Classification: Confidential

IMS

SWIGGY

LAPTOP POLICY

INFO
SEC

Document Control

Document #	Laptop Policy	**Approved By**	Praseed Nair
Version	3.0	**Reviewed By**	Gajanan Kulkarni
Classification	Internal	**Created By**	Shreya Hota
Approved on	18/07/23	**Status**	Approved

Disclaimer

1. Do not forward or copy data in part or full without explicit permission of Infosec Team
2. At a minimum, this procedure will be reviewed/updated annually
3. Change history must be updated when any edits are made to the document
4. Please contact infosec@swiggy.in to request changes to the document

Revision History

Version	Date	Approver	Author	Change Description
3.0	18 July 2023	Praseed Nair	Shreya Hota	Reformatted as per ISO standard
2.5	09 July 2022	Rajeev Kumar	Gajanan Kulkarni	No changes
2.4	09 July 2021	Rajeev Kumar	Gajanan Kulkarni	Miner changes in formatting
2.3	10 July 2020	Rajeev Kumar	Gajanan Kulkarni	No Change
2.2	10 July 2019	Rajeev Kumar	Gajanan Kulkarni	No Change
2.1	*13 July 2018*	Rahul Jaimini(Director)	Gajanan Kulkarni	No Change
2.0	13 July 2017	Rahul Jaimini(Director)	Gajanan Kulkarni	Miner changes
1.0	20 Aug 2016	Rahul Jaimini(Director)	Harshith Gowda	First Version

Access List

List of Users	Access Type	Type of Media	Retention Period
Steering Committee	Read	Soft Copy	Default
INFOSEC Team	Read/Write/Modify	Soft Copy	Default
Employees	Read	Soft Copy	Default

TABLE OF CONTENTS

1.0 Purpose:

This document serves to outline Bundl Technologies Pvt Ltd. & It's subsidiaries *(called as "The Company" hence fourth in the document) policy on the use and storage of company provided laptops and that are being used for official purposes. The policy intends to minimise Company exposure to information security risk as well as increase the user's personal safety and safeguard the company's hardware investment.

The Company relies heavily on its ability to access up-to-date and complete business information; the loss or unauthorised modification of data on portable devices can impact heavily on the company's ability to function effectively or management's ability to make informed business decisions. It is therefore essential for all laptop users to adhere to the contents of this policy.

2.0 Scope:

This policy applies to any laptop owned and used for Company. Resources to conduct Company business or interact with internal networks and business systems, whether owned or leased by The company, the employee, or a third-party employee, contractors, consultants, temporary, and other workers at Company and its subsidiaries are responsible for exercising judgment regarding appropriate use of information and company data security in accordance with Company policies and standards, and local laws and regulation.

3.0 Applicability:

This policy and the procedures herein applicable for all employees, contractors, interns, vendors and who all use Company provided laptops for official purposes.

4.0 Policy Guidelines:

i). Eligibility

The Company & Its subsidiaries Employees will be provided with a laptop as it is essential to their productivity and function. When issued with a company laptop, users accept to abide to the company's laptop usage policy. Laptops shall be provided to employees purely at the discretion of the management. The decision of the management to provide an employee with a laptop or a desktop shall be based on the following factors

1. The nature of the employee's job (e.g. need to operate system simultaneously along with other official interactions)

2. Their working environments/conditions (whether or not they have permanent/individual office space)

3. The criticality of an employee's availability outside of working hours.

Keeping in view these factors certain position at Company shall be provided with below company owned laptops models on a priority basis:

Laptop Model	Designation
Dell/Lenovo/HP (i3,4Gb,500/256Gb SATA/SSD)	Franchise Partners, 3PL, Any non-Tech vendor
Dell/Lenovo/HP(i5,8Gb,500Gb SATA/SSD) (Laptop & Desktop)	Rest all
Dell/Lenovo/HP(i7,16Gb, 256/512Gb SSD) (Laptop & Desktop)	A-Team, Heavy excel/applications users
Dell/Lenovo/HP (i7,8Gb, 256/512Gb SSD) (Premium laptop)	Sr. Management team
Mac Book Pro	A-team/Technology
Mac Book Air	PMs / Non-Tech Grade 11 & Above

ii) Issuance & Registration

All employees that are provided with company owned laptop shall be required to undergo the laptop issuance and registration procedure as per onboarding and Access management policy & procedure. Upon issuance, the IT Executive shall ensure that the laptop is equipped with all necessary security software

No one can use personal laptop for official use in any circumstances. In case of exceptions it would require Department head & CTO (Chief Technology Officer) approval with risk acceptance form.

iii). Intended Use of Laptops

Every laptop user must ensure that the laptop is being used only for official purposes and in the course of the rightful discharge of their duties and not for generating, transmitting, corresponding any content that is contrary to company policies. This may lead to the user being subject to disciplinary or any other appropriate action as per company policies.

An employee using company provided laptops is responsible for the security of that laptop, regardless of whether the laptop is used in the office, at one’s place of residence, or in any other location such as a hotel, conference room or while travelling.

5.0 Laptop Security Controls:

All laptops acquired for employees on behalf of the company shall be deemed company property. Each employee issued with a laptop and shall be responsible for the security of that asset, regardless of whether the asset is used in the office, at the employee’s place of residence, or in any other location such as hotel, conference room, car or airport. Laptop and users shall ensure security of the laptop in each of the following domains as per the stated guidelines.

i). Physical Security, Theft & Lost Prevention

In order to ensure physical security of laptops and data therein, all laptop users are required to undertake the following actions:

1. The physical security of company provided laptops is the user’s personal responsibility. He/she is therefore required to take all reasonable precautions, be sensible and stay alert to the risks.

2. Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended laptop.

3. Never leave the laptop unattended when using it outside the office.

4. Lock the laptop away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel.

5. Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.

6. Carry and store the laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage.

7. Keep a note of the make, model, serial number and the Company asset label of your laptop but do not keep this information with the laptop.

ii). Data Security Controls

Laptop users are expected to ensure the security of the data within their laptops. In this regard, they are to adhere to the following:

1. Ensure all laptops are configured for domain, choose a long, strong encryption password/phrase and keep it secure.

2. You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone.

3. Corporate laptops are provided for official use by authorized employees. Do not loan your laptop or allow it to be used by others.

4. Avoid leaving your laptop unattended and logged-on. Always lock or log off before walking away from the machine.

iii). Virus Protection

Viruses are a major threat to valuable organizational data and laptops are particularly vulnerable if their anti-virus or similar solution is not kept up-to- date. In this regard employees are to ensure the following in order to safeguard their systems from potentially harmful viruses.

1. The anti-virus or similar solution MUST be up-to-date.

2. Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.

3. Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically if your virus definitions are up to date, but you can also initiate manual scans if you wish to be certain.

4. Report any security incidents (such as virus infections) promptly to the IT Help in order to minimize the damage

5. Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting the IT Helpdesk. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

6. Be especially careful to virus-scan your system before you send any files outside the organization.

iv). Data Backups

Company Employees are responsible for maintaining an appropriate backup of their laptop, especially of the work-related documents and data files created during the normal course of your job responsibilities. It is prudent and expected that Employee establish a process of copying the data files he/she use on the laptop to other than “C” drive storage area (or other appropriate network storage) as an added precaution against data loss.

v). Use of Unauthorized Software /Content

1. Company laptop users are required to ensure that they do not download, install or use unauthorized software programs. Unauthorized software could introduce serious security vulnerabilities into Company network as well as affecting the working of your laptop. Software packages that permit the computer to be ‘remote controlled’ (e.g. PCAnywhere) and ‘hacking tools’ (e.g. network sniffers and password crackers) are explicitly forbidden on Company equipment unless they have been explicitly pre-authorized by IT for legitimate business purposes.

2. The user shall not install any unauthorized accessories/software like messengers, chatting, addons software or any malicious software, which may cause problems to the functioning of the Laptop and strictly adhere to Company’s software usage policy.

3. If there is damage on account of the above the user will be liable to pay the damages at cost to the Company/the same will be deducted from their monthly salary.

All changes to the policy will be at the discretion of the company.

6.0 Disposal of Laptop:

The following procedures shall be followed for the disposal of Laptop:

- All data existing on the Laptop shall be deleted by the IT team through secure methods such as wiping the hard disks.
- The IT team shall format the hard drive of all laptops and desktops before disposal/ re – assignment of the devices to a different employee.
- All application and configuration data shall be cleared from servers by the IT team prior to disposal or movement of the devices outside Company premises.

Decommission policy for IT hardware devices are as below:

a) For laptops, the device should be decommissioned after 3 to 5 years as per device health

b) For desktops, the device should be decommissioned after 4 to 5 years as per device health

c) For printers, the device should be decommissioned after 5 years

7.0 Insurance policy, procedure and guidelines:

All Company Laptops shall get cover in Insurance once they procured

In case of accidental damage of Laptop, User shall immediately (within 24hrs) intimate to IT department by Email to it-insurance@swiggy.in / it-support@swiggy.in and filling Company Insurance claim form

In case of loss and theft of the laptop, user shall immediately intimate to IT department by Email to it-insurance@swiggy.in / it-support@swiggy.in and user shall also responsible to get an FIR from Police station and submit the same within the 48 working Hrs of the incident to IT department for further process of Insurance

IT department shall process the incident by filling Insurance incident report form (Click here to download the form). with third party vender to claim Insurance and maintain a register with all the details for Incidents (e.g. Unique incident number, date, etc.)

IT department shall process Insurance claim within the timeline of 7 working days which will result in to whether an Asset will cover under insurance or not

User shall responsible for the over and above expenses than claim received from Insurance vender and difference amount shall be debited from the User's salary or full and final settlements

In case of Insurance got rejected due to User negligence act, User shall be responsible to pay as per OEM costing and depreciation cost in case of loss/Damage of the laptop

Click here to view Insurance document

Users shall adhere that loss or damage or theft for Non-insured assets like peripherals/essentials (e.g. charger, data card, hard disk, pen drive, etc.) shall be user's responsibility and it could lead to deduct the amount (to be worked out by the Finance department of the company) from user salary

Users shall take utmost care to protect the Company Laptop as well as peripherals/essentials and shall actively participate and contribute to the information security initiatives taken up by Company.

Absconding

Once IT department receives or intimated regarding absconding cases of the organization IT department shall responsible to share list of assets allocated to User with their Serial numbers and approx. cost to HR team and Legal team.

8.0 Disclaimer:

IT Compliance Team of Bundl Technologies reserves all rights and is the exclusive owner of all intellectual property rights over this information security policy and procedure document. This information security policy and procedure document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as floppy diskettes, hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior written consent from the Head of IT.

9.0 Acronyms Used:

Acronym	Expanded Form
EUC	End User Computing team
*BUNDL Technologies	Bundl Technologies Pvt Ltd & It's Subsidiaries/Swiggy
NO ONE	Any of Employee, Contractors, Interns, trainees, etc.
HO IT	Head of IT
CTO	Chief Technology Officer
CT -IT	Compliance Team - IT
3PL	Third Party Logistic partners