This Data Breach Notification Policy ("Policy") applies to all employees, contractors, and third parties of ABS Company ("Company"). It establishes the procedures for the immediate reporting, investigation, and communication of any unauthorized access, loss, or disclosure of sensitive Company data in compliance with applicable data protection regulations, including the UK Data Protection Act 2018 and the EU General Data Protection Regulation (GDPR).

**1. Immediate Reporting of Data Breaches**

* **Employee Responsibility:** Any employee or contractor who suspects or becomes aware of a data breach must report it immediately—no later than **within two (2) hours** of discovery—to the designated Incident Handler, David Parker, via email (dparker@abscompany.com) or phone extension 1234.
* **Initial Report Details:** The report should include the nature of the breach, affected systems or data, suspected cause, time of occurrence, and any mitigating actions taken.

**2. Internal Management and Investigation**

**Incident Handler Role:** David Parker will lead the breach response team and coordinate all actions to contain, analyze, and remediate the breach.

**IT Team Responsibilities:** The IT department will:

* Isolate affected systems to prevent further data loss.
* Preserve evidence for analysis and regulatory requirements.
* Assess the technical cause and scope of the breach.

**Legal Team Responsibilities:**

* Evaluate legal obligations under relevant data protection laws.
* Advise on notification obligations to regulatory authorities and affected individuals.
* Prepare any required reporting documentation.

**Communications Team Responsibilities:**

* Draft and review external and internal communications to ensure consistent, clear messaging.
* Coordinate with stakeholders to manage public relations and media inquiries, if applicable.

**3. Notification Timelines**

* **Regulatory Notification:** The Company must notify the relevant Data Protection Authority **within 72 hours** of becoming aware of the breach, unless the breach is unlikely to result in a risk to individuals’ rights and freedoms.
* **Individual Notification:** When the breach poses a high risk to affected individuals (such as exposure of sensitive personal data), ABS will:
  + Notify those affected as soon as possible.
  + Provide clear information on the nature of the breach, potential consequences, and measures taken to mitigate harm.
  + Offer guidance on protective steps individuals should take.

**4. Documentation and Follow-Up**

* All breach reports, investigation findings, and notifications shall be documented and stored securely by the Incident Handler.
* A post-incident review will be conducted to determine root causes and implement improvements in data security and breach prevention.
* Training and awareness programs will be updated accordingly.

**5. Compliance and Accountability**

* Failure to report or properly manage data breaches may result in disciplinary action, including termination.
* This Policy will be reviewed annually or following significant incidents to ensure compliance with evolving legal requirements and best practices.

*By adhering to this Policy, ABS Company commits to safeguarding personal and sensitive information, maintaining trust, and fulfilling its legal obligations in data protection.*

Picture of signature

Olivia Wilson

Manager