Data Breach Notification Policy Template

This sample template outlines the process and responsibilities for notification in the event of a data breach affecting online services. Adjust the content to meet your specific requirements and regulations.

1. Purpose

The purpose of this policy is to establish protocols to promptly notify affected parties and regulatory bodies in the event of a data breach related to our online services.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who have access to sensitive user data processed or stored by our online services.

3. Definition

- **Data Breach:** Any unauthorized access to, disclosure of, loss, or theft of personal data held by the organization.

4. Responsibilities

- **Information Security Team:** Investigate, assess, and contain breaches.
- **Data Protection Officer (DPO):** Assess the risk of the breach and lead communication efforts.
- **All Staff:** Report suspected or confirmed breaches immediately.

5. Data Breach Notification Procedure

1. **Incident Identification**
   Any staff member who becomes aware of a potential data breach must immediately report it to the Information Security Team or DPO.
2. **Containment and Assessment**
   The Information Security Team will assess the scope and impact of the breach and take steps to contain it.
3. **Risk Evaluation**
   The DPO will evaluate the risks associated with the breach, including the types of data involved and potential harm to individuals.
4. **Notification**
   - **Regulatory Authorities:** Notified within legal timeframes as required (e.g., within 72 hours under GDPR).
   - **Affected Individuals:** Notified without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
5. **Documentation**
   All breaches, regardless of severity, must be documented in the breach register.
6. **Review and Remediation**
   After resolution, conduct a post-incident review and update security measures as necessary.

6. Notification Content

Notifications to affected individuals should include:

- A description of the breach
- Types of data affected
- Likely consequences of the breach

- Measures taken or proposed to address the breach
- Contact information for further inquiries

7. Record-Keeping

All data breaches must be recorded in the breach register, including facts about the breach, its effects, and remedial action taken.

8. Review

This policy will be reviewed annually or after any significant data breach.

9. Contact

Role	Name	Email
Data Protection Officer	[Name]	[Email]

Version: 1.0
Last Updated: [Date]