BUNDL TECHNOLOGIES Pvt. Ltd

IT Service Delivery

IT ADD-ON DEVICE ALLOCATION MANAGEMENT POLICY & PROCEDURE

Title of work:	ADD-ON Device allocation & Management Policy	Year of Creation of Work:	**2020**
Category:	Internal	Full Date of Publication:	03 Dec 2020
Version:	1.2	Total Pages:	8
Description:	This document will provide details about assigning add-on IT devices to BTPL resources	Reviewed by:	IT Head, HR Head & InfoSec
Author:	IT Compliance	Approved by:	IT Head (Raman K)

DOCUMENT CONTROL INFORMATION

Ver. Rev #	Page No / Section	Description of Change	Author	Reviewed By	Approving Authority	Date of Release
1.2	All pages	No Changes	IT-Compliance	IT Head, HR Head & InfoSec	IT Head (Raman K)	1st Dec 2022
1.1	All pages	No Changes	IT-Compliance	IT Head, HR Head & InfoSec	IT Head (Raman K)	3rd Dec 2021
1.0	All pages	First Version	IT-Compliance	IT Head, HR Head & InfoSec	IT Head (Raman K)	3rd Dec 2020

REFERENCES: Requirement of ISO/IEC 27001:2013, SSAE 16, SOC 1, SOC2.

TABLE OF CONTENTS

1.0 Purpose

The purpose of this document is to ensure proper process in place for provisioning better end user experience while working remotely & making ease of processing office work with compatible handy devices. This policy provides brief understanding about Add-on IT asset provisioning, de provisioning and management.

2.0 Scope

The policy only includes add-on IT devices such as special laptops, mobile phones and tabs for the usage by the employee of the company.
This policy shall be applicable for eligible employees and allocation would be based on business requirement along with appropriate business justification from functional head.

3.0 Policy

- Add-on devices shall be allocated on need to have basis with valid business justification
- Allocated device would be registered in the name of Swiggy / BTPL
- Add-on devices shall be allocated only to eligible personals
- Every request must be approved from requestor's functional head
- One employee shall be assigned only one add-on device in their tenure with BTPL
- Allocated device shall be hardened as per infosec team guidelines and policies
- All devices shall be enrolled with Swiggy's device management tool
- Allocation of device shall be subject to availability & stock of requested device
- Employees shall be responsible for the application installed on the allocated device. In case of malicious applications found to be present in the device, then the device would be isolated pending action from the Infosec team.

4.0 Guidelines

Each employee must ensure that the device 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 add-on devices is responsible for the security (Physical) of that device, regardless of whether the device 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.

Keep a note of the make, model, serial number and the Swiggy asset label of your add-on device however, do not keep this information with the same device.

Corporate add-on devices are provided only for official use and for authorized employees. Do not loan your device or allow it to be used by others

Employees are solely responsible for maintaining backup of the data stored in their allocated device

Employees are required to intimate the Infosec via email team before taking the allocated device outside of India.

If the device is found to be in use outside of India without prior intimation to the Infosec team, then the same would be treated as a security breach and the device will be made non-functional.
Employees must use their Swiggy ID as device registration ID(Eg: Apple ID, One drive ID, Google ID)

5.0 Exceptions

Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the Employee. These may arise, for example, because of local circumstances, conditions or legal reasons existing at any point of time.

Exceptions to the Information Security Policy may have to be allowed at the time of implementation of these policies and procedures or at the time of making any updates to this document or after implementation on an adhoc basis based on business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.

All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through an Exception E-mail sign-off on the same shall be maintained including ad-hoc requests.

BUNDL Technologies shall also list parameters to ensure that before acquiring new applications or other software and hardware, the set of applicable policies and guidelines shall be matched with the available security mechanisms of the product to ensure that the product has the necessary features. If not, then exceptions shall be approved before acquiring the desired product. Similarly, while developing new applications, the necessary security policies and guidelines have to be incorporated in the application or exceptions shall be obtained for the same from the IT Compliance Team

6.0 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.

7.0 Acronyms Used

Acronym	Expanded Form	Acronym	Expanded Form
Functional Head	The person heading department	BTPL	Bundl Technologies Pvt. limited
Swiggy	BTPL		

END