
# Data Breach Policy

# Document Control

| | | | |
|---|---|---|---|
| **Document #** | Data Breach Policy | **Approved By** | InfoSec Head, HR Head, Legal Head |
| **Version** | 1.2 | **Reviewed By** | GRC Head |
| **Classification** | Public | **Created By** | GRC Team |
| **Approved on** | 10/07/2025 | **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 | Author | Reviewer | Approver | Change Description |
|---|---|---|---|---|---|
| 1.2 | 10/07/2025 | GRC Manager | GRC Head | InfoSec Head, HR Head, Legal Head | Periodic review |
| 1.1 | 10/07/2024 | GRC Manager | GRC Head | InfoSec Head, HR Head, Legal Head | Company name and logo change |
| 1.0 | 18/07/2023 | GRC Manager | GRC Head | InfoSec Head, HR Head, Legal Head | Initial Document |

**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 |

# Acronyms Used

| Acronym | Expanded Form | Acronym | Expanded Form |
|---|---|---|---|
| PII | Personally Identifiable Information | | |
| Swiggy | Swiggy Ltd. | | |
| HR | Human Resources | | |
| Swiggy Ltd. | Swiggy and all of its subsidiaries | | |
| | | | |

# Review

This document shall be reviewed on an annual basis or as per the need.

# INDEX

## Contents

# 1 Introduction

## 1.1. DOCUMENT OBJECTIVE

The purpose of this policy is to establish a clear, structured framework for detecting, reporting, assessing, responding to, and resolving all actual or suspected data breaches involving Company Information Assets and Personally Identifiable Information (PII).

This policy ensures compliance with regulatory obligations (e.g. India DPDP Act, etc.), contractual requirements, ISO 27001:2022 (especially A.5.24 Information Security Incident Management), ISO 27701:2019 (specific requirements for PII Controllers and Processors), and PCI DSS (requirements for handling Cardholder Data).

## 1.2. SCOPE

This policy applies to:

- All Swiggy Ltd. employees, contractors, third-party workers, and business partners with access to Swiggy's systems and data.
- All information assets, including systems, networks, applications, and physical documents, used or owned by Swiggy Ltd.

## 1.3. Roles and Responsibilities

| ***Role*** | ***Responsibility*** |
|---|---|
| ***All Employees/Contractors*** | *Immediate reporting of any suspected data breach to the InfoSec Team to InfoSec@swiggy.in* |
| ***Security Incident Response Team (InfoSec team)*** | *First response, triage, containment, and initial investigation. Coordination with the DPO and Legal.* |
| ***Data Protection Officer (DPO)*** | *PII Breach assessment, determination of regulatory reporting obligations (DPDP, etc.), and managing communication with regulatory bodies.* |
| ***Head of Information Security*** | *Owner of the Incident Response Process. Ensures compliance with ISO 27001 requirements (Incident Management).* |
| ***Legal/Compliance Team*** | *Review and approval of external communications, notifications, and adherence to legal requirements.* |

## 1.4. REFERENCE DOCUMENT

1.4.1. IMS_IT Security Policy
1.4.2. ISO/ IEC 27002: 2022
1.4.3. ISO/IEC 27701: 2019

## *1.5. DEFINITIONS*

### 3. Definitions

| ***Term*** | ***Definition*** |
|---|---|
| ***Data Breach*** | *A security incident that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, transmitted, stored or otherwise processed data (Information Assets and PII).* |
| ***PII Breach*** | *A Data Breach specifically involving* ***Personally Identifiable Information****, requiring notification under PIMS (ISO 27701) principles.* |
| ***Cardholder Data (CHD)*** | *All data on the payment card (primary account number, expiration date, service code) and sensitive authentication data (SAD) like CAV2/CVC2/CID/PIN data (PCI DSS).* |
| ***Incident Response Team (IRT)*** | *The designated group of personnel responsible for managing the breach, typically led by the Head of Information Security.* |

# 2 Data Breach Response Procedure

2.1. The response process must follow a structured, multi-phase approach:

### *Phase 1: Preparation (ISO 27001:2022 A.5.24)*

- **Training:** Ensure all staff are trained on incident reporting procedures.
- **Resources:** Maintain up-to-date contact lists for the IRT, DPO, regulators, and third-party forensic specialists.
- **Testing:** Conduct annual **incident response simulations/drills** to test the effectiveness of this policy.

### *Phase 2: Detection and Reporting (ISO 27001:2022 A.5.26)*

- **Immediate Action:** Any personnel who suspects a data breach must **immediately report it** through the designated **InfoSec channel (e.g., dedicated email)**.
- **Logging:** The InfoSec team must ensure all events are **accurately recorded** from the moment of detection, including date, time, system, and observed impact.

### *Phase 3: Assessment and Triage (ISO 27001/27701)*

- **Severity Assessment:** The InfoSec Team determines the severity and impact, identifying the affected systems, data types, and volume.
- **PII Breach Identification (ISO 27701):** The DPO must quickly determine if the breach involves **PII** (e.g., customer names, addresses, financial IDs) and if it is likely to result in a **risk to the rights and freedoms of data subjects**.
- **CHD Identification (PCI DSS):** If the breach involves the **Cardholder Data Environment (CDE)**, the SIRT must immediately engage the **designated PCI contact** and follow specific forensic procedures.

### *Phase 4: Containment and Eradication*

- **Containment:** Isolate affected systems, segment networks, and disable compromised accounts to limit further damage.
- **Forensics:** Engage internal or external **digital forensic experts** as required, especially if CHD or high-value PII is involved.
- **Eradication:** Remove the root cause of the breach (e.g., patch vulnerability, remove malware, reconfigure access control).

### *Phase 5: Notification and Communication (ISO 27701)*

| ***Recipient*** | ***Notification Requirement*** | ***Deadline*** |
|---|---|---|
| ***Supervisory Authority (e.g., Data Breach Committee)*** | *Mandatory if the PII breach is likely to result in a risk to the rights and freedoms of individuals.* | *As per applicable regulation (e.g., within 72 hours under GDPR).* |
| ***PII Principals (Data Subjects)*** | *Mandatory if the PII breach is likely to result in a high risk to the rights and freedoms of individuals.* | *Without undue delay.* |

| ***Recipient*** | ***Notification Requirement*** | ***Deadline*** |
|---|---|---|
| ***Acquiring Banks/Payment Brands*** | *Mandatory if Cardholder Data is known or suspected to be compromised (PCI DSS).* | *Immediately upon confirming CHD involvement.* |
| ***Internal Management*** | *Inform the Steering Committee and senior leadership.* | *Within 24 hours of confirmation.* |

### *Phase 6: Recovery and Post-Incident Activity*

- **System Restoration:** Restore systems from secure backups, ensuring the vulnerability is fully mitigated.
- **Control Enhancement:** Implement corrective and preventive actions to prevent recurrence, ensuring alignment with the continual improvement goals of the IMS.

## *6. Policy Compliance and Review*

Compliance with this policy is mandatory. Failure to comply may result in disciplinary action up to and including termination of employment or contract. This policy shall be reviewed annually, or sooner if significant changes occur to regulatory requirements or the organizational security posture.