Vivriti Cyber Security Policy

Version	Approval Date	Prepared By	Approved By
V2	07-Nov-2022	Info Sec	Board
V2.1	03-Nov-2023	Info Sec	Board
V2.2	07-Feb-2024	Info Sec	Board

Contents

1 Introduction

The purpose of this document is to provide details of Vivriti's Cyber Security policy that is applicable at Vivriti. This document has been prepared as per the guidelines by RBI Master Circular. At any given point, Vivriti shall put its utmost effort and due diligence to ensure cyber risks are within acceptable limits by regularly assessing them and applying necessary controls as required to bring the same within acceptable limit.

1.1 Scope

The policy applies to all individuals who access, use or control Vivriti Capitial owned resources. This includes but is not limited to Vivriti Capitial'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 Capitial's resources, network.

This 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 Capitial.

1.2 Objectives

Formulation of a detailed Information Security policy and adhering to it will help us in

- Safeguarding all company data and protecting resources that are proprietary and confidential.
- Optimizing the use of the company's resources including IT infrastructure and equipment
- Ensuring availability of adequate resources for the regular conduct of our business without causing any adverse impact to our clients and stakeholders.
- Ensure PII of customers/employees are safeguarded in addition to confidentiality, integrity and availability of company data.

1.3 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.

2 Cyber Security Policies

2.1 Email Usage policy

2.1.1 Policy brief & purpose

Email is an important and essential communication mechanism to perform our everyday jobs. It is a resource that needs to be judiciously used to ensure its effectiveness and to ensure that it doesn't adversely impact the rest of the organization.

2.1.2 Scope

This policy applies to all employees (temporary and fulltime), vendors and partners who are assigned (or given access to) a corporate email. This email may be assigned to an individual (e.g. employeename@companydomain) or department (e.g. hr@companydomain.com.)

2.1.3 Appropriate Usage

- Employees should use their company email primarily for work-related purposes.

Employees can use their official email to:

- Communicate with current or prospective customers and partners.
- Log in to company purchased software they have legitimate access to.
- Share their email address to peers 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.

2.1.4 Inappropriate Usage

Official email should not be used to

- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Sign up for any site that is not related their business purpose like ecommerce site, social media etc.
- 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 coworkers
- 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.

Our company has the right to monitor and archive corporate emails.

2.1.5 Protection

- Employees shall 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 report the same to the info sec team or forward it to infosec@vivriticapital.com before proceeding to engage.

2.1.6 Monitoring

- Vivriti will monitor all email communication and employees shall not expect any privacy whatsoever when using firm email system.

2.1.7 Email signature

- Employees must use only Vivriti approved signature in their official email.
- The signature shall contain the organization logo, name, the employee contact information and designation as applicable.

2.1.8 Disciplinary action

Employees who don't adhere to the present policy shall face disciplinary action as per the disciplinary process policy up to and including termination. Example reasons for termination are:

- Using a corporate email address to send confidential data without authorization.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.
- Using a corporate email for an illegal activity.

2.2 Internet Usage Policy

2.2.1 Objectives

Internet usage is essential in today's corporate world. To ensure that employees are very productive, the firm has invested in a high-speed network at a high-cost outlay. This policy is laid down to ensure that this expensive resource is used optimally for the firm's benefit and to prevent inappropriate or illegal internet use that creates risks for our company's legality and reputation.

2.2.2 Scope

This employee internet usage policy applies to all our employees, contractors, volunteers and partners who access our network and computers.

2.2.3 Appropriate Usage

- To complete their job duties.
- To seek out information that they can use to improve their work.

2.2.4 Inappropriate Usage

- Download or upload obscene, offensive or illegal material.
- Send confidential information to unauthorized recipients.
- Invade another person's privacy and sensitive information.
- Download or upload movies, music and other copyrighted material and software.
- Play games over the Internet.
- Visit potentially dangerous websites that can compromise the safety of our network and computers.
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.
- Employees are advised to be careful when downloading and opening/executable files and software. If they're unsure if a file is safe, they should ask [their supervisor/ IT manager/ etc.]
- The company has installed anti-virus and disk encryption software on the laptops. Employees may not deactivate or configure settings and firewalls.
- Using our internet connection to steal or engage in other illegal activities.

2.2.5 Monitoring

- All Internet usage will be monitored by the IT department for disallowed use. The IP address and username of the originator of the Internet traffic shall be gathered and stored for a period as per legal and regulatory requirement.

2.2.6 Protection

- Vivriti IT department will block certain websites that the company deems as dangerous or illegal. All websites in the following classes will be blocked.
    - Adult/Sexually Explicit Material
    - Advertisements & Pop-Ups
    - Gambling
    - Hacking
    - Illegal Drugs
    - Intimate Apparel and Swimwear
    - Peer to Peer File Sharing
    - Personals and Dating
    - SPAM, Phishing and Fraud
    - Spyware
    - Tasteless and Offensive Content
    - Violence, Intolerance and Hate
- If a site is incorrectly blocked/tagged as offensive, employees can request the IT department to be unblocked with adequate business justification and supervisory approvals.

2.2.7 Disciplinary Action

The IT team will monitor employee usage of the Internet. Employees who don't conform to this employee internet usage policy will face disciplinary action as per the disciplinary process policy. Severe violations shall cause for termination of employment, or legal action when appropriate. Examples of serious violations are:

- Using our internet connection to steal or engage in other illegal activities.
- Causing our computers to be infected by viruses, worms or other malicious software.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.

2.3 Social Media Policy

2.3.1 Policy brief & purpose

Social media is a place where people exchange information, opinions and experiences to learn, develop and have fun. Whether employees are handling a corporate account or use one of their own, they should remain productive. This policy provides practical advice to avoid issues that might arise by careless use of social media in the workplace.

2.3.2 Scope

All employees of Vivriti, and contractors, interns are covered by this policy.

2.3.3 Policy elements

- "Social media" refers to a variety of online communities like blogs, social networks, chat rooms and forums. This policy covers all of them.
- We consider two different elements: using personal social media at work and representing our company through social media.

2.3.4 Using personal social media

- Employees at Vivriti are barred from accessing personal accounts at social media sites such as Facebook, Hangouts etc.
- Anyone associated with Vivriti as an employee/contractor/Vendor/Intern are banned from posting any conflicting or confidential information about Vivriti.

2.4 Portable Media

- By default, all the external media ports are blocked in Vivriti's machines. If anyone is in need of using external medial like hard drive,it is only permitted in exceptional circumstances with proper business justification and HOD approval.
- 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 Capitial reserves the right to inspect and erase portable media that is used on our network.

2.5 Confidentiality

- Vivriti Capitial 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) or any other information flagged as such shall be classified as confidential. 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.
- Any access must be provided to information using the principle of least privilege and shall provide access to informational resources on a need-to-know basis.

2.6 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; that 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.
- HR should ensure that Software developers and all other relevant personnel involved in the development of software for Vivriti Capital are undertaking secure development training on a periodic basis.

- Upon termination of employment, including the completion of any contract position, the HR should ensure that Infrastructure team and Admin team is notified and disabling all of the departing employee's user accounts and privileges before signing off on their last working day.

2.7 Access Control

2.7.1 Password

- Users must be forced to change their passwords during the first log on, and at 45 -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 five successive login failures shall result in account lockout which will get unlocked in 30 mins. If it has to be unlocked immediately, it requires administrator intervention.
- Default accounts shall be disabled and/or default passwords associated with such accounts shall be changed.

2.7.2 Remote Access

- Frequently users will be required to access the Vivriti Capital'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) and the associated security policies must be applied.
- Online Communication from within Vivriti Capital's offices to an external party may only use Vivriti Capital'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.

2.7.3 Operations Security

- Vivriti Capital'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 minimize downtime or unusual business disruption.
- System changes or re-configurations of standard IT components without proper authorization or approval are not allowed. Only additions and/or changes of software components can be made by users on workstations with prior approval from IS team and IT team.
- The following system changes are strictly prohibited unless special authorization of IS team and IT team 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.

2.7.4 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.
- 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 Capitial, 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 Capitial's security requirements.

2.7.5 Wireless Security

- Passwords for Guest wireless networks shall be changed on a quarterly basis.
- Only approved wireless access points to be used.
- Wireless networks shall always be encrypted.

2.8 Logging And Monitoring Events

2.8.1 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.
  - Database logs
  - Any other logs as required to be complaint with legal and regulatory requirements.
- Any security issues discovered will be reported to the IT Security Department for investigation.

2.8.2 User Monitoring

- In order to maintain the security of the Vivriti Capitial's IT systems (including to prevent cybersecurity threats) and to protect the assets and data, Vivriti Capitial'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 Capitial will be in accordance with applicable law.

2.9 Workstation Security

- All workstations (Laptops) must have all Vivriti Capitial approved security tools pre-installed and fully encrypted.
- Administrator access on the workstation must be restricted only to IT Team and controlled with least privilege principles.
- Anyone else in need of Admin access should seek necessary approval with business justification and the access should be provided only for some pre-defined duration after which it should be renewed.
- 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.

2.10 Secure Software Development

- Application Security checkpoints are to be implemented across all stages of software development.
- It shall include source code audits by professionals by having assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.
- Secure coding guidelines are developed and adhered to.
- 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, by incorporating secure coding principles and security testing based on global standards.
- Code should be tested for common weakness like OWASP Top 10 and SANS 25 and CIS 20 controls are to be complied and tested.
- Containerized application environment shall be prepared and implemented for exclusive business use that is encrypted and separated from other smart phone data/applications.
- There should be measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case there is a need.

2.11 Patch/Vulnerability & Change Management

- Vivriti Capital 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 to be managed 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 shall be done and apply necessary patches to remove 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 Capital' s network to external network and interconnections with partner, vendor and service provider networks are securely configured.

2.12 Authentication Framework For Customers

- Implement authentication mechanism to provide positive identity verification to customers.
- Customer identity information should be kept secure.
- Vivriti Capitial will be the identity provider for identification and authentication of customers for access to partner systems using secure authentication technologies.
- Multi Factor Authentication to be implemented wherever necessary.

2.13 Vendor Risk Management

- Vivriti Capitial shall be accountable for ensuring appropriate management and assurance on security risks in outsourced and partner arrangements.
- Vivriti Capitial carefully evaluate the need for outsourcing critical processes like facility management services, desktop management, UPS management etc.
- Selection of vendor/partner to be done 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 to be in place.
- Access to all information resources (online/in person) that are consumed by Vivriti Capital, to be made accessible to RBI officials when sought, though the infrastructure/enabling resources may not physically be located in the premises.
- Further, Vivriti Capitial to adhere 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
- Third Party Risk Assessment to be done periodically (once in a quarter) and any new risks identified to be documented and mitigated.

2.14 Advance 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 Capitial shall have Anti-malware, Antivirus protection including behavioral 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.
- This should also include tools and processes for centralized management and monitoring.

2.15 Data Leak Prevention Strategy

- Vivriti Capitial shall have a comprehensive data loss/leakage prevention strategy at firewall level, email level and end point 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.

3 Metrics

- Vivriti Capitial 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.

4 Policy Enforcement And Compliance

- Vivriti Capitial 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 Capitial Intellectual Property.
- To this end, and for overall assurance of the confidentiality, integrity, and availability of Vivriti Capitial information systems, an independent review of compliance with this Policy shall be conducted on a regular basis.
- Vivriti Capitial 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 Capitial employee who does not comply with this policy may be subject to disciplinary action, up to and including termination.
- Access to Vivriti Capitial's information systems and resources is a privilege, not a right, and may be revoked or suspended at any time.

5 Waiver Criteria

- The policy is intended to address information security requirements. If needed, waivers shall be formally submitted to the Information Security Committee/ IT Steering Committee, including justification and benefits attributed to the waiver.
- The policy waiver period have 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.

6 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 board.

7 Glossary

7.1 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-