedience to any reasonable order of a superior. | L I / L II (depending on impact) |
| 15 | Giving false information regarding one's name, age, qualification or previous service at the time of joining the services of the company | L III |
| 16 | Failure to take corrective action on written reprimand/ post Level II disciplinary action | L III |
| 17 | Violation of TechM's Code of Conduct | L II/ LIII (depending on impact/ extent of damage) |
| 18 | Taking/giving bribes or an illegal gratification whatsoever in connection with Tech Mahindra's business or one's own interests | L III |
| 19 | Threatening, abusing or assaulting any superior or co-worker | L III |
| 20 | Undertaking additional employment whether for any consideration or not/ Operating a business, usurping business opportunities, organized political activity. | L III |
| 21 | Abuse of company policy / facilities | L III |

| | | |
|---|---|---|
| 22 | Theft or fraud in company premises, including material objects as well as critical information asset | L III |
| 23 | Dishonesty with claims/ reimbursements | L III |
| 24 | Sexual harassment | L III |
| 25 | Indulging in hacking | L III |
| 26 | Making statements on behalf of Tech Mahindra without prior authorization or using Tech Mahindra trade names, logos, or trademarks without prior written authorization. | L III |
| 27 | Publicly disparage, defame, slander or otherwise criticize the Company and/or Group Company, its directors or officers, without any valid reasons, in any manner that would damage the business or reputation of the Company, their products or services. | L II/LIII |

The Regional Head – HR and the concerned Business Head/Function Head/Location Head will decide upon the punitive action to be initiated depending upon the fact of the matter and its impact on business, Company's reputation or its Value System.

## 7. DISCIPLINARY COMMITTEE

A Disciplinary Committee consisting of 3-4 senior members representing the location shall be formed.

The Committee shall generally look into Level 3 misconducts or any level of misconduct escalated to it and which need interpretation and application of collective wisdom of the members in order to arrive at decision on disciplinary measures.

The Committee shall be responsible for examining the nature of misconduct, the evidence recorded; findings of the investigation carried out and arrive at a decision as to the disciplinary measures to be initiated against the delinquent associate/s.

## 8. PROCESS OF INVESTIGATION

### FOR LEVEL I

As soon as the incident is reported, the line manager/HR shall carry out the investigation and if the allegation is true, the associate will be given a written warning by HR and the incident will be recorded in the personal file. The case shall also be recorded by HR in the Discipline Diary maintained at the location as well as in the associate records.

### FOR LEVEL II

As the incident gets reported, HR/ other concerned functions shall carry out an investigation. A report shall be prepared on the methodology of investigation and the findings of the same. The associate involved shall be given an opportunity to defend himself/herself against the charges. If the associate is found guilty, the level and quantum of punitive measures shall be decided by the Location HR Head in

consultation with the Functional Head/ Business Unit Head, where need be. The case shall be recorded by HR in the Discipline Diary and associate records.

**FOR LEVEL III**

For misconducts in the category of Level III, the disciplinary committee shall carry out a detailed enquiry and prepare a report. The investigation shall be done in a completely confidential manner. Once the findings are arrived at, the associate concerned shall be given the opportunity to defend the charges leveled against him. The Disciplinary Committee will deliberate and arrive at a decision as to the disciplinary measure to be initiated. The decision so arrived at by the Disciplinary Committee would be final and all concerned shall abide by the same. The decision will be communicated to the delinquent associate and subsequently implemented. The case shall be recorded by HR in the Discipline Diary and associate records.

## 9. COMMUNICATION OF DISCIPLINARY ACTION

The person facing the disciplinary action should be communicated, wherever applicable, in writing the following:

- Incident and violation.
- Required corrective action.
- Consequences of repeating the violation and/or failure to take corrective action.

## 10. DISCIPLINE DIARY

The HR function shall maintain a Discipline Diary to record the disciplinary cases during the year. The Discipline Diary shall include the following information:

- Person against whom disciplinary action is initiated
  - Employee No.
  - Associate Name
  - Associate Designation
  - Department/Project
- Person initiating the disciplinary action
  - Line Manager
  - Level of misconduct
  - Nature of misconduct [in detail]
  - Disciplinary action taken
  - Any deviation from standard procedure with reasons for deviation
- Person authorizing the disciplinary action
  - In case of Level I and II of disciplinary actions: Any/all levels of supervision and Management
  - In case of Level III of disciplinary actions: Disciplinary committee members

## 11. POLICY REVIEW

The policy will be owned by HR who will be responsible for making suitable amendments, if any, from time to time.

## 12. DOCUMENT HISTORY

| Version | Date | Author (function) | Reviewed by | Approved by | Nature of changes |
|---|---|---|---|---|---|
| Issue 1.0 | 23 Aug 2013 | HR | Function Head | Function Head | Change of Policy Template |
| Issue 1.1 | 01 Feb 2018 | Salonee Dhingra | Murali Madhav | Phanindra Kuruganty | Updated Nature of Misconduct (Section 6) |
| Issue 1.2 | 8 May 2018 | Sweta Gope | Roshan Zameer | Phanindra Kuruganty | Updated Nature of Misconduct (Section 6) |
| Issue 1.3 | 15 Feb 2019 | Amoolya Nekkanti | Roshan Zameer | Phanindra Kuruganty | Updated Misconduct – Others (Section 6.2) |
| Issue 1.4 | 23 Jul 2019 | Saloni Aswani | Chitersen Yadav | Sudhanshu Bhatnagar | Updated Misconduct – Others (Section 6.2) |

## 13. APPENDIX: ANNUAL REVIEW HISTORY

| Annual Review Conducted On | Version Reviewed | Is Change Required (Y/N) | Document Uploaded in BMS (Date) | Remarks |
|---|---|---|---|---|
| 01-06-2016 | 1.0 | N | 27 June 2016 | Annual review conducted. |
| 15-09-2017 | 1.0 | N | 18th Sep, 2017 | Annual review conducted. |