Model Data Breach Notification Policy

This model policy is suggested for adoption by any entity in India handling "Data" and is designed to meet the compliance requirements under Information Technology Act 2000/8 and also follow the global best practices in this regard.

This policy should be considered as part of, and should be synchronized with the provisions contained in the overall Information Security Policy and Privacy Policy of the entity.

The "Entity" should be properly identified and defined by the user organization/company

Any entity which intends to use this policy may contact Naavi for necessary permission.

Model Data Breach Notification Policy

[Version: 25th October 2015]

We hereby give notice to all stake holders that as a part of our Information Security Practice, we adopt the following as our "Data Breach Notification Policy".

We handle data of different types such as

a) Data belonging to our Managerial functions such as Marketing, Finance, Administration, HR etc. (Internal Corporate Data)
b) Personal Data of Employees and Contractual partners. (Employee Data)
c) Data belonging to third parties, such as our Customers and users of our services.(Third Party Data)

This Data Breach Notification Policy applies only to Third Party Data and not to Employee Data or Internal Corporate data and defines the process to be invoked in the contingency of an occurrence of a security breach which may have an adverse impact on the confidentiality, integrity, availability, authenticity and accountability of the data.

A "Data Breach" is any incident where the third party data which could include "Personal", "Sensitive personal" and "Other" information belonging to third parties and handed over to us for processing, storage, transmission or use is compromised or suspected to have been compromised as to its confidentiality, integrity, availability, authenticity and accountability.

"Personal Data" means any information that is identifiable with a living individual and includes the Name, Address, Phone Number, etc.

"Sensitive Personal Information" means such information as defined under Information Technology Act 2000/8 (ITA 2008) and includes passwords, financial or health information of individuals, biometric information etc.

"Other" information means such information that does not fall into the category of "Personal" or "Sensitive Personal" information but handed over to us for processing by a third party and includes transaction information that is collected either automatically or otherwise during the course of interaction between us and the third party.

Data Breach:

We adopt information security practices commensurate with the nature and scale of our activity to meet the risks that are identified by us under our information risk mitigation program.

There could however be contingent incidents when despite our information security measures, data may be accessed by an unauthorized persons and such instances are recognized as "Data Breach instances" for the purpose of "Notification" under this policy.

Exceptions:

a) When data is unauthorizedly accessed by an employee of our organization who is not normally authorised to access the data, the incident may be considered as a "Information Security Breach Incident" and action initiated to address the incident as per the Information Security policy of the organization. However such incidents are not considered as "Data Breach Incidents" for the purpose of notification under this policy.
b) When data is demanded by a law enforcement agency under any valid provision of law and furnished in compliance of such demands, the incident is not considered as a "Data Breach Incident" for the purpose of notification under this policy. Action may be initiated in such cases as per the Information Security Policy of the organization.
c) When data is "Potentially accessible" by an unauthorized person because of an identified vulnerability, but there is no clear indication of such access, the incident may be considered as a "Information Security Breach Incident" and action initiated to address the incident as per the Information Security policy of the organization. However, such incidents are not considered as "Data Breach Incidents" for the purpose of notification under this policy.
d) When data is handed over to a third party based on a valid authorization and in terms of the contractual obligations between us and the third party the incident is not considered as a "Data Breach Incident" for the purpose of notification under this policy.
e) When the data which is suspected to have been breached is **not** associated with personal identification, the incident is not considered as a "Data Breach Incident" for the purpose of notification under this policy. Action may be initiated in such cases as per the Information Security Policy of the organization.

f) When the data which is suspected to have been breach is “Encrypted”, unless the decryption key associated with the encrypted data is also suspected to have been breached to the same attack source, the incident is not considered as a “Data Breach Incident” for the purpose of notification under this policy. Action may be initiated in such cases as per the Information Security Policy of the organization.
g) When the data which is suspected to have been breached is already in the public domain for whatever reason, the incident is not considered as a “Data Breach Incident” for the purpose of notification under this policy. Action may be initiated in such cases as per the Information Security Policy of the organization.

First Response

Whenever an incident is flagged as a “Potential Data Breach Incident” under this policy subject to the exceptions mentioned above, we shall immediately conduct a preliminary internal investigation to identify the impact of the suspected data breach and determine whether a data breach notification is required under this policy.

External Investigation

Where necessary, the internal investigation team may refer the matter to a specialized external agency to investigate and determine the nature of the suspected breach and its impact before further action is initiated under this policy.

Examination of Investigation Reports

The reports of the internal team and the external team where available shall be verified by the Chief Information Security Officer (CISO) and submitted for further action to the CEO or other internal bodies as may be required under the Information Security Policy of the organization.

Issue of Data Breach Notification Release

The CEO after considering the opinion of the CISO and other internal bodies as the case may be, will issue a “Data Breach Notification Release” to the CISO indicating the action to be taken which should include instructions as to whom the notification is required to be given, when and with what information.

Evidence Preservation

In all suspected data breach investigation, irrespective of the final outcome of the investigation, all evidence collected during the investigation is preserved and archived in a legally acceptable format so as to be retrievable when necessary with appropriate authentication.

Data Beach Notification Release

Whenever the incident is confirmed to have resulted in the breach of data as defined in the policy, following actions shall be taken within 30 days from the confirmation of the data breach.

1. All individuals whose data is suspected to have been breached shall be individually informed through last known e-mail of the affected individual with appropriate documentary confirmation of receipt.
2. The notification shall indicate the date of suspected incident, the nature and suspected cause of the incident and the data suspected to have been compromised
3. The incident at this stage will be deemed to automatically invoke the **"Grievance Redressal Policy"** of the entity and a the copy of the data breach notification would be served to the affected data subject through the Grievance Redressal officer with a disclosure that the data subject may continue the Grievance Redressal process if he would like to prefer any claim for damage.
4. The notification shall also indicate whether the incident is covered by Cyber Insurance and what steps have been taken for prevention of similar incidents in future.
5. A consolidated report of the data breach incident along with the post incident action taken by the organization shall be reported to the Director In-CERT.

Sanctions

Where the investigation has found the involvement of negligence of any of the employee/s and non compliance of information security policy of the organization, the Company shall initiate necessary action as per the **Sanction Policy** adopted by the organization.

Police Complaint

Where the data breach incident has been caused by a deliberate act of either an employee or an outsider, a formal complaint is lodged with the local Police authorities and a copy of FIR kept in records.