Vivriti Capital Limited

Vivriti Disciplinary Process Policy

Version 2.1

Contents

Document Summary			
Project/ Track Name	Vivriti Capital	Approved by	ISMGC
Document Name	Disciplinary process policy	Review Type	
Document No	ISP-25	Review Date	31-10-2022
Revision no	2.0	Full/Delta Review	Full
Object Type	Policy Document	Review Size (Pages/FP/LOC)	10 Pages

Revision History						
Version	**Author**	**Date**	**Affected Sections**	**Reviewer**	**Approver**	**Approval Status**
2.0	Lakshmi Balaji	Oct 31, 2022	All	Prasenjit Datta	ISMGC	Approved
2.1	Goutham Vaidyanathan	15-10-2023	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.

1 Important Note

2 Purpose

The purpose of this policy is to detail the classification criteria and responsibilities for the disciplinary process at Vivriti Capital. This Policy supports the high-level policy statements defined in the Human Resource Security Policy and the Information Security Policy.

3 Scope

This policy applies to all individuals who access, use or control Vivriti owned resources. This includes but is not limited to Vivriti Capital's employees and third parties (contractors, consultants and other workers including all personnel affiliated to external organizations) with access to the Vivriti Capital's resources, network. This policy is applicable for all the locations of Vivriti Capital.

4 Roles and Responsibilities

S.No.	*Key Practice*	*Responsibility of*
1.	Disciplinary Process	Head - Human Resource (HR) Department

5 Policy Statements

5.1 General

- Employees, contractors and third-party staff at Vivriti Capital are expected to comply with and abide by all the policies, guidelines, rules and agreements as amended from time to time. In the event of
  (a) breach of any of the policies, guidelines, rules and agreements.
  (b) misconduct by any employee of Vivriti Capital,
  he/ she shall be liable for disciplinary action. The process for disciplinary action shall be owned by the HR Department.

5.2 Third Party Staff

In case of third parties' staff breach of agreement, misconduct and non-performance, Vivriti Capital's Management shall have the sole discretion to initiate disciplinary action in consultation with Legal, HR and any other concerned departments. This shall vary from being a verbal warning to the third-party vendor to termination of services of the vendor or even legal proceedings, as the case may be.

6 Guidelines for Information Security Offence Classification

These guidelines provide guidance in categorizing an observed or reported offence according to specific severity to take effective disciplinary action. These guidelines shall be consulted by the Information Security Management and HR Department involved in deciding on the disciplinary action.

Indicative categorization of the security incidents is provided in the table below:

Type of violation		Severity		
		High (threat on Vivriti information breach which highly affects CIAP)	**Medium (Moderate level of threat of Vivriti information)**	**Low (negligence act – no information breach)**
Physical Security				
1	Making or allowing an unauthorized entry into restricted areas (Server Room, UPS, EB Room, Facility Room, Store Room)	X		
2	Entry into Vivriti premises without identification badges		X	
3	Piggybacking/ tailgating in the Vivriti premises		X	
4	Smoking, eating, alcohol or drinking in secure areas (server room, UPS room)		X	
5	Improper handling of backup tapes, etc. (e.g., bringing magnetic material near such storage media, not ensuring proper atmospheric conditions for their storage, etc.)		X	

Type of violation		Severity		
		High (threat on Vivriti information breach which highly affects CIAP)	**Medium (Moderate level of threat of Vivriti information)**	**Low (negligence act – no information breach)**
6	Unauthorized removal of any type of Vivriti IT assets and equipment from the premises	X		
7	Unauthorized relocation of Vivriti IT assets and equipment inside the premises		X	
8	Leaving laptops unattended in insecure areas	X		
9	Non-adherence to environmental precautions for server room	X		
6.1.1.1.1 **E-Mail Security**				
10	Unauthorized use of another person's e-mail	X		
11	Sending viruses through e-mail attachments	X		
12	Inappropriate auto forwarding of e-mail		X	
13	Using e-mail in a manner that: • interferes with normal business activities or hampers employee productivity. • embarrasses Vivriti Capital. • consumes more resources. • involves solicitation.	X		

Type of violation		Severity		
		High (threat on Vivriti information breach which highly affects CIAP)	**Medium (Moderate level of threat of Vivriti information)**	**Low (negligence act – no information breach)**
	• Compromises privacy of any individual. • Is associated with any for-profit outside business activity.			
14	Blanket forwarding of e-mail		X	
15	Sending profane, obscene, or derogatory e-mails	X		
16	Sending any confidential/PII information to any unauthorized person inside/outside vivriti.	X		
17	Using Vivriti email address for conducting a personal business or for an illegal activity	X		
18	Send insulting or discriminatory messages and content	X		
6.1.1.1.2 **Passwords**				
16	Password sharing / disclosure for confidential/ restricted or highly sensitive information assets by end users	X		
17	Insecure storage of critical passwords of privileged IDs	X		
18	Requesting / making unauthorized password resets of other users in their absence	X		
19	Requesting / making password resets of other users in their absence for	X		

Type of violation		Severity		
		High (threat on Vivriti information breach which highly affects CIAP)	Medium (Moderate level of threat of Vivriti information)	Low (negligence act – no information breach)
	emergency business purposes without appropriate approval			
20	Non-use of screen saver / power-on passwords on user desktops		X	
21	Non-use of screen saver / power-on passwords on server consoles	X		
22	Not changing default passwords		X	
23	Not disabling default passwords on critical systems	X		
24	BYOD without approval from IT/Infosec/Admin	X		
25	Not disabling default credentials with elevated privilege	X		

The following are examples of some behaviour that may be subject to accelerated disciplinary action:

- Fraud / Embezzlement / Theft.
- Falsification of records.
- Breach of confidentiality and privacy.
- Improper use of company equipment/ misuse of company guidelines.
- Downloading unauthorized content including using proxy servers etc

7 Guidelines for Managers and above

- The primary objective of Vivriti Capital is to correct, not punish the employee. Therefore, before taking disciplinary action, the supervisor shall meet with the employee to discuss

the problem or concern and to provide the employee an opportunity to ask questions or to explain the performance or conduct.

- In cases where disciplinary action shall result in a loss of employee pay or benefits (suspension or termination), departments shall give the employee an opportunity to receive and present information and ask questions before making a decision regarding the disciplinary action.
- Managers may, at their discretion and judgment, follow a progressive escalation procedure to address personal conduct or work performance issues.
- All actions shall follow progressive escalation procedure - regardless of the heading under which action is taken. However, the manager may exercise discretion to escalate action at any stage if the situation warrants in consultation with Human Resource Department.
- In cases of a suspected or breach of Vivriti policy violation/ integrity concern, the Reporting Manager must raise the matter to the HR Department for review and a final decision on all such cases shall be taken by the HR Department.
- Managers shall make every effort to protect the confidential nature of any disciplinary action discussion.

8 Employee's opportunity to receive and present information

The elements of this opportunity are:

- For the employee to be provided information, in writing by the supervisor, relating to the nature and manner of the infraction or deficiency.
- To ask questions, to explain, to respond and to give information about the allegations in a meeting or in writing to an authorized representative in the HR Department.
- To have the employee's information considered by the decision maker prior to a final determination of disciplinary action being issued; and
- To receive written notification of the final decision.

9 Policy Enforcement and Compliance

Compliance with this policy is mandatory and Vivriti Capital 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 Capital 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.

10 Waiver Criteria

This 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.

11 ISO 27001 References

- A.7.2.3 Disciplinary Process

12 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 annually at a minimum.

Any change will require the approval of the Information Security Management and Governance Committee (ISMGC).

13 Glossary

Term	Definition
Asset	Asset is anything that has value to the organization.
Information Security and Privacy	The preservation of confidentiality, integrity, availability and privacy 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-