Vakrangee
सशक्त परिवर्तन

INFORMATION SECURITY & MANAGEMENT POLICY

Contents

1. Introduction

We are committed to ensuring the Confidentiality, Integrity, and Availability (CIA) and providing comprehensive protection to its information assets against the consequences of confidentiality breaches, failures of integrity and/ or interruptions to their availability. To provide adequate protection to information assets, we have built the Information Security Management System (ISMS) which includes the respective policies to be followed in a diligent, consistent, and impartial manner. We have implemented procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed on our systems and ensure that information is available only to authorized persons as and when required.

This document details our policies to ensure the protection of our information assets, and to allow the use, access, and disclosure of such information in accordance with appropriate standards, laws, and regulations.

All workforce members, employees, customers, and third parties who use our information processing facilities are required to comply with this Information Security policy. All our existing policies, relating to personnel, administration, protection of confidential information, and other areas would apply equally to the information systems environment.

Our Information Security & Management Policy is fully compliant with THE INFORMATION TECHNOLOGY ACT, 2000 (Government of India).

2. Applicability

We are committed to comply with all applicable regulations and law of the land in all locations related to our operations and information processing.

The key regulation that is complied with includes laws related to corporate governance, employee relations, data privacy, intellectual property, and financial reporting.

3. Scope

The scope of this policy covers all information assets owned or provided by us, whether they reside on the corporate network or elsewhere.

Information Security policies apply to all our business functions. The Information Security policies apply to any person (employees, consultants, customers, and third parties), who accesses and uses our information systems.

We have established, implemented, maintained, and continually improved the Information Security Management System within the context of its overall business activities and risks we may face in accordance with the requirements of the ISO 27001:2013 standard. The ISMS processes used are based on the Plan, Do, Check, and Act (PDCA) model.

3.1 Plan (Establish the ISMS)

We have established policies, related processes, objectives, and procedures relevant for managing risks and improving information security to deliver results in accordance with our overall policies and objectives.

3.2 Do (Implement and operate the ISMS)

We have adopted and implemented procedures and processes to ensure compliance and adherence to the ISMS framework. We have made all the necessary resources available to ensure implementation and operation according to the ISMS.

3.3 Check (Monitor and review the ISMS)

Our compliance team ensures regular and continuous monitoring by conducting periodic assessments, reviews, and audits of our Information Security policy.

3.4 Act (Maintain and improve the ISMS)

Continual improvement in the effectiveness of ISMS is demonstrated the use of Security Policy, Security Objective, Audit Results, Analysis of Data, Corrective and Preventive Actions, and Management Review.

4. Leadership and Commitment

We are committed to security. Our top management has constituted Vakrangee Corporate Security and Compliance Team, which is responsible for defining and improving the ISMS.

We have also 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 of 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

5. Policy

The following is the information security management policy statement adopted by us:

“We are committed to ensuring integrity, confidentiality, availability, and security of our physical and information assets at all times for serving the needs and expectations of our interested parties both within organization and from external parties including clients, suppliers, regulatory, and governmental departments in line with our vision, mission, and values while meeting all legal, statutory, regulatory, and contractual requirements. Our information systems, the information and data they contain are fundamental for our daily operations and future success.”

The Information Security measures include:

5.1 Governance and Organization Structure

We have established a Corporate Security and Compliance Team (CSC) made up of key personnel who are responsible to identify areas of security and compliance concern across our organization and act as the first line of defence in enhancing the appropriate security and compliance posture. This team reports to the Chief Technology Officer.

The team comprises of the workforce who are knowledgeable in legal cross-regulation, policy, products, and IT, and are interested in ensuring five of the trust principles—confidentiality, integrity, availability, privacy, and security—with regard to data protection by law, compliance, and standards across the organization. The Chief Technology Officer has assigned the responsibilities and authority to Data Protection Officer for overseeing and maintaining information security and compliance as per the standard and industry best practices.

The governance of these programs is performed by the Corporate Security and Compliance Committee, consisting of executives and other department heads from across the organization.

5.2 Personnel Security

We have established a formal sanctions policy and process for personnel failing to comply with established information security and compliance policies and procedures.

We have established personnel security requirements, including security roles and responsibilities for third-party providers, and monitors provider compliance.

We screen individuals requiring access to any business, production environment information and information systems before authorizing access. The only workforce with the highest clearance has access to our data center data. Workforce access is logged, and passwords are strictly regulated. We follow as needed basis access principles to production data to only a select few of these workforces who need such access to provide support and troubleshooting.

As per the established process, on termination of individual employment, we terminate information system access, conduct exit interviews, 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.

We have developed a world-class practice for managing security and data protection risk.

- **Awareness and Training**
  - **Information security awareness, education and training -** All workforce members complete a minimum requirement of annual information security and privacy awareness and training program. All employees of the organization and, where relevant, suppliers and contractors receive appropriate update on training and any changes in organizational policies and procedures, as relevant for their job function on a semi-annual periodic basis. We have developed effective education and awareness training program in line with their internal information security policies as well as in compliance with the ISO Framework.

As part of this program, additional role-based training is provided to the employee, before they start handling sensitive and confidential information. Information Security and Compliance Training Guide is provided as a quick reference guide to all employees. Training logs identifying the training class, attendee, and date are kept by the HR department

ISO 27001 certification is a globally recognized international standard outlining the best practices for Information Security Management Systems. It sets out what best practices and systematic approach an organization's technical, legal, and physical controls should have for information risk management and periodic risk assessment. ISO 27001 requires numerous controls for the establishment, maintenance, and certification of an information security management system (ISMS) which is a set of policies, procedures, processes and systems that manage information risks, such as cyber-attacks, hacks, data leaks or theft.

Vakrangee is ISO 27001:2013 Information Security Management System (ISMS) certified company since 2009 offering a robust model for security risk assessment, security design, implementation, and management. Certification to ISO 27001:2013 demonstrates that Vakrangee has defined and put in place best-practice information for security processes. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks.

Vakrangee information security management system (ISMS) is a set system used to manage and control information, risks in security as well as maintaining the integrity, protection and preservation and confidentiality of information. Vakrangee information security management system (ISMS) includes policies around access control, incident management, data protection, business continuity, physical security, human resources and technical procedures.

Further, We have identified various types of behaviours that contribute to building security culture in an organisation. Vakrangee has used multiple channels of communication, enforcement, clear policies, rules and norms. Secure behaviour is also encouraged through recognition, e.g., a security certificate, and strong messages to defaulters. Secure behaviour is strongly influenced through raising awareness.

The various types of behaviour are reproduced here for reference along with the specific measures adopted by Vakrangee to embed these behaviours into the daily practice of bank employees:

- **Information security is practiced in daily operations -** The information security management committee has conveyed its expectations of employees by stressing the principle of zero tolerance for unacceptable behaviour relating to information security, rewarding good behaviour, recognising and rewarding people for good work towards risk management. This has ensured that information security is practiced in daily operation.

- **People respect the importance of information security policies and principles -** The security culture has been built over time through constant efforts in creating awareness. Employees now understand the importance of information security and take security initiatives seriously. Audit has also played an important role in enforcing various security policies and principles.

- **People are provided with sufficient and detailed information security training, guidance and are encouraged to participate in and challenge the current information security situation -** Introduction of any new process involves ensuring open interaction with all the affected parties. The issues are discussed in workshops and buy-in is achieved through two-way dialogue—allowing everyone to clarify any doubts they may have. Extensive training is provided for every new information security initiative, not only to the information security group but to all stakeholders.

- **Everyone is accountable for the protection of information within the enterprise -** The information security management committee is responsible for identifying and managing the risk whereas the business heads are held ultimately accountable. This makes all the stakeholders feel responsible as well as accountable for protection of information within the enterprise.

- **Stakeholders are aware of how to identify and respond to threats to the enterprise -** Threat identification is part of the training provided to stakeholders Stakeholders are encouraged to report incidents. 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.

- **Management proactively supports and anticipates new information security innovations and communicates this to the enterprise -** The enterprise is receptive to account for and deal with new information security challenges. There is full management support to interact with industry and share knowledge and experience with a larger audience as well as learn from others.

- **Business management engages in continuous cross-functional collaboration to allow efficient and effective information security programmes -** The structure of various committees is an example of continuous cross-functional collaboration. Making information security independent of the IT function has provided a much broader reach and direct access to various business groups across the organisation.

- **Executive management recognises the business value of information security -** The Information Security management committee works at a strategic level, reporting to the Board of the company. This has empowered the Information security committee to drive various information security initiatives with a great amount of freedom. This is a good indication of management's recognition of the business value of information security

- **Disciplinary Action in case of Violation of Information Security Policy**
  Adherence to Information Security Policy is considered is considered as an important parameter while evaluating performance of employees. In case, any employee is found violating any sections of the Information Security Policy, disciplinary and/or legal action is taken according to the Sanction Policy.

- **Information security Awareness and Training Program for the Board**
  The board members at our institution are responsible for oversight and implementation of a sound Information security and management program, including the overall guidance and direction of setting a cultural value related to risk awareness, driving policy and strategy, defining a global risk profile and creating security initiatives and priorities for the organization.

All Board members complete a minimum requirement of annual information security and privacy awareness and training program dedicated for the Board of Directors

We have further formed a dedicated Information security and management committee. The primary purpose shall be to act on behalf of the Company's Board in fulfilling the Board's oversight responsibility with respect to the Company's Information security strategy formulation and implementation. Also overseeing information use and protection, including but not limited to data governance, privacy, compliance, and cybersecurity.

The key training board program includes:

- A thorough understanding of changes in regulatory issues and impacts and changes in business as it relates to the overall practices at our organization.
- An effective understanding of security as it relates to the enterprise risk model from a high level.
- Understanding and getting Realistic feedback on what the highest risk policy and processes are? And where are the security vulnerabilities within the institution?
- Understand the impact of security failures on the business and the potential effect on stakeholders, competition etc.
- Understanding from the Information security committee the consequences of security incidents and repercussions of inadequate training in terms of loss of revenues and lack of customer and investor confidence.
- Focus in ensuring that security initiatives and improvements are measured and monitored on a regular basis and all are part of an evaluation process.
- Drive the point of personal and individual responsibility that each board member and employee has in terms of owning and participating in the training and education process.

5.3 Information Asset Management

We have established a formal Asset Management policy; and the process is necessary to facilitate effective management, control, and maintenance of the assets/information to its operations environment by classifying assets as per the functionality or criticality.

This policy to identify, classify, label, and handle Information Assets of Vakrangee, and to apply protection mechanisms commensurate with the level of confidentiality and sensitivity.

The confidentiality and sensitivity of information shall be maintained through an

Information Asset classification scheme. The level of security to be accorded to our information depends directly on the classification level of the asset, which is associated with that information.

The Information Asset Inventory must contain the following information as a minimum:

- Information Asset Identification
- Information Asset Description
- Information Asset Location
- Information Asset Owner/Custodian
- Information Asset Classification
- Our Information

Our information may include, but is not limited to:

- All proprietary information that belongs to us such as user manuals, training materials, operating and support procedures, business continuity plans, and audit trails.
- Personnel information relating to our employees.
- All client information & product research-related data held by us.
- All software assets such as application software, system software, development tools, and utilities.
- All physical assets, such as computer equipment, communications equipment, removable media, and equipment relating to facilities.
- All services, such as power, lighting, Heating, ventilation, and air conditioning (HVAC) associated with our information systems.
- People assets.
- Intangibles asset such as our reputation and image.

5.4 Access Control

The access controls required to meet the security objectives of the Information Security policy. Access control management is paramount to protecting our information resources and requires implementation of controls and continuous oversight to restrict access.

Confidentiality, Integrity, and Availability (CIA) are fundamental aspects of protection of systems and information, and are achieved through logical, physical, and procedural controls. It is vital for the protection of systems and information authorized users who have access to our systems and information are aware of and understand how their actions may affect security and privacy.

The policy is organized into the following key sections which map directly to the ISO 27001 Access Control Domain security objectives:

- Business Requirements for Access Control
- User Access Management
- User Responsibilities
- Application and Application Access Control
- Mobile Computing and Teleworking

Access control is established by imposing standards for protection at the operating system level, at the Application level, and at the Database level. Access to our computer systems shall be based on the principles of "least privilege" and "need to know" and must be administered to ensure that appropriate level of access control is applied to users as well as system support personnel to protect our information systems.

Administrative (also known as "root") access to systems is limited to employees who have a legitimate business need for this type of access. Administrative access to network devices is logged.

All access to our systems and services are reviewed and updated on a quarterly basis to assure proper authorizations are in place commensurate with job functions.

Access to electronically stored records containing personal information shall be electronically limited to those workforces having an authorized and unique login ID assigned.

Wherever practical, all visitors, who are expected to access areas other than common space, granted access to office space containing personal information should be required to sign in at a designated reception area where they shall be assigned a visitor's ID or guest badge unless escorted at all times. Visitors are always required to wear visitor ID in a plainly visible location on their body unless escorted at all times.

Wherever practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved person in any area where files containing personal information are stored.

Facility management and Housekeeping personnel (or others after normal business hours and not also authorized to have access to personal information) are not to have access to areas where files containing personal information are stored.

All computers with an Internet connection or any computer that stores or processes personal information must have a recently updated version of software providing virus, anti-spyware, and anti-malware protection should always be installed and active.

5.5 Physical and Environmental Security

Our data centers are hosted in some of the most secure facilities available today in different geographic locations which are far away from each other and in different seismic zones. We use industry best practices that are protected from physical and logical attacks as well as from natural disasters, such as earthquakes, fires, and floods. Physical security measures for these data center include intrusion protection measures and security guards. Within our office premises, we employ best industry-standard physical security controls.

5.6 Operational Security

We have established a formal policy and process for the requirements and key information security considerations for information technology operations, including the definition of standard operating procedures, change management, configuration management, release management, information backup, and restoration.

A. Risk Management:

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.

We are not willing to accept any risk that might damage customer trust,in addition to 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.

5.7 Communication Security

We have deployed an information technology network to facilitate its business and make it more efficient for various risks. We have also establish management direction, principles, and standard requirement to ensure that the appropriate protection of information on our networks are maintained and sustained. Few controls which in place to achieve the protection of exchanged information from interception, copying, modification, misrouting, and destruction as follow:

A. Network Controls

We monitor and update our communication technologies periodically with the goal of providing network security as per industry best practices cryptographic techniques are used to protect the confidentiality, integrity, and authenticity of sensitive and confidential information. Firewall rules and access restrictions are reviewed for appropriateness on a regular basis.

B. Infrastructure Controls

We use an Intrusion Detection System (IDS), a Security Incident Event Management (SIEM) system and other security monitoring tools on the production servers hosting our product service. Notifications from these tools are sent to our Security Team so that they can take appropriate action.

C. Secure Communication

All data transmissions to our services are encrypted using TLS protocols, and we use certificates issued by SHA 256 based CA ensuring that our users have a secure connection from their browsers to our service. We use the latest and updated cipher suites. Our Products are always communicated via HTTPS using Transport Layer Security (TLS), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.

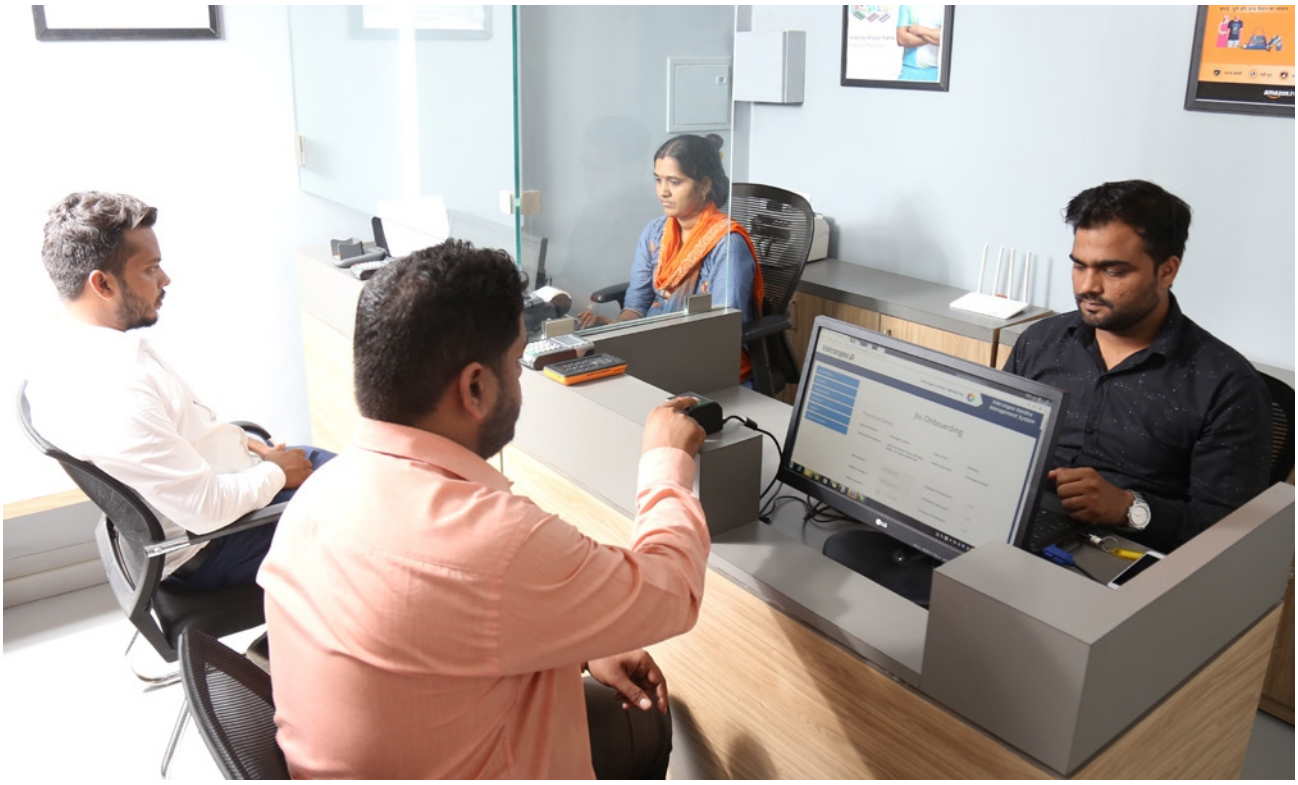
Our Product is always connected to the web-app via HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.

Retention and disposal guidelines for all business correspondence including messages, in accordance with the defined standard.

D. Segregation of the network

Testing, Production and Development environment is segregated.

Agreements have been established for the secure transfer of business information to external parties (such as customers, suppliers, and other interested parties).



The roles and responsibilities for management of network security shall be clearly defined, communicated and reviewed on a regular basis to ensure optimum operative effectiveness and necessary segregation of duties shall be done to attain the said objective.

5.8 System Acquisition, Development, and Maintenance

We have established Software Development Lifecycle adopted for planning, requirement analysis, design, development and testing. There are controls in place to achieve the information security and data protection requirements as follow:

A. Product Security

Our product security practices are measured using industry standard and methodologies security models. We follow Agile methodologies for feature delivery and Scrum is used for new feature delivery. The SDLC for the our Product services includes many activities to enhance security and privacy posture.

We use Definition of Done (DoD) to maintain the quality of deliverables, a clear and consistent Definition of Done is an effort to create an objective framework for quality. DoD provides a clear guideline to the team and to the stakeholders around exactly what needs to be done for each Story, Sprint, Release, and Task to ensure a consistent and sustainable quality of deliverables. It ensures transparency and quality fit for the purpose of the product and organization.

B. Code Security

Our Product code is stored in a secure system hosted by most secure data center facilities. We adopt a strict, least access privileges principle for providing access to the code. Commits to production code are strictly reviewed, and approval is restricted to a team of empowered group of people.

C. Record Retention and Data Destruction Policy

Our responsibility is to protect the integrity and confidentiality of personal data held by us about our clients, employees and partners. Individual employees also have an obligation to protect the integrity and confidentiality of personal data and to prevent unauthorized disclosure of data whether it is oral, printed, hand-written or computer based.

As per policy, we shall not be keep data for longer than it is necessary for that purpose. Data shall be destroyed after the retention period in a way which does not breach the data protection rights of our employees, vendors and customers.

All office paperwork for destruction shall be shredded or placed in the designated confidential waste bins provided in the offices.

Destruction is agreed by the ISMS Committee or Executive Board Director or Management.

5.9 Third-Party Vendor

We provide essential services and business functions which rely on IT solutions and applications contracted by third-party vendors, which may be primary or subcontractors.

We maintain the integrity and accuracy of our information to meet our goals and obligations, both to the business and to people. To ensure this, it is essential that information is secured in line with professional best practices as well as statutory, regulatory, and contractual requirements that maintain confidentiality, integrity, and availability of all information assets.

We have established a formal Third-Party Vendor Management policy and put in place contracts and dealings with third-party vendor which have acceptable levels of data protection and information security in place to protect information (such as personal & company data) and maintain the confidentiality, availability, and integrity of information and are fit for the purpose. Information security requirement shall vary according to the type of contractual relationship with each vendor. There are a few controls in place to achieve protection of data, information, and information system as follows:

information should be limited wherever possible according to clear business needs.

Basic information security principles such as least privilege, separation of duties, and defence in depth applied.

We have the Rights to Audit the information security and privacy practices of the vendor and/or the subcontractor.

Vendor access to our information resources is granted solely for the work contracted and for no other purpose.

On termination of a vendor or its employee from the contract for any reason, the vendor shall ensure that all sensitive and confidential information is collected and returned to us or destroyed within 24 hours.

The security of information is fundamental to our compliance with data protection legislation and a key focus in its ISO 27001 risk assessment, procurement, and management strategy.

A. Due Diligence

Before contracting with a third-party vendor, it is incumbent upon us to exercise due diligence in reaching as much understanding as possible of the information security approach and controls the company has in place. It is important that the documented "vendor due to diligence assessment" procedure is followed so that all the required information is collected, and an informed assessment can be made.

B. Contract

All our contracts shall clearly define each party's data protection and information security responsibilities toward the other by detailing the parties to the contract, effective date, functions or services being provided (such as defined service levels), liabilities, limitations on use of subcontractors and other commercial/legal matters normal to any contract.

The processing must be governed by a contract in writing between the controller and the processor, setting out the following:

- Subject matter and duration of the processing
- Nature and purpose of the processing
- Type of personal data and categories of data subjects involved
- Obligations and rights of the controller and processor

5.10 Reporting Security and Privacy Breaches

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.

Apart from this, any employee can raise issue in case if he/she finds anything suspicious with respect to information security. The following escalation matrix is to be followed.

- Level 1 - Information Security Officer - infosec@vakrangee.in
- Level 2 - Data Protection Officer / Group CTO - sanjayn@vakrangee.in
- Level 3 - Director - R&D (Board Representative) - drhayat@vakrangee.in

We agree to provide a prompt written notice within the time frame required under Applicable Data Protection Law(s) to an employee / customer if it knows or suspects that a security incident has taken place. Such notice shall include all available details required under Applicable Data Protection Law(s) for the customer to comply with its own notification obligations to regulatory authorities or individuals affected by the security incident.

Under no circumstances should a user attempt to resolve any security and privacy breach on their own without first consulting the our Data Protection Officer. Users may attempt to resolve security and privacy breaches only under the instruction of, and with the express permission of the Data Protection Officer

5.11 Business Contingency and Disaster Recovery

We have established a formal business contingency management (BCM) plan and a Disaster Recovery Plan (DRP) to minimize downtime of the critical business process, and recovery within required and agreed business timescales in the event of a disaster. We havealso created a clearly defined framework for the ongoing management of the BCM activities and provide guidelines for the development, testing, maintenance, and implementation of business continuity plans.
We test our Business Continuity Plans and Disaster Recovery / Incident response plan on a semi-annual basis.

A. **We defined two categories of systems from the disaster recovery perspective:**

   a. **Critical Systems**

      These systems host application servers and database servers or are required for the functioning of systems that host application servers and database servers. These systems, if unavailable, affect the availability of data and must be restored, or have a backup process to restore these, immediately on becoming unavailable.

   b. **Non-Critical Systems**

      These systems include the ones that are not considered most critical. These systems, while they may affect the performance and overall security of critical systems, do not prevent critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

B. **Backup**

   To prevent data loss due to human error, our application databases are backed up every hour in an automated fashion

C. **Data Replication**

   Our customer and application databases are timely replicated on backup servers along with our CDN servers which are geo-redundant.

D. **Location**

   We store customer data in a secure data center at different geographical location

E. Internet Redundancy

We are connected through multiple ISPs to ensure availability of applications and information. Even, if any of the link fails or experiences a delay locally or at ISP level services shall be available.

DRP is tested on a regular basis; and the results are documented, and revisions are made, as necessary.

5.12 Compliance

We have established a formal Compliance Policy and Procedure which addresses aspects of compliance required to be adhered to and fulfilled with respect to our Information Security Policies. This policy also addresses the legal and compliance requirements pertaining to relevant statutory legislation, and contractual and regulatory obligations which we are supposed to adhere to in order to protect its documents, records, and assets, thereby preventing the misuse of information processing facilities. Such efforts would help us to establish, maintain, and sustain the desired information security and privacy posture aligned with the our strategic business plan, based on the best practices, standards, and principles.

We are committed to and conducts its business activities lawfully and in a manner that is consistent with its compliance obligations.

We have identify all relevant regulatory and legislative requirements in lien of its contractual requirements and organization's operational requirements and defining, documenting, and updating it on a regular basis.

All records, as mandated by statutory/legal/regulatory authorities in India or of foreign origin, for which we are responsible for compliance, shall be protected from intentional or unintentional damage through natural causes.

The retention limit of statutory records shall be as mandated by the applicable legislation. However, for business records/documents, the business group heads and or HODs shall determine the retention limit with justification.

We shall always seek to protect the privacy of the personal information of its customers, employees, and third parties with whom we have signed the third-party agreement. Divulging of facts shall be done only in keeping with statutory/contractual/regulatory/legal requirements. Such information shall always be protected from getting misused, leaked, or falsified or traded with any interested party knowingly or unknowingly.

Where logs are required to be maintained as per contractual/regulatory/statutory/legal requirement, these shall be maintained for a specified duration.

Data or records that are no longer required for business, legal, and/or regulatory purpose shall be disposed of securely.

Legal restrictions on the use of assets in respect of which there are IPRs (such as copyright, software license, trademarks, design rights, and others) shall be complied with.

Intellectual Property Rights of software programs, documentation and other information generated by or provided by our users, consultants, and contractors for the benefit and be the property of the the organization, -

Intellectual Property Rights shall be included in all contracts.

Relevant statutory, regulatory, and contractual requirements for our information assets shall be defined explicitly. Such requirements shall include, but are not limited to:

- Information Technology Laws (IT Act 2008/2011 Amended) (GOI)
- Software Licensing Requirements
- Intellectual Property Rights (IPR) Laws
- Labor and General Employment Laws
- Health and Safety Laws
- Environmental Laws

As part of the information security audits by independent consultants or body, the appropriate confidentiality and non-disclosure agreements shall be signed with them. And any access granted to the external shall be restricted immediately after completion of the audit.

Compliance requirements are used to enforce a minimum level of security and privacy within the organization. These are by no means a "finish line" for security and privacy.

A. Information Security Program

We agree to implement appropriate technical and organizational measures designed to protect Customer Personal Data, Employee and third-parties data, as required by the Applicable Data Protection Law(s). Further, We agree to regularly test, assess, and evaluate the effectiveness of its Information Security Program to ensure the security of the Processing. We have a comprehensive privacy and security assessments and certifications performed by regulatory or third parties. Such certifications include ISO 27001: 2013, BS 10012:2017 certifications.

Any employee/user/workforce member shall abide by Information Security & Management Policy and in case of any violation of the policy may be subject to disciplinary and/or legal action according to the Sanction policy.

5.13 Information Security / Cyber security Risk insurance Policy

Vakrangee is committed to safeguarding and protecting information and any other information entrusted to us by all of our stakeholders. This means we take cyber security issues very seriously and recognise the importance of privacy, security, and community outreach. 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.

We have a robust Information security / Cyber security Risk Insurance cover in place. Our Cyber security Risk insurance Policy cover is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage.

Following is the list of the key coverage's :-

- Loss of Personal Information
- Loss of Corporate Information
- Outsourcing Liability
- "Network Security/ Liability Cover"
- Data Administration Investigation / Data Administration Fines
- Proactive Forensic Services
- Repair of Individual Reputation
- Repair of Companies Reputation
- Notification Costs
- Monitoring Costs
- Electronic Data Cover
- Multimedia Liability Cover
- Cyber/Privacy Extortion
- Business/Network Interruption
- Emergency Professional Fees
- PCI-DSS Fines & Penalties Cover
- Cyber Terrorism
- Cover for Auto Inclusion of Newly acquired subsidiaries
- Extended Reporting Period
- Reward Expenses
- E-Theft/Fradulent Funds Transfer
- E-Communication
- Punitive , Exemplary & Multiplied Damages
- Psychological Support Expenses
- Territory & Jurisdiction

Vakrangee
सशक्त परिवर्तन

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