Third Party On-Boarding and Off-Boarding Process Policy

VCPL-ISP -14-V1.0

DOCUMENT AND RECORD CONTROL

Version Control

Document Control ID	VCPL-ISP-14 _Third Party On-Boarding and Off-Boarding Process
Issued Date	16-September-2022
Effective Date:	16-September-2022
Owner:	ISMS

Revision Table

Date	Version	Affected Sections	Author
16-September-2022	1.0		Mr Ramesh T.P

Release Authorization

Task	Author	Title
Prepared by	Mr Ramesh T.P	Deputy Vice President

Reviewer Authorization

Name	Title	Signature	Date
Mr. Prasenjit Datta	Head of Technology	Prasenjit Datta	16-September-2022

Approval Authorization

Name	Signature	Date
Board of Directors		

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

TABLE OF CONTENTS

1. Purpose 3
2. Scope 3
3. Pre-On-Boarding of the Third-Party Vendor 3
4. Post On-Boarding of Third-Party Vendor 5
5. Off-Boarding of the Vendor 5
5.1 Functional Workflow of Vendor On-Boarding and Off-Boarding 7
6. Risk Mapping for Third Party Vendor 7
7. Approval Matrix 9
8. Compliance Requirement 9
9. Non-Company Security Baseline 11
9.1 Identification and Authentication 11
9.2 Access Control 11
9.3 Hard Disk Encryption 11
9.4 System Hardening 12
9.5 Anti-Virus and Firewall 12
9.6 Patching and Backup 13
9.7 Network Access Control 13
10. References 13
11. Appendix A – Recommended Security Products 14

1. Purpose

Vivriti Capital provides access to its premises and information processing assets to various vendors and third parties. This standard provides a process flow of a secure relationship with the third parties and vendors and minimize chances of information breaches or loss of services which may further lead to financial and/or reputational or legal consequences.

2. Scope

The guidelines are applicable to all vendors, contractors and third parties who are not under the payroll of Vivriti Capital. Vivriti Capital shall enforce the security procedures on the third parties appropriately and monitor/audit them as and when required.

Bring your own device document is meant to provide support for:

- All workstations not owned or leased by Vivriti Capital.
- All workstations managed by Vivriti Capital for client if client did not provide their own written security requirements.
- All Vivriti Capital owned or leased workstations on which client provided OS images are deployed.
- All personal workstations where Vivriti Capital guest image is installed, all workstations used by vendors/ Contractors/ Clients that need to operate from Vivriti Capital offices for extended durations utilizing their own workstations and/or client/ vendor provided images.

Workstations are defined as any computer (e.g., desktop, laptop, netbook or tablet) which has the ability to access, store or process data, can connect to any Vivriti Capital network or Internet and which runs a full version of the OS.

3. Pre-On-Boarding of the Third-Party Vendor

Steps	Action Item	Description	Responsible	Accountable
1	Vendor Identification Request	Respective function head will place the request to identify the vendor based with the requirement list.	Team Manager	Business / Function Head
2	Identification of the Vendor	Respective team identifies a third-party vendor as per the requirement for its Internal use.	Human Resource Team / Team Manager	Human Resource / Business / Function Head
3	Non-Disclosure Agreement	A Non-disclosure agreement should be signed between the third-party vendor and Vivriti Capital before the commencement of the services.	Human Resource Team	Head of Human Resource

Steps	Action Item	Description	Responsible	Accountable
4	Vendor Risk Assessment	A vendor risk assessment is performed by the Vivriti Capital Information Security team to validate the effectiveness of the security controls implemented by the third-party vendor.	Information Security Team	Head of Information Security
5	Compliance Status on Third Party Vendor	Vivriti Capital Information security team validates the security controls implemented by third party vendor and provides the report of compliance to the business owners. If the Security controls implemented by the third party found to be ineffective, Information security team informs HR / Application / Business team to identify an alternate vendor.	Information Security Team	Head of Information Security
6	Defining Scope and Access Level for the Third-Party	The Engineering team defines the scope post the confirmation from the Information Security team.	Team Manager	Business / Function Head
7	Contract Execution	Legal team will execute the contract with scope and information security clauses and data loss penalty clauses defined in third-party vendor contract.	Legal Team	General Counsel
8	Access Creation Request to Vivriti Capital Tools / Applications	The Engineering initiates the request for access creation to the Vivriti Capital applications, Vivriti Capital Platform (Production and Non-production), Vivriti Capital email address creation, GitHub,	Team Manager	Business / Function Head

Steps	Action Item	Description	Responsible	Accountable
		Confluence, Slack, VPN & Development server access to the third-party vendor.		

4. Post On-Boarding of Third-Party Vendor

Steps	Action Item	Description	Responsible	Accountable
1	Access Creation Request Raised in Ticketing System	The HR / Business / Application team should raise a ticket to the IT, DevOps & Administration team for the access creation.	HR / Team Manger	HR Head / Business / Function Head
2	Approval for the Access Creation Request for Third Party	The access creation request must be approved by the functional/business head.	VP / Business / Functional Head	Chief Technology Officer (CTO)
3	Access Provision to the Third Party	The requested accesses are created by the IT, DevOps and Administration team to the third-party vendor and communicated the Human resource / Application team.	IT, DevOps and Administration Team	Manager IT / DevOps / Admin
4	Monitoring of the Third-Party Vendor	Post on-boarding, the vendor will be monitored by the Information Security team periodically.	Information Security Team	Head of Information Security

5. Off-Boarding of the Vendor

Steps	Action Item	Description	Responsible	Accountable
1	Access Revocation Request for Third-Party	The Off-boarding request will be raised by the HR/respective team	HR / Team Manager	HR Head / Business / Function Head

Steps	Action Item	Description	Responsible	Accountable
2	Revocation of Access	The removal of access to Vivriti Capital applications to the third party.	IT, DevOps and Admin Team	Manager IT / DevOps / Admin
		If any transaction of data required from third-party vendor, Application team should raise a request to the IT and DevOps before removal of the access.	Team Manager	Business / Function Head
3	Confirmation on the Access Revocation from IT/DevOps and Admin	Post access revocation a confirmation email will be communicated to the HR/Application team.	IT, DevOps and Admin Team	
4	Data and Assets Collection from the Vendor Laptop/ System(s)	All the data and assets related to the Vivriti Capital such as documentation and source code, data files etc.,	Team Manager	Business / Function Head
5	Data Deletion	The contract manager of the vendor must confirm that all the data related to Vivriti Capital has been deleted from their system.	Contract Manager / Team Manager	Business / Function Head
6	Email Communication from the Vendor on the Secure Data-Deletion Confirmation	A confirmation email for the secure data deletion related to Vivriti Capital to be shared with Team manager and Compliance team.	Contract Manager / Team Manager	Business / Function Head
7	Review of Legal and Security Clauses	Compliance team to review the legal terms related to Confidentiality, Network & Compliance, Limitation of liability and Data Processing Addendum(DPA) and provides the confirmation for the contract closure.	Infosec Team	Infosec Head

Steps	Action Item	Description	Responsible	Accountable
8	Confirmation on the Access Revocation	A final confirmation email from the team manager to be shared with Engineering team and Compliance for the closure of the contract.	Team Manager	Business / Function Head

5.1 Functional Workflow of Vendor On-Boarding and Off-Boarding

6. Risk Mapping for Third Party Vendor

S. No	Prerequisites	Why	Action Items	Owner	Risk	Monitoring Process
1	Application should have the Role based access control in order to provision access	Ensure to have the access required for business / operation purpose	Evaluation of RBAC	IT / DevOps	Full access to application will expose the entire data in the application. Customer data / details exposure.	Team manager / Business owner should review the access periodically and any deviation should be reported to IT/DevOps. Audit logs should be reviewed by InfoSec. InfoSec team will perform the monthly reconciliation process to ensure off boarded vendor/employee access revoked. Team manager / Business owner should

S. No	Prerequisites	Why	Action Items	Owner	Risk	Monitoring Process
						inform to IT / DevOps to remove the access as on when employee left the vendor organization.
2	Vendor Risk assessment should be performed	Verification of Security standards	Template should be given by InfoSec	InfoSec	Probability of Data loss / theft	Infosec Team should conduct the Risk Assessment and report should be submitted to Business team.
3	NDA should be signed	For Non-Disclosure and Confidentiality agreement	Vivriti Capital NDA template should be signed by both the parties	Legal / Business Owner	Proprietary information will be exposed to Vendors. Process Non-conformity	NDA Clauses should be reviewed by General Counsel.
4	Security / Penalty clauses should be added in case of loss of data from vendor as part of the agreement	In case Data breach by vendor	Adding a clause	Leal / Contract	Legal issues from Customers in case of Data breach or any violations. Financial / Reputation impact to the Organization.	Security Clauses should be reviewed for all contracts and Both parties should sign the contract and accepted by General Counsel.
5	BGV reports of the person who is working on the project	Integrity	Vendor should provide the details	Vendor	Confidentiality Integrity	BGV Reports should be reviewed by Security Team.

7. Approval Matrix

S. No	Access Provisioning / Deprovisioning	Team Manager	Business Owner (Director and Above)	VP CloudOps	IT / DevOps Team	CTO
1	Recommended by business team for limited access with details	X				
2	Approved by		X	X		
3	Approval for Exceptions					X
4	Ticket creation with an Approval email	X				
5	Access Provisioned by				X	
6	Recommended by	X				
7	Approved by					
8	Ticket should be created for revocation	X				
9	Access De-provisioned by				X	

8. Compliance Requirement

All new systems must be designed to comply with this standard prior to being introduced into Vivriti Capital environment.

Existing systems must develop a remediation plan to get into compliance to this standard and for remediation of any new vulnerabilities within the timelines provided in the Vivriti Capital System Security and Patch Management Policy.

The below requirements are minimum standards. It is always acceptable to implement measures that are more stringent than what is documented below. Exceeding the minimum does not warrant a security exception.

The following table provides a guide to help users determine if the device should fall under the Non-Company Workstation, Vivriti Capital Windows Workstation or Vivriti Capital Mac Workstation standards.

Scenarios	Vivriti Capital Managed	Client / Vendor Managed	Applicable Standard Non-Vivriti Capital Premise Home/Third Party Network
Client / Vendor Image on Client / Vendor Hardware	√	√	Non-Company Workstation Security Standard (NCWS) + Contract
Client Image on Vivriti Capital Hardware	√	√	NCWS + Contract + Polling Exception required
Vivriti Capital Altered Image on Vivriti Capital Hardware	√	√	WS + Security or Tech Exception required

Vivriti Capital Managed	Operating System and Security Tools are Managed by any of Vivriti Capital, Technology Services (Customer Support) or Vivriti Capital Project Dedicated IT Support Team.
Client / Vendor Managed	Operating system and security tools are managed directly by the client or vendor.
Vivriti Capital Premise / Non-Vivriti Capital Premise	Typical physical location of the workstation when performing standard business services.
Shared Network	Workstation which utilizes both client and Vivriti Capital workstation per client requirement.
Home / Third Party	A workstation which utilizes a person’s home or 3rd party network.
NCWS	Vivriti Capital Non-Company Workstation Standard must be followed.
WS	Vivriti Capital Windows Workstation Standard must be followed.
Contract	Client image must additionally follow specific controls from the contract agreement between Vivriti Capital and the respective client.

9. Non-Company Security Baseline

9.1 Identification and Authentication

Control	Vivriti Capital	Client Delivery
All Non-Company Workstations must comply with the relevant controls listed in Vivriti Capital Access Control Policy.	√	√
Password lockout standard must comply with Vivriti Capital Password Policy.	√	√
Must utilize a unique login name that is linked to the user's name in order to ensure accountability.	√	√

9.2 Access Control

Control	Vivriti Capital	Client Delivery
All workstations must use the NTFS file system.	√	√
Set screensaver to start after 10 minutes of inactivity and password protect on resume.	√	√
Disable default shares: C Drive, D Drive and Admin Drive.	√	√

9.3 Hard Disk Encryption

Control	Vivriti Capital	Client Delivery
All workstations that are not owned or leased by Vivriti Capital but used to perform Vivriti Capital or client work should deploy hard disk encryption in full disk encryption mode so as to encrypt all the data stored on their hard disks.	√	√
Hard disk encryption tool must comply with requirements provided in the Vivriti Capital System Security Policy.	√	√

Note: Encryption of client owned devices can be accomplished through encryption software provided by the client or purchased separately.

9.4 System Hardening

Control	Vivriti Capital	Client Delivery
Operating systems used must still be supported by the vendor. Operating systems that are no longer supported by the vendor are not permitted.	√	√
If the workstation is used to access Vivriti Capital resources, it cannot have any peer-to-peer software installed.	√	√

9.5 Anti-Virus and Firewall

Control	Vivriti Capital	Client Delivery
All workstations are required to have personal firewall software installed, always updated and running.	√	√
Firewall software denies connections by default, with allowed connections specified in the rule base.	√	√
Auto-blocking is enabled and set to block at least some unsolicited inbound traffic.	√	√
Block any unnecessary TCP and/or UDP ports that are not required per business or contractual requirement. Any exceptions should be restricted to/from specific machines.	√	√
Logging is enabled to detect critical access attempts to the workstation.	√	√
All workstations are always required to have anti-virus software installed and running.	√	√
Automatically check for and download Virus signature updates on at least a daily basis.	√	√
Real-time protection enabled for all files that are accessed or modified.	√	√
Users have the ability to run on-demand or scheduled scans.	√	√
All detected viruses are automatically cleaned or quarantined.	√	√
Settings for the above requirements can only modified by an authorized user.	√	√

Note: For Non-Vivriti Capital machines running the same version of Antivirus as Vivriti Capital, you can request a copy of our standard configuration file to verify they have adequate security settings.

9.6 Patching and Backup

Service / Programs	Vivriti Capital	Client Delivery
Latest patches must be applied to operating system and any applications installed on the workstation. Mandatory patching timelines and differences in vulnerability severities are explained in the Information System Security Policy.	√	√
All workstations are required to have a method of automatically implementing software/security patches. Common methods include: ● Windows Automatic Updating ● Third party automatic updating software	√	√

9.7 Network Access Control

Service / Programs	Vivriti Capital	Client Delivery
For workstations needing to access Vivriti Capital internal network in offices where VPN client has to be installed.	√	√

10. References

Vivriti Capital Policies and Standards

Name	Category	Link
Information System Security Policy	Global Policy	<LINK>
Acceptable Usage Policy	Global Policy	
System Security Policy	Global Policy	
Patch Management Policy	Global Policy	
Antivirus Policy	Global Policy	
Password Policy	Global Policy	
Access Control Policy	Global Policy	
Network Security Policy	Global Policy	

11. Appendix A – Recommended Security Products

Personal Firewalls	
Zone Alarm	http://www.zonelabs.com/
McAfee Personal Firewall Plus	http://www.mcafee.com/us/
Anti-Virus	
Symantec Anti-Virus	http://www.symantec.com
McAfee VirusScan	http://www.mcafee.com/
Trend Micro OfficeScan	http://www.trendmicro.com
Microsoft Forefront	http://www.microsoft.com
Hard Disk Encryption	
Checkpoint Pointsec	http://www.checkpoint.com/pointsec/
MS Bitlocker	http://windows.microsoft.com/en-us/windows7/products/features/bitlocker
PGP Whole Disk Encryption	http://www.symantec.com/endpoint-encryption

---End of Document---