



PC and Laptop Policy

Issued On –July 14, 2015
Version – 1.0



सवाल आपका है

Policy Nomenclature

Policy Title: PC and Laptop Policy

Policy Authorizer: COO

Decision



Cognizant Officer (Person handling queries relating to the policy):

Name: Kishore Karmakar

Department: IT

Email Id: Kishore.Karmakar@ibc24.in

Extension:125

Table of Contents

S.NO.	Topic	Page No.
1.0	Objective	4
2.0	Scope	4
3.0	Criteria for Evaluation	4
4.0	Laptops Approval	4
5.0	Security and Usage	5-6

1.0 Objective

- a) To lay down appropriate guidelines on issuance of Desktop/Laptop,
- b) Data Card & Email Id to the employees upon joining & during the course of their employment with SBMMPL.
- c) To ensure appropriate usage of these facilities.
- d) To ensure proper management & security of these facilities.

2.0 Scope

It applies to all permanent & temporary employees of IBC24.

3.0 Criteria for Allocation

3.1. **Laptops** – The Laptops shall be issued to the employees:

3.1.1. All HODs

3.1.2. Sales Staff

And, to the employees handling the following nature of jobs:

3.1.3. Employees who travel frequently as part of their jobs & require laptops for their meetings.

3.1.4. Employees who require computers after office hours.

3.2. Data Card shall be issued to all those employees who have been issued a laptop.

3.3. Desktop/Workstation shall be issued to the employees/ multiple employees whose role requires them to be in office for more than 80% of their times & to those who do not require access to computers during field working hours.

3.4. Email Id shall be issued to all employees of IBC24 during their tenure of service with the company.

4.0 Laptops Approval - The issuance of laptop shall require go through an approval process.
IBC24 - PC and Laptop Policy ,

4.1. For all HODs & Sales Staffs, necessary approvals to be taken from the HR Head.

4.2 For cases where the need is defined by the nature of the job, the approval has to be taken from the department head, HR Head & the COO. In such cases, requisition along with the justification of need has to be mandatorily mentioned.

5.0 Security & Usage - Employees are expected to use the given facilities in wise & judicious manner. For a number of reasons, employees are also expected to ensure security.

5.1. Desktop/Workstation

5.1.1. Employees are expected to switch off their desktops while leaving from the Office.

5.1.2. For security reasons, the employees are expected to lock their systems while leaving their workstations.

5.1.3. The user shall not upload his personal data on the desktop/Workstation/Network Storage or any other system or location.

5.2. Laptop & Data Card

5.2.1. It is the employee's responsibility to take appropriate precautions to prevent loss/damage/ theft of the laptop & data card.

5.2.2. The laptop will be configured with the standard format & requirements, the user shall get them updated from IT on time to time basis. It is the user's responsibility to inform IT on regular intervals.

5.2.3. The employee is not allowed to download games, videos, software & any data of personal use on the laptop/Desktop/Workstation.

5.2.4. The employee shall refrain from accessing any non official website on the Laptop.

5.2.5. The employee shall maintain monthly backups to avoid any data loss for added security.

5.2.6. The user is responsible for the data security & therefore shall check the installed anti-virus from time to time for renewing them.

5.2.7. Ownership of the laptop will reside with the company & the employee shall return.

5.2.8. The user is expected to use data card for official purpose only.

5.2.9. Cases of Loss/ Theft due to employee's negligence:

5.2.9.1. Cases of Loss/ Theft shall be immediately reported to IT & HR.

5.2.9.2. Claims for insurance shall be done by the organization in such cases.

5.2.9.3. However, if the claim is rejected by the insurance company, the cost of laptop shall be recovered from the employee.

5.2.9.4. The excess amount deducted by the insurance company while settling the claims shall be recovered from the employee.

5.3. Email Id

5.3.1. The employee shall use his official email id only for official communications & not for personal communications & vice versa.

5.3.2. The user shall send mails up to a maximum size of 5MB.

5.3.3. The user shall check & empty his junk/ spam folder on a regular basis.

5.3.4. In case the user suspects a phishing email, he is expected to report the same to IT department at the earliest.

5.3.5. In case of multiple users handling one system, the employee shall access his email using webmail account.

5.3.6. Each time the employee log into webmail, he is expected to log it out after Usage.

5.3.7. The employees shall change their passwords on a regular basis for added data security.

IT / HR reserves the right to alter/ amend/ modify the policy at any time without prior intimation.