BUNDL TECHNOLOGIES Pvt. Ltd

INFORMATION SECURITY

Electronic Data Disposal & Media Management policy

Title of work:	Bundl Technologies	Year of Creation of Work:	**2019**
Category:	Internal	Full Date of Publication:	March 2019
Version:	1.2	Total Pages:	6
Description:	Describes management of Electronic Data	Reviewed by:	Praseed Nair – (GM InfoSec)
Author:	Gajanan Kulkarni (IT-Compliance)	Approved by:	Rajeev Kumar – (AVP-IT)

If this volume is lost or stolen, the holder must immediately notify HO IT & Compliance Dept of Bundl Technologies. If found, please return to HO IT & Compliance Dept of Bundl Technologies, please contact IT compliance Office of Bundl Technologies, for clarifications, comments, and suggestions with respect to any matter in this document.

DOCUMENT CONTROL INFORMATION

Ver. Rev #	Page No / Section	Description of Change	Reference	Author	Reviewed By	Approving Authority	Date of Release
1.2	All pages	No Change	CR-2020-03	Gajanan Kulkarni	Praseed Nair – (GM InfoSec)	Rajeev Kumar – (AVP-IT)	07 May 2022
1.1	All pages	No Change	CR-2020-03	Gajanan Kulkarni	Rajeev Kumar – (AVP-IT)	Rajeev Kumar – (AVP-IT)	07 May 2021
1.0	All pages	First Version	CR-2020-03	Gajanan Kulkarni	Rajeev Kumar – (Director-IT)	Rajeev Kumar – (Director-IT)	09 March 2020

This document shall be review & updated at least annually or as an when it is required.

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

TABLE OF CONTENTS

1.0 Purpose 4
2.0 Scope 4
3.0 Policy 4
4.0 Procedure 5
5.0 Consequences 5
6.0 Definations 5
7.0 Disclaimer .....
8.0 Acronyms Used 6

1. PURPOSE:

Data confidentiality is a critical part of legal and ethical concern. The purpose of this policy is to provide for proper cleaning or destruction of sensitive/confidential data and licensed software on all computer systems, electronic devices and electronic media being disposed, recycled or transferred either as surplus property or to another user allocation.

2. SCOPE:

Swiggy employees and other covered individuals (for e.g. but not limited to vendors, independent contract Employees, etc.) in their handling of Swiggy's data, information and records in electronic form during the course of conducting Swiggy business (Eg. administrative, financial, Analytical, Product, Customer care, technological, or service).

3. POLICY:

The Swiggy requires that before any computer system, electronic device or electronic media is disposed, recycled or transferred either as surplus property or to another user, the system, media or device must be either:

- properly sanitized of Swiggy sensitive/confidential data and software, or
- properly destroyed.

Any official Swiggy records must be appropriately retained / disposed based on the Swiggy's internal requirements & needs prior to erasure or destruction of the system, device or media.

The specific procedures and requirements to be followed when cleaning or destroying computer systems, electronic devices and electronic media.

3.1 Sanitization practices to be followed:

- Before assigning any new Laptop/Desktop/server or any IT Asset to new User/project, the asset shall be hardening with appropriate method
- For any IT Assets (laptop/Desktop/servers/Network devices/printer, etc.) allocation of existing devices, IT team shall ensure low level formatting/factory reset is done before allocating.

4 PROCEDURES:

- Clearing: Overwriting the media
- Purging: Magnetic erasure of the media
- Destruction: Physical destruction of the media
- All electronic storage media should be sanitized when it is no longer necessary for business use, provided that the sanitization does not conflict with Swiggy data retention policies.
- All electronic storage media should be sanitized prior to sale, donation or transfer of ownership. A transfer of ownership may include transitioning media to someone in your department with a different role, relinquishing media to another department, or replacing media as part of a lease agreement.
- All Swiggy employees are responsible for the sanitization of non-reusable electronic media before disposal. Similar to shredding paper reports, CDs and other non-rewritable media should be destroyed before disposal.
- All Business unit heads are responsible for the sanitation of all WMU owned electronic devices and computer systems in their units prior to removal from a department. This responsibility may be delegated within the Swiggy as deemed appropriate.
- Any disposal of computer equipment and media storage devices must comply with all surplus disposal procedures

5. CONSEQUENCES:

Employees, Contractors and anyone who violate this Swiggy policy may be subject to disciplinary action for misconduct and/or performance based on the administrative process appropriate to their employment.

Personals who violate this Swiggy policy may be subject to proceedings for compliance misconduct based on criticality of the incident.

6. DEFINITIONS:

These definitions apply to these terms as they are used in this document.

Sanitization (of computer hard drives)	Removing data on a system through one or more various methods that may include overwriting or erasing data.

7. 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.

8.0 Acronyms Used

Acronym	Expanded Form	Acronym	Expanded Form
Contractors	Any third-party employees or Vendors	CT -IT	Compliance Team - IT
Lead	Lead- IT Infrastructure	HO IT	Head of IT
EUC	End User Computing	BUNDL Technologies	Bundl Technologies Pvt Ltd

END