CYBER SECURITY POLICY

VER 1

27TH JANUARY 2022

Document and Record Control

Version Control

Document Control ID	VSM-ISP-11 CYBER SECURITY POLICY
Issued Date	27-January-2022
Effective Date:	27-January-2022
Owner:	ISMS DEPARTMENT

Revision Table

Date	Version	Brief Description	Author
27-January-2022	0.1	Cyber Security Policy -Draft	Babu Gopinathan

Release Authorization

Task	Author	Title
Prepared by	Babu Gopinathan	Information Security

Reviewer Authorization

Name	Title	Signature	Date
Mandakini Kumari	Head – Technology	Mandakini	27-January-2022

Approval Authorization

Name	Signature	Date
Board of Directors		

TABLE OF CONTENT

1. Office Of Responsibility

Chief Technology officer, Information Security & Risk

2. Purpose

The Policy is aligned to the Information Security Program Charter which adheres to the risk management approach for developing and implementing Information Security Policies, standards, guidelines and procedures. this document is to provide details of Vivriti Asset Management' s Cyber Security policy that is applicable at Vivriti Asset Management. This document has been prepared as per the guidelines by RBI Master Circular. The Master circular requires NBFCs to put in place the following policies

- IT Governance
- IT Policy
- Information Security
- Cyber Security
- IT Operations
- IS Audit
- Business Continuity Planning
- Disaster Recovery Management
- IT Services Outsourcing

3. Scope

The policy applies to all individuals who access, use or control Vivriti Asset Management owned resources. This includes but is not limited to Vivriti Asset Management's employees, third parties (contractors, consultants and other workers including all personnel affiliated to external organizations), investors, customers, other internal and external stakeholders with access to the Vivriti Asset Management's resources, network.

The Policy does not cover issues related to general physical and building security. It covers, however, physical security aspects of buildings or parts of buildings that directly affect the security of information owned by Vivriti Asset Management.

4. Cyber Security Policy Statement

The cyber security policy is an indicative document which serves several purposes including the descriptions for acceptable use of resources. This policy also describes user privilege and responsibilities.

4.1. Email Usage

E-mail is a business communication tool which all employees are requested to use in a responsible, effective and lawful manner. You can find the detailed e-mail usage requirements in the dedicated policy named Email Usage Policy.

Employees should use their company email primarily for work-related purposes. Vivriti Asset Management is flexible and allows employees to use official email for personal reasons, but this should be limited, and employees should use discretion when using email for personal reasons.

Employees can use their email to:

- Communicate with current or prospective customers and partners.
- Log in to purchased software they have legitimate access to.
- Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

Inappropriate Usage: Official email should not be used to

- Sign up for illegal, unreliable, disreputable, or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Register for a competitor's services unless authorized.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their co-workers
- Our company has the right to monitor and archive corporate emails.
- Create or distribute any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin

4.1.1. Protection

- Employees should always be vigilant to catch emails that carry malware or phishing attempts
- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait titles
- Check email and names of unknown senders to ensure they are legitimate
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If an employee isn't sure that an email they received is safe, please check with the IT team at **[IT Support Mail]** before proceeding further.

4.1.2. Monitoring

Vivriti Asset Management will monitor all email communication and employees should not expect any privacy whatsoever when using firm email system

4.1.3. Email Signature

Employees must use only Vivriti Asset Management approved signature in their official emails.

4.1.4. Internet Usage Policy

Vivriti Asset Management provides Internet access to all staff to assist them in carrying out their duties such as looking up details about suppliers, products, accessing governmental information and other work-related information.

- Occasional and limited personal use of the Internet is permitted if such use does not:
  - Interfere with work performance & productivity.
  - Include downloading or distribution of large files.
  - Have negative impact on the performance of IT systems.
- When using Internet access facilities, you should comply with the following guidelines:
  - Keep your personal use of Internet to a minimum
  - Check that any information you use from the Internet is accurate, complete and current
  - Respect the legal protections of data, software, copyright and licenses.
  - Immediately inform the I.T. Security team of any unusual occurrence.
  - Do not download or transmit text or images which contain any software, material of obscene, threatening, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
  - Do not use the company's equipment to make unauthorized access to any other computer or network.
  - Do not represent yourself as another person.

- It is STRICTLY FORBIDDEN to upload Company non-public Information such as any of the following to external file transfer or storage sites, like Box, Dropbox or personal Google Drive:
  - Source Code, object code, user documentation and all other software development details
  - Project related information
  - Personally Identifiable Information
  - Company strategy and business plans
  - Corporate IT infrastructure arrangements including any log files
  - Intellectual Property, such as: Copyrights, Patents and Trade Secrets
  - Employee personal information such as salaries, appraisals, medical records or health care details
  - Any information concerning our clients and prospects including details of our client projects, client proposals, contracts, fees or strategic plans

- Information related to our clients' customers, including any details stored within Vivriti Asset Management's software products, such as transaction or bank account details
- Any other company non-public information.

Internet usage requirements are described in detail in the dedicated policy named Internet Usage Policy. Users must read this policy and comply with it.

4.1.5. Portable Media

The use of portable media is only permitted in exceptional circumstances. When portable media is used it should be afforded a level of protection commensurate with the level of risk, up to and including blocking of all read/write operations for the highest of risk environments. The intended purpose is to protect customer and company information from being transferred via unauthorized means.

Vivriti Asset Management reserves the right to inspect and erase portable media that is used on our network.

4.1.6. Confidentiality

- Vivriti Asset Management users must take precautions to protect company information and make all possible efforts to maintain the confidentiality of personal information, business information and other proprietary informational resources.
- Personally Identifiable Information (PII) shall be classified as confidential, as shall any other information flagged as such. Users must not transfer or store confidential information in any location not previously approved and secured by the Infrastructure security team.
- Company information must not be stored on the local hard drive of any workstation, but stored only on provided, network-based locations.
- Information Security staff must provide access to information using the principle of least privilege and shall provide access to informational resources on a need-to-know basis.

4.2. Human Resources

- Information security must be covered in the Human Resources (HR) policies. The HR policies should ensure, as a minimum, that security is adequately covered in job descriptions; those personnel are adequately screened, trained and that confidentiality agreements are signed by all new employees and contractors.
- A training plan and training material must be in place to ensure that the right level of Security Awareness is created and maintained within the organization.
- Software developers and all other relevant personnel involved in the development of software for Vivriti Asset Management are required to undertake secure development training on a periodic basis.
- Upon termination of employment, including the completion of any contract position, Infrastructure team is responsible for disabling all of the departing employee's user accounts and privileges.

4.3. Access Control

4.3.1. Password

- Users must be forced to change their passwords during the first log on, and at 60-day intervals.
- Passwords shall not be displayed or transmitted in clear text and shall be suitably protected via approved cryptographic solutions. Passwords shall be stored in an encrypted format. A history of passwords shall be maintained to prevent the reuse of passwords. A maximum of six successive login failures shall result in account lockout until an administrator unlocks it. Default accounts shall be disabled and/or default passwords associated with such accounts shall be changed.

4.3.2. Remote Access

- Frequently users will be required to access the Vivriti Asset Management's Information systems from outside the office, for example employees working from home, travelling consultants and/or employees working in Sales / Business Solutions.
- For remote access to the Corporate IT Infrastructure resources only the officially supported and approved facilities by the internal IT department are to be used (ie FortiClient VPN). The associated security policies must be applied. Online Communication from within Vivriti Asset Management's offices to an external party may only use Vivriti Asset Management's approved communication channels. Personal internet connections or connectivity devices (e.g. using personal data modems and Mobile Hotspot connections, remote access connections, personal VPNs etc.) are strictly prohibited.

The detailed Electronic Communication Requirements are described in the dedicated policy named Communications Security Policy.

4.4. Operations Security

- Vivriti Asset Management's network environment must be segmented to protect and isolate confidential resources. An annual penetration testing to be conducted to stay in compliance with data security standards.
- All changes must be conducted in a controlled and approved way to ordnance with the Operations Security Policy.
- System changes or re-configurations of standard IT components are not allowed. Only additions and/or changes of software components can be made by users on workstations based on customer project requirements. The following system changes are strictly prohibited unless special authorization of the Corporate or local IT Manager has been granted: Installation of:
  - Unauthorized connectivity devices (e.g. data modems)
  - Any component suitable to gain unauthorized access to restricted areas
  - Merging of two networks by physically integrating them on a network node
  - Disabling virus protection
  - Any other non-standard software or hardware component.

4.5. Network Security

- A secure and trusted network is essential as well as critical to the security of our business:
- External facing networks should be firewalled to an appropriate level
- Physical and logical network changes should only be made by approved users
- Networks should be segregated on a regional and/ or business line basis
- Appropriate controls should be in place at network interfaces
- WAN services should only be acquired through approved vendors
- Network event logging and monitoring should be implemented
- Third-party users shall not connect their computing devices to the wired or wireless network of Vivriti Asset Management, unless authorized.
- Company computers and networks may be connected to third-party computers or networks only with explicit approval after determination that the combined systems will be in compliance with Vivriti Asset Management's security requirements.

4.6. Wireless Security

- Passwords for Guest wireless networks should be changed on a regular basis
- Only approved wireless access points should be used
- Wireless networks should always be encrypted

4.7. Logging And Monitoring Events

4.7.1. Event Logging And Monitoring

Adequate monitoring controls to detect attacks and unauthorized access to its information processing systems must be implemented. The level of monitoring required shall be determined by risk assessment and any relevant or applicable legal requirements shall be identified to ensure that the monitoring activities comply with the requirements. Monitoring may consist of activities such as the review of:

- Automated intrusion detection system logs
- Firewall logs
- User account logs
- Network scanning logs
- Application logs
- Help desk tickets
- Vulnerability Scanning
- Other log and error files.

Any security issues discovered will be reported to the IT Security Department for investigation.

4.7.2. User Monitoring

In order to maintain the security of the Vivriti Asset Management's IT systems (including to prevent cybersecurity threats) and to protect the assets and data, Vivriti Asset Management's IT Security team monitors many aspects of user behaviour including but not limited to:

- Monitoring Internet access usage
- Reviewing material downloaded or uploaded via the Internet
- Reviewing e-mails sent or received by users, provided that there is a well-founded suspicion about a breach of provisions of this Policy or of applicable laws, or if there is a legal or regulatory requirement in this respect
- Reviewing installed software on user's computers
- Logins to and use of Company's network as well as use of PCs.

Any monitoring done by Vivriti Asset Management will be in accordance with applicable law.

4.8. Workstation Security

- All workstations (Laptops) must have all Vivriti Asset Management approved security tools pre-installed and fully encrypted.
- Administrator access on the workstation must be controlled with least privilege principles.
- Only install software's from trusted sources
- Do not allow unauthorized users to access your workstation
- Apply software and virus updates as needed using automated workstation software
- Take appropriate steps to maintain the physical security of your workstation.

4.9. Secure Software Development

Application Security checkpoints are to be implemented across all stages of software development. It shall include source code audits by professionally by having assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.

Secure coding guidelines are developed and adhered. Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling are clearly specified at the initial and ongoing stages of system development/acquisition/implementation.

Proper segregation (logical) shall be available between all stages of software development like development, staging and production.

Software/Application development approach shall be based on threat modelling, incorporate secure coding principles and security testing based on global standards and secures rollout. Like OWASP Top 10, SANS 25 and CIS 20 controls are to be tested.

Containerized application environment shall be prepared and implemented for exclusive business use that is encrypted and separated from other smart phone data/applications; measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.

4.10. Patch/Vulnerability & Change Management

Vivriti Asset Management shall follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.

Appropriate systems and processes are in place to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/Databases/Applications/Middleware, etc.

Changes to business applications, supporting technology, service components and facilities are managing using robust configuration management processes, configuration baseline that ensures integrity of any changes thereto.

Periodically conduct VA/PT of internet facing web/mobile applications, servers & network components throughout their lifecycle (pre-implementation, post implementation, after changes etc.)

Periodically conduct Application security testing of web/mobile applications throughout their lifecycle (pre-implementation, post implementation, after changes) in environment closely resembling or replica of production environment.

As a threat mitigation strategy, identification of the root cause of incident and apply necessary patches to plug the vulnerabilities.

Periodically evaluate the access device configurations and patch levels to ensure that all access points, nodes between (i) different VLANs (ii) LAN/WAN interfaces (iii) Vivriti Asset Management' s network to external network and interconnections with partner, vendor and service provider networks are securely configured.

4.11. Authentication Framework For Customers

Implement authentication mechanism to provide positive identify verification to customers. Customer identity information should be kept secure. Vivriti Asset Management will be the identity provider for identification and

authentication of customers for access to partner systems using secure authentication technologies.

4.12. Vendor Risk Management

Vivriti Asset Management shall be accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements. Vivriti Asset Management carefully evaluate the need for outsourcing critical processes like facility management services, desktop management, UPS management etc. And selection of vendor/partner based on comprehensive risk assessment done by the IT team.

Established appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities are in place.

Reserve Bank of India shall have access to all information resources (online/in person) that are consumed by us, to be made accessible to RBI officials by the Vivriti Asset Management when sought, though the infrastructure/enabling resources may not physically be located in the premises.

Further, Vivriti Asset Management adheres to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders. Background checks, non-disclosure and security policy compliance agreements are mandated for all third-party service providers

4.13. Advanced Threat Protection (Real-Time)

A robust perimeter defence shall be in place to protect against the installation, spread, and execution of malicious code at multiple points in the enterprise.

Vivriti Asset Management shall have Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – (Endpoints such as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. Including tools and processes for centralized management and monitoring.

4.14. Anti-Phishing

Vivriti Asset Management shall subscribe at firewall level for Anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites/rouge applications.

4.15. Data Leak Prevention Strategy

Vivriti Asset Management shall have a comprehensive data loss/leakage prevention strategy at firewall level to safeguard sensitive (including confidential) business and customer data/information.

This includes protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

4.16. Metrics

Vivriti Asset Management shall develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators. Few illustrative metrics included coverage of anti-malware software and their updating percentage, patch latency, extent of user awareness training, vulnerability related metrics, etc.

5. Roles And Responsibilities

Each role involved in this policy shall have main responsibilities as follows:

The Chief Technology officer of Product & Infrastructure Security

- Managing and implementing this policy and related policies, standards and guidelines
- Monitoring and responding to potential and/or actual IT security breaches
- Ensuring that staff are aware of their responsibilities and accountability for information security
- Act as a consulting contact for all security related issues.
- Act as a central point of contact on Information Security for both staff and external organizations.
- Acts as an approval authority for the Information Security policy and its exceptions.

Information Security Steering Committee (ISSC)

- Review and signoff changes to Information Security policies prior submitting for approval from IS head.
- Responsible for information risk within Vivriti Asset Management advising the executive management on the effectiveness of management of security and privacy issues across the organization and advising on compliance with relevant legislation and regulations.
- Responsible for cascading and ensuring the implementation, operation, monitoring, maintenance and improvement of the Information Security Management System

Managers

- Ensuring that the Information Security policy and associated standards and guidelines are properly communicated and understood within their respective organizational units.

- Defining, approving and implementing procedures in their organizational units and ensuring their consistency with the Information Security Policy and associated standards and guidelines.
- Determining the level of access to be granted to specific individuals.
- Ensuring staff have appropriate training for the systems they use
- Ensuring staff know how to access advice on information security matters.

All Employees

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the Information Security Policy and associated standards and procedures.

All employees are responsible for information security and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action.

In particular, all employees should understand:

- What information they are using, how it should be used, stored and transferred in terms of data security
- What procedures, standards and protocols exist for the sharing of information with other parties
- How to report a suspected breach of information security within the organization
- Their responsibility for raising any information security concerns.

All individuals are responsible with adhering to the provisions of this Policy and all related policies, standards, guidelines and procedures and must report every incident of misuse or abuse of which they become aware as described in this policy.

6. Policy Enforcement And Compliance

Vivriti Asset Management recognizes its burden to exercise due care for the safeguarding of data in its custody including, but not limited to, Personally Identifiable Information (PII), Financial information and Vivriti Asset Management Intellectual Property. To this end, and for overall assurance of the confidentiality, integrity, and availability of Vivriti Asset Management information systems, an independent review of compliance with this Policy shall be conducted on a regular basis.

Vivriti Asset Management must adhere to applicable Reserve Bank of India's (RBI) Master directions for Non-Banking Financial Companies and RBI's IT Framework. This is not intended to be an exhaustive list of applicable regulatory requirements with respect to state or local laws that must similarly be complied with.

Further, all employees shall comply with relevant national and local legal, regulatory, and contractual requirements. Any Vivriti Asset Management employee who does not comply with this policy may be subject to disciplinary action, up to and including termination. Access to Vivriti Asset Management' information systems and resources is a privilege, not a right, and may be revoked or suspended at any time.

7. Waiver Criteria

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

The policy waiver period has maximum period of 4 months, and shall be reassessed and re-approved, if necessary for maximum three consecutive terms. No policy shall be provided waiver for more than three consecutive terms.

8. Iso 27001 References

- A. 5.1.1 Policies for Information Security
- A. 5.1.2 Review of the Policies for Information Security
- Clause 5.1 Leadership and commitment
- Clause 5.2 Policy

9. Related Policies

- Acceptable Use Policy
- Clear Desk and Clear Screen Policy
- Access Control Policy
- Communications Security Policy
- Asset Management Policy
- Backup and Restore Policy
- Legal and Compliance Policy
- Cryptography Policy
- Human Resource Policy
- Disciplinary Process Policy
- Information Security Aspects of Business Continuity Management Policy
- Information Security Incident Management Policy
- Operations Security Policy
- Mobile Device Management Policy
- Information Security Policy
- Organization of Information Security Policy

- Password Policy
- Physical and Environmental Security Policy
- Risk Management Policy
- System Acquisition, Development and Maintenance policy
- Information Security Supplier Relationship Policy
- Information Transfer Policy
- ISMS Roles and Responsibilities

10. 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).

11. 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-