Breach Notification Procedure

Domain:	Data Privacy
Document Owner:	Data Protection Officer (DPO)
Document Approver:	Top Management
Version #:	1.0
Effective Date:	13-07-2021

Version History:

Release Date	Version No	Change Description/ Reason	Created / Revised by	Approved by
13-05-2022	1.0	First Copy	Pavan Agrawal	Harish Arora

1.0 PURPOSE:

The purpose of this procedure is to define the process of reporting / notifying the breaches, especially data privacy related breaches, internally and externally as applicable.

2.0 SCOPE:

This procedure applies to all types of breaches, including information security and personal data, which may occur within Organization.

3.0 TERMS AND DEFINITIONS:

Information Security	:	Confidentiality, Integrity, Availability of information.
DPO	:	Data Protection Officer
Security Event	:	A security event is a change in the everyday operations of a network or information technology service indicating that a security policy may have been violated or a security safeguard may have failed.
Info Sec Incident	:	An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of any information security related policy.
Security Breach	:	A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach may be intentional or unintentional.
Data Breach	:	A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. A data breach may be intentional or unintentional.
Personal Data Breach	:	A data breach involving personal data or personally identifiable information of any living person or individual. Personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Data Subject	:	Data Subject is an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an

identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Supervisory Authority : 'Supervisory Authority' means an independent public authority which is established by a Member State pursuant to Article 51 of GDPR. 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority;

4.0 RESPONSIBILITIES:

- Responsibility of implementing this policy shall be with DPO.
- Responsibility of reporting or notifying breaches related to Personal Data, internally or externally, shall be with DPO.

5.0 PROCEDURE:

5.1 Identification of Breaches

- The breaches are identified through monitoring of various activities, logs, events etc. which shall be proactively done by concerned Teams handling the monitoring activities. Breaches identified through such monitoring mechanisms shall be reported to Incident Response Teams through Incident reporting mechanism defined by Organization.
- The breaches shall also be reported by users, employees, contract staff, temporary staff etc. Such breaches shall be reported through incident reporting mechanism designed by Organization.
- The breaches may also be reported by external parties such as customers, vendors, suppliers, service providers etc. Such breaches shall be reported to immediate contact within the Organization by the external party, who then may inform DPO about the breach.
- All types of breaches identified shall be responded, addressed and resolved following incident response processes defined by Organization. Primary responsibility of handling breaches shall be with Incident Handling Teams such as IT Team, Cloud Team, Application Team etc.

- Wherever any breach involves personal data or is suspected to impact personal data, the Data Protection Officer (DPO) shall be informed immediately. DPO shall be involved in the entire process of breach resolution and reporting wherever personal data is involved or impacted.

5.2 Internal Reporting of Breaches

- Any personal data breach, reported through any possible method within Organization, shall be reported to Management immediately or atleast within 12 hours of detection / identification of breach.
- Reporting responsibility shall be primarily with concerned Incident Handling Team. For Personal Data related breaches or breaches impacting personal data, DPO shall be involved along with Incident Handling Team.
- Reporting of breaches shall be done through email or in person or through formal reporting format, as defined by Organization.
- For Personal Data related breaches, minimum information to be covered while reporting is -
    - Nature of Data Breach,
    - Where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,
    - The likely consequences of the personal data breach,
    - Measures taken or proposed to be taken to address the personal data breach,
- Timely reporting of breaches, and update on the actions being taken shall be provided to Management during the breach management process.
- Post containment of breach, detailed report with possible causes and corrective actions shall be presented to Management for their information and guidance.

5.3 External Reporting of Breaches

- External reporting requirements for the breaches, shall be identified and determined through –
    - Legal Requirements (Laws, Acts, Regulations applicable)
    - Requirements of Supervisory Authorities, if applicable, in case of Personal Data related breaches.

- Contractual Obligations (Requirements, Terms, Clauses and Conditions which are laid down within Contract or Agreement between Organization and any external party. Such external party may be Customer, Supplier, Service Provider, Outsourced Contractor etc.)

- Based on the external reporting requirements identified, the responsibility of making such reporting / notification shall also be identified and assigned. For Personal Data related breaches Data Protection Officer (DPO) shall be responsible to handle the external reporting and notification.
- The external reporting or notification for Personal Data related breaches, shall include minimum information such as –
  - Nature of Data Breach,
  - Time, Date etc. of reporting / identifying breach,
  - Where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned,
  - The likely consequences of the personal data breach,
  - Measures taken or proposed to be taken to address the personal data breach,
  - Where appropriate, measures taken or proposed to be taken to mitigate the possible adverse effects of personal data breach,
  - The name and contact details of the data protection officer (DPO) or any other relevant contact person where more information can be obtained.
- Periodical updates shall be provided to external party, during the period of containment / resolving the breach.
- After the breach has been resolved, detailed report specifying why the breach occurred (causal analysis) and what actions have been planned / taken to avoid re-occurrence (corrective / preventive actions) shall be submitted to external party (as applicable).
- The personal data breaches shall be reported to below entities / parties, as applicable –
  1. **Supervisory Authority** – The breaches shall be reported to applicable Supervisory Authority, immediately without any undue delay but within maximum time limit of 72 hours from the time of breach occurrence.
  2. **Joint Controller –** Identified Joint Controller or Party who may have provided the personal data to Organization, if applicable. Such communication / notification shall be done by Organization immediately, without any undue delay, from the time of breach occurrence.
  3. **Data Processor / Data Sub-Processor –** Notifying any third party or entity who may be acting as Processor / Sub-Processor while handling personal

data, about the personal data breach based on applicability. Such notification shall be made immediately, without any undue delay, from the time of breach occurrence.

4. **Data Subjects / Individuals -** Notifying Data Subjects or Individuals to whom the personal data belongs. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, Organization shall consider communicating the personal data breach to the data subjects or individuals, whose personal data is being processed. Such notification / communication shall be done with immediate effect, without any undue delay, from the time of breach occurrence. Wherever notifying data subjects may seem to be disproportionate in efforts, Organization shall consider releasing public communication or similar measure thereby ensuring that the data subjects are informed in equally effective manner.

- The responsibility of identifying the breach notification requirements and executing the same shall be with Data Protection Officer (DPO) designated by Organization.
- DPO, in consultation with Top Management wherever required, shall issue formal notification or reporting to external party, informing them about the breach which has occurred and actions being taken to contain the breach and restore the impacted / affected system back to normal.
- Regular updates shall be provided to concerned external party by DPO till the time breach is completely resolved and operations are restored to normal.
- Post resolution, causal analysis and corrective action / preventive action planning shall be done for the breach and updates shall be provided to external party as applicable.
- Records of communication shall be maintained, as applicable, by DPO.

6.0 REFERENCES

- Incident Management related Policy / Procedure
- Breach Notification Form

7.0 DOCUMENT REVIEW:

- This document shall be reviewed at least once in 12 months, from the date of initial release or revision, to check suitability and adequacy.