Data Breach Policy

Purpose:
The purpose of this Data Breach policy is to establish the goals and the vision for the breach response process.

Scope:
This policy applies to all the employees and customers of Our Organisation that have been onboarded to the platform.

Policy:
As soon as a theft, data breach, or exposure containing Our Organisation Sensitive information or protected data is identified, the process of removing all access to that resource will begin.

The CEO/CTO of Our Organisation will chair an incident response team to handle the breach or exposure. The team includes:

- IT Infrastructure Team.
- Finance Team.
- Legal Team.
- Human Resources Team.
- The affected employee whose data has been breached.
- If required, a few additional team members who are related to that data.

The CEO/CTO of Our Organisation will be contacted about the theft, breach, or exposure. The IT team will examine the breach or exposure to determine the root cause.

Any Our Organisation employee found in violation of this policy will be subjected to disciplinary action, up to and including termination of employment. Any third-party client/partner organization found in violation will have their contractual work terminated if any are active.

1.1 Identify a Personal Data Breach/Suspected Personal Data Breach.
There are several reasons why there can be a breach of personal data

For example:

- Loss or theft of computer hardware or information, on which data is stored or accessible.
- Loss or theft of paper files.
- Hacking attack.
- Inappropriate access controls allowing unauthorized/unnecessary access to data.
- Equipment failure.
- Human error.
- Unforeseen circumstances such as a fire or flood.

1.2 Reporting an Incident
It is vital that as soon as a Personal Data Breach is identified or suspected it is immediately reported to the IT Security team. To improve our understanding of the risks to data and address them before breaches occur, we would also encourage individuals to report ‘near misses’ (i.e. situations where a data breach would have occurred but for a miracle or "luck"). Near misses should be reported in the same way as a real breach, with the distinction that it was a near miss made very apparent. The General Data Protection Regulation requires that all relevant breaches are reported to the supervisory authority (the Information security head) ‘without undue delay, not later than 72 hours after having become aware of it’.

As much information as is immediately available should be collated and should be completed and emailed to security@[companydomain. com] as soon as possible and within twelve hours of the breach being identified at the very latest.

The Data Protection Officer (DPO) along with his team will analyze the form, update the Personal Data Breach Log, and ascertain whether any immediate corrective/containment/escalation actions are required.

1.3 Investigating an Incident

Depending on the type and severity of the incident the Data Protection Officer along with his team will assess whether a full investigation into the breach is required. Where required the Data Information Security Officer along with his team will appoint an appropriate investigation team who will complete a full breach report.

The investigation will:

- Determine the incident's nature, the types and quantities of the data involved, and the identities of the data subjects.

- Take into account the size of a breach and the sensitivity of the data at stake.

- Perform a risk assessment.

- Identify actions the organization needs to take to contain the breach and recover information.

- Analyze the ongoing risk and the steps necessary to stop the incident from happening again.

1.4 Reporting Breach to the Information Commissioner or Data Subject

The Data Protection Officer will coordinate breach reporting to the Information Commissioner within 72 hours of becoming aware of a relevant breach. The DPO will also evaluate whether the breach is ‘likely to result in a high risk to the rights and freedoms’ of the data subject. If this is found to be the case, the occurrence will also be immediately disclosed to the data subjects. Any such report will be coordinated by the Data Protection Officer and his Team. Assistance will be required from other teams including Marketing and Communications, and the Print Room and should be made available on demand.

A risk to people’s freedoms can include physical, material, or non-material damage such as discrimination, identity theft or fraud, financial loss, and damage to reputation. When assessing the likelihood of the risk to people’s rights and freedoms, Our Organisation will consider:

- The type of breach.

- The nature of the data, as well as what it indicates about certain people.

- How much data is involved?

- The individuals involved (e.g. how many are involved, how easy it is to identify them).

- How bad the consequences for the individuals would be and the nature of the Our Organisation's work and the resultant severity of a breach.

1.5 Escalation

The Personal Data Breach Log will be reviewed regularly by the CEO/CTO who will determine whether any updates to Policy and Procedures are required, and coordinate any training and communications messages from the lessons learned. They may escalate a breach to the Board of Directors if required.

1.6 Timescales for Notification to Supervisory Authority

- Where a notifiable breach has occurred, Our Organisation will notify the Information Commissioner Officer (ICO) without undue delay and at the latest within 72 hours of it becoming aware of the breach. If notification is made beyond this timeline, Our Organisation will provide the ICO with reasons for the same.

- If it has not been possible to conduct a full investigation into the breach to give full details to the ICO within 72 hours, initial notification of the breach will be made within 72 hours, giving as much detail as possible, together with reasons for incomplete notification and an estimated timescale for full notification. Following the initial notification, the ICO will get additional correspondence asking them to supply the remaining information.

1.7 Content of Breach Notification to The Supervisory Authority

The following information will be provided when a breach is notified:

- A description of the nature of the personal data breach including, where possible; the categories and an approximate number of individuals concerned and the categories and an approximate number of personal data records concerned.

- The name and contact information of the data protection officer, who can provide more information.

- A description of the personal data breach's likely effects.

- An explanation of the steps taken—or those proposed—to handle the personal data.

- Breach, including, when necessary, the steps taken to lessen any potential negative repercussions.

1.8 Timescales for Notification to Affected Individuals

- Where a notifiable breach has occurred, which is deemed to have a high risk to the rights and freedoms of individuals, Our Organisation will notify the affected individuals themselves i.e. the people whose information was compromised, in addition to the supervisory authority. This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

- A situation with high risk can be one in which identity theft is a serious concern right away or in which certain types of data are made public online.

1.9 Content of Breach Notification to The Affected Individuals
When a breach is reported, the following details will be given to the impacted parties:

- A description of the nature of the breach.

- The name and contact details of the data protection officer where more information can be obtained.

- The anticipated effects of the personal data breach are described, along with.

- A description of the measures taken, or proposed to be taken, to deal with the personal data.

- Breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

1.10 Record of Breaches

Our Organisation records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It documents the facts about the breach, its consequences, and the corrective measures implemented.

ENFORCEMENT

We expect all employees to comply with this policy and any related policies, standards, processes, procedures, and guidelines. Failure and/or refusal to abide by this policy may be deemed a violation. Compliance with the policies will be a matter of periodic review by the Information security officer / Information Security Team. Any employee found to have violated this policy may be subject to disciplinary action, as deemed appropriate by management and Human Resources policies.

- **Monitoring:** The company employs appropriate technology solutions to monitor policy/ procedure compliance.

- **Self-Assessment:** The CEO/CTO are required to conduct self-assessment within their areas of control to verify compliance with this policy/ procedure.

- **Security Audits:** Internal Audit may assess the implementation of and compliance with this policy/ procedure as part of its audit program.

SPECIAL CIRCUMSTANCES AND EXCEPTIONS

All exceptions to this policy/ procedure will require a waiver explicitly approved by one of Our Organisation's CEO/CTO.