Audit Policy

VCPL-SEC-05-V1.0

DOCUMENT AND RECORD CONTROL

Version Control

Document Control ID	VCPL-SEC-05_Audit Policy-V1.0
Issued Date	01-September-2022
Effective Date:	01-September-2022
Owner:	Infosec

Revision Table

Date	Version	Affected Sections	Author
01-September-2022	Draft		Lakshmi/Ramesh

Release Authorization

Task	Author	Title
Prepared by	Mr Ramesh T.P/ Lakshmi	

Reviewer Authorization

Name	Title	Signature	Date
Mr. Prasenjit Datta	Head of Technology		

Approval Authorization

Name	Signature	Date
Board of Directors		

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.

TABLE OF CONTENTS

1. Purpose

The Audit Program is planned to take into consideration the status and importance of the process and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency, and methods are predefined. Selection of auditors and conduct of audits ensures in achieving objectivity of the audit process.

Vivriti Capital shall conduct ISMS audits and appropriate follow up to ensure compliance with the Vivriti Capital's ISMS policies, procedures, standards, and guidelines within scope of the ISMS, by devising standard documentation for planning and reporting audits and audit findings and ensuring the implementation of a prompt and accurate remedial action.

Vivriti Capital shall also conduct technical compliance review to evaluate and assess its networks and application and ensure adequate protection from latest vulnerabilities.

Vivriti Capital shall also conduct internal audits to ensure that the IT processes and technologies implemented are compliant with the Vivriti Capital's security policies and standards.

As a part of this, the accountability and course of activities for corrective actions and preventive actions taken for taking action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence are documented in next sections.

2. Scope

The document intends to define the framework for conducting periodic internal audit of Information Security Management Systems (ISMS) established at Vivriti Capital. This follows Vivriti Capital Information Security Policy where the management has committed continual monitoring at management level to ensure compliance with the Information Security Policies and Procedures adopted within Vivriti Capital.

2.1 Modification Guidelines

The document is owned and maintained by the Information Security Committee. Any requests for changes to this document must be provided to VP, Information Security and will update the document, as appropriate. Until the document is updated, approved, and posted into the Vivriti Capital policies and procedures, the existing process must be followed, unless a deviation request has been granted.

2.2 Exception Request

It is expected that employees implementing ISMS process will apply their best judgment in every situation to determine the best course of action for Vivriti Capital. This may occasionally require exception from the approved ISMS process. Any exception to this procedure must be requested and documented.

2.3 References

The guidelines have reference to Information Security Policy of Vivriti Capital, and these documents must be read in conjunction.

3. Ownership and Responsibilities

Vivriti Capital aims at continually improving the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review of the Information Security Management System implemented at Vivriti Capital.

The ISMS internal auditor must monitor the processes being followed by the various teams and must conduct periodic reviews to ensure the compliance with Vivriti Capital ISMS policies, procedures, standard, and guidelines.

A comprehensive internal audit shall be conducted half-yearly with results being reported to Vivriti Capital management for corrective and preventive action.

Half-yearly Internal Assessment can be conducted by the independent auditor or with the help of Third-Party Vendor.

4. Review

The procedure would be reviewed every year, else whenever required.

5. Procedure

5.1 Managing an Audit Program

Vivriti Capital grants the authority to the Information Security Committee for managing audit program for Information Security Policies and Procedures and their implementation in Vivriti Capital with the intent to:

- Establish the objective and scope of the audit program.
- Establish the responsibilities, resources, and procedures.
- Ensure the implementation of the audit program.
- Monitor, review and improve the audit program; and
- Ensure the appropriate audit program records are maintained.

Objectives of an audit program are based on consideration of:

- Management system requirements.
- Standards requirements.
- To obtain and maintain confidence in the ISMS.
- Confirm to the requirements of the ISO 27001, SOC2 and other relevant legislation and regulations.
- Confirm to the identified information security requirements.
- Confirm effective implementation; and
- Perform as expected.

Extent of audit is determined by:

- Scope, objective and duration of each audit.
- The results of previous audits or a previous audit program review.
- Significant changes in organization or ISMS processes; and
- Compliance status.

5.2 Preparing Audit Plan and Conducting Audits

- Information Security Committee shall prepare a half-yearly plan for ISMS audit, which shall include ISMS controls audit and results of technical testing for Information Systems presently being outsourced to external agency/auditors. The audit plan shall be approved by Vivriti Capital management.
- In the event of any change in the Audit Plan, the Team shall prepare a revised audit plan and communicate the same to steering committee for SOC2 implementation.
- For technical testing of Information Systems, the prior approval of the Asset Owner shall be obtained. Adequate precautions shall be taken before the execution of technical testing.
- The execution of audits may be outsourced to capable third parties and internal audit compliance team. The Team shall provide the auditor with information regarding the areas of focus and the audit report formats.
- Audit tests that could affect system availability shall be run outside business hours.
- Audit requirements for access to systems and data should be agreed with appropriate management.
- Requirements for special or additional processing shall be identified and agreed.

5.3 Access Controls for Auditors

- Audit tests shall be limited to read-only access to software and data.
- Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.
- All access shall be monitored and logged to produce a reference trail.

5.4 Deliverables

The following deliverables may be created as a result of this process:

- Internal Audit Program (Half-yearly Audit Calendar)
- Audit Reports
- Corrective and Preventive Actions (as per the CAPA Procedure)

- Statement of applicability if there are any changes

5.5 Measurements

- Compliance status of previous audit report per business function audited:
  - Number of audit observations overdue Vs. Total no of audit observations reported.
  - Number of audit observations closed Vs. Total number of audit observations for business function.

---End of Document---