Data Privacy Program

This policy was last modified in March 2021. Please note that this privacy statement will be updated periodically to reflect any changes in the way we handle your personal data or any changes in applicable laws

CORPORATE OFFICE:
Vakrangee Corporate House
Plot No. 93, Road No. 16, M.I.D.C., Marol, Andheri (East), Mumbai – 400093, Maharashtra

Table of Contents

1. Data Privacy Program 4
2. Understanding compliance requirements and business drivers 8
3. Reputational Risk 9
4. Data Management, Compliance and Governance 10
5. Management 10
6. Manage Privacy Policy 11
7. Strategy and Requirements for Data privacy and information security Management 12
8. Formally establish Governance oversight 13
9. Classification Standards 14
10. Operational risk planning 14
11. Choice and Consent 15
12. Data Collection & Privacy Policy 15
13. Use, Retention and Disposal 16
14. Accountabilities and responsibilities 17
15. Data Lifecycle Management 17
16. Access to personal information 17
17. Disclosure to Third Parties 18
18. Security for Privacy 18
19. Data Quality 19
20. Monitoring and Enforcement 20
21. Data protection with Data Governance 21
22. Establish Program and operational Governance 21
23. Policy Self-Assessment 22

23.1 Regular employee training on data privacy and information security management 22

24. Process and procedure for employee training on data privacy management 24
25. Privacy Program Management Organizational Structure 26

25.1 Governance structures in place for privacy management 26

26. Establish Minimum Security Awareness 34
27. Security Awareness throughout Vakrangee 35
28. Security Awareness Training Content 36

29. Define Metrics to Assess Awareness Training 39
30. Data Protection and Security Awareness Program Checklist 39
30.1 Creating the Data Protection and Security Awareness Program 39
30.2 Implementing Data Protection and Security Awareness Program 40
30.3 Sustaining Data Protection and Security Awareness Program 41
30.4 Documenting the Data Protection and Security Awareness Program 41
31. Data Protection Policy 41
31.1 Data Protection: A Right? 42
31.2 Protection of personal data 42
31.3 Data subjects can access their accounts to erase, rectify, complete or amend personal information 42
31.4 Clear and accessible mechanisms for data subjects to raise concerns about data privacy 43
31.5 Disclosures without data subject Consent 44
32. Privacy Risk Assessments 44
33. Risk Management 45
34. Regulatory and Information Security Audits: 46
34.1 Regular privacy risk assessments or audits on the company's technologies and practices affecting user data 46
34.1.1 ISO 27001:2013 Information Security Management System (ISMS) 47
34.1.2 ISO 20001-1:2011 IT Service Management System 48
34.1.3 ISO 9001:2015 Quality Management System (QMS) 49
34.1.4 ISO 27701:2019 Privacy Information Management System 50
35. Audits evaluates the flow of data within our business. 52
35.1 Audits identifies vulnerable points and problem areas. 52
35.2 Audits determines whether we must alter security policies and standards or not. 53
35.3 Audits recommends how to leverage information technology in our business security. 53
35.4 Audit delivers an in-depth analysis of our internal and external IT practices and system. 54
36. Management and Oversight 55
37. Remedy for victim in case of violations of company's data sharing practices 56

1. Data Privacy Program

An effective data protection program minimizes organization's sensitive data footprint and helps keep business-critical and regulated data secure and out of the hands of attackers. The best way to develop and maintain such a program is to think of it as an ongoing process, not a project. The efficiency of the **Data Privacy Program** heavily depends on the efficiency and visibility of the core privacy strategy. While technology is a vital part of managing privacy, we need to improve security to meet data privacy compliance requirements. It's important to remember that compliance for its own sake is not security but creating a robust security program that addresses compliance needs will serve you well. It is important to note that approaching compliance as a separate effort, rather than as an integral part of the security program, may cause problems.

We handle data protection and privacy by categorizing all data based on our sensitivity (confidentiality), criticality (availability), identifiability (privacy) and compliancy; this categorization is then used to determine the safeguards required. We operate under the framework which is primarily based upon **ISO 27001:2013** which states:

Information Security	The protection of the confidentiality, integrity and availability of information.
Information Privacy	Establishing rules which govern the collection and handling of personal information.
Information Compliance	Adherence with all applicable IT regulatory requirements or implementing compensating controls or documenting exception requests.

Vakrangee has adopted best practices to improve security so that we can meet data privacy objective:

1. **Evaluate In-House Capabilities and Design the Program**
    a. Set up the internal project leadership and program management team

b. Appoint an executive champion for the program
c. Review and update the security program mission goals
d. Evaluate the in-house security and compliance capabilities

2. Adopt a logical approach to a data protection strategy

a. Minimum-security baselines are in place
b. Identify and locate sensitive data
c. Understand how it's created and used
d. Classify and prioritize data assets

3. Conduct a Privacy Impact Assessment

a. List out privacy regulations Vakrangee currently responsible for complying with
b. List privacy-related data Vakrangee currently storing
c. Privacy-related data stored location
d. Detail Data Access list
e. Current policies and procedures for managing the collection, storage, processing, distribution and disposal of privacy-related data

4. Define sensitive data

a. Unique list of sensitive data
b. Unique list of confidential data

5. Understand the data lifecycle

a. Understand data lifecycle stages - create, store, use, share, archive and destroy

b. Policies to apply to best protect it

6. Locate sensitive data

a. Identify sensitive data
b. Apply a hybrid approach to protecting it
c. Apply security controls to known data
d. Enumerate the unknown data
e. Monitor the creation of new data
f. Identify privacy and data protection roles

7. Assess Risks and Create Awareness

a. Create a personal data inventory.
b. Assess the personal data you store.
c. Conduct a data risk assessment for all identified personal data.
d. Update existing policies and procedures
e. Create new ones to cover the gaps and conduct training on them.

8. Design, Implement, Manage and Enhance Operational Controls

a. Implement the physical, technical and administrative safeguards
b. Update and distribute privacy notices
c. Formalize the data dispute resolution process and procedures
d. Ensure formalized reporting is in place
e. Update or implement the Vakrangee's data breach response plan

9. Establish a data security process

a. Consider resources (people, skill sets, technology)
b. Time (Are you out of compliance or responding to an incident?)
c. Buy-in (communicate the importance of change to get buy-in from both senior management and the user community).

10. Manage compliance and data governance

a. Compliance doesn't mean your data is secure
b. Need more-stringent standards for data privacy and protection than the privacy laws
c. Add governance

11. Conduct a Privacy Data Clean-up

a. Ensure the proper data retention periods are in place,
b. Strict adherence to the data disposal procedure

12. Protect new data

Apply the **PPT** process:

a. Process for identifying and handling new data
b. Make People aware of the process and
c. Use Technology to automate as much of the process as possible.

13. Formulate classification levels for advanced protection

a. classify data according to its level of sensitivity
b. classify data according to security objective
c. classify data according to potential impact of unauthorized disclosure.

d. classify data according to role-based, data-oriented, access or location-based, and hybrid

14. Demonstrate Ongoing Compliance

a. Data Management, Compliance and Governance end to end process
b. An effective governance structure (people, roles, structures, and policies) and set of governance functions in place for privacy management

2. Understanding compliance requirements and business drivers

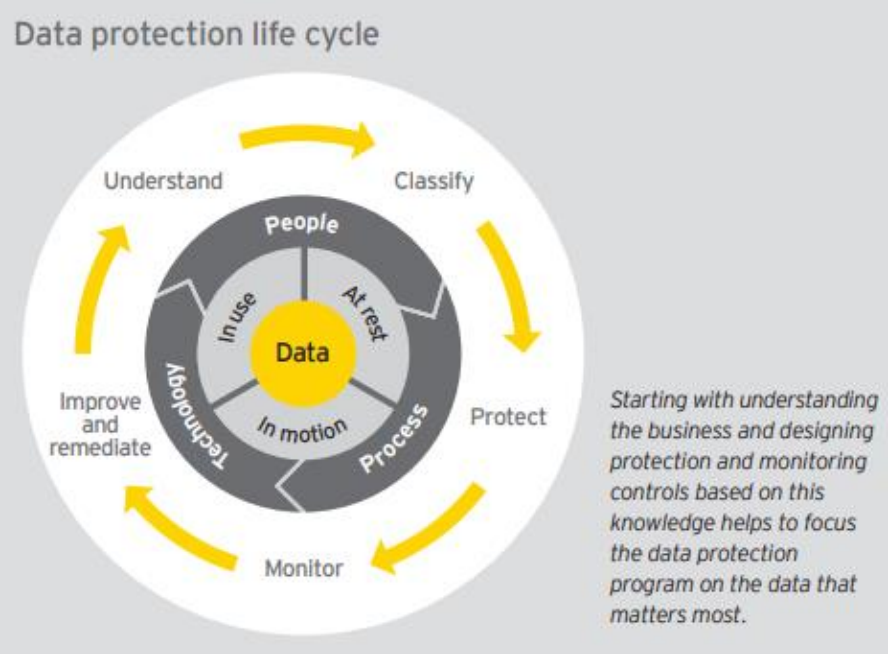
We have set two common drivers for data protection programs:

a. Complying with legal, regulatory or industry compliance requirements to protect specific data types
b. Protecting data that is essential to the organization's ability to win in the marketplace (e.g., intellectual property, trade secrets, proprietary information, and merger and acquisition plans). Relevant statutory, regulatory, and contractual requirements for our information assets is defined explicitly. These requirements include, but are not limited to:
    - Information Technology Laws (IT Act 2008/2011 Amended) (GOI)
    - Data Protection 2019
    - Software Licensing Requirements
    - Intellectual Property Rights (IPR) Laws
    - Labor and General Employment Laws
    - Health and Safety Laws
    - Environmental Laws

There are also several types of regulatory and compliance requirements related to data protection; this includes industry-based regulations and laws, which require the

protection of certain types of Personally Identifiable Information (PII). While many of these regulations are subject to interpretation on the details of what types of technical controls are required, all regulations require these types of data to be protected from inappropriate access or disclosure.

We have implemented data loss prevention technology and other technical controls to protect Personally Identifiable Information (PII). Additionally, we have contractual agreements in place with customers and business partners, which require specific data protection controls to be in place; for example we asked our vendors to implement data loss prevention technology to monitor and prevent sensitive data from being transmitted through unencrypted channels such as email.



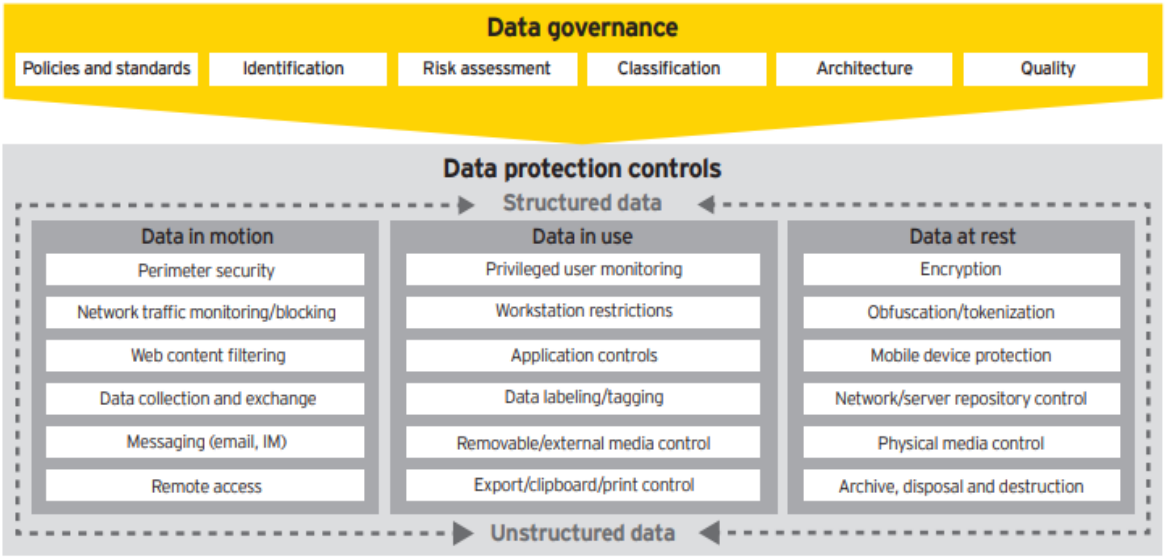
3. Reputational Risk

We Vakrangee respect our privacy to maintain our reputation which is the most significant risk management challenge today. Reputational risk is regarded as the

greatest threat to a company's commercial value of business. The potential that negative publicity to an institution will cause a decline in the customer base, reduce revenue and lead to costly litigation.

4. Data Management, Compliance and Governance

Vakrangee's data privacy challenges is addressed by Data Management, Compliance and Governance divisions along with risk management functions. Privacy is the rights and obligations of Vakrangee's with respect to the collection, use, retention, disclosure, and disposal of personal information. This can be a name, email address, Government information and data, tax return etc.



5. Management

Our senior management defines, documents, communicates, and assigns accountability for its privacy policies and procedures. We are committed to security. Our senior management has constituted Vakrangee Information Security Committee,

which is responsible for defining and improving the Information Security Management System (ISMS).

Senior management have demonstrated leadership and commitment with respect to the information security management system by:

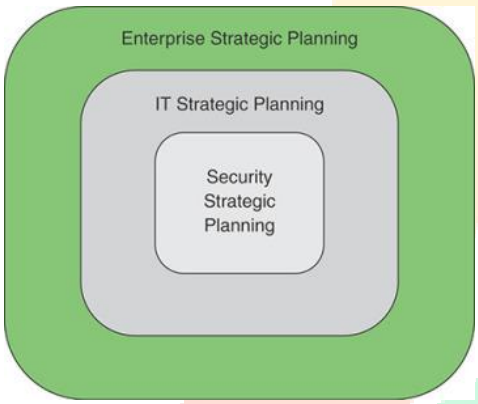
- Ensuring that the information security policy and the information security objectives are established and are compatible with our strategic direction
- Ensuring integration of ISMS requirements into our processes Ensuring that the resources needed for ISMS are available
- Communicating the importance of effective information security management and conforming to the information security management system requirements
- Ensuring that ISMS achieves its intended outcome(s)
- Directing and supporting persons to contribute to the effectiveness of ISMS
- Promoting continual improvement
- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

6. Manage Privacy Policy

We have data privacy policy to ensure enforcement of compliance with mandatory regulatory, internal compliance, best practices, legal and ethical requirements along with need for managing risk. These requirements are embedded into the policy and privacy statements to provide guidance to personnel on their accountabilities and responsibilities. This assists the personnel in carrying out any activity that includes Private and confidential information. This helps manage the risks in operations thus aligning with risk appetite and tolerance levels. The privacy statements also provide the need for capturing private information along with the rights that the customers enjoy in relation to the same. The guidance further is supported by the procedures and guidelines.

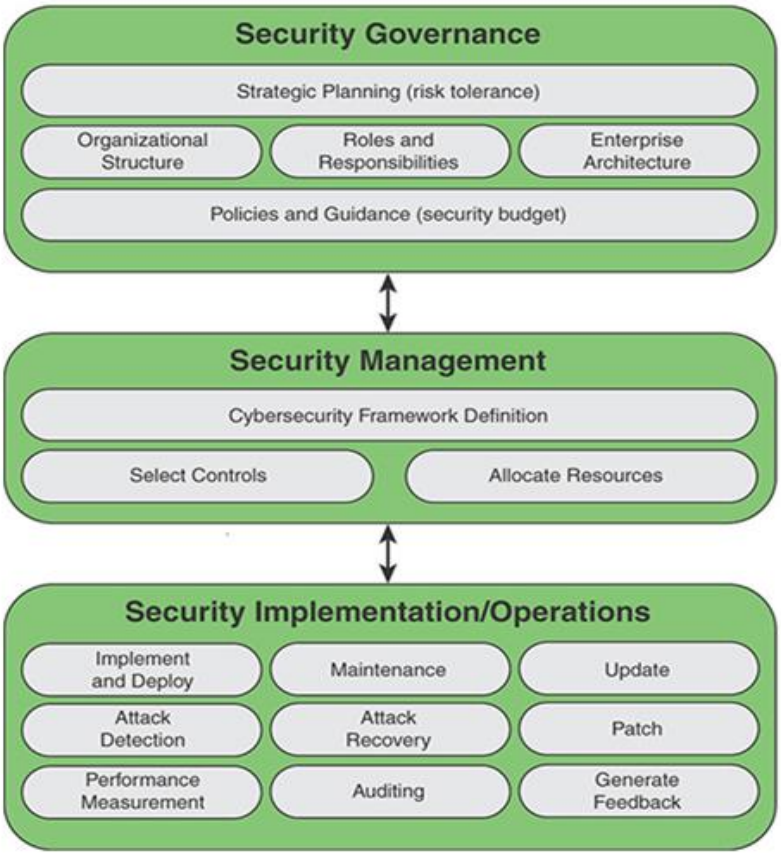
7. Strategy and Requirements for Data privacy and information security Management

We have developed and updated Data Management Strategy to include the Data Privacy management aspects. Data Management Strategy and Data Privacy Management are Security Strategic Planning which are part of IT Strategic Planning which is aligned with Vakrangee's objectives and Enterprise Strategic Planning. In addition, we have also described the target structure and Vakrangee's structure for Data privacy and information security Management.



8. Formally establish Governance oversight

Further, Roles and responsibilities are defined, communicated, and enabled. We have established an **Information Security Committee** made up of key personnel whose responsibility is to identify areas of security and compliance concern across the organization and act as the first line of defense in enhancing the appropriate security and compliance posture. This team reports to the CISO (**Executive Level Management**). Vakrangee's Information Security Committee takes the responsibility of drafting policy, having reviews performed, publication and communication to the grassroots of enterprise. Further, Policy and standards are ensured to be reviewed Information Security Committee and approved by Executive Level Management as an expanded responsibility.



9. Classification Standards

The working groups are commissioned by Information Security Committee to draft and publish the standards to classify data, in view of privacy and confidentiality.

10. Operational risk planning

Operational Risk Governance Structure and processes are in place and are operational. A risk assessment process is commissioned every year by second line of defense using the Risk Control Self-Assessment procedures, to identify new risks, understand the impact of events, and frequency of occurrence including the risk scores. Information from existing historical loss events are considered for response options. The response options include the procedures to record, assess impact, escalate, notify responsible internal and external parties, commission root cause analysis and changes to control environment. Awareness is taken forth through a communication strategy and learning programs to strengthen the first line of defense in the enterprise. In-Flight risks are recorded by the first line of defense that will be taken through the Risk Governance, Risk Analysis, Response and closure.

Please Note:

Vakrangee always provides notice to its system users, customers, partners, employee and all other stake holders about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

The privacy notice describes as:

a. Personal information collected
b. The purpose for which it will be used
c. Indication of legal requirement, if any for collection
d. Consequence of not accepting to provide personal information
e. If the information will be disclosed and under what scenarios, to which parties

f. The retention, security, quality and monitoring aspects

g. The entities, geographies, jurisdictions, types and sources of information

11. Choice and Consent

We always describe the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.

We also ensured that the choices of individuals are captured with accuracy and the same is ensured with consistency wherever the consent, Opt-Ins and Opt-Outs are trickled along the data lifecycle. The data domain and datasets associated with customer preferences, processes or functions for which the customer opted in/out, last updated dates and other data elements actively managed.

Our Data Privacy management ensures that the policy and procedures capture the receival of customer's consent when private information is being used for a new purpose.

12. Data Collection & Privacy Policy

Vakrangee collects personal information, the Data Privacy Management ensure alignment of the privacy policies with regulators across jurisdictions. The collection of data from a customer is related to the Obtain phase - where data is obtained from the customer. We acquire Financial information, tax information and demographic information to quote an example.

When data is being acquired regarding a customer from third parties, our Data Governance ensure oversight over procedures for establishing engagement, communication, recording agreements for data quality and data transfer. The data privacy management team ensure that not only the data acquired from the customer but also the data that is derived like the customer purchasing behavior is adequately

classified for risk and managed in accordance to policy and guidelines. We also record in the metadata repository, the processes, or functions that each data element is being acquired in. Further, the systems, people who are acquiring the data also recorded the same. This simplifies the data landscape in scope of Privacy.

13. Use, Retention and Disposal

We limit the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.

Vakrangee retains personal information for only if necessary, to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes such information. The Data privacy and information security division define adequate framework for defining entitlements. The same will be published, communicated across the enterprise through data controllership and data ownership.

Vakrangee's Data Governance ensures that aspects of use, retention and destruction of data are documented in line with legal, regulatory and internal requirements within the policy. For example, financial information of an individual like "Gross Salary before tax" can be used for processing business transactions such as payroll and taxes, or other compensation schemes. In this scenario, the data element "Gross Salary before tax" will be associated with processes such as payroll that apply and update this data element. This kind of mapping will be performed with the systems (payroll) and People (accountant, payroll analyst) who apply and maintain Gross salary before tax.

Vakrangee as a data owner take the responsibility of classifying the data element, defining entitlements, defining data to process/system/people mapping. While the downstream systems, People, process SMEs ensure that the entitlements associated with the data element are being followed and adherence documented.

14. Accountabilities and responsibilities

Vakrangee as a data owner are accountable while data governance is responsible to classify the data elements, defining entitlements, any associated distribution rules and defining data to process/system/people mapping. Data Governance is responsible to ensure that the classifications and entitlements are available for private information in metadata repository. Data Owner is responsible to review classifications applied to data on a yearly basis or when there is a change to the data element and its context. This is associated with leveraging the data element that is classified “Direct Customer Identifying data”, “Indirect Customer Identifying Data” or Security Classifications “Internal”, “Restricted”, “Highly Restricted”. If this includes obtaining a new consent from the customer, the relevant service will be triggered.

15. Data Lifecycle Management

Further, Data lifecycle management strategy defined and endorsed by relevant stakeholders. Data lifecycle management roadmap developed and implemented. Storage governance structure, archival procedures, data transfer and Decay processes and procedures operational. Data Owner formalizes the accountabilities of the data owners and SMEs in data lifecycle management for e.g. the function commission to erase or destroy records in accordance with the decay and retention policies, regardless of the method of storage (electronic, optical media, or paper based).

16. Access to personal information

We have policy to provide individuals with access to their personal information for review and update. When individuals request access to their personal information,

the most current and accurate information provided on authorization from data owner. Any further requests on maintenance or updating of existing records will be taken through the procedures to update personal information. While the same needs to be updated in the folder where the same data element exists. The changes to personal information are auditable.

The data owners report on the changes to the personal information to the line of business and the data governance division quarterly. We follow the best practices as per data privacy management, to have the latest, most accurate and current information updated for the data elements classified as Private.

We have proper managed Access Control, which is for protecting our information and resources. Also, it has controls implemented for continuous oversight to restrict access. Access to electronically stored records containing personal information shall be electronically limited to those workforces having an authorized and unique login ID assigned.

17. Disclosure to Third Parties

We have policy to discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

The data quality function ensures that data that is transferred to third party is accurate, complete, consistent, relevant, and valid. The profile of data stored in the metadata repository by the profiling group while the Data Quality rules defined by the data owners and SMEs. The Third-party sourcing agreement clearly define the purpose for which the data will be used.

18. Security for Privacy

We protect personal information against unauthorized access (both physical and logical). Privacy policies adequately address security measures to safeguard the

privacy of personal information whether in electronic, paper, or other forms. Security measures are consistent with the sensitivity of the personal information. The Data privacy and information security function calls for creation of a communication and training program. Further, it describes the need for an education and training program to ensure stakeholder understanding, compliance to the data privacy and information security program. Data governance team ensures that data Classifications including Data management characteristics, Data security and privacy classification are established. Data owner and data governance team ensure that privacy by design is embraced. The controls for security for private data, are established at a data service level wherever applicable rather than at an application level. The data privacy, information security and governance team ensure that the guidelines for data controls are placed for new changes or changes to existing capabilities. Once the Privacy Impact Assessments are performed, the gaps are analyzed and a program focusing on establishing a control environment for such data is commissioned in line with the funding model. Any non-adherence to establish controls will be signed off by the data governance team with adequate evidence to bypass the controls. Use of encryption is mandated by data owners wherever data is being transmitted. The level of controls includes administrative, technical, and physical controls to secure sensitive data.

The data quality function ensures that adequate integrity controls are in place to maintain the data while data privacy and information security ensures that modification is being performed by designated roles. The Data governance function will be aligned with information security policy.

19. Data Quality

Vakrangee maintain accurate, complete, consistent, timely, and relevant personal information for the purposes identified in the notice

Data Quality operating model and processes is defined and made operational. Data is profiled, analyzed and described for Data Quality against the dimensions, in enterprise repositories and golden sources. The data owners will document data quality rules based on the characteristics of the data from profiling. The data controllers along with the senior management ensure that data elements are extended and enriched, based on the context. The data delivery services will be ensuring adequate abstract environment requirements and data transfer requirements are met. The data quality function ensures that adequate integrity controls are in place to maintain the data while data privacy and information security ensures that modification of data is performed by designated roles. The data quality assessment and monitoring are performed based on the nature of the data operation and the lifecycle stage. Further, the KCIs are continuously monitored by data controllers and data owners in the Control scorecard. Any errors in the data handled by the data remediation function with adequate root cause analysis documented.

20. Monitoring and Enforcement

Vakrangee monitors compliance with its privacy policies and procedures and has procedures to address privacy related inquiries, complaints and disputes.

The Governance function enforces authority, formalizes accountability while evaluating, directing, and monitoring the data privacy management activities. The KCI scorecards for data quality, metadata, architecture, and security are ensured to be available and monitored continuously for breaks in process. The escalation procedures are established and ensured to be followed by personnel. The evidence of control effectiveness and efficiency made available for audit by the governance function.

21. Data protection with Data Governance

The right data is used by a person in the right role and only in the right context. We adhere to the applicable government body regulations, legal, and contractual requirements. Since, we have many types of sensitive information, taking data protection for granted is a recipe for disaster. Vakrangee has strong data privacy and information security teams, cutting edge tools and mature processes, this can be victimized by data loss events. Users with authorized access present a huge challenge as they can act carelessly or with malicious intent. To meet this challenge, we need to be able to apply additional safeguards and increased monitoring of the data that is most important to protect. Without input and direction from the business and data governance team, information security professionals cannot strategically align controls and monitoring capabilities to the data that matters most. Additionally, unless end users actively participate in identifying and labeling sensitive information, data protection program investments may yield little practical value.

22. Establish Program and operational Governance

Once the program Governance is in place, Governance is taken to every change in Vakrangee, where Policy and standards are enforced and auditable. This ensures that every new capability or change to existing process, system is assessed for privacy impact. The assessment plan clearly articulates how the data privacy program will be measured and evaluated. Further, Metrics are put, to track program adherence, progress and outcomes. Data privacy and information security management team ensures that all privately classified data elements are classified, and entitlements recorded in the Metadata repositories.

23. Policy Self-Assessment

The approach and mechanism to policy self-assessment internally and externally established. The self-assessments are conducted on the processes, systems and people based on the culture. Further, the risk scorecards and performance scorecards are updated to showcase the risk profile of Vakrangee and its appetite to risk taking. Further, the appetite and tolerance limits are updated yearly by the Governance and risk functions or are cascaded from the group to the data privacy management division. With any external changes like environment changes, market changes the appetite and tolerances analyzed for impact.

23.1 Regular employee training on data privacy and information security management

In today's digital world, it's easy to share information at the click of a button. As a result, standards for privacy protection continue to rise, which makes it harder to keep up with the changing laws that regulate our personal information. All workforce members complete an annual information security and privacy awareness training program. As part of this program, additional role-based training is provided to the employee before they start handling sensitive and confidential information.

Role of Senior Management Team:

a. Identifies needs for prioritized training and provide targeted training to groups and departments with high event rates.
b. Evaluates the effectiveness of data protection training materials and delivery.
c. Identifies significant reasons for event generation, which lead to improved training, correcting broken business process and identification of high value

mitigating controls. There is event review team who closes incidents with root cause indicator.

d. Identifies individuals that require direct training or disciplinary action and highlight groups that handle significant volumes of sensitive data and those which need top-down improvement and communications. We embed data protection measures into employee's performance measures which is a powerful incentive to understand and apply data protection policies and data handling guidelines.
e. Estimates the number of employee weeks per month dedicated to data protection event handling.
f. Evaluates compliance with acceptable service levels for event resolution. This can be split into time to initial evaluation and time to closure if validated events are escalated to secondary parties for closure.
g. Provides insights into the types and volumes of data loss events over time. Grouping by policy or rule provides specific details about the trends for specific types of sensitive data.
h. Identifies potential compliance issues, such as unencrypted credit card numbers stored in unstructured files.

We provide information about the percentage of unstructured files that contain classification labels. This can be combined with other policies to determine a percentage of files that contain sensitive data and have been labelled with a classification level.

Employee awareness training on data privacy and information security management be conducted as an on-going program to ensure that training and knowledge is not just delivered as an annual activity, rather it is used to maintain a high level of security awareness daily.

But as the privacy landscape and associated trends and regulations shift, the end goal of privacy awareness training remains the same. Periodically we help our employees to achieve a mindset where protection of personal data comes as second nature. It is important to implement a privacy awareness training program so all our employees can actively protect sensitive data.

24. Process and procedure for employee training on data privacy management

Step 1 - Assemble the Security Awareness Team

The first step in the development of a formal data privacy and information security and security awareness management program is to assemble a security awareness team. This team is responsible for the development, delivery, and maintenance of the on-data privacy management and security awareness program. It is recommended the team be staffed with personnel from different areas of Vakrangee, with differing responsibilities representing a cross-section of Vakrangee. Having a team in place will help ensure the success of the data privacy and information security awareness management program through assignment of responsibility for the program. The size and membership of the data privacy and information security awareness team will depend on the specific needs of Vakrangee and its culture.

Step 2 - Determine Roles for Data Privacy and Information Security Awareness

We have Role-based privacy management and security awareness program which provides Vakrangee's a reference for training personnel at the appropriate levels based on their job functions. The training can be expanded upon—and subject areas combined or removed—according to the levels of responsibility and roles defined in Vakrangee. Our goal is to build a reference catalogue of various types and structures of training to help Vakrangee's deliver the right training to the right people at the right time. Doing so will improve a Vakrangee's data privacy and information security

as well as help maintain compliance. Whether the focus is a singular, holistic, or a tiered approach, the content can be scoped to meet a Vakrangee's requirements.

Step 2.1. Identify levels of responsibility

The first task when scoping a role-based security awareness program is to group individuals according to their roles (job functions) within organization. A simplified concept of this is shown in Figure 1.

Figure 1: Security Awareness Roles for Organizations

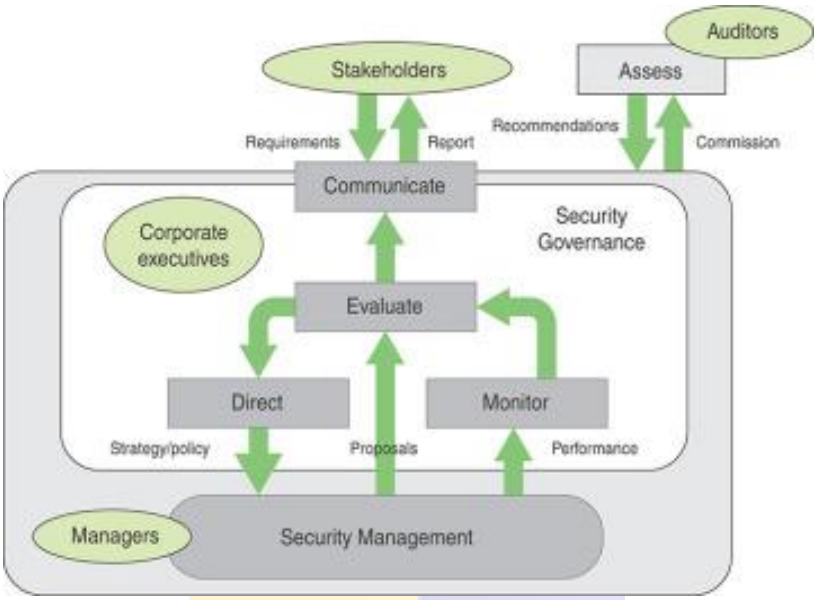
The diagram above identifies three types of roles, **All Personnel, Specialized Roles, and Management**. A solid awareness program will help All Personnel recognize threats, see security as beneficial enough to make it a habit at work and at home, and feel comfortable reporting potential security issues. This group of users be aware of the sensitivity of data even if their day-to-day responsibilities do not involve working with data. Additional training for those in Specialized Roles focusses on the individual's obligation to follow secure procedures for handling sensitive information and recognize the associated risks if privileged access is misused. Each of these specialized roles requires additional training and awareness to build and maintain a secure environment. Additionally, specific training may be required to include understanding of data privacy and information security awareness program.

Management has additional training needs that may differ from the two previous areas. Management needs to understand Vakrangee's data privacy, security policy and security requirements enough to discuss and positively reinforce the message to employees, encourage staff awareness, recognize and address data privacy and information security related issues they occur. The data privacy and information security awareness level of management may also need to include an overall understanding of how the different areas fit together. Accordingly, managers of staff with privileged access have a solid understanding of the security requirements of their staff, especially those with access to sensitive data. Management training will also help with decisions for protecting Vakrangee's information.

25. Privacy Program Management Organizational Structure

25.1 Governance structures in place for privacy management

Our organizational structure is very robust to deal with data privacy, risk management and security operations. We ensure that organizational activities, like managing IT operations, are aligned in a way that supports the organization's business goals.



We have a Decentralized Privacy Governance Model where we have divided roles and responsibilities between departments, the clear role of the data protection officer (DPO) is in place.

Vakrangee Privacy Vision and Mission Statement

Mission:

Safeguarding data protection rights by driving compliance through guidance, supervision and enforcement.

Vision:

To ensure appropriate data privacy safeguards are in place across the organisation, by below principles:

Access: the control over the privacy of information provided and processed

Transparency: transparent about the data collected and how that information will be used

Security: Using strong security and encryption techniques, protect the data entrusted to us using our products and services

Legal Protections: we respect global as well as local privacy laws and will work to ensure legal rights of privacy are respected and adhered to.

Privacy Strategy

As per our privacy strategy we have below activity in place:

- due diligence in place which thoroughly analyzes and even changes some of our business processes as per demand.
- reconciliation of daily operations with personal data protection.
- checklists for releasing a new product or a service, changing vendors or IT systems,
- data processing inventories up to date.

Data privacy and information security team Structure

We have a well-equipped Data privacy and information security team whose responsibility is not only to provide privacy training and make all employees aware about privacy policies, procedures, data protection, data security, cyber security, information security etc. but also make sure all privacy policies and procedures should be follow by employees. So that all employees must understand and employ the fundamental practices required to protect personal data. They should be aware of secure methods to collect, store and transmit personal data through to secure methods of data retention and data removal. They also make sure that business contact data should be secure and well stored.

As per our privacy governance model there is holistic privacy program implemented in Vakrangee with strong senior management, business owner and other key stakeholders support. Senior management team and business owner trust the organization's Data privacy and information security team because they are very well educated about the importance of data protection and the organization's privacy strategy, policies, and procedures. They are very much aware and bear the responsibility for data protection. They take ownership to reconcile their business with the proper rules and regulation. Key stakeholders are very much part of privacy leaders or they appoint business line privacy leaders. Under proper

guidance and right advice of these key stake holders, the Data privacy and information security team solve issues proactively.

Data privacy and information security team responsibilities are:

- to liaison with business owners and build a business line privacy leader role within the organization.
- Create an Information Security organization structure with proper defined roles and responsibilities for privacy management and privacy program.
- This organizational structure has been considered as related to strategy, operations, and management for any responsibilities and reporting.
- Every member of the team has clear responsibilities for maintaining compliance.
- Ensure data privacy and information security team create helpful checklists, promote privacy awareness, and define tasks.
- Create and maintain the inventory, initiating, and doing privacy impact assessments, managing privacy assets, etc.
- Ensure data Protection Officers and privacy experts within the organization are properly engaged with organisation privacy program**.**
- Organization's privacy policies and procedures are followed in every step of the business process
- Ensure all product or service of Vakrangee have records of processing activities and is up to date.
- Ensure existing staff are switched between different roles and get new data protection responsibilities alongside their current responsibilities.
- Ensure for clear segregation of duties, proper roles & responsibilities defined
- The position of all these members are within the organization's department either under legal, or IT, or compliance, or other etc.

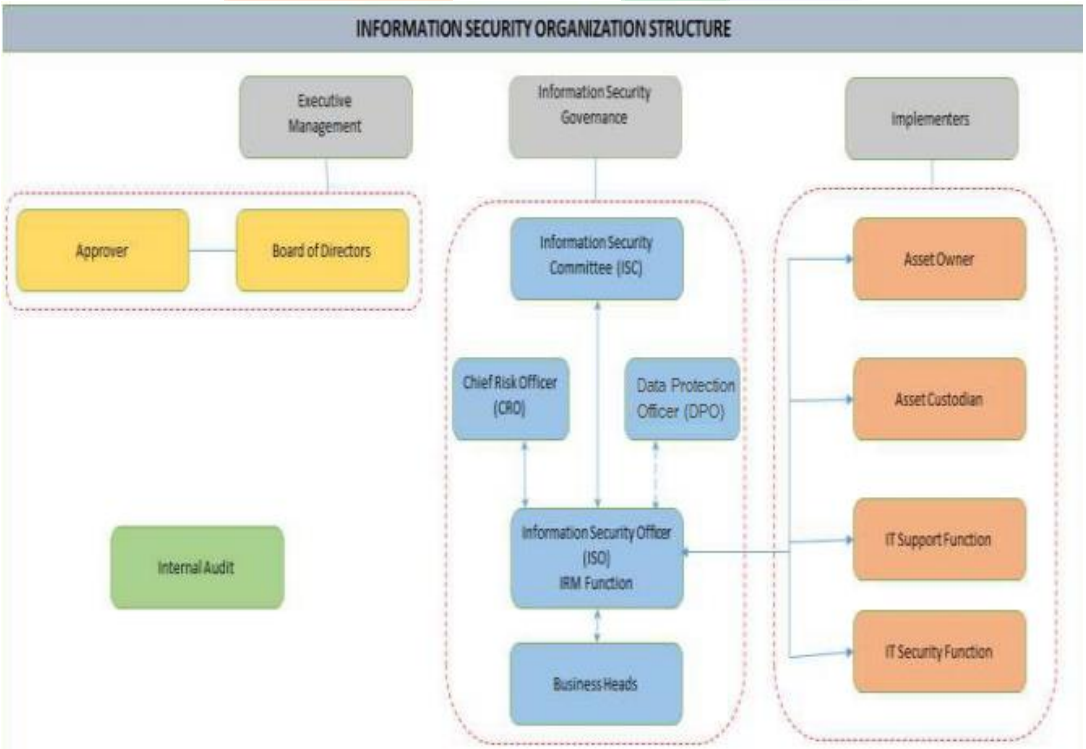
Data Protection Officer (DPO)

Clause 40 of the Data Protection Bill 2019 mandates every significant data fiduciary to appoint a Data Protection Officer (DPO). In today's cyber world data is the focal point and appointing a dedicated Data Protection Officer will help not just in protecting the data but it will facilitate efficient use of data and the better customer service leading to organizational growth. DPOs address privacy and data protection tasks that face by our organisation**.**

Duties of a Data Protection Officer

- DPO has expertise in data protection laws and practices including an in-depth understanding of the compliances national and international.
- DPO are designated based on professional qualities and expert knowledge of data protection law and practices and the ability to fulfill the tasks set out in the Regulation.
- DPO's primary focus is to make sure that the organization processes personal data of data subjects (employees, customers, and other individuals) in a compliant way with applicable data protection laws.
- DPO cooperate with other organizational units that are involved in processing personal data.
- DPO inform and advise the company about data protection obligations and to align internal processes and navigate company policies to be compliant.
- Cooperate with other organizational units that are involved in processing personal data.
- DPO operate independently, with full support from business owners, key stakeholders, senior management, and board and have access to all needed resources to do the job according to best practices.
- DPO are responsible for supervising the implementation of a data protection strategy, making sure it is compliant with all applicable data protection laws.

- DPO involve in issues related to the data processing activities within the organization.
- DPO knows the apprehension of the processing operations carried out.
- DPO oversees the data privacy and data protection policies to ensure the operationalization of those policies through all organizational units.
- DPO understands information technologies and data security.
- DPO has insight into the business sector and the organization.
- DPO has ability to promote a data protection culture within the organization.
- DPO reports directly to highest level of management and is given the required independence to perform his/her task
- DPO is involved promptly in all issues relating to the protection of personal data
- DPO is sufficiently well resourced to be able to perform his/her task
- Senior management ensure that any other tasks or duties assign to DPO do not result in a conflict of interest with their role as a DPO.

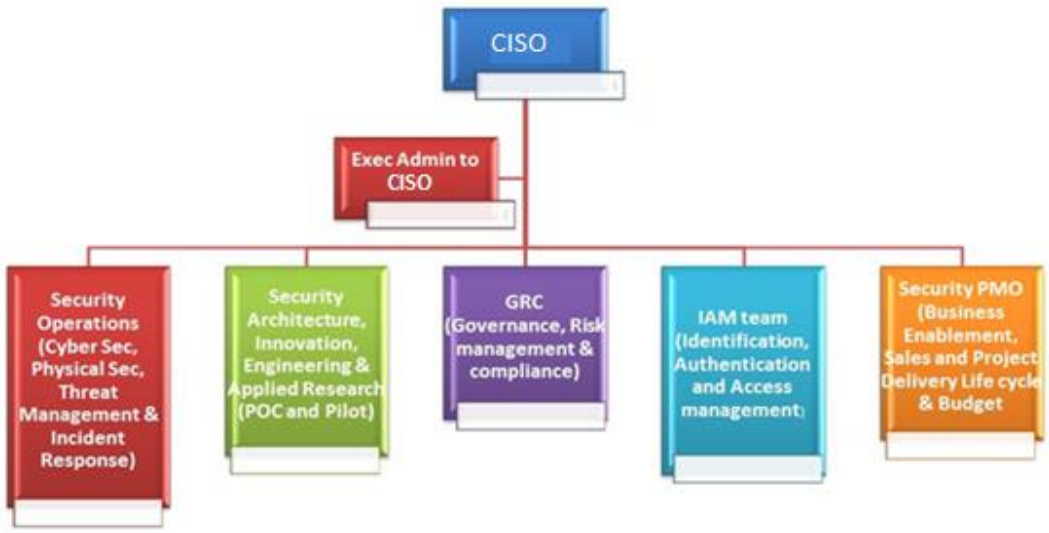


Management Level	Role	Title	Responsible Person	Roles and Responsibilities	Reporting To
Executive Level Management	CISO	Director R&D (Board Representative)	Dr. N Hayatnagarkar	Communicating with lines of business the expectations and requirements for data governance. Sponsoring, reviewing & approving, championing the enterprise strategic plan and policy. Identifying and prioritizing data quality initiatives.	Board of Director
Information Security Committee	DPO	Group CTO	Sanjay Nandwana	Overseeing enterprise data governance program development.	CISO
				Supervising the implementation of a data protection strategy, making sure it is compliant with all applicable data protection laws.	
				Reporting to CISO all the incidences or issues related to information security and data privacy with CISO	
				Overseeing the data privacy and data protection policies to ensure the operationalization of those policies through all organizational units.	
				Ensuring that the organization processes personal data of data subjects (employees, customers, and other individuals) in a compliant way with applicable data protection laws.	

	Chief Risk Officer	Group CTO	Sanjay Nandwana	Pushing data governance into their areas by actively promoting improved data governance practices. Making decisions at a strategic level in a timely manner given the appropriate knowledge to make that decision.	CISO
	Information Security Officer	Head IT Process	Ritu Thakkar	Establishing and enforcing security policies to protect an organization's computer infrastructure, networks and data to protect information security breach which can be in disruption to the business, loss of confidential or commercially sensitive data, and financial loss. Approving things that need to be approved – i.e., data policy, data role framework, methods, priorities, tools, etc.	CTO
Implementors	Asset owner	Infra Support	Yogesh Mayekar	Responsible for setting the data's security classification and delegate some day-to-day responsibility.	Information Security Officer
	Asset custodian	System Administrator	Divyesh Patel	Implement controls on behalf of the data owner, day-to-day management of data, controlling access, adding and removing privileges for individual users, and ensuring that the proper controls have been implemented.	Information Security Officer
	IT Support Function	Head IT Support	Rahul Sharma	Acting as the point person in the common data matrix and regular change control process.	Information Security Officer

	IT Security Function	Network Administrator	Prabhakar Dakare	Acting as the point communications person for their business unit to document and communicate issues pertaining to specific domains of data to the proper data domain.	Information Security Officer

CISO have a team as shown in diagram:

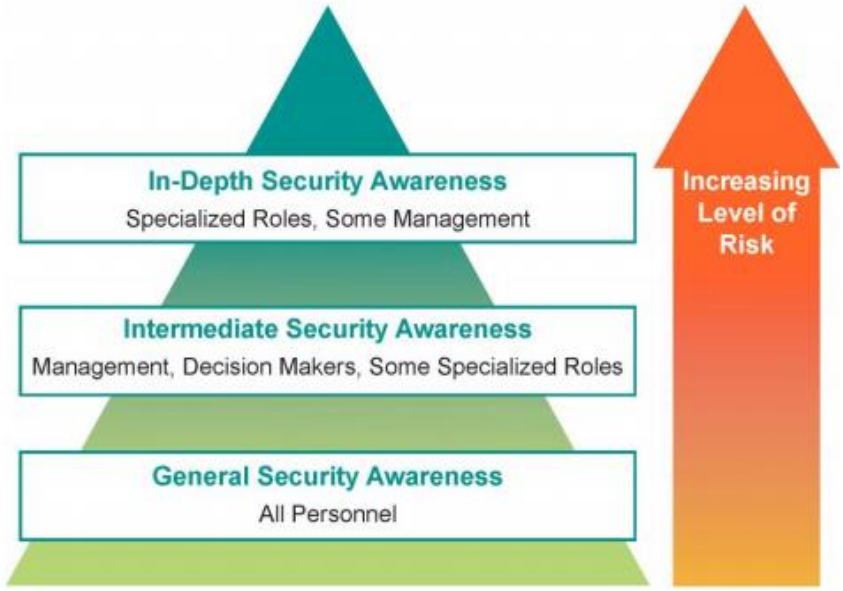


26. Establish Minimum Security Awareness

Establishing a minimum awareness level for all personnel is the base of the security awareness program. Security awareness may be delivered in many ways, including formal training, computer-based training, e-mails and circulars, memos, notices, bulletins, posters, etc. The security awareness program be delivered in a way that fits the overall culture of Vakrangee and has the most impact to personnel.

The following diagram depicts how the depth of awareness training increase as the level of risk associated with different roles.

Figure 2: Depth of Security Awareness Training



27. Security Awareness throughout Vakrangee

The key to an effective data privacy and information security awareness program is in targeting the delivery of relevant material to the appropriate audience in a timely and efficient manner. To be effective, the communication channel also fit Vakrangee's culture. By disseminating data privacy and information security awareness training via multiple communication channels, Vakrangee ensures that personnel are exposed to the same information multiple times in different ways. This greatly improves how people remember the information presented to them. Content may need to be adapted depending on the communication channel. The communication channel used match the audience receiving the training content and the type of content, as well as the content itself.

Electronic communication methods can include e-mail notifications, eLearning, video and audio post etc. It is important to target electronic security awareness notifications to the appropriate audience to ensure the information is read and understood. It is easier for electronic notifications to go unread or ignored by busy

personnel. By targeting the material and communication channel to relevant personnel, the data privacy and information security awareness team can improve adoption of the data privacy and information security awareness program. Non-electronic notifications may include posters, internal mailers, newsletters, and instructor-led training events. In-person security awareness events that involve active participation by personnel can be extremely effective.

As per the established process, on termination of individual employment, we terminate information system access, retrieve all organizational information system-related property, and provide appropriate personnel with access to official records created by the terminated workforce that are stored on organizational information systems.

Vakrangee senior management team provide leadership support for the security awareness program which is crucial to its successful adoption by employee. Managers are encouraged to:

a. Actively encourage personnel to participate and uphold the security awareness principles.
b. Model the appropriate security awareness approach to reinforce the learning obtained from the program.
c. Include security awareness metrics into senior management and staff performance reviews.

28. Security Awareness Training Content

It is recommended training content be determined based on the role and Vakrangee's culture. The data privacy and information security awareness team may wish to coordinate with the appropriate Vakrangee units to classify each role in order

to determine the level of data privacy and information security awareness training required for those specific job duties. This is vital in development of content, as it is just as easy to “over-train” an employee as it is to “under-train” an employee. In both cases, if information is not properly absorbed, it could lead to unnecessary Vakrangee risk. Regardless of role, it is recommended that all staff receive basic data privacy and information security awareness training, developed in accordance with Vakrangee policy. In addition to general data privacy and information security awareness training, it is recommended personnel be exposed to general concepts of cardholder data security, to promote proper data handling throughout Vakrangee, according to their role in Vakrangee. Training materials be available for all areas of Vakrangee. data privacy and information security awareness training materials may be developed in-house, adapted from a professional Vakrangee’s work, or purchased from a vendor.

Below is an example of content that is commonly included in general data privacy and information security awareness training:

- Vakrangee’s Security awareness policy
- Vakrangee’s Data Privacy Policy
- Impact of unauthorized access (for example: to systems or facilities)
- Importance of strong passwords and password controls
- Secure e-mail practices
- Keeping sensitive documents from prying eyes
- Handling data
- How to Identify Phishing Email Scams
- Best Practices for Data Protection and Data Management
- Compliance with Privacy Policies
- Compliance with ISO Policies
- Keeping Software Patches Top of Mind
- Turning Away Social Engineering Attempts

- Knowing What Identity Theft Looks Like
- Best Practices for Choosing a Password
- All About Safe Browser Use and Screen Locking
- How to Report an Incident
- Secure practices for working remotely
- Avoiding malicious software – viruses, spyware, adware, etc.
- Secure browsing practices
- Mobile device security including BYOD
- Secure use of social media
- How to report a potential security incident and who to report it to
- Physical security
- Cyber Surfing
- Dumpster Diving
- Protecting against social engineering attacks
    - In Person – Physical Access
    - Phone – Caller ID Spoofing
    - E-mail – Phishing, Spear Phishing – E-mail Address Spoofing
    - Instant Messaging

29. Define Metrics to Assess Awareness Training

Metrics can be an effective tool to measure the success of a security awareness program and can also provide valuable information to keep the security awareness program up-to-date and effective. The metrics used to measure the success of a security awareness program will vary for Vakrangee based on considerations such as size, industry, and type of training. The table below displays some metrics of a successful security awareness program and can be used as a starting point for developing metrics.

30. Data Protection and Security Awareness Program Checklist

Having a checklist may help Vakrangee's plan and manage their security awareness training program. The information listed below may be used to assist with security awareness training and education planning. Inclusion and use of this information are not a requirement.

30.1 Creating the Data Protection and Security Awareness Program

a. Identify compliance or audit standards that Vakrangee adhere to.
b. Identify security awareness requirements for those standards.
c. Identify Vakrangee goals, risks, and security policy.
d. Identify stakeholders and get their support.
e. Create a baseline of Vakrangee's security awareness.
f. Create project charter to establish scope for the security awareness training program.
g. Create steering committee to assist in planning, executing and maintaining the awareness program.

h. Identify who you will be targeting—different roles may require different/additional training (employees, IT personnel, developers, senior leadership).
i. Identify what you will communicate to the different groups (goal is shortest training possible that has the greatest impact).
j. Identify how you will communicate the content—three categories of training: new, annual, and ongoing.

30.2 Implementing Data Protection and Security Awareness Program

a. Develop and/or purchase training materials and content to meet requirements identified during program creation.
b. Document how and when you intend to measure the success of the program.
c. Identify who to communicate results to, when, and how.
d. Deploy security awareness training utilizing different communication methods identified during program creation.
e. Implement tracking mechanisms to record who completes the training and when.

30.3 Sustaining Data Protection and Security Awareness Program

a. Identify when to review your security awareness program each year.
b. Identify new or changing threats or compliance standards and updates needed; include in annual update.
c. Conduct periodic assessments of Vakrangee security awareness and compare to baseline.
d. Survey staff for feedback (usefulness, effectiveness, ease of understanding, ease of implementation, recommended changes, accessibility).
e. Maintain senior management commitment to supporting, endorsing, and promoting the program.

30.4 Documenting the Data Protection and Security Awareness Program

Document security awareness program including all previously listed steps within "Creating the Security Awareness Program," "Implementing Security Awareness," and "Sustaining Security Awareness.

31. Data Protection Policy

Data protection is commonly defined as the law designed to protect data subject's personal data. A strong data protection framework can empower individuals, restrain harmful data practices, and limit data exploitation. It essential to provide the much-needed governance frameworks nationally and globally to ensure individuals have strong rights over their data, stringent obligations are imposed on those processing personal data (in both the public and private sectors), and strong enforcement powers can be used against those who breach these obligations and protections.

31.1 Data Protection: A Right?

The protection of personal data has long been recognized as a fundamental aspect of the right to privacy. In recent years it has been recognized as a standalone right. For example, data protection has been included as a standalone right under the Charter of Fundamental Rights of the European Union (2012/C 326/02) under Article 8 (in addition to Article 7 of the Charter which upholds the right to privacy). Article 8 reads:

31.2 Protection of personal data

a. Everyone has the right to the protection of personal data concerning him or her.
b. Such data processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
c. Compliance with these rules are subject to control by an independent authority.

31.3 Data subjects can access their accounts to erase, rectify, complete or amend personal information

As per Vakrangee's data protection policy, personal data will be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
b. There will be no secret processors of data, sources, or processing. Individuals or data subject are made aware of the collection and processing of their data, as well as the purpose of its use, who is controlling it, and who is processing it

c. every reasonable step taken to ensure that personal data that are inaccurate (incorrect or misleading), having regard to the purposes for which they are processed, are erased or rectified or amend without delay ('accuracy').
d. Data subject / an individual can make a request for deleting/ modify/erased/rectify its personal data in writing with reasonable reason.
e. Company has reasonable grounds to refuse to erase/delete/modify personal data
f. When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of
g. Individual or data subject have a range of rights which enables them to control their personal data, and any processing

31.4 Clear and accessible mechanisms for data subjects to raise concerns about data privacy

h. There are clear and accessible mechanisms for individuals or data subjects to raise concerns about data privacy
i. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')
j. adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimization') accurate and, where necessary, kept up to date
k. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

l. personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and Vakrangee measures in order to safeguard the rights and freedoms of individuals ('storage limitation')

m. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or Vakrangee measures ('integrity and confidentiality')."

31.5 Disclosures without data subject Consent

We may share personal information with government authorities/ law enforcement agencies in response to warrants, or court orders, in connection with any legal or regulatory process, or to comply with relevant laws. We may also share your personal information in order to establish or exercise our rights, to defend against a legal claim, to investigate, prevent, or take action regarding possible illegal activities, suspected fraud, safety of person or property, for audit purposes, or a violation of our policies.

32. Privacy Risk Assessments

Once we have an initial understanding of data collection, usage and sharing, the next step is to conduct Privacy Risk Assessments to understand the current and future privacy risks from those practices to the individual consumers and to us.

The purpose of a Privacy Risk Assessment is to provide an early warning system to detect privacy problems, enhance the information available internally to facilitate informed decision-making, avoid costly or embarrassing mistakes in privacy compliance, and provide evidence that we are attempting to minimize our privacy risks and problems. Documenting the risk assessment process and findings helps to

ensure the consistency of repeated assessments, effective oversight, successful remediation of potential issues, and a reduction of risk to us.

A privacy risk assessment can identify risks and facilitate mitigation. Risk assessments provide more value when conducted on a regular basis. Regular privacy risk assessments on the company's technologies and practices affecting user data. We determine the specific frequency based on the scope of the assessments, the nature of the data, and the risks to us. We conduct assessments on an annual basis. We also perform ad hoc assessments after any material changes to the internal operations or to the external business, regulatory, economic, or legal environments in which we operate. Risk assessments is a valuable tool for us to reduce the risks associated with increasingly complex issues.

Documenting the risk assessment process and findings helps to ensure the consistency of repeated assessments, effective oversight, successful remediation of potential issues, and a reduction of risk to us.

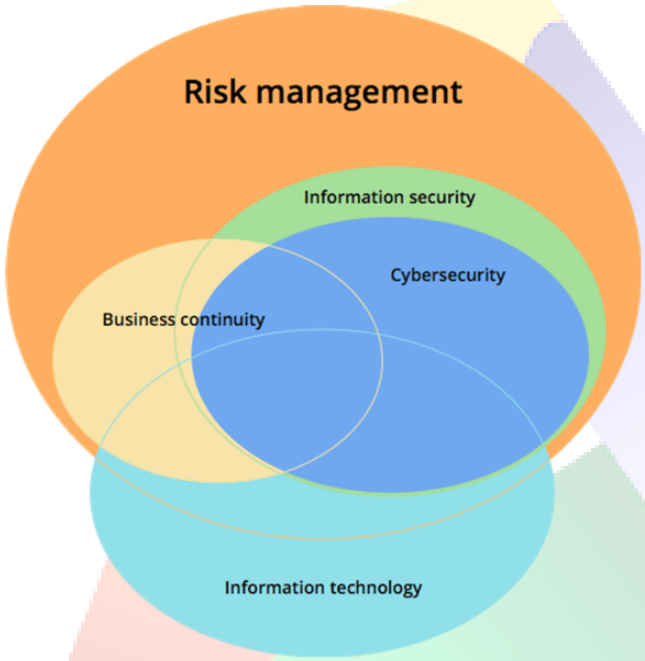
33. Risk Management

The most important thing in Vakrangee is that information security, cybersecurity, and business continuity have the same goal: to minimize the risks of business operations. Vakrangee is having a comprehensive IT risk management process that rolls into an organization's enterprise risk management function.

We have established and implemented robust Risk Management Procedure and Process in place and conduct periodic risk assessments for the organization using the baseline methodology based on ISO 27001 standard framework with cross-reference with ISO 9001, PCI DSS and industry best practices.

Vakrangee is not willing to accept any risk that might damage customer trust. In addition, any risks that threaten to make us non-compliant to regulations and standard. Risk Treatment Plan involves prioritizing, evaluating, and implementing appropriate controls as per the risk computation.

Information security is part of overall risk management in Vakrangee, with areas that overlap with cybersecurity, business continuity management, and IT management, as displayed below.



34. Regulatory and Information Security Audits:

34.1 Regular privacy risk assessments or audits on the company's technologies and practices affecting user data

To demonstrate transparent and effective IT governance practices we have established a security baseline through internal audit, statutory audit, annual audits (internal and external), Technology Audits, surveillance audits (surveillance 1 and surveillance 2) and recertification audits for e.g., ISO audit, ATM Information

Security Assessments audit, Information Security Audits by third party auditor and these information security audit reports are also been shared with regulatory bodies, Government authorities and alliance partners.

We are into Banking & White Label ATM services hence we come under the purview of the Financial regulator of the Country, i.e Reserve Bank of India (RBI), National Payments Corporation of India (NPCI) and other regulatory bodies to ensure that we are following best practices, industry standards and all applicable laws. Under ATM Licensing obligation and Banking Business Service Agreement with partner banks we have to submit various Information Security Audit & Compliance Reports, Process Audit Reports to Reserve Bank of India, National Payment Corporation of India, partner banks and other regulatory bodies and government authorities on periodic basis.

Further, Vakrangee is also an ISO (**International Organization for Standardization**) Certified company with the following standards relevant to Technology:

34.1.1 ISO 27001:2013 Information Security Management System (ISMS)

ISO 27001 is the international standard which is recognized globally for managing risks to the security of information we hold. Certification to ISO 27001 allows us to prove to our clients and other stakeholders that we are managing the security of our information. Vakrangee holds ISO 27001:2013 which is the current version of ISO 27001, provides a set of standardized requirements for an Information Security Management System (ISMS). The standard adopts a process-based approach for establishing, implementing, operating, monitoring, maintaining, and improving our Information Security Management System (ISMS).

The ISO 27001 standard and ISMS provides a framework for information security management best practice that helps us to:

- Protect client and employee information
- Keeps confidential information secure
- Manage risks to information security effectively
- Achieve compliance
- Manages and minimizes risk exposure
- Protect the company's brand image


SHAMKRIS

CERTIFICATE OF REGISTRATION

SHAMKRIS GLOBAL certify that the

Information Security Management System of

VAKRANGEE LIMITED

Complies with requirements of ISO 27001:2013

Scope of Certificate

CAB-05

ISO 27001 2013.pdf

34.1.2 ISO 20001-1:2011 IT Service Management System

Vakrangee hold an ISO Certificate for 20001-1:2011 IT Service Management System Standard. ISO 20000-1 is the international standard specifically focused on IT Service Management, provides a set of standardized requirements for an IT service management system (SMS). It ensures day to day service delivery is carried out in a way that drives customer satisfaction through improved service and leads. ISO 20000-1 helps to ensure the effective running and delivery of IT services, continually improve processes and drive customer focus. Reduction in

incidents and improved incident management. Improving corporate image and credibility. Reduction in response times and interruptions to IT service. A culture of continuous improvement. Greater understanding of roles and business objectives. Ensuring legislative awareness and compliance. Protecting the company, assets, shareholders, and directors. Increased customer satisfaction from internal and/or external customers. Provides us with a competitive advantage. Enhanced customer satisfaction that improves client retention. Consistency in the delivery of your service or product.


SHAMKRIS

CERTIFICATE OF REGISTRATION

SHAMKRIS GLOBAL certify that the

Information Technology Management System of

VAKRANGEE LIMITED

Complies with requirements of ISO 20000-1:2011

Scope of Certificate

ISO 20000-1 2011.pdf

34.1.3 ISO 9001:2015 Quality Management System (QMS)

Vakrangee hold ISO 9001:2015 Quality Management System (QMS) Standard, is internationally recognized as the world's leading quality management standard. The purpose of the standard is to assist in meeting statutory and regulatory requirements relating to the product while achieving excellence in the customer service and delivery. The standard can be used throughout an organisation to improve the performance or within a site, plant or department. It contains eight key principles of quality management which is not auditable but do form the fundamental characteristics of quality management: Customer focus and customer satisfaction,

Leadership, Involvement of people, Process approach, A systematic approach to management, Continual improvement, Factual approach to decision making, Mutually beneficial supplier relationship. QMS enhanced customer satisfaction and improved customer loyalty leading to repeat business. Integration and alignment of internal processes which will lead to increased productivity and results


SHAMKRIS

CERTIFICATE OF REGISTRATION

SHAMKRIS GLOBAL certify that the

Quality Management System of

VAKRANGEE LIMITED

Complies with requirements of ISO 9001:2015

Scope of Certificate

ISO 9001 2015.pdf

34.1.4 ISO 27701:2019 Privacy Information Management System

Vakrangee hold an ISO Certificate for 27701:2019 Privacy Information Management System Standard. ISO 27701 is a privacy extension to ISO 27001 Information Security Management and ISO 27002 Security Controls. ISO 27701 is an international management system standard which provides guidance on the protection of privacy, including how organizations should manage personal information, and assists in demonstrating compliance with privacy regulations around the world. Below are the benefits of ISO 27701:

- Builds trust in managing personal information

- Provides transparency between stakeholders
- Facilitates effective business agreements
- Clarifies roles and responsibilities
- Supports compliance with privacy regulations
- Reduces complexity by integrating with the leading information security standard ISO 27001

SHAMKRIS®

CERTIFICATE OF REGISTRATION

SHAMKRIS GLOBAL certify that the

Privacy Information Management System of

VAKRANGEE LIMITED

"Vakrangee Corporate House", Plot No. 93, Road No. 16, M.I.D.C.
Marol, Andheri (East), Mumbai – 400 093

Complies with requirements of ISO 27701:2019

Scope of Certificate

Delivering Banking, ATM, e-Governance, e-Commerce, Insurance and other strategic alliances and partner's services/products by creating franchisee network and monitoring the performance, impact of our outreach and roll-out initiative by insuring front-end service delivery points within the reach of each and every citizen with prompt, accurate, secure and reliable integrated services/products to end customers through online devices with strong management and field team till the block level end by being the last-mile link connecting India's rural and urban citizens with the modern ecosystem.

Certificate No. : PI 1116 Date of Last Issue : 23/03/2021

Date of Initial Registration: 23/03/2021 Date of Expiry : 22/03/2024

CAB-05

Surveillance Audit
2nd Year: 12 / 2021 2nd Year: 12 / 2022

The Certificate is Valid ONLY if the annual surveillance completed & updated on website

Signed on behalf of SHAMKRIS GLOBAL

This certificate remains the property of SHAMKRIS GLOBAL. This certificate and all copies or reproductions of the said Scale shall be returned or destroyed if requested by SHAMKRIS GLOBAL.

To verify the validity of this certificate, kindly visit our website : www.shamkris.com or call us on +91-22-28540566

ISO Certifications are valid for the period of 3 years, and during the period of 3-year organization must undergo - a Re-certification Audit and two Surveillance Audits done by the Certification Body (CB) only. The cycle begins with a Re-certification Audit and this is followed by 2 Surveillance Audits. For all these audit, the certification body auditors look at the implementation of every process, check for conformance to the ISO standard, as well as company documentation, looking key

processes (such as management review, internal audit, and corrective actions), process effectiveness, and continual improvement.

Vakrangee is having a strong internal control system, including effective internal audit function, policies and practices are followed and senior management takes appropriate and timely corrective action in response to internal control weaknesses identified by internal auditors. Audits are security assessment to ensure that security guidelines are followed. Audits ensure well established security posture which help us measure the effectiveness of information security of Vakrangee eco systems. Internal and external security reviews serve as a baseline and we make sure the level of risk discovered should be consistent or even decline over time.

35. Audits evaluates the flow of data within our business.

Data is one of our key assets that requires top security controls. IT security auditors determine the type of information we have, how it flows in and out of our organization, and who has access to that information. All technologies and processes related to our anti-data breach measures are reviewed to make sure that no data will be lost, stolen, misused, or mishandled.

35.1 Audits identifies vulnerable points and problem areas.

IT system is a vast one with several components including hardware, software, data, and procedures. Expert auditors can pinpoint if there's any potential problem area in

our system through a few ways. They can check if our hardware or software tools are configured and working properly. They may also retrace security incidents from the past that might have exposed our security's weak points. An on-site audit may focus on carrying out tests in terms of network vulnerability, operating system, access controls, and security application.

35.2 Audits determines whether we must alter security policies and standards or not.

The auditing process starts with the pre-audit, where auditors obtain relevant documentation about previous audits, as well as copies of current policies and procedures. Afterward, they analyze and test our entire system on-site. Throughout the auditing process, the auditors are documenting everything they have discovered regarding the safety and effectiveness of our IT system. By the time they complete the audit, they would have had a clear assessment if we have adequate security measures that are consistently implemented within our organization. For example, they might discover instances of unauthorized wireless networks that could pose risks beyond acceptable levels.

35.3 Audits recommends how to leverage information technology in our business security.

The technologies we use should match the level of security that our business needs. That's why part of an IT security audit's function is to help understand how to choose the right security tools for our organization. The auditors can also determine if we need to either centralize our security solutions across all devices or make use of special software for each risk area. Security experts performing the audit can also advise us if we are underspending or overspending on our IT system, so we could

allocate our security resources properly. They could discourage us from trying to secure every server or app if they feel the level of risk does not merit it.

35.4 Audit delivers an in-depth analysis of our internal and external IT practices and system.

IT security audit report contains a detailed list of the findings of the auditing team, complete with an executive summary, supporting data, and appendices. It highlights problem areas and proposed solutions regarding risk areas, compliance with industry standards, security policies, and the like.

The auditing team can also lay the groundwork for any improvements or enforcements needed in this area.

So, we plan for Audits to:

a. Ensure integrity, confidentiality and availability of information and resources
b. Monitor all security measures to ensure conformance of our security policies
c. Investigate security incidents recorded in security logbook

Security Audit is done to protect entire system from the most common security threats which includes:

a. Access to confidential data
b. Unauthorized access of the department computers
c. Password disclosure compromise
d. Virus infections
e. Denial of service attacks
f. Open ports, which may be accessed from outsiders

It is the responsibility of all Departments of Vakrangee to place an appropriate system of internal audit, which provides an independent assessment of security

policies. To execute these policies, internal audit team also take proper action and generate reports/documents based on internal audit. The internal audit team and organization lead auditor is responsible for internal Audit within all department and operations.

When requested and for the purpose of performing external audit, any access needed will be provided to members of External Audit team. This access includes:

a. User level and/or system level access to any computing or communications device
b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on respective Dept. equipment or premises
c. Access to work areas (offices, cubicles, storage areas, etc.)
d. Access to reports / documents created during internal audit.
e. Access to interactively monitor and log traffic on networks.

36. Management and Oversight

Vakrangee's senior management assign a specific individual or group of individuals with responsibility for implementing the risk assessment process, conducting the assessments, and managing any resulting remediation. The risk assessment process may also necessitate reports to senior management about the results and subsequent remediation activities.

High-profile data breaches and government investigations have brought privacy and information security risks to the attention of boards of directors, investors, and consumers like never. Risk assessments can be a valuable tool for Vakrangee to reduce the risks associated with these increasingly complex issues.

37. Remedy for victim in case of violations of company's data sharing practices

Our Security Incident Response Plan is designed to promptly and systematically respond to security, privacy, and availability incidents that may arise. The incident response plan is tested and refined on a regular basis. Security Incident Response Policy & Procedure has become an important component of our Information Security programs.

A data breach refers to an incident exposing personal data in an organization's possession or under its control to the risks of unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks. Data breaches often lead to financial losses and a loss of consumer trust for the organization. In addition, individuals whose personal data have been compromised (the "affected individuals") could be at risk of harm or adverse impact if we as an organization and individual do not take steps to protect themselves. Hence it is important for organizations to be accountable towards individuals by preventing and managing data breaches.

In a data breach incident, we also ensure that our employees are aware of their roles and responsibilities (e.g. reporting, investigating, taking remedial actions) in managing the data breach. Each data breach response needs to be tailored to the circumstances of the incident.

First a prompt written notice within the time frame required under Applicable Data Protection Law(s) to a customer. Under no circumstances should a user attempt to resolve any security and privacy breach on their own without first consulting our Data Protection Officer (DPO). Users may attempt to resolve security and privacy breaches only under the instruction of, and with the express permission of the Data Protection Officer

The actions taken after a data breach follow four key steps (using the acronym of **C.A.R.E**):

Step 1 - Containing the data breach to prevent further compromise of personal data.

An organization should act swiftly as soon as it is aware of a data breach, whether suspected or confirmed. an assigned individual or individuals should be notified of all suspected/confirmed data breaches immediately upon detection. He/she should then activate the data breach management team as the team is responsible for carrying out the actions that can reduce the potential impact of a data breach. Upon being notified, the individual members of the team should act on the information received according to their assigned role.

An initial assessment of the data breach should be conducted to determine the severity of the data breach. It will also allow the organization to notify other stakeholders such as the internal or external legal counsel specializing in data protection and technical forensics specialists to be ready so that their expertise will be available on short notice. The initial assessment should include (but not be limited to) the following:

a. Cause of the data breach and whether the breach is still ongoing
b. Number of affected individuals
c. Type(s) of personal data involved
d. The affected systems and/or services
e. Whether help is required to contain the breach

The details of the data breach and post-breach response(s) should be recorded in an Incident Record Log to allow follow-up investigations or reviews.

Step 2 - Assessing the data breach by gathering the facts and evaluating the risks, including the harm to affected individuals.

Where assessed to be necessary, continuing efforts should be made to prevent further harm even as the organization proceeds to implement full remedial action.

Upon containment of the data breach, the organization should conduct an in-depth assessment of the data breach. Assessing the extent and likely impact of the data breach will help the organization identify and take the appropriate steps to limit the impact2 of a data breach.

We also need to check whether the data breach is unlikely or likely to result in significant impact or harm to the affected individuals; and consider, and if necessary, take steps to reduce any potential harm to the affected individuals. Organizations may also implement fixes to system errors/bugs to prevent further disclosure of/access to personal data.

Step 3 - Reporting the data breach to the data protection agency and affected individuals, if necessary.

Step 4 - Evaluating the organization's response to the data breach incident and consider the actions which can be taken to prevent future data breaches. Remediation efforts may continue to take place at this stage.

Steps taken by Vakrangee in case of violations of data breach:

In case of any data breach user has following remedies to protect his/her fundamental right of privacy of his/her personal information & data.

a. Immediate inform to victim about a breach occurred, type of data breach, affecting information or information exposed, its consequences like data can be used to commit fraud and provide solution or remedial action
b. Provide details about the situation took place
c. Asked and assist victim to change and strengthen all online logins, passwords and security Q&A of data affected along with other data and take precautionary measures of two-factor authentication for logins
d. Asked victim to stay alert and monitor your logins or accounts closely

e. Provide a special offer to victim and help repair the damage
f. Report to senior management
g. Notify Data Protection Authority (DPA)
h. Post the details of the personal data breach on organisation website as a precautionary measure
i. Ask victim to report any unusual activity
j. Increase monitoring by organisation and victim as a preventive action or any unusual activity

So, developing an effective data protection program may seem like a daunting task at the outset, but if you take it step by step, and employ the right people and technology, it is easily doable. Moreover, the alternative—ignoring data protection and hoping nothing bad happens—makes no sense for any responsible organization.

Thank You

CORPORATE OFFICE:
Vakrangee Corporate House
Plot No. 93, Road No. 16, M.I.D.C., Marol, Andheri (East), Mumbai – 400093, Maharashtra