

BUNDL TECHNOLOGIES PRIVATE LIMITED

Information Security



Data Breach Policy

Title of work:	Information Security - Data Breach policy	Year of Creation of Work:	2021
Category:	Internal	Full Date of Publication:	01 June 2021
Version:	1.0	Total Pages:	10
Description:	Describes Data Breach Policy & action plan	Reviewed by:	Head of IT,Legal,HR
Author:	IT Compliance Team	Approved by:	Head of IT,Legal,HR

Copyright, 2021. BUNDL TECHNOLOGIES PRIVATE LIMITED, All Rights Reserved, This internal document is the property of Bundl Technologies Pvt. Ltd (Company). All use, disclosure, distribution, and/or reproduction not specifically authorized by HO IT & Compliance Dept of the Company (HOIT) are prohibited. The information contained in this document is proprietary & internal and is intended for use only by the person to whom it is specifically issued in the first place. This document is not to be loaned to anyone, within or outside the Company. Copying or distribution of this document without consent of HOIT is unauthorized and illegal.

If this volume is lost or stolen, the holder must immediately notify HOIT & Head Legal of the Company. Please contact HO IT for clarifications, comments, and suggestions with respect to any matter in this document.

TABLE OF CONTENTS

1.0	<u>Policy Statement</u>	4
2.0	<u>Responsibilities</u>	5
3.0	<u>Definition</u>	6
4.0	<u>Procedure</u>	6
5.0	<u>Disclaimer</u>	9
6.0	<u>Acronyms Used</u>	9

1. Policy Statement

The aim of this Policy is to standardise the response towards any data breach and ensure that they are appropriately logged and managed in accordance with the best practices and applicable laws including Information Technology Act, 2000 (as amended from time to time), so that:

- Data breach incidents are swiftly reported.
- Data breach incidents are recorded and documented
- Data breach incidents are investigated in a timely manner and appropriate actions are taken thereon
- Steps are taken for impact assessment and curative measures thereof to avoid repetition.
- Data breach incident and measures taken are reported to the management

COVERAGE:

This Policy shall cover all employees of the Company and its subsidiaries and any third party personnel having access to information technology (IT) infrastructure of the Company.

2. Responsibilities

Incident Type	Incident Owner	Description	Responsibility
Stolen/Lost IT Assets	Service Delivery	Incidents relating to loss of any IT Asset	Data breach management Committee & InfoSec team
Cyber security breach	InfoSec	Incident related to any IT Policy Violation compromise of user account or IT systems, loss of data in any way whatsoever	
Physical security	Admin	Incidents where physical security gets compromised (Eg. tailgating/unauthorised access to premises)	
Data breach	InfoSec	Incidents related to any breach of data including but not limited to confidential data, personally identifiable data, proprietary information amongst others	

3. Definition

Data Breach: A breach of data security leading to the unauthorized or unlawful acquisition, destruction, loss, alteration, disclosure, access or use of data or information that compromises the confidentiality, integrity or availability of information maintained in Company's computer resources which includes without limitation transmitted, stored or processed data

4. Procedure

If you witness any instance of violation of InfoSec policy, report immediately at infosec@swiggy.in.

Security Incident team shall review all such reported incidents and shall form a report with recommendations, which shall be presented before the Data security Management committee (Committee) for decision.

The Committee shall consist of following members shall be responsible for implementing this Policy:

Head of Human Resource

Head of IT/InfoSec

Head of Legal

This procedure as shall be followed by the Committee in different instances of data breach is as follows:

- Security Incident team shall raise the violations / incidents with a detailed report to the Committee for deciding the way forward in a manner provided under InfoSec Security Incident Guidelines.
- All high risk and critical cases action plans shall be reviewed and confirmed by the Committee.

The aim of the Committee shall be to ensure that where data breach has occurred, the incident is properly reported, investigated and necessary actions are taken to rectify the situation in a manner detailed above.

A data security breach can come in many forms, but the most common forms are as follows:

- Loss /theft of paper or other hard copy(Eg. Legal documents, HR Documents hard copy)
- Data posted or mailed to the incorrect recipient
- Loss or theft of equipment (IT asset, personal mobile, etc.) on which data is in use in any manner
- Cyber attacks
- Unauthorized data transferred to personal cloud, email, physical media, or any other form of storage
- Unescorted visitors accessing data
- Unauthorized data disclosure/theft from covered individuals
- Non-secure disposal of data

4.1 Data Breach Categorisation & Action Plan:

Data breaches are categorised into three different categories of criticality - Red, Orange and Yellow as detailed in the below Table. Please note in case of data breach incidents not covered below, the same shall be categorized by the Committee in its sole discretion.

Violation Category	Specific Violation		
	Red (High)	Orange (Medium)	Yellow (Low)
Data Security Privacy	Password sharing / confidentiality not maintained with respect to passwords	Leaving Computer Unlocked in non-compliance of IT Policies	
	Stealing ID/Password by any fraudulent method	Documents lying unattended in office, printer area	
	Sharing Company's sensitive and confidential information with external agents competitors/individuals by any means	Using/Downloading Unauthorised Software	
	Usage of Company's desktop/laptop/tablet as a server to share unauthorised and confidential information		
	Transferring/Storing Company's information on unauthorized external storage devices.		
	Violating norms of recording, capturing(photograph) of meetings/slides		
Information Security Services	Misuse of Office Communication System	Trying to solve hardware issues by unauthorised support services	
Physical Security	Sharing access card with unauthorised people		Staff not using their access cards while entering-following others

Further, note that InfoSec Security Incident Guidelines shall be followed at all times whilst dealing with any data breaches in a manner provided above.

4.2 Action Plan:

This policy serves as a guide that may be considered for disciplinary action against offenses committed. However, basis seriousness of offence, it will be at the discretion of management to apply a severity level as well as choose an appropriate disciplinary action

Category	Instances and Associated Functions
Red	1st offence - Termination from Service
Orange	1st offence - 2nd level formal written warning letter
	2nd Offence - Termination
Yellow	1st Offence - 1st Level Formal Verbal Warning
	2nd offence - 2nd level formal written warning letter
Yellow	3rd Offence - Termination

5.0 Disclaimer

Bundl Technologies Pvt Ltd 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.

6.0 Acronyms Used

Acronym	Expanded Form	Acronym	Expanded Form
Security Incident	Any security event occurred to BTPL Information	Evidence	Required documentation as a proof of Security Incident
IT Head	Heading BTPL IT	Swiggy	BTPL
Direct & Indirect Employees	On-roll/off-roll and anyone who is working or processing or dealing with Swiggy's information	BTPL	Bundl Technologies Pvt Ltd. (Swiggy)

END