PDS INFOTECH PVT LTD

Data Breach Policy

Ref No: ISMS/PDS/5.2/21.1

1. Scope

- Security incidents involve the wrongful handling or disclosure of information and may give rise to data breaches where personal data is involved. Although this policy concentrates on personal data breaches, it applies equally to security incidents generally, including containment, investigation, improvement actions, and lessons learned.
- Personal data breaches may occur through error (in operation or judgement), resulting in the wrongful disclosure or loss of personal data. The primary focus of this policy is personal data, although most of the same considerations apply to other sensitive information, including commercially sensitive or confidential business data.
- Much of the information the Company handles is sensitive, and it is essential that all personnel take special care to ensure it is handled correctly, in compliance with Company procedures and applicable legal obligations. Information must be classified and handled in accordance with the Company's Information Classification and Management Policy. The Company will consider disciplinary action where instructions for handling personal data are not followed; malicious intent or action will be treated accordingly.
- Most data breaches under consideration here are likely to be human-error incidents, where personal information belonging to a customer, employee, or other data subject is sent to the wrong recipient or disclosed by mistake. However, this policy applies to all breaches, whether caused by staff or by system failure (automation error, poor design, malfunction, or failure).

The procedures below cover: (a) action to contain the incident in the event of a data breach; (b) the decision on internal escalation and notification; (c) actions to investigate the breach and its short- and longer-term mitigation, including accurate incident logging; and (d) action to be taken in respect of the individual(s) responsible for the breach, where applicable.

2. Actions to Be Taken in the Event of a Data Breach

2.1 Immediate Notification

- When any member of staff becomes aware that personal information has inadvertently been sent to the wrong person or otherwise disclosed, lost, or compromised, they must immediately inform:
  - Their line manager and the designated privacy lead.
  - In their absence, a Director, the Information Security Committee, or the senior manager present.
- Failure to notify immediately on discovery significantly increases the Company's risk and exposure and may result in disciplinary proceedings.
- Staff should seek advice as above before taking any remedial action on their own initiative.

2.2 Initial Investigation

- The designated privacy lead, or another individual nominated by the Information Security Committee, will carry out an initial investigation of the data incident to establish the timeline, facts, and scale, and will inform Directors and relevant stakeholders on whether a data breach has occurred, along with recommendations.
- This initial investigation should ordinarily be undertaken within 24 hours of the data incident being reported, and should include an initial assessment of the risks to the individual(s) affected.

2.3 Managing the Incident — The CARE Approach

- Contain — take immediate action to prevent further disclosure or damage.
- Assess — pause and plan by considering the scale and impact of the breach.
- Respond — put the plan into action, having considered the available options.
- Evaluate — reflect on and report the success of the actions taken, and consider next steps or further action.

2.4 Line Manager Actions

- The line manager of the staff member involved in the data breach should, as soon as practical and once authorized, carry out the following:
    - Consider whether the Communications team should be informed, in the event the incident may become public knowledge or reach the media.
    - Contact whoever received the information by mistake and request that they return or delete it, as appropriate, and confirm that this has been done. Establish whether it has been further disclosed.
    - Inform, by email, the individuals whose personal data has been sent to the wrong destination (referred to as "data principals" under the Digital Personal Data Protection Act, 2023), and offer to speak with them personally.
- The notification email to affected data principals should include:
    - The line manager's or designated privacy lead's name and contact details.
    - The estimated time of the breach, a summary, and the type of information disclosed.
    - The measures taken or planned to retrieve the information, with a commitment to inform the individual once this is done and to keep them updated on developments.

2.5 Full Investigation and Reporting

- The designated privacy lead should conduct a full investigation of the data breach and report findings to the Directors within one week of the initial investigation. The findings should include:
    - A full description of the nature, cause, and timing of the data breach.
    - Identification of the data principal(s) affected, and any data processors involved.
    - An assessment of the risks to the individuals concerned.
    - The cause(s) and process failures behind the breach, and the individual(s) responsible, where applicable.
    - Remedial action already taken, planned future actions, and timescales.
    - A recommendation on regulatory notification (see Section 3).

2.6 Questions to Address

- Was the individual involved sufficiently trained, including completion of the Company's security awareness training?
- Was the prescribed procedure followed? Is that process functioning as intended?
- What checks took place to support the success of the process?

2.7 HR Involvement

HR should be kept informed of all developments, so that they can advise the lead investigator and provide support to staff involved in the incident.

2.8 Follow-Up with Recipients

If the recipient who received the information by mistake has not responded within 48 hours, they should be contacted again by email and phone, with attempts logged. This cycle should be repeated until a resolution is reached.

3. Regulatory Notification

- Under the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025, the Company must notify the Data Protection Board of India, upon becoming aware of a personal data breach. Affected data related principals must also be notified, describing the nature of the breach, the data involved, protective measures, and the Company's contact details for queries.
- The designated privacy lead is responsible for coordinating all regulatory notifications and maintaining evidence of timely compliance.

4. Roles and Responsibilities

- Designated Privacy Lead: Leads investigation, coordinates regulatory notification, and reports to Directors.
- Line Managers: Take immediate containment action and notify affected data principals in coordination with the designated privacy lead.
- Information Security Committee: Oversees this policy, nominates investigators, and reviews lessons learned.
- HR: Supports staff involved and advises on disciplinary matters where relevant.
- Communications Team: Manages any public-facing or media communication arising from a breach.
- All Personnel: Report suspected breaches immediately and cooperate with investigations.

5. Review

This policy shall be reviewed at least annually, or upon significant organizational or regulatory change, to ensure continued alignment with ISO/IEC 27001:2022, and the Digital Personal Data Protection Act, 2023.