**DATA INCIDENT or BREACH**

**NOTIFICATION POLICY**

|  |  |  |  |
| --- | --- | --- | --- |
| Document owner | |  | |
| Document scope | |  | |
| Last updated | |  | |
| Next review | |  | |
| Revision | **Description of change** | **Author** | **Effective Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Purpose.** This Breach Notification Policy specifies COMPANY's procedure for handling data breaches. The goal of this policy is to ensure that we respond appropriately to data breaches and provide necessary notifications in accordance with applicable laws. Adhering to this policy helps to prevent further harm resulting from a data breach. It ensures that those affected are informed on how to protect themselves.

**Scope.** This policy applies to all personal and sensitive data controlled or processed by COMPANY, regardless of format. It covers all employees, contractors, consultants, temporary staff, or any other individual or entity acting on behalf of COMPANY. COMPANY adheres to data privacy and protection laws such as United States, California, Virginia, Utah, International GDPR, GDPR-UK Canada. All COMPANY employees and staff must report actual or potential data protection compliance failures. The individual in charge of this Policy is the DPO, who holds overall responsibility.

This Policy applies to all COMPANY employees, part-time employees, and independent contractors. The DPO will conduct an annual review and monitoring of the Policy to ensure its effectiveness, relevance, and adherence. As needed, updates will be provided to the leadership team by the DPO.

**Data Breach Response Team.** The Data Breach Response Team (DBT) was created to quickly and efficiently respond to any accidental or unauthorized access or disclosure of personal data. The team will be headed by the Data Privacy Officer (DPO). It will consist of members from various departments, including Technology, Operations, Community, PR/Marketing, HR, Finance, BD, Legal, and Compliance.

**Breach Response Process.** Upon being notified of a (suspected or confirmed) data breach, the DBT shall immediately activate the data breach & response plan:

* Confirm the Breach
* Contain the Breach
* Assess Risks and Impact
* Report the Incident
* Evaluate the Response & Recovery to Prevent Future Breaches

**NOTE:** The following procedures and processes are a high-level review of how the DBT will manage a data breach or incident. This process is subject to applicable state, federal, and international laws, rules, and regulations.

1. **Confirm the Breach.** If a data breach occurs, the DBT shall take immediate action. First, DBT shall confirm that the breach has indeed happened. Depending on the risk level, it may be necessary to proceed to step 2, Contain the Breach, even if the breach has not been confirmed.
2. **Contain the Breach.** The DBT shall enact the following measures to Contain the Breach, where applicable:
   1. Shut down the compromised system that led to the data breach.
   2. Establish whether steps can be taken to recover lost data and limit any damage caused by the breach. (eg: remotely disabling/wiping a lost laptop containing personal data of individuals.)
   3. Prevent further unauthorized access to the system.
   4. Reset passwords of accounts and/or passwords that have been compromised.
   5. Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system.
3. **Assess Risks and Impact.** Knowing the risks and impact of data breaches will help COMPANY determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.
   1. **Risk and Impact on Individuals**
      1. How many people were affected? A higher number may not mean a higher risk, but assessing this helps overall risk assessment.
      2. Whose personal data had been breached? Does the personal data belong to employees, customers, or community members? Different people will face varying levels of risk due to a loss of personal data.
      3. What types of personal data were involved? This will help to ascertain if there are risks to reputation, identity theft, safety, and/or financial loss of affected individuals.
      4. Any additional measures in place to minimize the impact of a data breach? E.g., a lost device protected by a strong password or encryption could reduce the impact of a data breach.
   2. **Risk and Impact on Clients and 3rd Parties (vendors, partners etc.)**
      1. Was client / partner data involved? If yes, how many clients and which ones?
      2. What type(s) of client/3rd party data was involved? (eg, confidential information, personal information, sensitive personal information)
      3. Were the contractual obligations for notification and reporting to affected clients met?
   3. **Risk and Impact on COMPANY**
      1. **What caused the data breach?** Determining how the breach occurred (through theft, accident, unauthorized access, etc.) will help identify immediate steps to take to contain the breach and restore public confidence in a product or service.
      2. **When and how often did the breach occur?** Examining this will help COMPANY better understand the nature of the breach (e.g. malicious or accidental).
      3. **Who might gain access to the compromised personal data?** This will ascertain how the compromised data could be used. In particular, affected individuals must be notified if personal data is acquired by an unauthorized person.
      4. **Will compromised data affect transactions with any other third parties?**  Determining this will help identify if other organizations need to be notified.
4. **Report the Breach.** COMPANY is legally required to notify affected individuals if their personal data has been breached and will abide by the notification timelines required by the applicable laws (see above related documents). This will encourage individuals to take preventive measures to reduce the impact of the data breach and also help COMPANY rebuild consumer trust.
   1. **Whom to Notify:**
      1. Notify the insurance company. MUST OCCUR IMMEDIATELY.
         1. **INSURANCE COMPANY CONTACT**
         2. **CYBERINSURANCE CONTACT**
      2. Notify individuals whose personal data have been compromised.
      3. Notify clients whose confidential information has been compromised.
      4. Notify other third parties such as vendors, banks, credit card companies, or the police, where relevant.
      5. Notify the relevant authorities if criminal activity is suspected and evidence for investigation should be preserved (eg, hacking, theft, or unauthorized system access by an employee.)
   2. **When to Notify Individuals:**
      1. Notify affected individuals without undue delay if a data breach involves personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data.
      2. Notify affected individuals when the data breach is resolved or if status changes.
   3. **How to Notify Individuals.**
      1. **Must confirm individual state requirements.** Use the most effective ways to reach affected individuals, considering the situation's urgency and the number of individuals affected (e.g., media releases, social media, mobile messaging, SMS, e-mails, telephone calls).
      2. Notifications should be simple to understand and specific and provide clear instructions on what individuals can do to protect themselves.
   4. **When to Notify Clients and 3rd Parties.** Depends on specific contractual obligations
   5. **How to Notify Clients and 3rd Parties.** Depends on Notice Clause LINK TO FORM
   6. **COMPANY standard terms: What to Include in Notification for Individuals and Clients/Third parties.**
      1. How and when the data breach occurred, and the types of personal data involved in the data breach.
      2. What COMPANY has done or will be doing in response to the risks brought about by the data breach.
      3. Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused.
      4. Contact details and how affected individuals can reach the organization for further information or assistance (e.g. helpline numbers, e-mail addresses, or website).
5. **State Attorney General Requirements.** Depending on state law and number of individuals affected, COMPANY may be required to provide written notice to the state Attorney General.
   1. **California** AG notification required if 500+ individuals are affected must notify via the form: <https://oag.ca.gov/privacy/databreach/report-a-breach>
   2. **Virginia** - NOTIFICATION REQUIRED NO MATTER WHAT <https://www.oag.state.va.us/CCSWEB2/files/Data_Breach_Notification_Req.pdf>
   3. **Massachusetts**
   4. **Colorado**
   5. **Utah** AG for 500+ or more state residents. If the breach involves 1,000 or more residents, then a notification to each consumer reporting agency is also required.
   6. **Washington**
6. **Evaluate Response and Recovery to Prevent Future Breaches.** COMPANY will review the cause of the data breach and assess the adequacy of current protection and prevention measures after taking necessary steps to address the breach. If needed, they will discontinue any practices that contributed to the breach to prevent similar incidents from happening again. Consider
   1. **Operational and Policy Related Issues.**
      1. Were audits regularly conducted on both physical and IT-related security measures?
      2. Are there processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse?
      3. Were there weaknesses in existing security measures such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices, networking, or connectivity to the Internet?
      4. Were the methods for accessing and transmitting personal data sufficiently secure, eg: access limited to authorized personnel only?
      5. Should support services from external parties be enhanced, such as vendors and partners, to better protect personal data?
      6. Were the responsibilities of vendors and partners clearly defined in relation to the handling of personal data?
      7. Is there a need to develop new data-breach scenarios?
   2. **Resource-Related Issues.**
      1. Were sufficient resources allocated to manage the data breach?
      2. Should external resources be engaged to better manage such incidents?
      3. Were key personnel given sufficient resources to manage the incident?
   3. **Employee-Related Issues.**
      1. Were employees aware of security-related issues?
      2. Was training provided on personal data protection matters and incident management skills?
      3. Were employees informed of the data breach and the learning points from the incident?
   4. **Management-Related Issues:**
      1. How was management involved in the management of the data breach?
      2. Was there a clear line of responsibility and communication while managing the data breach?

**Related Documents**

**Definitions.**

**Data Breach.** The definition of “breach” will depend on the applicable law, rule, regulation, or specific contract terms. However, “data breaches” include those security breaches in which the confidentiality of data is compromised.

**GDPR - Personal Data Breach.** <https://gdpr-info.eu/art-4-gdpr/> A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;