PDS INFOTECH PVT LTD

Data Breach Policy

(Ref No. ISMS/PDS/5.2/21)

Scope of this policy

1. **Security Incidents** (SI) involve wrongful handling or disclosure of information and can give rise **Data Breaches** where personal data is involved. Although this policy concentrates on personal data breaches, the policy equally applies to SIs, including containment, investigation, improvements and lessons.

2. Personal data breaches may occur as an error (in operation, or judgement) where the result has been the wrongful disclosure, or loss of private personal data. The primary focus is on personal data, although most of the same considerations apply to other sensitive data, for example containing commercially sensitive information.

3. Much of the information we deal with is sensitive and it is essential that all IPSA staff take special care to ensure it is handled correctly in compliance with our procedures and legal obligations. IPSA information is generally classified as OFFICIAL, and may be OFFICIAL SENSITIVE and where necessary protective marking should be obvious and supplied with handling instructions. IPSA will consider disciplinary action where instructions for handling personal data are not followed. Malicious intent and actions will be treated accordingly.

4. Most data breaches under consideration here are likely to be human error incidents, where personal information belonging to one or more MPs or members of MPs' staff is sent to someone else or published by mistake. However, all breaches, whether staff related or system related (automatic, poor design, malfunction or failure), including redaction, will use this policy.

5. The procedures outlined below cover:

- Action to be taken to contain the incident in the event of a data breach.
- Decision on whether Project Manager & Director should be notified, and then following reporting ICO procedures in a timely manner.
- Actions to investigate the breach, and short- and longer-term mitigation. In particular to accurately capture the incident and record the log entries.
- Action to be taken in respect of the individual(s) responsible for the breach.

Actions to be taken in the event of a data breach

8. When any member of staff becomes aware that personal information has inadvertently been sent to the wrong person, he or she must inform:

- Their Line manager and the Data Protection Officer.
- In their absence, the , a Director or the senior manager present.
- Failure to notify immediately on discovery significantly increases risk and exposure for IPSA and may result in disciplinary proceedings.

9. Staff should seek advice (see 8 above) before taking any remedial action.

10. The Data Protection Officer, or another individual nominated by the Senior Information Risk Owner (), will carry out an initial investigation of the data incident to establish the time line, facts and scale and inform the , and other Directors, on whether a data breach has occurred and any recommendations.

This investigation should ordinarily be undertaken within 24 hours of being informed of the data incident. It should include an initial assessment of the risks to the individual(s) affected.

11. Manage the incident using the CARE approach:

- Contain – immediate actions to prevent further disclosure or damage
- Assess – to pause and plan by considering the scale of the breach
- Respond – putting the planning into action having considered the options
- Evaluate – to reflect and report on the success of the actions and consider next steps or further more assertive action.

12. The line manager of the member of staff who has committed a data breach should carry out the following actions as soon as practical and Authorised:

- Consider if the Communication Manager should be informed in the event the incident may become public knowledge or available to the media, who will also consider briefing the Minister for Data Protection (Dept. DCMS).

- Contact whoever received the information by mistake and ask them either to return or delete it, depending on which is appropriate. They should also be requested to confirm that this has happened. Has it been further disclosed?

- Inform by email the people whose personal data has been sent to the wrong destination, and offer to speak to them personally. (They are referred to as “data subjects” below, as shorthand). The email should contain:

    - The line manager’s name and contact details.
    - Estimated time of breach, a summary, information type disclosed ○ The measures that have been, or will be taken to retrieve the information, with a commitment (a) to inform them when this has happened, and (b) to keep them informed of any developments.

13. The Data Protection Officer should then conduct a full investigation of the data breach and report the findings to the Directors within a week of the initial investigation. The findings should include the following:

- A full description of the nature, cause, and timing of the data breach.
- Identification of the data subject(s) affected, and controllers/processors.
- Assessment of the risks to the individuals concerned.
- The cause(s), process failures, of the breach and the individual(s) responsible.

- Remedial action already taken, future actions to be taken, and timescales.
- A recommendation as to whether the ICO needs to be informed.

14. Common Questions to address, and which will likely be asked by the ICO:

- Was the individual sufficiently trained, and had they completed the Civil Service Learning cource on Information Management?
- Was prescribed procedure followed? Is that process functional?
- What checks took place to support success of the process?

15. 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.

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