

Version	Approval Date	Prepared By	Approved By
V1	07-Feb-2024	Info Sec	Board



Table of Contents

Important Note: ..... 3

1. Introduction ..... 3

2. IT Governance Framework ..... 4

3. Governance and Structure ..... 4

1.1. Role of the Board of Directors ..... 4

1.2. IT Strategy Committee (ITSC) of the board: ..... 4

Roles and responsibilities of ITSC: ..... 4

1.3. Senior Management and IT Steering Committee: ..... 5

Roles and responsibilities of IT Steering committee: ..... 5

1.4. Reporting Structure: ..... 6

2. Roles and Responsibilities of CPO, CDO and CTO ..... 6

2.1. Chief Product Officer: ..... 6

2.2. Chief Data Officer: ..... 7

2.3. Chief Technology Officer: ..... 7

2.4. IT Functions: ..... 7

3. IT Security and Compliance ..... 8

3.1. Data Security: ..... 8

3.2. Compliance with RBI Guidelines: ..... 8

4. Risk Management ..... 8

4.1. Risk Assessment: ..... 8

4.2. Business Continuity and Disaster Recovery: ..... 9

5. Resource Management: ..... 9

6. Performance Management ..... 9

7. Technology Infrastructure ..... 9

7.1 Hardware and Software: ..... 9

7.2 Scalability and Redundancy: ..... 9

8. Data Management ..... 10

8.1 Data Classification and retention: ..... 10

9. Cybersecurity ..... 10

9.1 Cybersecurity and resilience Framework: ..... 10

9.2 Incident Response, recovery and Reporting: ..... 10

10. Vendor Management ..... 10

10.1 Vendor Selection: ..... 10

10.2 Vendor Audits and Compliance: ..... 11

11. Service Level Management ..... 11

12. IT Project Management..... 11

12.1 Project Management Processes: ..... 11

12.2 Change Management:..... 11

13. Compliance and Reporting ..... 11

13.1 Regulatory Reporting: ..... 11

13.2 Internal Audits and Compliance Checks: ..... 11

14. Training and Awareness ..... 12

14.1 Training Curriculum: ..... 12

14.2 Employee Awareness: ..... 12

15. Document Management ..... 12

16. Review and Revision ..... 12

17. Enforcement and Consequences ..... 12

17.1 Policy Violations: ..... 12

17.2 Reporting Violations: ..... 13

Appendices..... 13

IT Org Chart: ..... 13

Key Contacts: ..... 13

**Important Note:** This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

## 1. Introduction

- Objective: This policy aims to establish robust Information Technology (IT) practices ensuring data security, confidentiality, integrity, and availability in compliance with ISO 27001, ISO 27701 standards, and RBI's Master Directions.

- Scope: Applies to all employees, contractors, and third-party users of IT systems and data within the organization.

## 2. IT Governance Framework

The key focus areas of IT Governance shall include strategic alignment, risk management, resource management, performance management and Business Continuity/ Disaster Recovery Management.

Vivriti shall put in place a robust IT Governance Framework based on the focus areas that:

- specifies the governance structure and processes necessary to meet our organization's business/ strategic objectives.
- specifies the roles (including authority) and responsibilities of the Board of Directors (Board) / Board level Committee and Senior Management; and
- includes adequate oversight mechanisms to ensure accountability and mitigation of IT and cyber/ information security risks.
- Enterprise-wide risk management policy or operational risk management policy shall also incorporate periodic assessment of IT-related risks (both inherent and potential risk).

## 3. Governance and Structure

### 1.1. Role of the Board of Directors

- The strategies and policies related to IT, Information Assets, Business Continuity, Information Security, Cyber Security (including Incident Response and Recovery Management/ Cyber Crisis Management) shall be approved by the Board of Directors.
- Such strategies and policies shall be reviewed at least annually by the Board.

### 1.2. IT Strategy Committee (ITSC) of the board:

The IT Strategy Committee is responsible for guiding in preparation of Vivriti Capital Limited's IT strategy and ensuring that the IT Strategy aligns with the overall strategy of the Vivriti Capital Limited towards accomplishment of its business objectives. A list of committee members is attached in the appendix and meets quarterly to make strategic IT decisions.

#### **The composition of the ITSC shall be as:**

- (i) Minimum of three directors as members.
- (ii) The Chairperson of the ITSC shall be an independent director and have substantial IT expertise in managing/ guiding information technology initiatives; and
- (iii) Members are technically competent.

#### Roles and responsibilities of ITSC:

- Ensuring that the management has put an effective strategic planning process in place.
- Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business.
- Ensuring proper balance of IT investments for sustaining Vivriti Capital's growth and becoming aware of exposure towards IT risks and controls.
- Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable.

- Monitoring the method that management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sourcing and use of IT resources.
- Guide in preparation of IT Strategy and ensure that the IT Strategy aligns with the overall strategy of Vivriti towards accomplishment of its business objectives.
- Satisfy itself that the IT Governance and Information Security Governance structure fosters accountability, is effective and efficient, has adequate skilled resources, well defined objectives, and unambiguous responsibilities for each level in the organization.
- Ensure that Vivriti has put in place processes for assessing and managing IT and cybersecurity risks.
- Ensure that the budgetary allocations for the IT function (including for IT security), cyber security are commensurate with Vivriti's IT maturity, digital depth, threat environment and industry standards and are utilized in a manner intended for meeting the stated objectives; and
- Review, at least on an annual basis, the adequacy and effectiveness of the Business Continuity Planning and Disaster Recovery Management of Vivriti.

### 1.3. Senior Management and IT Steering Committee:

Vivriti shall establish an IT Steering Committee with representation at Senior Management level from IT and business functions. The IT Steering Committee is responsible for executing Vivriti Capital Limited's IT strategy, policies, and projects. A list of committee members is attached in the appendix and meets quarterly to review the overall progress and alignment towards the ITSC directions.

#### Roles and responsibilities of IT Steering committee:

The responsibilities of the Committee shall include the following:

- The committee will oversee the execution of all the Tech and Data Projects as per the strategy approved by the board.
- If envisioned with new ideas, the committee has the prerogative rights to recommend developing new products for enhancing digitalization.
- The committee can set the priority & delivery timelines for all products developed by the Tech and Data teams. The committee will help the CTO and CDO for any hurdles (Internal & External factors) during the product development phase.
- The committee, with its expertise in Finance & Technology areas, would evaluate the vision, usage, scalability, efficiency, benefits, ROI, from the products developed.
- Oversight and monitoring of progress of the project, including.
  - Deliverables to be realized at each phase of the project.
  - Milestones to be reached according to the timelines.
  - Role in respect of outsourced IT operations.
- Sponsoring or assisting in governance, risk, and control framework, and also directing and monitoring key IT Governance processes.
- Defining project success measures and following up progress on IT projects.
- Advice on infrastructure products and ensure IT/ IS and their support infrastructure are functioning effectively and efficiently.

- Provide direction relating to technology standards and practices.
- Ensure that vulnerability assessments of new technology is performed.
- Verify compliance with technology standards and guidelines.
- Consult and advise on the application of architecture guidelines.
- Ensure compliance to regulatory and statutory requirements.
- Provide direction to IT architecture design and ensure that the IT architecture reflects the need for legislative and regulatory compliance, the ethical use of information and business continuity.
- Ensure necessary IT risk management processes are in place and create a culture of IT risk awareness and cyber hygiene practices within Vivriti.
- Ensure cyber security posture of Vivriti is robust; and
- Ensure Overall, IT contributes to productivity, effectiveness and efficiency in business operations.
- Assist the ITSC in strategic IT planning, oversight of IT performance, and aligning IT activities with business needs.
- Oversee the processes put in place for overall business continuity and disaster recovery.
- Update ITSC and CEO periodically on the activities of IT Steering Committee.

#### 1.4. Reporting Structure:

The Chief Product Officer, Chief Data Officer and Chief Technology Officer (CTO) reports directly to the Managing Director and are responsible for the overall management of IT strategy, Organizational data, operations and delivery.

The organization chart is attached to the appendix.

## 2. Roles and Responsibilities of CPO, CDO and CTO

### 2.1. Chief Product Officer:

- Playing a pivotal role in driving Product initiatives across business. Executing in the most efficient way possible, leading to the overall efficiency of the Product and Design team in meeting product and business goals.
- Defining and execute a robust and comprehensive strategy, product roadmap and business plan.
- Defining product vision and strategy to grow the business. Owning the product roadmap, align the same in line with the overall business strategy in consultation with the management, board members and other stakeholders.
- Driving innovation into portfolio and product development process.
- Recruit, build and mentor great teams of product managers, product designers and product analysts.
- Responsible for doing thorough market benchmarking and take build-vs-buy calls based on cost benefit analysis.

## 2.2. Chief Data Officer:

- Responsible for designing and executing the data strategy and roadmap for the company.
- Engaging with senior business stakeholders to understand their business needs and oversee the management and flow of data throughout its lifecycle; optimize and maintain data pipelines.
- Manage data governance strategies, implementing master data management practices.
- In-charge of designing, developing, and maintaining data lake, OLAP DWH and other repositories, ensuring business intelligence systems meet organizational requirements.
- Implementing data analytics effectively into business processes, and prioritizing data quality initiatives to ensure accurate business outcomes.
- Building and deploying best in class AI/ML models to solve more critical challenges across the organization to drive business value.
- Conduct rigorous statistical analysis to derive insights and inform business decisions. Also design and implement data models that help in identifying patterns and trends.
- Build a culture of data driven decision making and providing the right tools and services to make it happen.
- Integrating data analytics and data science outcomes across various applications by working with engineering and product.
- Key stakeholder in taking any decision that involves the flow of data across the organization and evaluating larger implications.

## 2.3. Chief Technology Officer:

- Ensuring that the execution of IT projects/ initiatives is aligned with the Vivriti Capital Limited's IT Policy and IT Strategy.
- Ensuring that there is an effective organizational structure to support IT functions in the Vivriti Capital Limited.
- Putting in place an effective disaster recovery setup and business continuity strategy/ plan.
- As a first line of defense, the CTO shall ensure effective assessment, evaluation and management of IT controls and IT risk, including the implementation of robust internal controls, to
  - (i) secure the organization's information assets
  - (ii) comply with extant internal policies, regulatory and legal requirements on IT related aspects.

## 2.4. IT Functions:

- PMO
- IT Infrastructure
- Data Centre/Server
- Cloud Infrastructure
- IT Architecture
- Database Administration (DBA)
- Quality Assurance (QA) Testing

- Digitalization
- Engineering/Development
- Dev Ops
- Cloud engineering

Each functional head is responsible for the expected delivery outcome of their respective domains, including planning, implementation, and compliance with IT and Information security policies and regulatory requirements.

### 3. IT Security and Compliance

#### 3.1. Data Security:

- Data security is of utmost importance. All employees shall follow strict data security practices, including but not limited to:
  - Knowing and classifying data that they are handling as part of their job responsibilities.
  - Applying strict access controls to all corporate and individual/customer data with the principle of least privilege and access shall be granted only on a need to know basis.
  - All IT systems whether procured or internally developed (laptops, servers, network devices, applications, data base, printers, access doors etc) to have logging and audit trail enabled.
  - Encryption of sensitive data in transit and at rest
  - Any breaches or security incidents to be reported promptly to the InfoSec Team through [infosec@vivriticapital.com](mailto:infosec@vivriticapital.com) .
- For detailed information please refer to Data Protection Policy [VCL-IT-ISP-12 Data Protection policy]

#### 3.2. Compliance with RBI Guidelines:

- Vivriti Capital Limited is committed to complying with the Reserve Bank of India (RBI) guidelines and regulations related to technology framework for NBFCs. We will regularly review and align our IT practices to ensure adherence.

### 4. Risk Management

#### 4.1. Risk Assessment:

- Vivriti Capital Limited shall conduct regular risk assessments on the existing systems, third parties and partners to identify and assess IT and data-related risks. These assessments will cover areas such as cybersecurity, data breaches, operational disruptions, and compliance risks.
- For detailed information please refer to Risk Management Policy [VCL-IT-ISP-08 Risk Management Policy]



#### 4.2. Business Continuity and Disaster Recovery:

- A robust Business Continuity and Disaster Recovery (BCDR) plan shall be in place to ensure the uninterrupted operation of critical IT systems in case of disasters or disruptions.
- Regular testing and updates of the BCDR plan shall be conducted to test and maintain its effectiveness.
- The details are covered under business continuity and disaster recovery policy.

### 5. Resource Management:

- For every project, Vivriti shall have a clear resource management defined and executed by proper planning, scheduling, and allocating resources to complete a project. The responsibility lies with the individual department head; however, it is overseen by the CTO, CPO and CDO respectively for their business line.
- Resource management shall be taken into consideration in every stage of the project starting from project budget, portfolio management, operations planning, and this shall include all resources like (not limited to) time, IT Infra/tools requirement, human resources, materials, financial resources, Information, and data.
- The same shall start at project planning phase and will go on until project closure with the life cycle of resource analysis, resource planning, resource scheduling, resource allocation and tracking and overall reporting of resource management at an agreed frequency to the steering committee.

### 6. Performance Management

Performance management shall be an integral part of the overall IT governance and management. All employees will undergo a performance evaluation as per the human resource performance management policy.

A similar performance evaluation shall be conducted on critical IT systems with clearly defined Key result areas, outcomes, shortfall if any in expected performance and plan of action to bridge the identified gap.

### 7. Technology Infrastructure

#### 7.1 Hardware and Software:

- Vivriti Capital Limited shall maintain an up-to-date inventory of hardware and software assets to ensure ownership and classification defined and protection applied as per asset classification.
- Regular maintenance, upgrades, and replacement cycles will be implemented to ensure optimal performance and security.

#### 7.2 Scalability and Redundancy:

- The IT department shall plan for scalability and redundancy to meet the growing demands of the organization.

- Redundant systems and failover mechanisms as per business requirement shall be in place to minimize downtime.

## 8. Data Management

### 8.1 Data Classification and retention:

- Data shall be classified based on its sensitivity and importance.
- Data classification will guide access controls and encryption requirements.
- Clear guidelines shall be defined on data ownership, stewardship, and data access controls.
- The details on type of data and the corresponding retention, recovery, disposal are covered in data retention policy.
- Compliance with data privacy regulations will be a top priority. Details are covered under data privacy policy.

## 9. Cybersecurity

### 9.1 Cybersecurity and resilience Framework:

- Vivriti Capital Limited will maintain a comprehensive cybersecurity and resilience framework that includes:
  - Regular vulnerability assessments
  - Intrusion detection and prevention systems
  - Continuous monitoring of network traffic
  - Our readiness assessment and plan for quick recovery in case of a disaster/crisis.

All employees/contractors who have access to Vivriti's data in any form shall undergo cybersecurity training to enhance awareness.

### 9.2 Incident Response, recovery and Reporting:

- The Incident Response team comprising of SMEs from IT team, business team and Information security shall ensure recovery within the RTO and RPO for any incident.
- All security incidents shall be reported promptly as per the Incident Response Plan to minimize damage and prevent recurrence.

## 10. Vendor Management

### 10.1 Vendor Selection:

- Vendor selection criteria will include security risk assessments, regulatory compliance, and service level agreements and it shall strictly adhere to the organization wide Vendor Management Policy and department wise SOPs shall be defined on vendor selection and the due diligence.
- Wherever the services offered by the vendor involves Vivriti's data or IT services, Information security risk assessment shall be carried out before onboarding Vendor/purchasing the IT product/integrating with their IT environment.

- Contracts with vendors shall clearly define roles, responsibilities, and termination clauses.

### 10.2 Vendor Audits and Compliance:

- Regular vendor audits shall be conducted to ensure compliance with contractual and security requirements and Vivriti shall ensure that the services provided by vendor does not compromise on the expectation from Vivriti's business in terms of output, quality and information and data security.
- Vendors found non-compliant as per the contractual terms/service may face penalties or termination of contracts.

## 11. Service Level Management

- A Service Level Management (SLM) process shall be put in place to manage the IT operations while ensuring effective segregation of duties.
- Vivriti Capital Limited shall develop a technology refreshment plan for the replacement of hardware and software in a timely manner before they reach EOS.
- While adopting new or emerging technologies, tools, or revamping their existing ones in the technology stack, Vivriti shall follow a standard/recognized enterprise architecture planning methodology or framework such as The Open Group Architectural Framework (TOGAF).

## 12. IT Project Management

### 12.1 Project Management Processes:

- Vivriti Capital Limited follows standardized project management processes, which include initiation, planning, execution, monitoring, and closure.
- All IT projects must align with the organization's strategic goals and objectives.

### 12.2 Change Management:

- A well-defined change management process is in place to assess and implement changes to IT systems.
- All changes shall be thoroughly tested and approved by the management/steering committee before deployment to minimize disruptions.

## 13. Compliance and Reporting

### 13.1 Regulatory Reporting:

- Vivriti Capital Limited is committed to meeting all regulatory reporting requirements imposed by RBI and other relevant authorities.
- The Compliance Team will ensure timely and accurate reporting.

### 13.2 Internal Audits and Compliance Checks:

- Internal audits shall be conducted regularly to assess compliance with IT policies and regulatory requirements.

- Audit findings that are outside of the acceptable risk shall be addressed promptly, and corrective actions shall be implemented.

## 14. Training and Awareness

### 14.1 Training Curriculum:

- A comprehensive training curriculum will be developed to educate employees on IT policies, security practices, and compliance requirements.
- All employees are required to complete mandatory training.

### 14.2 Employee Awareness:

- Regular awareness programs will be conducted to keep employees informed about the latest cybersecurity threats and best practices.
- Employees are encouraged to report any suspicious activity promptly.

## 15. Document Management

- Documents related to IT policies, procedures, and project documentation will be stored securely and easily retrievable.
- Version control will be maintained for all documents.
- Document retention policies will specify how long documents should be retained.
- Secure disposal methods will be used to eliminate documents that have reached the end of their retention period.

## 16. Review and Revision

- This IT Policy will undergo regular reviews to ensure its relevance and effectiveness.
- The review schedule shall be determined by the IT Steering Committee which is no later than a year from the previous approval date.
- The IT Steering Committee and relevant department heads are responsible for initiating policy revisions and the same shall be approved by the board.
- Employees are encouraged to provide genuine feedback if any for continuous improvement.

## 17. Enforcement and Consequences

### 17.1 Policy Violations:

- Violations of this IT Policy, including data breaches and security lapses, will be dealt with as per Disciplinary Process Policy [VCL-IT-ISP-25 Disciplinary Process Policy].
- Consequences may include warnings, suspension, termination, or legal action, depending on the severity of the violation.

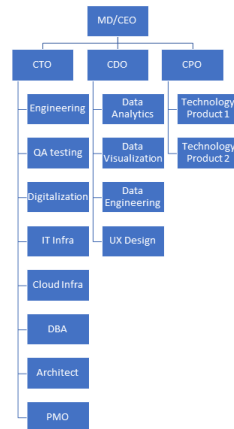
## 17.2 Reporting Violations:

- Employees must report policy violations promptly to the IT steering committee or the designated authority.
- A confidential reporting mechanism will be provided for reporting sensitive matters.

## Appendices

### IT Org Chart:

## IT Org Chart



### Key Contacts:

#### IT Strategic committee:

Sl.no	Members	Designation
1	Ms. Namrata Kaul	Independent Director
2	Mr. John Tyler Day	Nominee Director
3	Mr. Vineet Sukumar	Managing Director
4	Santanu Paul	Independent Director
5	Mr. Prasenjit Datta	Chief Information Officer and Chief Technology Officer

#### IT Steering committee:

Sl.no	Members	Designation
1	Mr. Vineet Sukumar	Managing Director
2	Mr. Prasenjit Datta	Chief Information Officer (CIO) and Chief Technology Officer (CTO)

4	Mr. Mohan Sushantam	Chief Product Officer and Chief Data Officer
5	Mr. Gautam Jain	Chief Business Officer
6	Mr. Ashish Kumar Malani	Chief Credit Officer
7	Mr. Hemang Mehta	Chief Risk Officer
8	Mr. Prasanna M	Chief Sales Officer
9	Mr. Srinivasaraghavan B	Chief Financial Officer
10	Mr. Ajit K Menon	Group Head – Operations

----- End of Document -----

