Security Awareness Policy

VCPL-IT-ISP-07 V2.0

DOCUMENT AND RECORD CONTROL

Version Control

Document Control ID	VCPL-IT-ISP-07 Security Awareness Policy V2.0
Issued Date	29-September-22
Effective Date:	29-September-22
Owner:	Info Sec Team

Revision Table

Date	Version	Brief Description	Author
29-September-22		Security Awareness Policy – Draft	Lakshmi Balaji
29-September-22	2.0	Security Awareness Policy	Lakshmi Balaji

Release Authorization

Task	Author	Title
Prepared by	Lakshmi Balaji	Info Sec Officer

Reviewer Authorization

Name	Title	Signature	Date
Mr. Prasenjit Datta	Head of Technology	Prasenjit Datta	29-September-2022

Approval Authorization

Name	Signature	Date
Board of Directors	Approved	08-Nov-2022

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

TABLE OF CONTENTS

1. Office of Responsibility

Vice President, Information Security & Risk.

2. Purpose

As stated in the Company Information Security Program Charter, the Company will follow a risk management approach to developing and implementing Information Security policies, standards, guidelines, and procedures. The Information Security Program is designed to protect information assets by developing Information Security policies to identify, classify, and define the acceptable use of company information assets.

The Security Awareness Policy defines Company objectives for establishing a formal Security Awareness Program, and specific standards for the education and communication of the Information Security Program Charter and associated policies, standards, guidelines, and procedures.

3. Scope

The Policy applies to all employees, contractors, consultants and vendors who access, use or control company resources.

4. Policy

4.1 Objectives

- The Company Information Security Program Charter, relevant policies, standards, and guidelines shall be properly communicated to Company employees. All newly hired employees are required to complete security awareness and compliance training and acknowledge company security principles upon hire (within 30 days of hire) and annually thereafter. Contractors and third-party service providers/vendors are required to complete security awareness training and acknowledge company security principles prior to accessing company resources. Specific requirements for the delivery of security awareness education and training are provided in the Security Awareness Training Standard.

- Management shall ensure that employees are briefed on their security role(s) / responsibilities, acknowledge terms and conditions of employment prior to obtaining access to the organization's information systems; are provided with guidelines regarding the security expectations of their roles; are motivated to comply with security policies; and continue to have the appropriate skills and qualifications for their role(s).

- Human Resources shall manage the awareness and compliance training process and tracking efforts for all end users. Human Resources shall collaborate with the Information Security & Risk department to ensure that all company awareness and compliance training meets company directives, regulatory statues, industry framework requirements, and best practices.

- Training records shall be maintained for all employees. Maintained records shall reflect training subject matter and completion details. Training records may be required to support security incident investigations, internal and external audit requirements, or client requests. Training session attendance shall be documented in each employee's

permanent file or available online for verification as needed. Training materials shall be maintained for auditing purposes.

5. Related Policies

- Information Security Program Charter
- Security Awareness Training Standard

6. Policy Compliance

6.1 Responsibilities

- The Chief Executive Officer (CEO) & Board members are the approval authority for the Security Awareness Policy.
- The Vice President of Information Security & Risk is responsible for the development, implementation, and maintenance of the Security Awareness Policy.
- Company management is accountable for ensuring that the Security Awareness Policy and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the Security Awareness Policy and associated standards and guidelines.
- All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves with the Security Awareness Policy and complying with its associated policies.

7. Policy Enforcement and Compliance

Compliance with this policy is mandatory and Vivriti department managers shall ensure continuous compliance monitoring within their department. Compliance with the statements of this policy is a matter of periodic review.

Any breach of this policy may constitute a security violation and gives Vivriti the right to conduct disciplinary and / or legal action, up to and including termination of employment or business relationship.

Disciplinary action will be dependent upon the severity of the violation which will be determined by the investigations.

8. Waiver Criteria

The policy is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security Management, including justification and benefits attributed to the waiver by the CEO.

The policy waiver shall be granted for a period of four months initially and shall be reassessed thereafter and can be extended up to a period of three consecutive terms. No waiver shall be provided for more than three consecutive terms on any of the policies.

9. Document Management

Technological advances and changes in the business requirements will necessitate periodic revisions to documents. Therefore, this document may be updated to reflect changes or define new or improved requirements as and when required and in compliance with the Information Security Program Charter.

Any change will require the approval of the Information Security Steering Committee (ISSC).

10. Glossary

Term	Definition
Information Security	The preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Policy	A plan of action to guide decisions and actions. The term may apply to government, private sector organizations and groups, and individuals. The policy process includes the identification of different alternatives, such as programs or spending priorities, and choosing among them on the basis of the impact they will have.

---End of Document---