Vivriti Capital Limited

Vivriti Information Security and privacy Awareness Policy

Version 2.1

Project/ Track Name	Vivriti Capital
Document Name	Security and Privacy Awareness Policy
Document No	ISP-07
Revision no	2.1
Object Type	Policy Document

Revision History

Version	Author	Date	Affected Sections	Reviewer	Approver	Approval Status
2.0	Lakshmi Balaji	06-10-2022	All	Prasenjit Datta	ISMGC	Approved by board on 08-Nov-2022
2.1	Goutham Vaidyanathan /Lakshmi Balaji	5-10-2023	All	Prasenjit Datta		Approved by board on 03-Nov-2023

Note: This policy is the revamped version of older version (V1.x) to meet the technology, regulatory and compliance requirement.

Distribution

Role	Department
All	All

Table of Contents

Office of Responsibility 4
Introduction 4
Objective 4
Scope 4
Policy 4
Classification of team:.................... 4
Training Frequency 4
New Hire Training 5
Mandatory new joiner training:.................... 5
InfoSec Policy Walk-Through Workshop.................... 5
Refresher Training.................... 5
Year-Round Information Security and Privacy Campaign.................... 5
Cybersecurity Awareness Month.................... 5
Monitoring and Compliance 5
Policy Review 5
Attendance.................... 6
New Joiners.................... 6
Existing employees.................... 6

Office of Responsibility

Information Security and Privacy Team and HR Team.

Introduction

This Security and Privacy Awareness Policy outlines the guidelines and procedures for establishing a comprehensive security and Privacy awareness program within Vivriti Capital Limited (VCL). The policy's focus is on categorizing teams based on their interactions with external parties and implementing a structured training approach to address security and privacy risks effectively.

Objective

By adhering to this Security and Privacy Awareness Policy, we aim to foster a security-conscious culture, mitigate risks tied to external communications, and safeguard our organization's sensitive information.

Scope

The Policy applies to all employees, contractors, consultants, interns, apprentices and CA-article assistants who access, use or control company resources.

Policy

Classification of team

Teams will be categorized into three levels based on their interactions with external parties:

- High-Risk Teams: Teams engaged in critical external communications involving confidential, proprietary, or regulated information.
- Medium-Risk Teams: Teams involved in moderately sensitive external communications that may include non-sensitive information.
- Low-Risk Teams: Teams with primarily non-sensitive external communications or general inquiries.

Training Frequency

Training frequencies are tailored to risk levels and employee needs:

- High-Risk Teams: Quarterly security and privacy training sessions to address emerging threats and reinforce best practices.
- Medium-Risk Teams: Biannual security and privacy training sessions to maintain awareness and promote secure communication habits.
- Low-Risk Teams: Annual security privacy training sessions to ensure foundational security principles are understood and followed.

New Hire Training

Mandatory new joiner training:

New hires will be assigned mandatory security and privacy training. It is expected that the same will be completed within three days of joining the organization. This training will cover general security and privacy awareness and foundational best practices.

InfoSec Policy Walk-Through Workshop

All newly hired employees will participate in a 30-minute cybersecurity and privacy policy walk-through workshop to familiarize themselves with the organization's security policies, procedures, and guidelines.

Refresher Training

Regular refresher training sessions will be conducted to reinforce security and privacy awareness:

- Monthly Refresher (10 minutes): All employees will receive a 10-minute course on any topic of security and privacy awareness update each month to highlight recent threats, emerging trends, and security reminders. Completing this course is mandatory.
- Annual Refresher (30 minutes): An annual refresher training session lasting 30 minutes will provide a deeper dive into security and privacy related topics, policies, and best practices to all employees once in a year.

Year-Round Information Security and Privacy Campaign

An ongoing awareness campaign will run throughout the year, emphasizing the importance of information security and data privacy. This campaign will employ various communication channels to disseminate security tips, case studies, mock drills, and success stories.

Cybersecurity Awareness Month

A month-long cybersecurity awareness campaign will be conducted in October to coincide with International Cybersecurity Awareness Month. The campaign will feature targeted activities, workshops, webinars, and resources to actively engage employees and enhance their security and privacy awareness.

Monitoring and Compliance

The Information Security and Privacy Team will periodically evaluate teams' compliance with security and privacy training obligations. Non-compliance will prompt reminders and additional engagement to ensure adherence to the policy.

Policy Review

This policy will undergo reviews by the Information Security and Privacy Team to evaluate its effectiveness and incorporate updates to align with emerging security and privacy challenges.

Attendance

New Joiners

All information security and privacy training assigned to new joiners is mandatory (100% attendance is required) and no exception shall be given.

Existing employees

Every existing employee must participate in a minimum of 85% of the trainings .

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