Vama Sundari Investments (Delhi) Private Limited - IT Policies

IT Policies – Index

S. No	Policy Name	Page Number
1	Acceptable Use Policy (ITPOL001- VAMA)	3
2	Backup and Recovery Policy (ITPOL002- VAMA)	15
3	Clean Desk Policy (ITPOL003- VAMA)	21
4	Data Privacy Policy (ITPOL004- VAMA)	25
5	Incident Management Policy (ITPOL005- VAMA)	39
6	Information Security Policy (ITPOL006- VAMA)	45
7	Internet Usage Policy (ITPOL007- VAMA)	55
8	IT Asset Management Policy (ITPOL008- VAMA)	62
9	IT Change Management Policy (ITPOL009- VAMA)	70
10	IT Equipment Disposal Policy (ITPOL010- VAMA)	77
11	Logical Access Control Policy (ITPOL011- VAMA)	83
12	Password Management (ITPOL012- VAMA)	91
13	Patch Management Policy (ITPOL013- VAMA)	97
14	Physical Access Control Policy (ITPOL014- VAMA)	106
15	Remote Access Policy (ITPOL015- VAMA)	112
16	Software Asset Management Policy (ITPOL016- VAMA)	117
17	IT Continuity and Cyber Crisis Management Plan (ITPOL017- VAMA)	124

DOCUMENT APPROVAL HISTORY

Version Number	Description - Document Revision	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

1. **Overview** 3
2. **Scope** 3
3. **Purpose** 3
4. **Ownership** 3
5. **Policy** 3
6. **Weakness & Incident Reporting** 9
7. **Intellectual Property/Ownership** 10
8. **Right to Audit** 10
9. **Governing Policy/Procedures** 11
10. **Enforcement** 12

1. Overview

The Entity intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to The Entity established culture of openness, trust and integrity. The Entity is committed to protecting The Entity employees, partners and the company from illegal activities or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of THE ENTITY. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every The Entity employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Scope

This policy applies to all employees, contractors, consultants, temporaries, and other workers providing services or working at The Entity, including all personnel affiliated with third parties. This policy applies to all equipment's that are owned or leased by The Entity.

3. Purpose

The purpose of this policy is to outline the acceptable use of computer assets including (Hardware, Software and Applications) at The Entity. These rules are in place to protect the employee and The Entity both. Inappropriate use could expose The Entity to many risks including virus attacks, compromise of network systems / services, and legal / compliance issues.

4. Ownership

The ISMS Steering Committee is the owner of this policy and System Administrator is responsible for maintaining it.

5. Policy

This policy defines DO's which is acceptable and Don'ts which are unacceptable as per The Entity

policy.

5.0 DO's

5.0.1 While The Entity network administration desires to provide a reasonable level of privacy, the Users should be aware that the data they create on the corporate systems remains the property of THE ENTITY. Because of the need to protect The Entity network, management cannot guarantee the confidentiality of information stored on any network device belonging to THE ENTITY.

5.0.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use and if there is any uncertainty, employees should consult their supervisor or manager.

5.0.3 Ethical use of resources by all employees. A culture encouraging participants to disallow misuse or abuse of any IT resources by self or peers.

5.0.4 Postings by employees from The Entity email address to newsgroups should contain a disclaimer stating that "The opinions expressed are strictly their own and not necessarily those of THE ENTITY", unless posting is in the course of business duties.

5.0.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, Malware, spy ware, or Trojan horse code.

5.0.6 When employees receive unwanted and unsolicited email (also known as SPAM), they must refrain from responding directly to the sender. Instead, they should forward the message to the system administrator who will take steps to prevent further transmissions.

5.0.7 Employees must treat electronic mail messages and files as "Confidential" information. Electronic mail must be handled as a "Confidential" and direct communication between a sender and a recipient.

5.0.8 The Entity electronic mail system is to be used only for business purposes. All messages sent by electronic mail are The Entity records. The Entity reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose.

5.0.9 Keep all credential secure and do not share. Passwords shall be minimum 8 characters long and should contain alphanumeric characters with special characters.

5.0.10 Authorized users are responsible for the security of their credential. User level passwords should be changed every 30 days. Password should not be written down, except for lodging with departmental security staff or secure safekeeping, where appropriate. Password should be changed whenever there is any indication of possible system or password compromise.

5.0.11 Ensure the system used by an employee is protected by approved virus-scanning software with a current virus database.

5.0.12 Employees should only connect office issued equipment, while not on The Entity premises, to the Internet by The Entity pre-defined service providers.

5.0.13 System should be secured with a password-protected screensaver with the automatic activation feature set at 3 minutes or less, or by logging-off when the computer/laptop is left unattended.

5.0.14 Because information contained on portable computers is especially vulnerable, special care should be exercised to protect information from being gleaned by others in a public place. Using

Notebook in public places (conferences, training rooms etc) calls for additional physical security, usage of Laptop Locks is advised.

5.0.15 Laptop/note book have a continuous threat of theft as they are easily visible. Keep in close custody. There have been incidents related to laptop thefts inside the car. Avoid getting tricked by incidents that drive your attention around the car when someone can open your door and pick up your laptop in a fraction of seconds.

5.0.16 Smart phones used for downloading office emails. They should be physically secured and an individual is responsible for protection.

5.0.17 In case of loss of Laptop/ Notebook/ smart phone report immediately to the IT infrastructure team so that the email configuration can be changed to avoid unauthorized access to your emails. A FIR should be lodged with the nearest police station and copy of FIR be sent to IT department at corporate office.

5.0.18 Users are responsible for physical protection of cryptographic keys. So ensure that they are kept in a secure manner and the opportunity of physical theft is minimal.

5.0.19 Interaction with any external entity (strategic partner, vendor, customers) requires careful consideration both in terms of information exchanges and verbal communication. Members of staff should ensure that the communication with any external service provider is being conducted with due consideration and based on “need to know”.

5.0.20 It is the responsibility of The Entity personnel to ensure that visitors accompanying them inside office premises follow the visitor declaration with respect to assets such as Notebook, USB drives, other electronic media devices such as CD, DVD etc.

5.0.21 Employees must position their computer screens such that no unauthorized person can look over their shoulder and see the sensitive information displayed.

5.0.22 Equipment’s should not be moved or displaced to other locations without authorizations.

5.0.23 During non-working hours all employees must lock-up all media (USB sticks, CD’s, Floppy’s, Paper, etc.). Unless information is in active use by authorized personnel, desks must be **absolutely** clear and clean during non-working hours.

5.0.24 No use of USB sticks, CD ROM’s from sources outside of The Entity offices.

5.0.25 Media may not be removed from the department without written authorization.

5.0.26 Shredders should be used for destruction of paper containing critical information.

5.0.27 Sensitive or confidential information when printed should be cleared from the printers immediately.

5.0.28 All the print given by the user shall be protected and can be printed only when credentials entered at printing machine.

5.0.29 Printers are to be used for documents that are relevant to the day-to-day conduct of business at THE ENTITY. The Entity printers should not be used to print large personal documents.

5.0.30 Installation of personal printers is generally exempted at The Entity due to the cost of maintaining and supporting many dispersed machines. In certain circumstances, however, where confidentiality, remote location, the need to print a large number of low volume print jobs, or other unusual situation is an issue, personal printers may be allowed once approved on a case to case basis by The Entity IT.

5.0.31 Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing).

5.0.32 Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with IT Help Desk.

5.0.33 Color printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) will do.

5.0.34 Report any malfunction of any printing device to IT Helpdesk as soon as possible. Enforcement Any employee who is found to have violated this policy may be subject to disciplinary action.

5.0.35 Ensure that paper documents/files, other assets are kept in lock and key, when no longer in use;

5.0.36 All employees shall lock their screen (Pressing Windows + L or Control-ALT-DEL) when no longer working in their PC/ notebook;

5.0.37 While using social media such as (but not limited) twitter/ Facebook /linked-In avoid disclosing information that reflects organization's performance in anyway. Avoid using any language comment that can damage the image and reputation of the organization.

5.1 Don'ts

5.1.1 Employees must not employ scanned versions of hand-rendered signatures to give the impression that the sender signed an electronic mail message or other electronic communications.

5.1.2 Sending of large number of emails to any outside address is prohibited unless written permission from the Information Technology Manager has first been obtained.

5.1.3 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted

music, and the installation of any copyrighted software for which The Entity or the end user does not
have an active license is strictly prohibited. Employees should not save games, jokes, mp3s or any such information for entertainment purposes.

5.1.4 Using The Entity computing asset to actively engage in procuring or transmitting material that is in violation of business code of conduct sexual harassment or hostile workplace laws in the user's local jurisdiction.

5.1.5 Making fraudulent offers of products, items, or services originating from any The Entity account.

5.1.6 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

5.1.7 Port scanning or security scanning is expressly prohibited unless prior notification to The Entity is made.

5.1.8 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet

5.1.9 Employees are prohibited from using The Entity electronic communication system for charitable endeavours, private business activities or amusement/ entertainment purposes.

5.1.10 Employees should not share folders on their workstations.

5.1.11 Employees are forbidden to use any messenger/chat applications such as (but not limited to) like MSN Messenger, Yahoo messenger, WhatsApp, ICQ etc.

5.1.12 Photography, video recording and audio equipment's should not be allowed inside critical sites without approval.

5.1.13 Do not print multiple copies of the same document – the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the photocopier to make additional copies.

5.1.14 Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer. Please report any planned print jobs in excess of 100 pages to the IT department so that the most appropriate printer can be selected, and other users can be notified.

5.1.15 Avoid printing e-mail messages. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.

5.1.16 Strictly prohibited to all employees for installing / Introduction of any malicious programs into the systems / network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5.1.17 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

5.1.18 Effecting security breaches or disruptions of network communication; Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

5.1.19 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

5.1.20 Providing information, data, code, document to any external parties / agencies or consultants, without proper authorization / approval or assigned as part of Job.

5.1.21 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

5.1.22 Use of unsolicited email originating from within The Entity networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by The Entity or connected via The Entity network.

5.1.23 Employees shall not send any official documents outside of The Entity offices without permission of their immediate superior either by electronic medium or otherwise.

5.1.24 Configuring external email service provider id/accounts in The Entity email account and using such email a/c for sending / receiving email.

5.1.25 Employees shall not engage in any blogging on social websites like Twitter, Facebook, LinkedIn etc. from outside office network that may harm or tarnish the image, reputation and/or goodwill of The Entity and/or any of its employees.

5.1.26 Employees shall not attribute personal statements, opinions or beliefs to The Entity when engaged in blogging on social websites like Twitter, Facebook, LinkedIn etc. from outside office network. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee should not,

expressly or implicitly, represent themselves as an employee or representative of THE ENTITY. Employees assume any and all risk associated with blogging.

5.1.27 Handling and disclosure of copyrighted, The Entity trademarks, logos and any other intellectual property shall not be used in connection with any blogging activity

5.1.28 Revealing or publicizing proprietary or confidential information representing personal opinions as those of the company

5.1.29 Downloading any software or electronic files without reasonable virus protection measures in place

5.1.30 Use or possess Internet scanning or security vulnerability assessment tools, without the permission of the Network Administrator.

5.1.31 Use the company logos or the company materials in any web page or Internet posting unless the company management has approved it, in advance,

5.1.32 Attempt to connect telnet or port scan of any remote systems on the Internet.

5.1.33 Use of internet for Chatting, Blogging, and accessing social media groups / network on The Entity systems using data card or external network is prohibited.

6. Weakness & Incident Reporting

A security weakness /incident may be a result of compromise to Confidentiality, Integrity, and availability, non-repudiation and/or Legal or Contractual Non-conformity. The impact of any security incident may result in serious consequences to the business and therefore an adherence to this policy is to avoid any such serious incident. Each employee is expected to participate in the conduct of ISMS. The following guidelines are defined:

a) Employees must promptly report all information security alerts, warnings, suspected vulnerabilities, weaknesses, and the like to the Information Security Manger using the incident reporting Form/Procedure.
b) Users are prohibited from utilizing The Entity systems to forward such information to other users, whether the other users are internal or external to THE ENTITY.
c) Users should not be found exploiting any identified weakness.

Areas that can be reported are as follows (not exhaustive):

Any event or weakness that can jeopardize the confidentiality, integrity and/ availability' of information assets is worthy of reporting. This can include physical controls, technology controls, personnel behaviors related to information assets, and procedural controls.

An example of each of these is give below:

Physical controls can cover all aspects of physical security such as weak doors, access control systems, entry and exit areas, and associated processes.

Technical controls can cover strengths and weakness such as password complexity (less than 6), lack of antivirus, email attachments, accidental or deliberate mass mails etc;

Personnel controls such as unauthorized access attempts, violation of company policy, violation of internet usage policy etc.

Administrative controls such as asset not identified, document classification, no documentation, no change and access definition etc.

Note that an employee can report his/her head of department/reporting manager.

Consequence Management/Disciplinary action Procedure (DAP)

Disciplinary action is an action towards the non-compliance to the stated objective in this policy. Any act deliberately or accidental, wherein the motive of the end-user is found to be malicious, shall lead to disciplinary action.

In case of clarifications on any areas of the ISMS, please contact to IT Manager.

7. Intellectual Property/Ownership

The Entity owns all hosted infrastructure including information stored, processed, and transmitted in the company offices. No employee can claim the content or intellectual property of the assets/hosted infrastructure as their own.

8. Right to Audit

All company owned infrastructure is owned by The Entity, and The Entity has the right to audit any part of the infrastructure at any point of time, without giving any notice to the employee. This is to ensure that in case of a security event, the organization would need evidence to demonstrate compliance, and if necessary bring the culprit to the court of law, the culprit can be insider or outsider to the organization.

9. Governing Policy/Procedures

Information Security Policy - All employees should review the apex information Security management systems Policy and adhere to it.

Review

This policy is reviewed annually or as and when it required; however, control mechanisms exist to ensure compliance activities are built-in organizational policies and practices**.**

Definitions

Term	Definitions
Information	Information is defined as anything having business value. Examples of information are customer information (such as Name, contact details, phone number etc.), financial performance, operational or communication information.
Information Asset	Information *assets* may be categorized into two categories: information *containing* assets, and information *supporting* assets. An example of information containing assets can be a business application which hosts the customer contact details, an example of information supporting assets can be personnel, paper, network infrastructure, external service providers and so on.
Security	Protection against loss of Confidentiality, Integrity, privacy, availability of an information asset.
Security Incident	An event resulting in organizational loss.
Threat	A disaster event. Threat materialization depends on the presence of vulnerabilities – either known or unknown vulnerabilities.
Vulnerability	An inherent weakness of loophole. Vulnerability may arise due to a design flaw, an implementation flow, or simply an absence of a control to prevent or detect any security incident.
Security Incident procedure	Procedure of reporting information security suspected vulnerabilities and events.

10. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

Contents

Overview **3**
Purpose **3**
Scope **3**
Policy **3**
Risk for Non-Compliance **6**

1. Overview

This Procedure defines the backup procedure and recovery procedure for servers, network devices, end user systems, storage which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the application server, and the Database server.

2. Purpose

The purpose of this policy is to safeguard the information assets of The Entity and to prevent the loss of data in the case of an accidental deletion or corruption of data, system failure by enabling secure backup and restoration processes on the media employed in the process.

3. Scope

This policy will be applicable to recovery and backup of all critical business data. This policy refers to the backing up of data that resides on servers, individual PCs and laptops. All users need to keep their data on server provided storage only except roaming laptop users. It is imperative that end-users save their data to the appropriate server provided storage only, in order that their data is backed up regularly in accordance with company regulations and backup policy. Roaming laptop users can keep their data on laptop and need to take monthly backup on provided network attached storage path outlined in this policy. Users does not need to transfer their server storage data that is saved on a network or shared drive, as these are backed up when the servers are backed up, as per our backup policy. IT team will be responsible for backing up server's data as per backup policy schedules and local Laptop/Desktops data backup need to take every Month by the individual users with the help of IT person.

4. Policy

Backup Window

All backups shall be initiated between the following hours (local time):

- Backup window shall be as per business & IT requirement.
- In case there is no specific requirement from business side, backup shall be scheduled daily, during off peak hours between 8pm – 6am or as per the server utilization/load.

Backup Types

Backups are categorized into the following types:

- Daily

- Weekly
- Monthly
- Offsite Backup

The frequency and type of backup shall be determined by the criticality & volatility of the application/service.

Backup Plan

All backups shall be documented as part of the backup plan. The backup may be taken using dedicated backup application/tool or may be performed/scheduled manually.

At a minimum, the following details shall be recorded as part of the backup plan for each backup performed:

- Frequency of backup
- Location of backup
- Type of Backup (Image / File Level)
- Asset/ Device Owner
- Backup plan shall be verified on a half-yearly basis.

Backup Media

All backups are to be performed on backup media managed by IT Team, i.e., enterprise-grade disks, SAN or NAS.

Backup Retention Period

- The backup retention period will be defined as per Backup type or may be defined as per business requirement.
- At a minimum, the following backup retention period shall be followed:

Table 1: Backup Frequency

Backup Level	Backup Type	Backup Frequency	Backup Count
File System	Incremental	Daily Backup	15
Image Level (VM)	Incremental	Daily Backup	7
File System	Full	Daily Backup	15
Image Level (VM)	Full	Daily Backup	7
File System	Full	Weekly Backup	10
Image Level (VM)	Full	Weekly Backup	10
File System	Full	Monthly Backup	12
Image Level (VM)	Full	Monthly Backup	12

Disaster Recovery and Offsite Backups

To mitigate risk of Disaster for critical applications and data, the backed-up data should be replicated to an offsite location:

- This shall be performed using dedicated secure connectivity between the primary site and the DR site.
- The frequency of backup may be determined by the Backup type or as per business requirement.

Reporting and Monitoring

- All backup status reports shall be shared internally within the IT Backup team and with the respective server/application owner(s).
- All backup status reports shall be reviewed daily to identify any backup failures.
- In case of a backup failure the concerned member shall raise an incident/ticket to re- initiate the backup till successful backup has been achieved.

Backup Restoration Testing

- Restoration testing shall be performed half-yearly on random sampling basis or as per business request raised through service desk ticket.
- Backup restoration testing shall be limited to data restoration of critical servers/applications only or as per business demand.

Backup Restoration

Restoration of backup shall be performed by IT Backup team, only upon receiving an approved service request.

Backup Media Disposal

- End of life backup media shall be disposed as per the e-Waste management process.
- IT team shall ensure that before disposal, no backup media shall contain an active backup image.

5. Risk for Non-Compliance

Risks arising due to non-compliance with this policy include, but not limited to:

- Data/Configuration integrity loss,
- System crash and avoidable interruptions,
- Security failures,
- Confusion/delay in system configuration,
- Loss of unavailability of important data

Compliance with this policy initiates the following key controls:

- Backups are done on regular interval.
- All the restorations are scheduled to ensure planned results.
- All backup logs are monitored on daily basis.
- If any issues are noticed in Backup logs, Backups are rescheduled.

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

1. **Overview** 3
2. **Applicability** 3
3. **Policy Norms** 3
4. **Monitoring and Control** 4
5. **Policy Review** 4
6. **Policy Circulation** 4
7. **Risk for Non-Compliance** 4

1. Overview

The objective of this policy is to specify guidelines of Clean Desktop/Laptop Policy at The Entity

2. Applicability

The policy applies to all workstations of The Entity, on The Entity' Network.

3. Policy Norms

- Computer/Digital media should be stored in safe place when not in use especially beyond work hours.
- Sensitive or critical information in any form should be locked away (ideally in fire-resistant safe) when not in use.
- If laptops are left in office, they must be either locked with locking cable or locked away in a drawer.
- Digital media, must be kept in Restricted area and must be kept closes and locked when not in use or when not attended.
- Users should not keep confidential data on desktop/laptop screen as it can be easily viewable by unauthorized people and there may be threat to data confidentiality.
- Any paper/ pre-printed documents when disposed should be shredded to pieces using shredders maintained for the purpose in the company.

4. Monitoring and Control

It is the responsibility of IT team to monitor and review that Employees/Outsource Service Providers is adhering to the defined Policy Norms.

- In case it is found by Head IT or by internal audit team that the employee is not adhering to the terms defined under the policy, the same shall be highlighted to the CEO / MD for required action.

5. Policy Review

The policy will be reviewed every year or if there is any major change in IT Infrastructure to incorporate changes if any.

IT Team will be responsible for reviewing the policy and communicating the changes made therein.

6. Risk for Non-Compliance

Risks arising due to non-compliance with this policy include, but not limited to:

- Unauthorized Access
- Information leakage
- Violation of IPR, laws and regulation

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes.

Table of Contents

1. **Overview** 3
2. **Purpose** 3
3. **Scope** 3
4. **Policy** 4
5. **Your Personal Data** 5
6. **Purpose and Legal Basis do We use Your Personal Data** 6
7. **Sharing of Your Personal Data with Third Parties** 7
8. **Processing of your personal Data** 8
9. **Indemnification** 12
10. **Policy Review Period** 13
11. **Roles and Responsibilities** 14
12. **Risk for Non-Compliance** 14

1. Overview

The Entity employees places great importance on security of your personal data and adhere to the strictest security and data protection standards. The Entity have implemented technical and organizational security measures to guarantee the security of your personal data. Information is stored on secure networks and access is restricted to those employees and partners who are entitled to access our systems.

2. Purpose

The purpose of this policy is to maintain the privacy of and protect the personal information of employees, contractors, vendors, interns, associates, customers and business partners of all The Entity employees and ensure compliance with laws and regulations applicable to The Entity.

This policy (the "Data Protection and Privacy Policy") explains which personal data concerning you we collect when you visit our website (the "Website"), offices or take any of our services, when and why we collect the personal data, how we use them, the conditions of our disclosure to third parties, as well as how we secure the stored personal data.

3. Scope

This policy is applicable to all The Entity employees, contractors, vendors, interns, associates, customers and business partners who may receive personal information, have access to personal information collected or processed, or who provide information to the organization, regardless of geographic location. All employees of The Entity are expected to support the privacy policy and principles when they collect and / or handle personal information or are involved in the process of maintaining or disposing of personal information. This policy provides the information to successfully meet the organization's commitment towards data privacy. All partner firms and any Third-Party working with or for The Entity, and who have or may have access to personal information, will be expected to have read, understand and comply with this policy. No Third Party may access personal information held by the organization without having first entered into a confidentiality agreement.

The following officers have specific duties under this policy:

- Head of Internal Audits;
- Head of Information Technology; and
- Chief Executive Officer

4. Policy

Data Privacy Principles This Policy describes generally acceptable privacy principles (GAPP) for the protection and appropriate use of personal information at The Entity employees. These principles shall govern the use, collection, disposal and transfer of personal information, except as specifically provided by this Policy or as required by applicable laws:

- **Notice:** The Entity shall provide data subjects with notice about how it collects, uses, retains, and discloses personal information about them.
- **Choice and Consent:** The Entity shall give data subjects the choices and obtain their consent regarding how it collects, uses, and discloses their personal information.
- **Rights of Data subject:** Upon request from individuals, The Entity will remove/block your personally identifiable information from our database, thereby cancelling your registration. However, your information may remain stored in archive on our servers even after the deletion or the termination of your account.
- **Collection:** The Entity shall collect personal information from data subjects only for the purposes identified in the privacy notice / SoW / contract agreements and only to provide requested product or service.
- **Use, Retention and Disposal:** The Entity shall only use personal information that has been collected for the purposes identified in the privacy notice / SoW / contract agreements and in accordance with the consent that the data subject shall provide. The Entity shall not retain personal information longer than is necessary to fulfil the purposes for which it was collected and to maintain reasonable business records. The Entity shall dispose the personal information once it has served its intended purpose or as specified by the data subject.
- **Access:** The Entity shall allow data subjects to make inquiries regarding the personal information about them, that The Entity shall hold. However, considering the security of data, no direct access to their personal information for review, and/or update can be provided. Any modifications / updating in the data will be done by The Entity.
- **Disclosure to Third Parties:** The Entity shall disclose personal information to Third Parties / partner firms only for purposes identified in the privacy notice / SoW / contract agreements. The Entity shall disclose personal information in a secure manner, with assurances of protection by those parties, according to the contracts, laws and other segments, and, where needed, with consent of the data subject.
- **Obligations for Sub-processor**: Where a processor (vendor or 3rd party acting on behalf of The Entity' data processor) engages another processor (Sub-processor) for carrying out specific processing activities on behalf of The Entity (controller), the same data protection obligations as set out in the contract or other legal act between The Entity and the processor shall be imposed on the Sub-processor by way of a contract or other legal act as under IT ACT 2000 (Draft Data Privacy Bill 2018). Where the Sub-processor fails to fulfil its data protection obligations, the initial processor (relevant vendor or 3rd party acting on behalf of The Entity' data processor) shall remain fully liable to The Entity for the performance of that Sub-processor's obligations.

- **Security for Privacy:** The Entity shall protect personal information from unauthorized access, data leakage and misuse.
- **Quality:** The Entity shall take steps to ensure that personal information in its records is accurate and relevant to the purposes for which it was collected.
- **Monitoring and Enforcement:** The Entity shall monitor compliance with its privacy policies, both internally and with Third Parties, and establish the processes to address inquiries, complaints and disputes.

5. Your Personal Data

Personal Data is information or an expression of opinion that identifies or may permit anindividual to be identified.

The Entity protects your personal data in accordance with applicable laws and our data privacy policies. In addition, The Entity maintains the appropriate technical and organizational measures to protect your personal data against unauthorized or unlawful processing and/or against accidental loss, alteration, disclosure or access, or accidental or unlawful destruction of ordamage thereto.

Categories of Personal Data do We Collect and Process:

We collect personal data of our employees, potential employees, clients, suppliers, business contacts, shareholders and website users. If the data we collect are not listed in this privacy statement, we will give individuals (when required by law) appropriate notice of which other data will be collected and how it will be used.

Specifically, the personal data we collect include the categories of personal data described in the sections, as well as any other categories of personal data referred to in this privacy statement or in other statements you have received.

Except for certain information that is required by law or by The Entity policies, your decision to provide any personal data to us is voluntary. You will therefore not be subject to adverse consequences if you do not wish to provide us with your personal data.

However, please note that if you do not provide certain information, we may not be able to accomplish some or all of the purposes outlined in this privacy statement, and you may not be able to use certain tools and systems or avail services which require the use of such personal data.

If you provide us with personal data of another person (for instance, a potential employee/referral), you are responsible for ensuring that such person is made aware of the

information contained in this privacy statement and that the person has given you his/her consent for sharing the information with The Entity.

The above-mentioned categories of personal data have been obtained either directly from you (for example, when you provide information to sign up for a newsletter or register to comment on a forum website) or indirectly from certain third parties (for example, through our website's technology). Such third parties include our affiliates, public authorities, public websites and social media, suppliers and vendors.

6. Purpose and Legal Basis do We use Your Personal Data

The Entity uses your personal data only where required for specific purposes. Please view the table below for (i) a list of the purposes for which The Entity uses your personal data and (ii) an overview of the legal basis for each such purpose.

Purpose	Legal basis
Managing our contractual and/or employment relationship with you.	Necessary for the performance of a contract to which you are a party.
Recruitment.	justified based on our legitimate interests for ensuring that we recruit the appropriate employees.
Facilitating communication with you (including in case of emergencies, and to provide you with requested information).	Justified on the basis of our legitimate interests for ensuring proper communication and emergency handling within the organization.
Operating and managing our business operations.	justified on the basis of our legitimate interests for ensuring the proper functioning of our business operations.
Complying with legal requirements.	Necessary for the compliance with a legal obligation to which we are subject.
Monitoring your use of our systems (including monitoring the use of our website and any apps and tools you use).	Justified on the basis of our legitimate interests for ensuring that you receive an excellent user experience and our networks and information are secure.
Undertaking data analytics, i.e. applying analytics to business operations and data to describe, predict and improve business performance within The Entity and/or to provide a better user experience.	Justified on the basis of our legitimate interests for ensuring the proper functioning of our business operations.
Marketing our products and services to you (unless you objected against such processing, as further described in the policy.	Justified on the basis of our legitimate interests for ensuring that we can conduct and increase our business.

Where the above table states that we rely on our legitimate interests for a given purpose, we are of the opinion that our legitimate interests are not overridden by your interests, rights or freedoms, given (i) the transparency we provide on the processing activity, (ii) our privacy by design approach, (iii) our regular privacy reviews and (iv) the rights you have in relation to the processing activity.

We will process your personal data for the purposes mentioned above based on your prior consent, to the extent such consent is mandatory under applicable laws. Your consent is given once you avail our services or taken employment with The Entity under a contract.

We will not use your personal data for purposes that are incompatible with the purposes of which you have been informed, unless it is required or authorized by law.

7. Sharing of Your Personal Data with Third Parties

We may transfer personal data to our service providers, professional advisors, public and governmental authorities or third parties in connection with a (potential) corporate or commercial transaction. Such third parties may be located in other countries. Before we do so, we shall take the necessary steps to ensure that your personal data will be given adequate protection as required by relevant data privacy laws and The Entity' internal policies.

Unless you are otherwise notified, transfers of your personal data will take place in accordance with the appropriate international data transfer mechanisms and standards.

Sensitive Data

We will ask for limited sensitive data, if you are seeking employment with us or availing any services like Home Loan etc. The data like criminal convictions and offences (including information about suspected criminal activities) etc. is sourced by Third Party appointed by us for background verification.

Data Security

We maintain organizational, physical and technical security arrangements for all the personal data we hold. We have protocols, controls and relevant policies, procedures and guidance to maintain these arrangements considering the risks associated with the categories of personal data and the processing we undertake.

We adopt market leading security measures to protect your personal data.

We are working towards an ISO27001 certification, which indicates that we will adhere to the highest and strictest information security standards. This is a security standard awarded by the British Standards Institution ("BSI") that serves as international certification that organization adheres to the highest and strictest standards. This certification is the only auditable international standard that defines the requirements for an Information Security Management System ("ISMS"), and confirms that The Entity' processes and security controls provide an effective framework for protecting our clients' and our own information.

- We have regular penetration testing performed by a third- p a r t y provider, which continues to show the strength of our technical defenses.

8. Processing of your personal Data

We have operations across India, your personal data we collect may be transferred or be accessible within India throughout The Entity India business and between its entities and affiliates.

Any such transfers throughout The Entity business take place in accordance with the applicable data privacy laws.

Retention Period of Your Personal Data

We will retain your personal data only for as long as is necessary. We maintain specific records management and retention policies and procedures, so that personal data are deleted after a reasonable time according to the following retention criteria:

- We retain your data as long as we have an ongoing relationship with you (in particular, if you have an account with us).
- We will only keep the data while your account is active or for as long as needed to provide services to you.
- We retain your data for as long as needed in order to comply with our legal and contractual obligations.

Your Rights with Respect to Processing of Personal Data

You are entitled (in the circumstances and under the conditions, and subject to the exceptions, set out in applicable law) to:

- Request access to the personal data we process about you: this right entitles you to know whether we hold personal data about you and, if we do, to obtain information on and a copy of that personal data. Direct access to our IT systems and applications willnot be provided.
- Request a rectification of your personal data: this right entitles you to have your personal data be corrected if it is inaccurate or incomplete.

- Object to the processing of your personal data: this right entitles you to request that The Entity no longer processes your personal data.
- Request the erasure of your personal data: this right entitles you to request the erasure of your personal data, including where such personal data would no longer be necessary to achieve the purposes.
- Request the restriction of the processing of your personal data: this right entitles you to request that The Entity only processes your personal data in limited circumstances, including with your consent.
- Request portability of your personal data: this right entitles you to receive a copy (in a structured, commonly used excel and machine-readable format) of personal data that you have provided to The Entity, or request The Entity to transmit such personal data to another data controller.

Use of Your Personal Data when you visit The Entity website

In addition to the information set out above, the following sections describe how we use personal data when you visit The Entity website:

The Entity collect personal data at its websites in two ways:

(1) directly (for example, when you provide personal data to sign up for a newsletter or register to comment on website); and

(2) indirectly (for example, through our website's technology).

We may collect and process the following personal data:

- Personal data that you provide by filling in forms on our website. This includes registering to use the website, subscribing to services. The data we collect is
  - Name
  - Company name
  - Industry Sector
  - City
  - Phone No.
  - Query
  - Email id

- Profile
- Experience
- Service type
- Current CTC
- Details of Fixed Assets
- Photographs
- Identity proofs (Aadhar, Pan, passport)

- If you contact us, we may keep a record of that correspondence.
- We may ask you to complete surveys that we use for research purposes, although you do not have to respond to them.
- We collect data from Facebook, LinkedIn, Blogs
- Any postings, comments or other content that you upload or post to The Entity website.
- Our website collects personal data about your computer, including (where available) your IP address, operating system and browser type, for system administration, to filter traffic, to look up user domains and to report on statistics.
- Details of your visits to our website, the pages you view and resources you access or download, including but not limited to, traffic data, location data, weblogs and other communication data. Please see the Cookies section below for more information.

Third Party Links on websites

Our website may include:

- Links to and from the sites of our other websites, partner networks.
- Certain programs (widgets and apps) of third parties. Where this is the case, note that such third parties may process your personal data collected through such programs for their own purposes.

We do not accept any responsibility or liability for such third parties' sites or programs. Please check such third parties' terms of use and privacy statements before using and providing any information to such third parties' sites and programs.

Use of personal data that we collect from our websites

We use personal data for the purposes described in the section above, as well as to provide you with information you request, track consignments, make payments, consignment pick up request, business process query, process online job applications, and for other purposes which we would describe to you at the point where it is collected. For example:

- Links to and from the sites of our partner networks, advertisers and affiliates.

- Certain programs (widgets and apps) of third parties. Where this is the case, note that such third parties may process your personal data collected through such programs for their own purposes.

We analyze your IP and browser information to determine what is most effective about our website, to help us identify ways to improve it and make it more effective.

Use of your personal Data when you visit our offices:

In addition to the information set out above, this section describes how we use personal data when you visit The Entity offices.

The Entity may collect, use, transfer, disclose and otherwise process your personal data in the context of facilitating communication with you (including in case of emergencies), operating and managing The Entity' business operations, complying with legal requirements, monitoring your use of The Entity' systems, undertaking data analytics and recruitment.

We process your personal data when visiting our offices. Your personal data is captured at Entry Gate, through CCTV and access management systems (in case such CCTV and access management systems are active.)

The Entity processes your personal data for the purposes set out in this privacy statement for one or more of the following reasons: (i) because The Entity is required to do so for compliance with a legal obligation to which it is subject, (ii) because such information is necessary for the performance of a contract to which you are a party, (iii) because the processing is necessary for the purposes of the legitimate interests pursued by The Entity or by a third party (as described in the last sentence of this paragraph), or (iv) where necessary in order to protect the vital interests of any person. The Entity has legitimate interests in collecting and processing personal data, for example: (1) to ensure that The Entity' networks and information are secure, (2) to administer and generally conduct business and (3) to prevent fraud.

Access to your personal data within The Entity will be limited to those employees who have a need to know the information for the purposes described in this privacy statement, which may include personnel in Security, HR, IT, Compliance, Legal, Finance, Sales, Marketing and Accounting, Corporate Investigations and Internal Audit. All employees within The Entity will generally have access to your business contact information (e.g. name, position, telephone number and e-mail address).

Use of Personal Data for Marketing Purposes

In addition to the information set out above, the following sections describe how we use personal data for marketing purposes:

Sources of marketing data

The bulk of the personal data we collect and use for marketing purposes relates to customer, customer referrals, individual employees of our clients and other companies with which we have an existing business relationship. We may also obtain contact information from public sources, including content made public at social media websites, to make an initial contact with arelevant individual at a client or other company.

Analyze personal data and data from other sources

We may combine data from publicly available sources, and from our different e- mail, website, and personal interactions with you (this includes information collected across our different websites such as our careers and corporate sites and information collected when you sign-up or log on to our sites or connect to our sites using your social media credentials (such as LinkedIn, Facebook). We combine this data to better assess your experience with The Entity and to perform the other activities described throughout our privacy policy.

Share personal data with third parties

In addition to the third parties mentioned in the section above, we may share your personal data with marketing agencies.

Your Rights Regarding Marketing Communications

Your Data and Content Creation Activities

The Entity partners with advertising agencies for content production. We may process your personal data for these TV, film, marketing, advertising or other related content creation, production and distribution activities.

- The personal data that we process for production purposes include images and footage of you and may include your location at the time of recording.
- If you are a member of public, we will diligently attempt to make you aware of our location and recording activities in advance and will give you an opportunity not to enter the location where recording is taking place and participate in them.
- If you are a focus of our recording activities (i.e. a contributor or talent such as an interviewee, extra or actor, as opposed to a member of public) we will also collect and process your name, contact information and any other information provided in any pre-recording questionnaires and/or release forms, such as next of kin details.

9. Indemnification

(i) We believe information gathered should only be used to help us provide you with better services. But due to the existing regulatory environment, we cannot ensure that all of

your private communications and other personal information will never be disclosed in ways not otherwise described in this Privacy Policy. Therefore, although we use industry standard practices to protect your privacy, we do not promise, and you should not expect, that your personal information or private communications will always remain private. Notwithstanding the above we will not disclose any of your personally identifiable information to third parties unless:

(ii) You (customers, vendors, employees, channel partners) hereby agrees and undertakes to keep The Entity and its Directors, employees harmless and fully indemnified, at all times, therefore, against any or all claims, liabilities, damages losses, costs, charges, expenses, proceedings and actions of any nature whatsoever made or instituted against The Entity (Company), its Directors & Employees or otherwise, directly or indirectly, by reasons of breach/loss of your personal data.

10. Policy Review Period

This policy is reviewed annually or as and when it required; however, control mechanisms exist to ensure compliance activities are built-in organizational policies and practices.

11. Roles and Responsibilities

Below are the specific roles and responsibilities for the defined policy:

- **Head of Internal Audit**
  - Shall ensure compliance by conducting internal audit

- **Head of Information technology**
  - Shall ensure that IT infrastructure and data is secured.
  - Conduct VAPT to bridge any gaps in IT Security
  - Monitor the flow of data/information In-Out of The Entity network and report to CEO.

- **CEO Roles & Responsibilities**
  - CEO must establish and nurture a security-minded culture across the board, including employees, partners and even outside vendors
  - Its CEO's responsibility how to equip the organization to deal with a fast-moving environment, where things happen that you've never seen before
  - CEO must ensure their organizations provide adequate funding to manage all those risks.
- **Employees**
  - Shall not share the data/documents of customers/ vendors with Third Party
  - Shall not copy the data on to their personal emails/mobiles/ laptops/tablets

12. Risk for Non-Compliance

Risks arising due to non-compliance with this policy include, but not limited to:

- Loss of Personal Data of customers, employee, vendors and other Partners
- Unauthorized Sharing of Personal Data
- Loss of Reputation of the Organization

Breaching this policy may result in disciplinary action wherein serious breaches may result in suspension or termination of employment or association.

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

1. **Overview** 3
2. **Purpose** 3
3. **Scope** 3
4. **Policy** 3
5. **Monitoring & Control** 4
6. **Policy Review Period** 5
7. **Roles and Responsibilities** 5
8. **Risk for Non-Compliance** 6

1. Overview

Business users expect smooth business operations without any disturbance. However, in reality it is a challenge to achieve with the available complex infrastructure components and applications. Proactive approach to incident management eliminates major incident occurrence.

2. Purpose

The objective of this policy is to make the organization resilient to any accidental or deliberate security incidents to Information Assets and the supporting infrastructure.

3. Scope

The scope of this policy includes all (but not limited to) Organization personnel and service/support contractors who have access to Organization information and supporting.

4. Policy

4.1 General information

The goal of Helpdesk Support Portal Management is to restore service operations as quickly as possible and minimize the adverse impact of a service outage or degradation on the organization. The activities associated with Helpdesk Support Portal Management primarily deal with recording the details of the incident, classifying the incident, investigating the incident, and ultimately resolving the incident.

4.2 Incident Reporting Procedure

a) Users need to log incident request by sending mail or manually adding incident request on Helpdesk Support Portal.

4.3 Incident Response Procedure

4.3.1 After the incident is reported, Location IT In-charge, shall immediately analyze the incident and categorize whether it is minor or major.

4.3.2 Manager IT shall try to find the damage caused by the incident to The Entity information processing facilities. However, if the severity of the incident is high and the resolution process is not within the purview of IT In-charge, it shall be escalated to Head IT/HOD.

4.3.3 The System Admin/ Incident response team should first apply short-term solution to contain the damage and minimize the risk, which is critical to an incident.

4.3.4 Identifying the type and severity of the compromise is essential to see what kind of resources is required to be allocated. It needs to be labeled based on the severity levellike High, medium and low Priority.

4.3.5 The "exact" nature of the incident needs to be identified for an effective counter measure procedure.

4.3.6 Determine the incident point of origin where exactly it is coming from. (For e.g. Single point or Multi point)

4.3.7 Also, identify the systems that have been compromised.

4.3.8 Identify if The Entity has to move the business functions to its Disaster recovery site. If so initiate the process.

4.3.9 Identify the evidences of the incidence and collect them all. It is essential to protect the collected evidence.

4.3.10 Where action against a person or organization involves the law, either civil orcriminal, the evidence collection and presentation will conform to applicable laws. This will include compliance with any published standard or code of practice for the production of admissible evidence.

4.3.11 All investigations of alleged criminal or abusive conduct will be treated as restricted information to preserve the reputation of the suspected party until charges are formalized or disciplinary action taken.

4.3.12 All internal investigations of information security incidents, violations, and problems will be conducted by staff authorized.

4.4 Recovery

In case of security incident like theft, start the procurement of the new device. If case of security incidents involving hacking or virus or other system related incidents bring back the systems to original state. The systems need to be brought back online in the minimum possible time. The following steps should be carefully carried out for an effective resumption of the work and to prevent any reoccurrence.

4.4.1 **Eradication –** Remnants of the incident (attacker toolkits, Trojan horse programs, viruses, etc.) must be removed from the system(s) affected by the incident.

4.4.2 **Operations Restoration –** Systems must be rebuilt, recovered, or replaced.

4.4.3 **Mitigate Reoccurrence Risk** - System vulnerabilities and inadequate controls exploited by the attacker must be addressed.

5. Monitoring & Control

5.1 It is the responsibility of the Head IT to monitor and review that internal IT team/Outsource Service Provider is adhering to the defined Policy Norms.

5.2 In case it is found by Head IT or by internal audit team that the employee is not adhering to the terms defined under the policy, the same shall be highlighted to the Director for required action.

6. Policy Review Period

6.1 The policy will be reviewed after every three years or if there is any major change in IT infrastructure to incorporate changes if any.

6.2 Head IT will be responsible for reviewing the policy and communicating the changes made therein.

7. Roles and Responsibilities

Below are the specific roles and responsibilities for the defined policy:

User

- Shall formally report the incident
- Shall fill request in Helpdesk support portal tool with complete details and impact assessment.

Change Manager, IT Head

- Shall determine the impact of incident.
- Basis the severity of impact IT Head will notify Director/MD, Employees and any third party to be impacted by the implementation.
- shall suggest and approve the corrective action to control the impact and approve.

Incident Controller (IT Head/Local IT In Charge)

- Shall Implement strategies as suggested by IT Team.
- Shall notify any parties to be impacted by the implementation.
- Shall confirm once the implementation sequence is completed.
- Shall communicate the result of the implementation to the relevant parties.

8. Risk for Non-Compliance

Risks arising due to non-compliance with this policy include, but not limited to:

- Data/Configuration integrity loss,
- System crash and avoidable interruptions,
- Security failures
- Loss of unavailability of important data

Compliance with this policy initiates the following key controls:

- Incidents are reported and contained.
- Changes are implemented as per priority and in a controlled manner.
- All the incidents are adequately documented for audit trail and proactive management.

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

1. Introduction 3

2. Scope 4

3. Policy Statement 4

4. ISMS Policy 4

4.1 Objective 4

4.2 Purpose 5

4.3 Policy Disclaimer 6

5. Information Security Policy 7

6. Information Security Awareness 7

7. Compliance Requirements 8

8. Roles and Responsibilities 8

9. Risk for Non-Compliance 9

10. References 9

1. Introduction

Technology is an enabler of business processes at The Entity With forever increasing usage of technology, to manage data, comes also the need to ensure that the data is protected from misuse, theft, etc. Information security has, therefore, assumed great importance for the success of an organization, as the intentional or unintentional misuse of information, information assets, and information processing facility may result into financial loss, business discontinuity, loss of goodwill, dissatisfaction of internal stakeholders, lawsuits and non- compliance with the regulatory provisions etc. Therefore, constant vigilance along with anextensive and properly implemented Information Security Management System (hereinafter referred in the document as ISMS) framework is deemed mandatory requirement for the organization's effective service delivery and continued contribution to economic growth.

This security policy deals with the following domains of security:

- People;
- Process; and
- Technology.

There are three main sources from which security requirements are derived:

- One source is derived from assessing risks to our organization, considering the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated,and potential impact is estimated.
- Another source is the legal, statutory, regulatory, and contractual requirements that our organization, contractors, and service providers have to satisfy, and also socio-cultural environment.
- A further source is the particular set of principles, objectives and business requirements for information processing that our organization has developed to support its operations.

ISMS policy is to implement the best practices to protect the **confidentiality, integrity, availability** of information assets.

2. Scope

This policy applies to all The Entity employees. It is the responsibility of all operating units to ensure that these policies are clearly communicated, understood and followed.

This polices also apply to contractors, and vendors/suppliers providing service to The Entity that bring them into contact with their Information assets in any form. The given entities employee who contracts for these services is responsible to provide the contractor/vendor/supplier with a copy of these policies before any access is given.

3. Policy Statement

This policy applies to all The Entity employees. It is the responsibility of all operating units to ensure that these policies are clearly communicated, understood and followed.
The Entity' information systems, and the information held by these systems, are fundamental to their operations and future success. The Entity aims at providing a secure environment to ensure confidentiality, availability and integrity of information and it's processing pertaining to our clients and ourselves.
All employees and associates of The Entity and related operations are responsible for promoting and exercising good security practices as stipulated in this information security policy so that information assets are properly protected, and business is securely done. Responsibility for security rests with all of us. We at The Entity are committed to provide better IT Services to our clients through:

- Adherence to laid down security policies and guidelines
- Ensuring information security
- Complying with laws & regulations
- Continuous enhancement in Information Security Posture
- Availability of services under stated contingencies
- Periodic Security awareness

4. ISMS Policy

4.1 Objective

Information is an important business asset of significant value to The Entity and is protected from threats that could potentially disrupt business continuity. This policy has been written to

provide a mechanism to establish procedures to protect against security threats and minimize the impact of security incidents.

The purpose of this policy is to protect the company's information assets from all threats, whether internal or external, deliberate or accidental.

The policy scope covers physical security and encompasses all forms of Information Security such as data stored on computers, transmitted across networks, printed or written on paper, stored external devices and CD's or spoken in conversation or over the telephone or any other; which may endanger the information due to unauthorized disclosure.

All employees of The Entity are responsible for implementing the Policy within their business areas. It is the responsibility of each employee to adhere to the policy. Disciplinary process will be applicable in those instances where any employee fails to abide by this security policy.

Information Security Policy of The Entity is intended to achieve, but not limited to the following:

- Information shall be protected against unauthorized access;
- Confidentiality of Information is assured at all times;
- Integrity of information is maintained;
- Availability of right type of information at the right place is maintained;
- Regulatory and legal requirements regarding intellectual property rights, data protection and privacy of personal information are met;
- Risk treatment plan is established, maintained and tested and
- All employees are given adequate training/awareness on Information Security.

All breaches of information security actual or suspected are reported and investigated at appropriate level to ensure understanding of the root cause, prepare knowledge repository to eliminate/minimize future occurrence and to take corrective/ preventive measures.

Any action that may expose the Company to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to any including termination of employment and / or criminal prosecution.

4.2 Purpose

All employees at The Entity share the Information Technology infrastructure. These facilities are provided to employees for the purpose of disbursing The Entity' business.

The Entity does permit a limited amount of personal use of these facilities, including computers, printers, email and Internet access. However, these facilities must be used responsibly by everyone, since misuse by even a few individuals has the potential to negatively impact on

productivity, result in disruption of company business and interfere with the work or rights of others. Therefore, all employees are expected to exercise diligence and have ethical behaviour when using the company's information and information processing facilities.

Any action that may expose the Company to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to any including termination of employment and / or criminal prosecution.

4.3 Policy Disclaimer

The use of the The Entity information and information processing facilities in connection with company business and limited personal use is a privilege but not a right, extended to various Company employees. Users of The Entity computing facilities are required to comply with all policies referred to in this document.

Users also agree to comply with applicable country and local laws and to refrain from engaging in any activity that would subject the company to any liability. The Entity reserves the right to amend these policies and practices at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with applicable laws.

To protect the integrity of The Entity information and information processing facilities and its users against unauthorized or improper use of those facilities, and to investigate possible use of those facilities in violation of The Entity policies, The Entity reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which is used in violation of The Entity rules or policies. The Entity also reserves the right periodically to examine any system and other usage and authorization history as necessary to protect its information and information processing facilities. The Entity disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

5. Information Security Policy

The Entity commits to ensure all data defined as confidential be protected on a need-to- know basis only to identified and authenticated entities, in all of its forms and on all media, during all phases of its life, from generation to destruction, such that it cannot be compromised, released to any other unauthorized entity, or otherwise have its confidentiality or integrity at risk.

Maintain integrity and availability of information by facilitating access; exchange of information within the organization on a need-to-know basis only to identified and authenticated entities; and institutionalization of secure work environment by complying with all contractual, regulatory requirements and protect proprietary information in all forms.

Establish and evaluate systematic risk management strategies, impart training to users (including third parties) to equip them to be aware of security weakness and report security incidents, security weakness and software/hardware malfunctions.

Formulate, implement, test and maintain a practicable business continuity plan to facilitate continual customer satisfaction.

6. Information Security Awareness

- Protecting The Entity Information Assets is a key responsibility for all employees.
- Each employee ensure that he/she must be aware of his/her roles and responsibilities.
- In this endeavor, Information Security team send IS security awareness emails and IS policy to all new joiners on The Entity domain (employees and named contractual ids).
- To ensure each employee (The Entity domain & contractual employee) must be aware of Information Security, all employees will again get notified periodically with awareness emails, documents and IS policy.

7. Compliance Requirements

- It is mandatory for all employees to ensure that they have read and understood the ISMS policy;
- In case of any doubts, they need to contact their respective manager for clarity;
- Non-compliance due to ignorance shall be treated as willful ignorance;
- Non-compliance to ISMS policy may result in disciplinary action; and
- Any non-compliance due to technical or business feasibility, the same is required to be validated by the respective line of business including acceptance of risk.

8. Roles and Responsibilities

- **IT Team:**
  - Shall review this document at least once in a year and/or when there is a significant change in the organization, technology adopted, business objectives, identified threats, external events
  - Policy Ownership,
  - Development and Maintenance Compliance audit & risk reviews
  - Coordinate for security compliance audit, minimum once in a year as per schedule.
  - Shall be responsible for maintaining updated copy of this document and its effective communication.

- **Security Operations:**
  - Procedure Development and Maintenance
  - User Provisioning and De-provisioning
  - Internet Security Configuration, Implementation and Administration, Monitoring

- **Users:**
  - Shall attend security awareness training arranged by The Entity.
  - Shall use Internet service judiciously.
  - Understand that Information Security is everybody's responsibility.
  - Report any security incident to IT team immediately.
  - Discharge his or her responsibility for information security.
  - Responsible for taking backups as well as for restoration of files residing on their desktop/Laptops.

9. Risk for Non-Compliance

Risks arising due to non-compliance with this Policy include, but not limited to:

- Unauthorized Access
- Malicious Code or virus propagation
- Information leakage, violation of IPR
- Misuse of the internet facility given to the employees, third parties of The Entity
- Threat to Image & reputation of The Entity
- Information disclosure,
- Violation of laws and regulation,
- Unavailability of service,
- Insecure IT operation,
- Inadequate security posture

10. References

- **Information Security standard ISO27001:**
  - Control Objective A.5.1 – Information Security Policy
  - Control Objective A.12.1 – Security requirements of information systems.
  - Control Objective A.12.4 – Security of system files.
  - Control Objective A.13 – Information security incident management.

- Control A.15.1.1 from Annexure A – Identification of applicable legislation
- Control A.15.1.2 from Annexure A – Intellectual Property Rights (IPR)
- Control A.15.1.4 from Annexure A – Data protection and privacy of personal information

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

1. **Objective** 3
2. **Scope** 3
3. **Applicability** 3
4. **Policy Statement** 3
5. **Detailed Policy** 3
6. **Procedures** 5
7. **Inappropriate Use of Internet** 6
8. **Roles and Responsibilities** 7
9. **Risk for Non-Compliance** 7
10. **Policy Review** 7

1. Objective

The Entity is aware of the IT Security exposures that arise out of Internet access through its network and local systems. Accordingly, it has deployed various controls that eliminates or reduces the risks andabuse arising out of Internet usage.

2. Scope

The policy is applicable to all the employees, consultant, contractor and external agencies having access to the Internet from within The Entity' internal network or accessing the internet through company provided data card or using external agencies network.

3. Applicability

This policy is applicable to all users who access The Entity' Internet services from/within The Entity' network.

4. Policy Statement

Internet access shall be provided to users after authorization. Users are prohibited from surfing, transmitting or downloading material that is obscene, pornographic, threatening or sexually harassing.

Users using internet shall be made aware of their responsibilities to use it for valid business reason and not as a mechanism to harass bully or produce defamatory remarks concerning other individuals or companies. All access is to be made to and from internet shall be controlled, logged and monitored.

5. Detailed Policy

- Internet access shall be provided to the employees only after authorization by their respective department heads, with appropriate justification.
- Any special website Access requirements shall be provided to the user after getting approval from authorized individuals.
- Users with Internet access shall ensure that they use the Internet connectivity and the IT resources for Internet connectivity for official and business purpose only.
- Employees of The Entity with Internet access shall not participate in Internet discussion groups, chat rooms, or other public electronic forums.
- Users will not be allowed to download any software/data from the Internet (Such restrictions will be enforced by various tools and may be changed /upgraded time to time). In case of user is mobile and using the company laptop, user has to ensure the appropriate access of Internet.

- IT shall be responsible for routinely logging web usage, web sites visited, and files downloaded by the users.
- User shall not reveal or publicize confidential or proprietary information which includes, but is not limited to: financial information, new business and product ideas, marketing strategies and plans, databases and the information contained therein, customer lists, technical product information, computer software source codes, computer/network access codes, and business relationships.
- Use of the Internet by employees of The Entity is encouraged in the execution of day-to-day business in as much as it supports The Entity goals. The Entity' standards of business conduct must be maintained whenever the Internet is used.
- User shall neither visit nor access pornographic, racist and illegal sites, or downloads from the same Internet sites that contain obscene or offensive materials. Access to many (if not all) sites considered to contain "unsuitable" material shall be prevented by using a filtering system. As new sites of this nature come online and come to the attention of The Entity, they shall be blocked as soon as possible.
- User shall not upload, download or otherwise transmit commercial software or any copyrighted materials.
- All browsers used to connect to the Internet shall be updated periodically for the latest patches and vulnerabilities.
- All content downloaded from Internet shall be thoroughly checked to make sure they do not include viruses, Trojan horses, and other malicious code. Every desktop/laptop will have The Entity approved antivirus with the latest virus definitions. Disabling antivirus software shall not be permitted. All desktops/laptops shall be configured to automatically scan any material downloaded from an Internet Web site.
- User shall not be using Internet for accessing sites promoting gambling, personal commercial benefits or money-laundering.
- Sharing of FTP & Internet access login ID and password is prohibited.
- User shall take reasonable care to access sites of hackers as these sites could lead to downloads of hostile codes or opening of a covert channel into The Entity.
- The Entity retains the right, to report any illegal activities to the appropriate authorities.

6. Procedures

General Access of internet

Internet access for all employees shall be provided via Firewall only. No direct internet access to be provided to any employee. Only employees with roaming profile may have other way to access the internet with end point restriction.

Approval by HR/ HOD

Internet access to employees shall be provided with default restricted internet settings.
Unrestricted Internet access to an employee shall be provided only after prior approval of the HOD/Management explaining the reasons and purpose for this access.
The request to get unrestricted internet access shall be raised on The Entity IT Helpdesk portal which shall be approved by concerned department head or management.

Personal use

Use of The Entity IT systems to access the Internet for personal purposes is strictly prohibited.

Prohibition of discussion group

The employees are discouraged to use social media websites like Twitter, Facebook and writing of Blogs while in the office premises. An employee will own the entire responsibility for posting on social media websites. Postings related to The Entity without the written consent from The Entity will be considered as breach of this policy. Disciplinary action will be taken against up to and including termination of employment.

Virus screening

Any information or data downloaded from the Internet should be screened through virus detection software before being used. No Software application should be downloaded and installed on IT equipment's without the approval of IT.

Transmitting confidential information

All information / data / code / soft copy of any Confidential or Restricted information nature should not be transmitted over the Internet without prior approval of the concerned division CEO and reasonable security measures such as encryption or other appropriate method.

Restriction on web sites

The Entity shall install appropriate controls to restrict access to certain type of websites within The Entity's network and maintains log details. Periodic review of these logs shall be done by the network administrator and report abnormalities to the Head IT for further action.

The control shall be defined on the following category.

- Porn
- Nudity
- Adult Contain

- URL Transition Site
- Drugs
- Crime and Suicide
- Gambling
- Violence
- Weapons
- Phishing and Fraud
- Militancy and Extremist

7. Inappropriate use of Internet

Using Internet inappropriately shall be against the company's policy and shall be strictly avoided. Inappropriate use includes but not limited to -

- Conducting illegal activities, including gambling
- Accessing, downloading or forwarding pornographic or illicit material.
- Revealing or publicizing proprietary or confidential information.
- Making or posting indecent remarks.
- Uploading or downloading commercial software in violation of its copyright.
- Downloading any software or electronic files without reasonable virus protection measures in place.
- Intentionally interfering with the normal operation of The Entity Internet gateway/proxy machine.
- Use the company logos or the company materials in any web page or Internet posting unless the company management has approved it, in advance.
- Attempt to inappropriately telnet to or port scan remote systems on the Internet.

8. Roles and Responsibilities

- **IT Team**
  - Policy Ownership,
  - Development and Maintenance Compliance audit & risk reviews.
  - Internet Security Configuration, Implementation and Administration, Monitoring.

- **Users:**
  - Shall attend security awareness training arranged by The Entity or shall read and understand all IT security awareness mail communications or newsletters.
  - Shall use Internet service judiciously.
  - Understand that Information Security is everybody's responsibility.
  - Report any security incident to Security breaches to IT team immediately.

9. Risk for Non-Compliance

Risks arising due to non-compliance with this Policy include, but not limited to:

- Unauthorized Access/Hacking
- Malicious Code or virus propagation
- Information leakage, violation of IPR
- Misuse of the internet facility given to the employees, third parties of The Entity
- Threat to Image & reputation of The Entity

Compliance with this Policy initiates the following key controls:

- Acceptable use of Internet resources
- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10. Policy Review

The policy will be reviewed every year or if there is any major change in IT Infrastructure to incorporate changes if any.

IT Team will be responsible for reviewing the policy and communicating the changes made therein.

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

1. **Overview** **3**
2. **Purpose** **3**
3. **Scope** **3**
4. **Policy Statement** **3**
5. **Policy Norms** **4**
6. **Monitoring and Control** **7**
7. **Policy Review** **7**
8. **Annexure 1** **7**

1. Overview

Assets of a company must be protected to ensure that the company's operation meets expectations, and to ensure that there is no discontinuity in operations. All the assets of the operation must be registered when information security is implemented. These assets can be either intangible assets, or tangible assets such as housing, computer equipment and furniture. Intangible assets include business connections, reputation, procedures, services, knowledge and human resources.

2. Purpose

The primary use of this document is to provide detailed procedures for implementing the Asset Management lifecycle. The document serves:

- As the process document to the Asset Owners for identifying, classifying and maintaining information assets.
- To define the procedures to record the assets into the asset register.

The objective of this policy is to protect the Information Assets depending on the **Confidentiality (C)**, **Integrity (I)** and **Availability (A)** of the information.

3. Scope

The scope of this document is to provide details related to the management and handling of information assets.

4. Policy Statement

All the information assets shall be identified, listed and ownership clearly defined. Asset owner shall record and maintain an inventory of information assets. All The Entity employees shall ensure that information resources are used only for its intended business purpose and that information resources are protected from unauthorized use, appropriation or corruption. Information shall be disclosed only to those people who have a legitimate business need for the information.

For each department, the concerned Department/Function Head shall identify all the important and critical information assets, whether in electronic or paper form. This shall include all the standard documents and reports generated from the business applications being used in that department as well as the important and sensitive documents being prepared by various users in those departments.

Information assets in any form, paper (printed/handwritten), electronic or non -electronic shall be classified according to their level of confidentiality and sensitivity to business by Functional Head or Asset Owner. If not designated, the default classification is "Internal" for paper/electronic information and "Restricted" for storage media such as Hard disk, Tapes, CD-ROM, DVD and USB Drives.

Access to "Confidential" or "Restricted" information asset shall be subjected to formal authorization from asset owner.

5. Policy Norms

5.1 Definitions

- **IT Fixed Asset:** An IT asset is any company owned information, hardware software and service that is used in the course of business activities in The Entity.
- **Asset Owner:** The term 'Owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. Where a department creates an asset to support their business processes, the Department Head is considered as an Asset Owner. The term 'owner' does not mean that the person has any property rights to the asset.
- **Asset Custodian:** An Asset Custodian is the person responsible for day-to-day operations / maintenance of assets.
- **Asset User:** An Asset User is a person with formal authority to use assets. He can create, transmit, store or dispose Information Assets depending on the authorization levels as approved by an Asset Owner. It is responsibility of every user to ensure that assets are adequately protected.
- **Confidentiality:** Confidentiality relates to ensuring that information can only be accessed by those with proper authorization.
- **Integrity:** Integrity relates to safeguarding the accuracy and completeness of information.
- **Availability:** Availability relates to ensuring that authorized users have access to information and associated assets whenever required.

5.2 Characteristics of IT Fixed Asset

5.2.1 Fixed Assets are acquired assets of a long-term nature (more than 1 year) to be used by The Entity.
5.2.2 Value of Device/equipment is more than Rs.1000
5.2.3 Should not be a repair part or supply item which includes tonner, mouse, keyboard, adapter etc.

5.3 Type of Assets

5.3.1 **Tangible**: Is an asset that has a physical form like laptop, desktop, printers, servers etc.
5.3.2 **Non-Tangible**: That is not physical in nature. Corporate intellectual property, including items such as patents, trademarks, copyrights and business processes, software's are intangible assets.

5.4 IT Asset Procurement and Asset Tagging

5.4.1 IT Asset Procurement / Acquisition Guideline

a) Received requisition request from user thru mail or IT Helpdesk Support Portal
b) Requisition sent to users HOD for approval through email.
c) Requisition sent to IT/Purchase for procurement process.
d) Issuing of Purchase Order.
e) After procurement, Asset labeling, pasting of FA sticker to be done under guidance of Account/Finance Team.
f) All the Physical Assets should be tagged with their asset number as soon as they are received and FA number generated by Account/Finance Team.
g) IF FA has been transferred to other location, it should be updated in Finance books Accounts Department after approval from Head IT.
h) In case Assets is Lost, Asset User should conduct a search for the missing asset and lodge a FIR with the nearest police station in consultation with Admin/IT department. Finance Department will remove the asset from Asset Register.
i) Old assets sold require payment receipts/sale bill in support of assets sold out.
j) Assets identified and need to be sell/ scraped/write off tentative sale price to be mentioned against each item by HEAD IT in proper format as described in Annexure 1. After compilation of final sheet, the data to be shared with accounts department for compilation and updating their records.
k) The Assets which are scrapped require a E-waste recycling certificate from the Vendor.

5.5 Records of IT Assets

5.5.1 For IT Department Data and information is important therefore have further classifiedassets as mentioned below:

a) Physical Asset
b) Software
c) Services
d) Information Asset

5.5.2 All identified Physical and Software Assets are recorded in ERP application by Account Department at the time of procurement.

5.5.3 The register is updated as and when a new asset is added to the Asset Register maintained by the Account Department Asset Register is consolidated, updated and maintained by Account/Finance Department.

5.5.4 All IT Assets should contain following information.

a) **C**ompany Name
b) Asset Code
c) Description of Asset (asset type, category, serial no, unique identification)
d) Asset No.

5.5.5 **Allocation of IT Assets:** The allocation of laptops/Desktops will follow the below criteria.

a) In case of laptop asset allocation user need to signoff Laptop issue note provided by IT Team.
b) In case of desktop allocation user need not signoff any issue note based on his request and approval he will get his desktop on his place.

5.6 Maintenance of IT Assets

5.6.1 The IT Asset Register identifies custodian for the IT Assets. The responsibility of the asset lies with the Asset User/ Asset Owner. The maintenance of the asset is done by the Asset Custodian.

5.7 Disposal of IT Assets

5.7.1 Retention time of assets is defined by the IT Team as 5 years or product end of life or commercial maintenance not possible.

5.7.2 Storage media like CD, DVD, USB Drive, Hard Disk and Tape Drive should be formatted and scrapped.

5.7.3 The information and Data Asset which includes hard copies is shredded before disposal so as to avoid any leakage of information outside The Entity.

5.7.4 The asset which contains critical information in case of disposal/scrap/buyback, the IT Department has to take approval from the Management and only after approval respective asset can be scrapped/disposed.

5.8 Review / Audit of IT Assets

5.8.1 The Asset register is updated as and when a new asset is procured or developed by The Entity.

5.8.2 The Asset register is audited at the time of physical audits at various Divisions/ branches of The Entity and audited FA list is submitted to the Account/Finance department for update of Asset Register.

6. Monitoring and Control

It's the responsibility of the Head IT to monitor and review that respective departments are adhering to the defined Policy norms.
In case it is found that the employee is not adhering to the terms defined under the policy the same shall be highlighted to the Management for required action.

7. Policy Review

The policy will be reviewed on yearly basis or if there is any major change in IT infrastructure to incorporate changes if any IT head will be responsible for reviewing the policy and communicating the changes made therein.

8. Annexure 1

Fixed IT Asset Disposal Format

Name of Unit/ Branch	
Fixed Assets No.	
Description of Assets	
Location of Assets to be disposed off	
Date of Purchase	
Purchase Price	
WDV as on 1st April of Current FY	
Recommended Disposal Price	
Signature IT Head	**DIRECTOR / CFO**

Fixed Asset Sales Format

Name of the Unit branch										
Fixed Asset No	**FA name**	**Location**	**Purchase Price**	**WDV as on 1st April FY**	**Recommended Disposal Price**	**GST inclusive or exclusive**	**HSN Code**	**GST Rate**	**Customer/ Vendor Address**	**GST No (vendor / customer)**

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

1. **Overview** 3
2. **Purpose** 3
3. **Scope** 3
4. **Procedure** 4
5. **Roles and Responsibilities** 6
6. **Risk for Non-Compliance** 6
7. **Policy Review** 7

1. Overview

The Information Resources infrastructure at The Entity is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management process is essential.

From time to time each Information resource element requires an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance, or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

2. Purpose

IT Change Management is the process of requesting, developing, approving, and implementing a planned or unplanned change within the IT infrastructure. It begins with the creation of a Change Request within The Entity IT Help Desk System. It ends with the satisfactory implementation of the change and communication of the result of the change to all interested users.

3. Scope

The intended scope of the change management process is to cover changes to The Entity Applications in the production environments.

Primary functional components include the following:

a. *Hardware* – Installation, modification, removal, or relocation of data centre computing equipment.

b. *Database* – Changes to databases or files such as updates, additions, reorganizations, and major maintenance.

c. *Application* – Application changes being promoted to production as well as the integration of new applications and the removal of obsolete elements.

4. Procedure

a) *Formal request for change* – The users can raise a change request through the IT Help Desk Self Service Portal integrated with Manual change request form. The changes to various applications managed in-house will be done by IT Team. And if the application is maintained and hosted by service provider, the service provider will do the changes in co-ordination with subject matter expert (SME) from IT.

b) *Analyse and Justify Change* – The change requestor and the System Administrator/SME will work to develop a specific justification for the change and identify the impact on infrastructure, business operations and budget, identify business as well as technical risks, develop technical requirements, and review specific implementation steps.

c) *Approve and Schedule the Change* – The respective IT System Administrator/SME will assess the urgency and impact of the change on the infrastructure, end user productivity and budget and define the priority (Major or Minor). In the event of a major or significant change the change request must be approved by the requestor Department Head and then by Head IT. Minor changes may not require as such changes shall fall into user error rectification which have no impact on the set processes. The IT SME in consultation with IT Head, will share the time required and expenses (if any) to the requestor and on approval will initiate the change.

d) *Plan and Complete the Change* – For Business Applications Navision all the changes shall be developed in DEV server and then transferred to QAS (test) server for testing to provide assurance that the change will have the desired result. After the completion of the testing phase the changes shall be transferred to Production server.

e) *Post Implementation Review* – A review will be conducted by the Change Management team comprising of requestor and members of its function / department to formally ensure the change has achieved the desired goals. Post implementation actions may include acceptance, modification, or reversal of the change.

f) Change Closure Request – Once the change is accepted by the user, the functional consultant will raise a change control request which will needs to be closed by requester within 5 days, lest the same will gets closed by IT after 5 days.

Tasks that require an operational process but are outside the initial scope of the Change Management process include:

a) Disaster Recovery
b) Urgent Changes

There are two types of urgent changes or emergency and exceptional. These types of changes are the only changes that may deviate from the outlined change process and are described in detail below.

a) *Emergency Changes:* Emergency changes may be necessary to recover from a system failure, hardware problems or application problems. Emergency changes provide the flexibility required for the timely response to immediate problems. These problems include fixes to prevent recurring/imminent system failure, negative impact on business or production problems.
b) *Exceptional Changes:* Extenuating circumstances will occur and changes will need to be made for certain business reasons. It is for this reason this category has been developed. These circumstances must be documented and included as part of the request package. In addition, mutual consent between the Technical Lead and the Change Management team must occur to allow for the possible re- prioritization of the Technical Lead's workload. Sign off at Dept. Head level will be required. Changes of this type are rare and high risk in nature in that they will not be subjected to the same criteria as those outlined above. The timeframe for implementation may need to be shortened and allowances for the appropriate number of announcements might not occur.
c) These changes must be authorized by Head-IT.

5. Roles & Responsibility

Below are the specific roles and responsibilities for the defined policy:

- **Change Requestor**
  - Shall formally request the change.
  - Shall fill change request in IT Helpdesk System with complete change requirement details.

- **Change Manager, ISMS Steering Committee**
  - Shall determine the complexity of the proposed change.
  - shall understand impact of change and approve.

- **Change Implementer**
  - Shall Implement Change according to standard build instructions.
  - Shall notify any parties to be impacted by the implementation.
  - Shall confirm once the implementation sequence is completed.
  - Shall communicate the result of the implementation to the relevant parties.

6. Risk for Non-Compliance

Risks arising due to non-compliance with this policy include, but not limited to:

- Unauthorized changes in the system and applications
- Data/Configuration integrity loss
- System crash and avoidable interruptions
- Security failures
- Confusion/delay in system configuration
- Loss of unavailability of important data

Compliance with this policy initiates the following key controls:

- Only authorized changes are implemented.

- Changes are implemented as per priority and in a controlled manner.

- All the changes are scheduled to ensure planned results.
- Emergency changes are attended with top priority and in details.
- Changes with high impacts are tested in advance for satisfaction.
- Changes are reversed if they are not successful.
- Only cost-effective and business required changes are implemented.
- All the major changes are adequately documented for audit trail and post implementation review.

7. Policy Review

The policy will be reviewed every year or if there is any major change in IT Infrastructure to incorporate changes if any.

IT Team will be responsible for reviewing the policy and communicating the changes made therein.

DOCUMENT HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

1. Policy 3
2. Scope 3
3. Purpose 3
4. Procedure 4
5. Importance of Data and Software Removal 4
6 Deleting Data - Technical Aspects 5
7. Policy Review 6

1. Policy

The Entity has defined policy for disposal of IT equipment's (including Data, Hardware and IT accessories) that is surplus / redundant / scrapped / outdated for use is as follows.

1.1. All such equipment's would be transferred to a central location as defined by IT team.

1.2. All such equipment that cannot be put in re use and IT Infra team has declared as scraped and put up a proposal for disposal to management with residual value may be either auctioned to the employees of the company or sold, either as part trade-in against new equipment or to an approved e-waste recycler or donated to charitable organization or community project as per approval of Management.

1.3. All such equipment's approved by management for disposal would be duly notified to Accounts/Finance team for appropriate adjustment in books of accounts and cleared from fixed assets register. Accounts/Finance team would ensure for clearance for all such written off in books and confirm to IT.

1.4. To facilitate adherence to the Pollution control and e-waste management and other laws in this respect, all computer hardware must be disposed of through the IT Department.

2. Scope

2.1 The Disposal Policy applies to all the employees, business partners, third parties, whoever using The Entity IT systems. All the locations including sales offices, marketing team, RO, Division offices, plants, warehouses and corporate are covered under this policy.

2.2 This policy applies to all personal computers / Laptops, other computing devices, network devices and accessory equipment that store / communicate / used to process electronic data, information, software programs and applications.

3. Purpose

3.1 Computer equipment or electronic equipment with printed circuit boards contains heavy metals, environmental toxins, and other hazardous materials. The proper disposal of this equipment is essential to avoid liability and to be an environmentally responsible corporate citizen.

3.2 In addition, computer hard disks may contain personal, confidential, and legally protected information that is still readable even when the files have been erased or the hard drive reformatted. Failure to destroy this information could lead to unauthorized access, identity theft, and liability to the company.

3.3 This policy outlines disposal requirements for protecting these IT assets by either of two methods: (1) destruction of the IT device; or, (2) complete removal of all electronic data from the computer storage device. The company must perform at least one of these actions before disposing of the device.

4. Procedure

To comply with the requirements of the Company's above policy, the following mechanisms have been put in place.

4.1 A department having surplus or redundant IT equipment shall immediately inform this fact to his department head under a copy to IT team.

4.2 All equipment for disposal will be collected at the IT team where it will be reviewed for possible internal redistribution and/or other disposal as per the policy above.

4.3 Hardware that can be used to replace older equipment elsewhere in the company will be refurbished / rebuilt to the standard build and redistributed. Any returned equipment will be processed as required.

4.4 All Data and Software installed on such equipment's is removed with the consent ofconcern user / function and hard disks is portioned and formatted.

4.5 Systems which have been declared for no further use by IT function are cleaned, tested and evaluated for method of disposal. All such systems are proposed for disposal and in an environmentally approved manner at no cost to the Company.

4.6 IT Department disposes these equipment's to e-waste recyclers, who in turn certifies that all the e-waste material has been disposed as per the e-waste disposal laws.

5. Importance of Software and Data Removal

5.1 There are a number of considerations to be made when moving or disposing of computer hardware. PCs may have company's sensitive data on the hard disk, this must be removed and where appropriate backed up and / or transferred to another PC. This is to satisfy the requirements of the Data Protection Act and to protect the company from the results of leakage of sensitive information.

5.2 All PCs and laptops are purchased with an Operating System license. This license is tied to the PC that it was supplied with and therefore cannot be retained for use with another PC. The PC can be disposed of with its original license in place but only where the original licensing documentation is available.

5.3 Software like MSOffice, Adobe etc. is purchased and licensed for use within the company and is therefore not transferable with a PC. All software must be removed from hardware that is being disposed of.

5.4 To ensure that these considerations are taken into account all PCs must be disposed of through the IT Services Department.

6. Deleting Data – Technical Aspects

6.1 Before disposing of any computer system, it is vital to remove all traces of data files, company licensed software and operating systems.

6.2 Merely deleting the visible files is not sufficient to achieve this, since data recovery Software could be used by a new owner to “undelete” such files. The disk-space previously used by deleted files needs to be overwritten with new, meaningless data - either some fixed pattern (e.g. binary zeroes) or random data. Similarly, reformatting the whole hard disk may not in itself prevent the recovery of old data as it is possible for disks to be “unformatted”.

6.3 There are a number of tools like Eraser, DBAN available for fully wiping hard disks that will completely wipe the contents of any specified files, or the whole of the free space on the disk.

6.4 A better approach is to use a Degausser to remove the data completely or format the hard disk, installing a clean copy of the original operating system, and then run a suitable application on the free space. This should leave a machine in a suitable state for disposal.

7. Policy Review

The policy will be reviewed every year or if there is any major change in IT Infrastructure to incorporate changes if any.

IT Team will be responsible for reviewing the policy and communicating the changes made therein.

Policy Name: Logical Access Control Policy	**Current Version**: 2.0

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Contents

Objective 3
Applicability 3
Policy Norms 3
Application Specific access control policies 7
Monitoring & Control 8
Policy Review 8

Objective

Objective of this policy is to cover user access to computer systems at various levels like operating system, database and application.

Applicability

This procedure is applicable to all employees, third parties and consultants accessing Information Systems resources of The Entity.

Policy Norms

Operating System Level Access Controls

a. For each user, access to the system must be protected by a password in line with the password policy of The Entity.
b. The number of unsuccessful login attempts shall be restricted to three.
c. Accounts, which are not used continuously used for over a period of thirty days, shall be disabled. The respective user shall be informed of the disabling.
d. Users shall log off from the workstation if he is to be away for an extended period.
e. Only one operating system may be installed on desktops/laptops, unless otherwise there is a specific need for project or test environment.
f. BIOS password shall be enabled for the computer systems for protecting unauthorized modifications to the hardware configuration.
g. Automatic CD-ROM recognition shall be permanently deactivated under operating systems that are capable of recognizing and reading automatically allowing programs stored on CD-ROMs to be executed directly on the computer.
h. Users shall be granted access to files, data and other resources as per the access rights approved by HOD's.
i. The user-ID and password should be authenticated as a whole. Authentication failure should provide an error message to the user that does not indicate whether the user ID is correct (e.g. "incorrect login" and not "incorrect password").

j. The user shall be prompted by the system for change of the user password after the lapse of specified period (180 days).
k. Users created for audit/maintenance purpose shall be disabled immediately after the work is over.
l. When a user is transferred or terminates employment, his account shall be blocked or deleted.
m. Up-to-date documentation of the system configuration for all critical machines shall be maintained to aid in orderly recovery of the system following an emergency.
n. System administrator(s) and Database administrator(s) shall ensure the uniqueness of user accounts on critical servers and databases respectively.

Guidelines specific to Windows systems

a. Screen lock shall be automatically initiated after 15 minutes of inactivity.
b. It shall be possible to deactivate a screen lock only after successful user authentication, i.e. following entry of a password.

Access Control-Application Level

a. Application shall provide for unique user IDs and passwords for all users.
b. Application shall prompt for change of user password after lapse of specified period.
c. Application shall ensure secrecy and security of the user passwords and the access rights granted to users.
d. The access privileges granted in the application shall be in accordance with the roles/duties assigned.
e. Allocation of the suspended, disabled user ID to new users shall be avoided.
f. Active user IDs of the transferred, retired, suspended or dismissed employees shall not be present in the system.
g. The user ID of staff on long leave, training/ onsite deputation etc. shall be suspended / disabled.
h. Users, created for maintenance purpose, shall be cancelled on completion of the job.
i. Users shall be restricted from viewing/examining the access control privileges granted to other users.

Access Control-Database Level

a. All users connecting to database shall authenticate themselves.

b. An auditing strategy shall be built to highlight security problems. Auditing of actions could include –
   - Unsuccessful attempts to connect to the database
   - Start-up and shutdown of the database;
   - Creating or removal of objects.

User Identification

User Identification code

All users shall be granted access to the computing resources through a unique identification code (user-ID).

User Credentials

User credentials shall consist of a user-ID and password that is unique to an individual. The IT shall be maintaining the records for user credentials.

Creation of User IDs

Creation of new Users

New users at operating systems, applications, and database and network levels shall be created based on formal authorizations by the HR /HOD. The forms shall contain the action taken by IT and remarks thereon.

Use of common user IDs

Common user IDs shall not be used. Common user IDs shall not be issued for multiple users when it is technically feasible to provide individual IDs.

Sharing of user IDs

There shall be only one user ID common across multiple systems and applications for a single user. For example, for a user called 'USER' with user-id as 'USER', this user-id shall be the same across the applications, operating systems network and other systems.

Control of user IDs

Disabling users inactive accounts

User accounts that have been inactive for more than 30 days shall be disabled. Systems Administrator shall re-enable them only on the request of the specific user and where required, with the approval of the respective department head.

Disabling default user IDs

Default user IDs shipped with all software shall be disabled.

Deactivation of user IDs

If the wrong password is entered three times, the user-ID shall be automatically deactivated and only the Administrator shall carry out reactivation, after ascertaining genuine request.

User ID expiration dates for non-employees

For contract employees and consultants, an ID expiration date that coincides with the conclusion of the contracted project shall be created.

System account suspension for failed login attempts

Three successive failures shall result in a user's account being locked; they shall not be able to login until their account is unlocked and the password reset. The user shall contact the IT Dept. for getting the account unlocked. A history of all such failed attempts shall be maintained and reviewed by IT Dept. periodically.

Inactivity time out

The terminals shall be deactivated after ten minutes of inactivity. Additionally, screen saver passwords shall be encouraged.

Notifying IT department of user job/function changes

The immediate supervisor of the user shall notify IT of changes in the user's job function in order to ensure that access privileges are appropriately maintained.

User Transfer or Termination Controls

Notification to IT upon user termination/ transfer

The HR shall immediately notify the Systems Administrator upon the resignation, termination or transfer of employees. The No Due Form, requiring clearance from all the departments when an employee is transferred or retires/resigns his job, shall also include clearance from the IT Department.

Revocation of user credentials

The Systems Administrator shall revoke all the user-ids upon termination or resignation of employee and revoke or modify access upon transfer of responsibilities.

Supervisor coordination with Systems Administrator

For situations where users with access to highly sensitive information are terminated, the employee's supervisor (or Head of the Department) is responsible for directly coordinating with theSystems Administrator to remove the user's access rights.

User clearance requirements

All PCs, keys, ID cards, software, data, documentation, manuals etc. of terminated personnel shall be returned to the employee's direct supervisor or the Administration Department.

Application Specific access control policies

Following procedures shall be adhered to while granting access rights to application users:

- For all application respective application owner shall control the creation of super user for the application.
- The users of The Entity shall not be granted any rights to control the operating system privileges and tools.
- Respective application owner shall only create the levels/ categories of the users.
- Access to database tables, parameters and commands shall be restricted to Systems Administrator/Database Administrator.

Access rights granted to Vendors

- Access given to Vendors for The Entity. information resources shall be restricted and governed by the same principle of 'least privilege' and 'need to know" basis. The Entity employee coordinating with the vendor is responsible for justifying and authorizing the access rights granted.
- Vendors shall be restricted to use The Entity information resources from within The Entity network. In other words, remote connectivity from their office to The Entity network shall not be allowed.

Monitoring & Control

1. It is the responsibility of the administrator to monitor and review that his team is adhering to the defined policy norms.
2. In case it is found by administrator or by internal audit team that the employee is not adhering to the terms defined under the policy, the same shall be highlighted to the HOD for required action.
3. It is the responsibility of the Data Centre administrator and application owner to review user access bi-annually at all the layers i.e. Application, database, and operating system.
4. There should be provision to log and monitor Super user/ admin user activity at the Application, database, and operating system. It is the Data Centre administrator and application owners of the manager to review activity logs monthly.

Policy Review

The policy will be reviewed on yearly basis or if there is any major change in IT infrastructure to incorporate changes if any.

IT Department and respective application owners will be responsible for reviewing the policy and communicating the changes made therein.

Policy Name: Password Management Policy	**Current Version**: 2.0

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

Abbreviations/ Definitions 3
Objective 3
Scope 3
Policy Statements 3

Abbreviations/ Definitions

AD	Active Directory
IPsec	Internet Protocol Security
OS	Operating System
RADIUS	Remote Authentication Dial-In User Service
SNF	Shiv Nadar Foundation
TACACS	Terminal Access Controller Access Control System
VPN	Virtual Private Network

TACACS: **T**erminal **A**ccess **C**ontroller **A**ccess **C**ontrol **S**ystem is an older authentication protocol common to UNIXnetworks that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

RADIUS: **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

VPN: Virtual Private Network is programming that creates a safe, encrypted connection. Typically, it is used over a less secure **network**, such as the public internet. It uses tunnelling protocols to encrypt data at the sending endand decrypt it at the receiving end.

Objective

The objective of this policy is to secure the company data from unauthorized access.

Scope

This policy applies to The Entity employees and its contractual employees, who use company provided laptop, computer or any other devices or service connected to the company network.

Policy Statements

- **Windows Domain Passwords:**
    - All windows-based end-systems / servers shall comply with the password length, complexity, expiryand associated parameters as defined below;

Password Management	Requirements
Password Construction Requirement (Length & Complexity)	Minimum length should be of Twelve (12) characters in combinationof alpha numeric or special characters. All passwords must be complex and contain at least three characters from the following fourcategories to meet complex password requirements: At least one character in upper case alphabets (A-Z).At least one character in lower case alphabets (a-z). At least one numeric character (0-9). At least one special character [e.g. $,!, #, %, *, &, (,), @] Should not match last 3 password
Password Expiry period	60 days
Reset Account Lockout counter after	After 5 Min.
Password History	Last 3 password history

- Microsoft default settings shall be employed for Windows Kerberos.

- **Compliance:**
  - Passwords shall be mandatory for all user accounts on all networks and/or standalone InformationSystems.
  - It is mandatory to change the password at first login.
  - Any password change shall be permitted only after successful authentication.

- **Lock-out:**
  - Account shall be locked out after 5 continuous bad attempts made by user within 15 minutes
  - Any account which has been locked out due to wrong attempts shall be reset by the respective local ITteam (User can also reset the password through Self-Service Portal).
  - Account resetting shall be in accordance to the Password management process.

- **VPN Passwords**
  - The application integrates with Active Directory and inherits the same Password policy as applied onAD.

- **Network:**
  - All Network Device Access Management happens through TACACS+ / RADIUS authentication serverand at the back-end AD User / ID Password shall be used for access.

- All policies that apply to AD Password Management are inherited for Network Device Access.

- **Remote Access / VPN:**
  - SSL Client based VPN access uses AD Password and inherits AD Password Policies. SSL VPN access shall also use AD Password Authentication and are hence in line with AD Password Policies.

- **Unix / Linux Passwords:**
  - All Unix / Linux based end-systems / servers shall comply, at the minimum, with the password length, complexity, expiry and age as defined in this policy.

- **Database Passwords:**
  - All database schemas shall comply with the minimum password length, complexity, expiry and age asdefined in this policy.

- **Administrator / Root Accounts:**
  - All admin / root accounts shall be more stringent (where-ever the underlying OS permits) and complex passwords.
  - All other password construct criteria shall remain same as highlighted in this document.
  - The root passwords of all Unix / Linux servers shall be shared with personnel only on role / need-basis.
  - The root / admin passwords shall be changed every 60 days or whenever a custodian / owner of rootaccount holder resign from the organization.
  - Use of One-time password or multi-factor authentication shall be ensured for users having super-user / administrator level access to system resources and should be made mandatory where access is from other than corporate network. This is applicable for System Administrators, Database Administrator, Network Administrator, and Firewall Administrator etc.

- **Confidentiality:**
  - Password shall never be displayed in clear text or stored in readable forms.
  - Password shall only be communicated to the intended user and changed after first logon.
  - Generic / Shared / Service-Account ID passwords shall be provided to owners only.
  - Password sharing shall not be allowed.

- **Default Passwords:**
  - All default passwords (software / device / systems) shall be immediately changed upon installation.

- **Password Storage:**
  - System files holding the authentication information or passwords shall be encrypted to protect from unauthorized access.

- **Password Reset:**
    - In the event a staff member, who has privileged access (administrative or special privilege) on Information Systems, has resigned or is terminated, the IT team shall ensure that the passwords to that privileged account are changed immediately after HR confirmation.

- **System Account Passwords:**
    - The password complexity / criteria for system or service accounts shall be the same as listed in the policy for other accounts. A longer, more complex password is highly recommended, if the software / operating system allows the same.

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Contents

Overview 3
Purpose 3
Scope 3
Entry & Exit Criteria 3
Policy 4
Patch Process 5
Policy Review Period 7
Roles and Responsibilities 8
- Patch Requestor 8
- IT Team 8
- Patch Implementer 8

Risk for Non-Compliance 9

Overview

The Information Resources infrastructure at The Entity is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong patch management process is essential.

Managing these patches is a critical part of providing a robust and valuable Information Resources infrastructure.

Purpose

The purpose of the Patch Management Policy is to manage patch in a rational and predictable manner so that IT department can plan patch accordingly. Patch implementations require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

This policy defines the guidelines to keep track of all patches implemented in the network and to keep track of all changes made to these objects.

Scope

This policy applies to all infrastructure servers and network devices that form a part of The Entity's IT landscape. It is imperative that everyone adheres to this policy so that IT Department canefficiently manage IT assets and maintain the integrity of user accounts created in Windows, Linux and Antivirus databases.

Entry & Exit Criteria

Entry Criteria:

- Whenever any Patch update is required on any information system.

Exit Criteria:

- When the change has been done and the systems are running in desired condition by IT team

Policy

The Entity' IT infrastructure including applications must be properly patched with the latest appropriate updates and patches from the OEM's in order to reduce system vulnerability and to enhance application functionality. The purpose of this policy is to establish standard procedures for the identification of vulnerabilities, potential areas of functionality enhancements as well as the safe and timely installation of patches. It's the only way to stay organized and to keep track of which patches have been deployed and why.

The "***Patch Management Process***" shall include the following: -

- Assessment of the potential impact, including security impact of the change(s) on critical systems and network devices;
- Identification of the patch authorizers;
- Formal approval procedure for the proposed patch update;
- Procedure for testing including security-testing of the patch updates;
- Rollback procedure for aborting and recovering from failed patch updates.
- All approved changes on the critical systems shall be tested prior to implementing them on the production systems.

Below is the list of documents to be reviewed before any change:

- Plan of action
- Roll back plan
- Test cases
- UAT sign-off
- VA/PT report and sign-off
- Release document (In case, of a release)

a. all patches must be downloaded from the relevant system vendor or trusted sources. Each patch's source must be authenticated, and the integrity of the patch verified. All patches must be submitted to an anti-virus scan upon download.

b. New servers and desktops must be fully patched before coming online in order to limit the introduction of risk.
c. New software's must be fully patched when installed on The Entity resources to limit the introduction of risk.

All patches must be tested prior to full implementation since patches may have unforeseen side effects.

Patch Process

Patch Sources

This policy applies to all software, servers, desktops, laptop computers operated by The Entity.

The following list provide the scope of IT infrastructure where patch management policy is applicable within Company along with formal patch sources.

Products/Configurations	OEM	Patch Sources
Server OS	Microsoft	OEM
Server OS	Linux	OEM
Laptop / Desktop OS	Microsoft	OEM
Database - MySQL	Oracle	OEM
Database - MS SQL	Microsoft	OEM
Database - Oracle	Oracle	OEM
Office Applications	Microsoft	OEM
Antivirus	Symantec	OEM
Firewall	Fortinet	OEM
Network Switches	Cisco	OEM

Patching Priorities

The following Patch Priority Matrix represents all systems and applications at The Entity, their relative priority for patching, and timeframes within which patches must be applied.

The Entity categorizes patches as High Priority and Low Priority:

High Priority Patches: Server Operating system, ERP, Databases such patches shall be applied in the development server and post testing are migrated to Non-Production (Test) and then to Production environment.

Low Priority Patches: Desktop, laptop-based Operating system & standard application like MSOffice, Antivirus, Acrobat Reader etc. the patches are applied as per and when the same are released by theOEM and its suitability to the users. For all other location's patches are pushed directly thru own resources.

All computers attached to The Entity network must have standard anti-virus system installed. The software must be active, automated to perform virus checks at regular intervals daily with a full disk scan once every week and have its virus definitions files kept up- to date. End users are prohibited de-activate, disable or uninstall antivirus software.

Such patches are reviewed by IT and applied every monthly.

Asset/Configuration	**Patch Testing Period**	**Patch Deployment Method**	**Post Deployment Testing**	**Patch Rollback**
Windows /Linux Operating System Servers	Critical - 30 Days, Non critical – 90 Days	Patches are tested; UAT is performed on a separate test environment before being deployed.	IT Admin team interacts with relevant [*user groups*] to check and verify successful deployments.	In case a faulty patch is identified IT team restores to the previous version – which is always part of the roll out procedure.
Windows /Linux Operating System Desktops / Laptop	Critical - 30 Days, Non critical – 90 Days	Patches are tested on a test laptop and desktop before being deployed on other machines. (Testing not mandatory)	The patches are deployed from OEM resources.	In case a faulty patch is identified IT team restores to the previous version – which is always part of the roll out procedure.
Office Applications	Critical - 30 Days, Non critical – 90 Days	Patches are tested on a test laptop and desktop before being deployed on other machines. (Testing not mandatory)	The patches are deployed from OEM resources.	
Navision	Critical - 30 Days, Non critical – 90 Days	Patches are tested; UAT is performed on a separate test environment	Interacts with Navision Consultant team to checks and verify the	In case a faulty patch is identified Navision team restores to the previous version – which is always part of

		before being deployed.	deployed patches.	the roll out procedure.
Database	Critical - 30 days. Non critical – 90 Days	Patches are tested; UAT is performed on a separate test environment before being deployed.	IT Admin team interacts with relevant [*user groups*] to check and verify successful deployments.	In case a faulty patch is identified DBA admin team restores to the previous version – which is always part of the roll out procedure.
Other hardware	Critical - 30 days. Non critical – 90 Days	Patched confirm from OEM before upgrading and install on systems.	IT Admin team interacts with relevant [*user groups*] to check and verify successful deployments.	In case a faulty patch is identified IT team restores to the previous version – which is always part of the roll out procedure.

In case exception to the above policy arises due to compatibility of any legacy applications or interoperability with the application stack, approval from relevant application owners will be taken.

Testing procedure

a. For server OS and various applications/programs, the patches shall be deployed on UAT, tested and then transferred to Production.

b. A back out plan that allows safe restoration of systems to their pre-patch state must be devised prior to any patch rollout in the event that the patch has unforeseen effects.

c. All configuration and inventory documentation must be immediately updated in order to reflect applied patches.

d. The system administrator shall conduct audits by himself and report to Head-IT to ensure that patches have been applied as required and are functioning as expected.

e. The system administrator shall conduct periodic patch updates to ensure that patches are applied within the stipulated timeline (30 days for critical and 90 days for non-critical)

Policy Review Period

The policy is reviewed and updated whenever there is a new infrastructure deployment where patch deployment is applicable. Otherwise as a matter of compliance annual review is to be conducted by IT Teams.

Roles and Responsibilities

Below are the specific roles and responsibilities for the defined policy:

- **Patch Requestor**
  - Shall formally request for Patch Update

- **IT TEAM**
  - Shall determine the complexity of the proposed Patch.
  - shall understand impact of Patch and approve.

- **Patch Implementer**
  - Shall Implement Patch according to standard build instructions.
  - Shall notify any parties to be impacted by the implementation.
  - Shall confirm once the implementation sequence is completed.
  - Shall communicate the result of the implementation to the relevant parties.

Risk for Non-Compliance

Risks arising due to non-compliance with this policy include, but not limited to:

- System vulnerability,
- Unauthorized patch updates,
- Data/Configuration integrity loss,
- System crash and avoidable interruptions,
- Security failures,
- Confusion/delay in system configuration,
- Loss of unavailability of important data

Compliance with this policy initiates the following key controls:

- Only authorized patch updates are implemented.
- Patches are implemented as per priority and in a controlled manner.
- All the patches are scheduled to ensure planned results.
- Patch's with high impacts are tested in advance for satisfaction.
- Patch updates are reversed if they are not successful.
- Only OEM approved patches are implemented.
- All the patch updates are adequately documented for audit trail and post implementation review.

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Contents

Objective 3
Applicability 3
Policy 3
Monitoring & Control 5
Policy Review 6

Objective

To prevent unauthorized access, damage and interference to business premises & information. To prevent loss, damage or compromise of assets and interruption to business activities. To prevent compromise or theft of information and information processing facilities.

Applicability

This policy applies to the physical premises at Corporate office, Branch Offices of The Entity.

Policy

Physical Access

- Security Personnel shall guard the building entry point to The Entity Premises.
- Visitors and Vendors shall make an entry in the Visitor's register. During their presence inside The Entity premises, they shall always be escorted, and their movements monitored.
- Personal laptops are not allowed for use in The Entity data center premises.
- CCTV Cameras have been deployed in critical areas and all the movements shall be monitored and recorded.
- Critical areas like Server Room have limited authorized access.
- Card Access will be configured to allowed employees in data center room.
- Vendors entering data center room are escorted by authorized IT team member. The entry of vendor is recorded in the register kept in server room.

Safety Equipment:

Appropriate safety equipment is to be installed, such as heat and smoke detectors, fire alarms, fire extinguishing equipment and fire escapes. Safety equipment is to be checked regularly in accordance with manufacturers' instructions. Employees are to be properly trained in the use of safety equipment. Combustible computer supplies such as stationery, other than immediate operational needs, should not to be stored within server room.

Ensuring Suitable Environmental Conditions:

Suitable environment control procedures shall be in place for smooth and reliable working of Information processing facilities. The environmental dangers that threaten the computer premises and the means by

which they may be lessened or eliminated shall be aptly identified and implemented. Countermeasures or contingency procedures are to be defined for environmental hazards such as fire, smoke, water, dust, vibration, electrical supply interference.

Issues to be considered by the Admin for implementing the above procedure:

- Serious fire damage could make it impossible to continue business operations.
- Flooding can cause severe disruption to business in any form.
- Failure of air conditioning equipment can unsettle business operations and potentially result in halting of business output.
- Smoking, eating and drinking is prohibited in computer equipment areas.
- Suitable Insurance Policy coverage for IT equipment's.

Power Supplies:

Equipment shall be protected from power failures and other electrical disturbances. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications. Various options shall be considered to achieve continuity of power supply:

- Un-interruptible power supplies with n+n configuration
- Back-up generator

UPS equipment shall be regularly checked to ensure its adequate capacity and shall be tested with the manufacturer's recommendations. UPS shall support orderly close down or continuous running is recommended for equipment supporting critical business operations. There shall be SLA that ensures the maximum uptime with the supplier/contractor for maintaining of UPS.

Cabling security:

Administration Division shall develop and implement the procedure for protection of power and telecommunication cabling. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception and damage. The following is an example of the security standards relating to cabling:
Issues to be considered for implementing the above procedure:

- Power and telecommunications lines to the information processing facilities shall be underground, where possible or subject to adequate alternate protection.
- Network cabling shall be protected from unauthorized interception or damage.
- Power cables shall be segregated from communication cables to prevent interference.
- For sensitive or critical systems further controls to consider:
- Installation of armored conduit and locked rooms or boxes at inspection and termination points.
- Use of alternate routings or transmission media.

Network cabling is to be protected from unauthorized interception and communications loss or damage by:

- Use of conduits;
- Avoiding routes through public areas;
- Installation of locked rooms or boxes at inspection and termination points
- Implementation of secondary transmission media and/or routings.

Equipment maintenance & Security:

IT Administrator is responsible for developing the procedure for equipment maintenance. IT Equipment's shall be correctly maintained to ensure its continued availability and integrity.

Issues to be considered for implementing the above procedure:

- Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications.
- Manufacturers' instructions regarding the protection of equipment, such as its protection against exposure to strong electromagnetic fields, is to be observed at all times.
- Only authorized maintenance personnel shall carry out repairs and service equipment.
- Records shall be kept of all suspected or actual faults and all preventive and corrective maintenance.
- Appropriate controls shall be taken when sending equipment off premises for maintenance. All requirements imposed by insurance policies shall be complied with.

IT equipment should be sited or protected to reduce the risks from environmental hazards and to minimize the opportunity for unauthorized access.
Critical equipment should be protected from power failures or other electrical anomalies.

Environmental Conditioning:

Appropriate air conditioners are to be installed to maintain temperature and humidity for the Server Room.

- Temperature for the server room be continuously monitored and temperature should be maintained within the set limits.
- Humidity in the server room should be maintained within set parameters.
- Regular checks are to be recorded and routine preventive maintenance schedule has to be executed.
- Supply air should be dust free and filtered before reaching the server room.

Monitoring & Control

It is the responsibility of the IT team to monitor and review that all employees are adhering to the defined Policy Norms.

In case it is found by IT team or by internal audit team that the employee is not adhering to the terms defined under the policy, the same shall be highlighted to the HOD for required action.

Policy Review

The policy will be reviewed after every year or if there is any major change in IT infrastructureto incorporate changes if any.

IT Manager & Admin Manager will be responsible for reviewing the policy and communicating the changes made therein.

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Contents

Purpose....3
Scope....3
Policy....3
General....3
Requirements....4
Enforcement....5
Policy Review....5

Purpose

The purpose of this policy is to define standards for connecting to The Entity's network from any host. These standards are designed to minimize the potential exposure to The Entity from damages which may result from unauthorized use of The Entity resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical The Entity internal systems, etc.

Scope

This policy applies to all The Entity employees, contractors, vendors and agents with an The Entity-owned or personally owned computer or workstation used to connect to the The Entity network. This policy applies to remote access connections used to do work on behalf of The Entity, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, MPLS, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

Policy

General

1. It is the responsibility of The Entity employees, contractors, vendors and agents with remote access privileges to The Entity corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to The Entity.
2. General access to the Internet for recreational use by immediate household members through The Entity Network on personal computers is permitted to limited use. The Entity employee is responsible to ensure the family member does not violate any The Entity policies, does not perform illegal activities, and does not use the access for outside business interests. The Entity employee bears responsibility for the consequences should the accessbe misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of The Entity network:

    a. *Networking & telecommunication Policy*
    b. *Acceptable Use Policy*

4. For additional information regarding The Entity remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., discuss with IT Head.

Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password. For information on creating a strong password see the Password Policy.
2. The Entity employees, vendors and contractors can access The Entity applications and network thru VPN solution which has 2 factor authentication the OTP verification is sent on email or mobile configured on VPN.
3. At no time should any The Entity employee provide their login or email password to anyone, not even family members.
4. The Entity employees, vendors and contractors with remote access privileges must ensure that their The Entity-owned or personal computer or workstation, which is remotely connected to The Entity corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
5. The Entity employees and contractors with remote access privileges to The Entity corporate network must not use non-The Entity email accounts (i.e., Gmail, Hotmail, Yahoo, AOL), or other external resources to conduct The Entity business, thereby ensuring that official business is never confused with personal business.
6. Routers for dedicated ISP lines configured for access to The Entity network must meet minimum authentication requirements.
7. Non-standard hardware configurations must be approved by IT Team. IT Team must approve security configurations for access to hardware.
8. All hosts that are connected to The Entity internal networks via remote access technologies must use the most up to date anti-virus software.
9. Organizations or individuals who wish to implement non-standard Remote Access solutions to The Entity production network must obtain prior approval from IT Team.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Policy Review

The policy will be reviewed after every year or if there is any major change in ITinfrastructure to incorporate changes if any.

IT Manager will be responsible for reviewing the policy and communicating the changes made therein.

Policy Name: Software Asset Management Policy	**Current Version**: 2.0

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	07-07-2021
1.0	No change	20-03-2023
2.0	Revised version	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

Introduction 3
Policy Objective 3
Software Use 3
Software Asset Management Lifecycle (Process Flow) Identification 3
Shareware, Freeware and Trial Software 5
License Management 5
Roles & Responsibilities 5
Review 6

Introduction

Software Asset Management (SAM) is set of procedures and processes necessary for the effective management, control and protection of software assets within the organization, throughout all stages of their lifecycle.

This policy document sets forth the management processes, tools and strategies for effective management of software assets.

Policy Objective

It is the policy of The Entity (company) to comply with all software copyrights and license agreements terms/conditions that apply to company owned software installed on various IT machines.

These guidelines apply to all users of the IT Facilities. All users should be aware of these guidelines, their responsibilities and legal obligations. All users are required to comply with these guidelines and associated IT policies.

Software Use

Licensed copies of software and applications shall be deployed on the computer systems within The Entity and in accordance to the license agreements, appropriate backups shall be made. No additional or other copies shall be made without the permission of the software owner or publisher.

Any unauthorized usage or deployment of a copyrighted software or piracy shall be treated as unlawful and shall be non-compliance towards the Acceptable Use Policy. Employees found or reported towards the non-compliance of the policy shall be liable to undergo appropriate disciplinary action.

Assistance with software copyright or license arrangements can be obtained from the IT Helpdesk and IT support teams.

Software Asset Management Lifecycle (Process Flow) Identification:

Selection of software is a collaborative process between IT department and other departments. It is the responsibility of IT department head to identify the software requirement of The Entity by involving all the stake holders. A recommended list of centrally purchased software will be presented in the annual meeting of The Entity.

Acquisition / New software Check-in:

1. To purchase software, users should obtain approval from their Head of Department and IT head. Necessary business justification, period of use, type of license and quantity of licenses should be provided along with the request.

2. Once the software has been received and installed, the IT Support person under the supervision of IT head is responsible for ensuring that the original media, license documents, manuals and other associated material are securely and appropriately stored as The Entity managed assets.
3. The list of approved software will be updated to reflect the new acquisition.

Software Distribution:
Software licenses will be distributed by the central IT team to different units and locations based on the following process:

1. User should check the approved software list for the availability of the desired software. In case the desired software is not part of the approved list, user needs to follow "Acquisition / New Software Check-in" process.
2. User should send in the request with necessary approvals from department heads.
3. IT team will check the availability of license and proceed with installation after ensuring availability of all necessary approvals and sufficient number of licenses count.
4. Software Inventory register will be updated with the updated count of deployed and available licenses.

Software Inventory:

1. The IT team shall maintain a register of all purchased software installed on all applicable IT assets.
2. The software register should include the following information (as a minimum):
    a. Name of the software.
    b. Software vendor's name.
    c. Date software was ordered.
    d. Serial number/asset no. of the hardware on which each copy of the software is installed.
    e. Name of the authorized user(s).
    f. A list of the associated documents/manuals and their location. In particular, this item should reference the location of the original software media and the license agreement document.
    g. Serial number (software key) of the software (where applicable).
    h. software agreement expiry date (if applicable)
    i. software renewal date (if applicable)
    j. Purchase Order Number

Software Removal

1. The IT team or their nominated representatives are responsible for ensuring that licensed software is removed from IT facilities when the software license expires. They are also responsible for ensuring that the original media, license documents, manuals and other associated material are disposed of in accordance with the relevant license terms and conditions.
2. Software should also be removed if it is no longer required, if the license has expired, or if the person who owns the machine terminates employment with the organization.

Shareware, Freeware and Trial Software

1. Shareware, freeware and trial software is copyrighted software that is distributed freely.
2. All installations of shareware, freeware or trial software should be reported to either IT team or IT Head or their nominated representatives, and records are to be kept in the software asset database.
3. It is the responsibility of the end user to ensure any freeware, shareware or trial software installed on any device they use which connects to the organization's computer network is installed and maintained in accordance with the software licensing agreement.

License Management

Reconciliation

Software reconciliation shall be carried out on a yearly basis at unit/ location level.

Periodic Scans/Audit Compliance

A periodic compliance and spot checks shall be carried out organization wide; to ensure the software usage is in-compliance, all software installed and being used is legitimate.

Roles and Responsibilities

The following responsibilities apply:

1. The IT team is responsible for ensuring that the organization uses only appropriately licensed software and that each software item is used in accordance with its prevailing license agreement.
2. The IT team or their nominated representatives are responsible for ensuring that all site licensed software is used and managed in accordance with these guidelines.
3. Each Plant/Unit should nominate a Software Asset Manager who is responsible for ensuring that software installed at the Plant/Unit level is used and managed in accordance with these guidelines and the prevailing software agreement.
4. All users of organization's IT facilities are responsible for ensuring that their use of software is in accordance with these guidelines.

Review

This policy is reviewed annually or as and when it required; however, control mechanisms exist to ensure compliance activities are built-in organizational policies and practices.

DOCUMENT APPROVAL HISTORY

Version Number	Document Revision Description	Approved/ Reviewed by Board on
1.0	Baseline Policy	18-03-2024

Document Control

- The policy shall be reviewed at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes within Vama Sundari Investments (Delhi) (referred to as The Entity).

Table of Contents

Policy Objective....3
Purpose....3
Applicability....4
Scope....4
Roles & Responsibilities....4
IT Continuity Controls....5
Disaster Recovery Planning....5
General Response & Recovery Strategy....6
Testing & Revision....7
Notification and Communication....7
Response to Media....8
Assumptions....8
Review....9
Annexure A:: Key Staff Person List....10
Annexure B:: Key Vendor Contact List....11

Policy Objective

The objective of this document is to provide guidelines for preparing for and responding to unforeseen or unexpected emergencies or other occurrences that pose a potential threat to the availability of The Entity IT systems and operations.

The following policy is applicable to all The Entity employees and relevant third-party personnel. The scope of this policy covers any IT systems or services that are essential to operations.

The major goals of this plan are the following:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To provide for rapid restoration of service.

This policy encompasses any type of disaster that could impact system and service availability. The types of disasters that could occur are varied, and each situation or particular disaster could include different variables and impacts. Disasters could include the following:

- Equipment failure
- Power outages
- Fire
- Flood or water leakage
- Severe weather
- Cyber crisis/ Ransomware attack

Disasters could also include those experienced by vendors or critical infrastructure upon which IT&S relies, such as cloud-based applications hosted by third-parties or an internet service provider.

Purpose

IT Continuity Plan establishes procedures to recover the disrupted information technology system (full/ partial) within the process functions. The following are the purposes have been established for this plan:

- Maximize the effectiveness of operations through the following phases:
  Notification/Activation phase - to detect and assess damage and to activate the plan
  Recovery phase - to restore temporary operations and assess damage to the system
  Reconstitution phase - to restore system processing capabilities to normal operations.
- Identify the activities, resources, and procedures needed to carry out processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated personnel and provide guidance for recovering [system] during prolonged periods of interruption to normal operations.
- Ensure coordination with other staff who shall participate in the IT Continuity Planning strategies.
- Ensure coordination with external points of contact and vendors who shall participate in the IT Continuity Planning strategies.

Applicability

The IT Continuity Plan applies to the functions, operations, and resources necessary to restore and resume The Entity IT operations. This plan applies to the Colocation Datacenter (for Central Applications) as well as local entity specific Data Centers.

Scope

The scope of the procedures documented in this IT Continuity Plan is restricted to IT services provided by The Entity IT department covering Colocation DC as well as Entity specific local DC.

The scope of the procedures covers the following systems:

- Protect employees
- Protect the company's assets
- Minimize the risk of a disaster occurred
- Minimize the impact of a disaster
- Minimize the loss of infrastructure and records
- Ensure adequate back-up systems wherever possible
- Ensure continuity of the business as quickly as possible following a disaster.
- Minimize the loss of revenue and costs.

Roles & Responsibilities

Roles and Responsibilities	
Head IT/ Head Data Centre	Ensures that the IT Continuity Policy is in alignment with the overall organization's mission and strategy and includes involvement from all areas of the organization.
Security Officer	Oversees the "day-to-day" management of the IT Continuity and Cyber Crisis Management Policy and is the *lead* for policy implementation. Performs "day-to-day" activities of the IT Continuity and Cyber Crisis Management Policy including but not limited to: • Participation in the development and update of the IT Continuity Policy (especially as it relates to contact details and associated responsibilities). • Initiating test exercises of the IT Continuity Policy. • To get BAS and VAPT conducted for the IT Infra and associated applications. Completing training on best practices of IT Continuity on a regular basis. Responsible for using individuals' knowledge of their departments to develop and maintain each department's Response and Recovery plan using the tools and templates provided by the Program Coordinator (role identified above)
IT Manager	Responsible for recovery of the IT Systems as per the recovery plan communicated by Head IT/ Security Officer.

IT Continuity Controls

The following sections outline the controls and procedures implemented to mitigate the operational impact of unforeseen disasters or emergencies and facilitate recovery of affected systems and business units.

The Entity have a robust, immutable backup solutions in place. Please refer to *ITPOL002- Backup and Recovery Policy* for the organizational backup policy. This policy provides guidelines to ensure that all sensitive information is being backed up and can be restored in case of any disaster.

Disaster Recovery Planning

The principal objective of the Disaster Recovery Plan is to develop, test, and document a well- structured and easily understood plan, which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency that interrupts information systems and business operations. Additional objectives include the following:

- Ensuring that all employees fully understand their duties in implementing the plan.
- Ensuring that operational policies are adhered to within all planned activities.
- Ensuring that proposed contingency arrangements are cost-effective.
- Establishing disaster recovery capabilities as applicable to key customers, vendors and other parties.

Scope of DR Plans and Criticality Analysis

An integral part of DR planning is determining what DR plans should cover. This includes identifying and prioritizing what IT services and supporting functions need to be the focus of DR plans. This process will be completed by performing a critical analysis of the IT services and supporting functions that are essential to operations.

IT department will maintain a list of critical systems that will be prioritized for restoration during a disaster or emergency. This list should include details such as system name, type, and function, as well as priority or criticality levels, recovery time objective, supporting vendors, and other details to assist recovery personnel.

The list of Critical Systems includes, but is not limited to, the following:

- Core Network Services
- Internet Services
- AD Services
- Central Application (e.g. Finance ERP, Fintech, HR ERP etc.)
- Any other Business critical application for respective entity
- O365(Email, MS teams office products, but mainly email(communications)
- Other Email services (if applicable)

If for some reason, the Network Manager is unable to perform the responsibilities associated with Disaster Recovery, Senior Network Staff will assume responsibility or designate another individual with the requisite technical skills, as is appropriate.

RTO and RPO are two important parameters of a Business Continuity Plan. RTO/RPO serves as essential business metrics for our internal teams to ensure that minimal data loss occurs in case of any disruption and there is optimal data backup available. While RTO/RPO depends on the criticality of data types, we target to maintain recovery time objective (RTO) and recovery point objective (RPO) of 5 days and 24 hours, respectively, unless a lower minimum is provided by any of our partners/regulators in respect of any particular application.

Critical Business Functions	Recovery Priorities – Maximum Acceptable Outage Time
Datacenter (Working Location)	Email – **4 Hours**
	MPLS/Internet – **8 hours** 2 dedicated ILLs with uptime of 99.5%, so rare chance of downtime of both the ILLs at the same time.
Central Colocation Data Center	Fin. ERP, HR ERP, IBS Fintech - **5 days**
	MPLS/Internet – **8 hours** Uninterrupted Internet connectivity provided by Data Center.

General Response & Recovery Strategy

This section provides general steps for disaster recovery. However, the specific order of operations and individual recovery activities will be determined by the cause and severity of the outage or disaster, and the specific recovery procedures established for each critical system.

Once the **IT Security Steering Committee** (comprising CFO, CHRO, CSO, Head IT and Head DC) has determined that a declaration of disaster is required, the following procedures will be executed:

- Perform an initial assessment of the damage and potential length of outage. This may include reviewing written or verbal damage assessment reports.
- Activate or identify alternate sites – employees may be instructed to work from a temporary location until the affected facilities are recovered. Simultaneously, a list of needed equipment/hardware will be created and procurement processes will be initiated.
- A plan and timeline for recovery of systems and services will be developed by the IT Security Steering Committee and distributed to internal and external stakeholders. This will include details related to whether restorations will occur at primary or alternate sites. If services and/or operations will be temporarily restored at an alternate site, plans should include estimated timelines for transferring services back to the primary site.
- The IT Security Officer will contact external stakeholders as needed, either by e-mail or phone, to alert them to the disaster/outage and provide an initial timeline of service recovery.
- The plan for recovery will be implemented including:
    - IT Security Steering Committee will begin prioritizing the recovery of information systems according to the criticality of the systems. This includes referencing the list of critical

systems (Asset Management Policy) as input.

- Security Officer will retrieve and distribute the individual recovery procedures for the impacted systems to individuals who will be performing IT recovery tasks.
- Backups will be retrieved for the systems that have been prioritized for restorations. ○

IT recovery staff will begin set up of new equipment and restoring critical backups.

- Prior to placing systems into production, IT recovery staff will verify that technical safeguards are functioning adequately. For example, firewalls, intrusion detection/prevention systems, antivirus protections, authentication controls are demonstrated to be working effectively.

- As critical systems are successfully restored, the IT Security Steering Committee should be notified so that they can contact relevant departments and teams. External stakeholders who were previously notified should also be informed of any updates to recovery timelines or that services have been successfully restored.
- If systems are restored to an alternate site, the IT Security Steering Committee will convene to evaluate the operational readiness of the primary site. Once the primary site is verified, the IT Security Steering Committee will instruct and guide the IT department to finalize plans and timelines for migrating systems and operations back to the primary site.

The Security Officer/IT Manager is responsible for maintaining detailed disaster recovery procedures for each major system containing sensitive and business critical data.

Testing & Revision

Testing of the Disaster Recovery Plan will be conducted on an annual basis, in either the form of a “table top” exercise or “fire drill” exercise. The Security Officer is responsible for planning and coordinating tests. Tests will include a “lessons learned” component to identify gaps or areas for improvement that should be incorporated into the plan.

The Security Officer must review and update all recovery plans whenever a new system is added to IT infrastructure, a significant change occurs to facilities, a significant change occurs in threat or business environments, or a significant change occurs in organizational structure.

Notification and Communication

In the event that critical IT systems and services are unavailable, relevant parties and stakeholders must be notified and updated throughout recovery efforts. The IT Department is responsible for compiling and maintaining a list of contact information for vendors, clients, business associates, and other relevant stakeholders (Ref. Annexure A and B). In the case an emergency or disaster, a Disaster Recover Contact List will be used to communicate with various IT&S stakeholders.

- In the event of disaster, Head IT and Head DC should collectively inform IT Security Steering Committee (Comprising CFO, CHRO & CSO) about the disaster and regularly update on the recovery process until back to normal.
- Default communication channel should be an email, yet a parallel communication channel should be

established as per the following guidelines. This communication channel can be used in case email is also down due to disaster.

- One WhatsApp group named as “SNF IT Security Steering Committee” comprising CFO, CHRO, CSO, Head IT and Head DC should be created.
- One WhatsApp group named as “SNF IT Disaster Recovery Group” comprising all the stakeholders (except CFO, CHRO & CSO) should be created.

Response to Media

In the case of a disaster or emergency, media outlets may contact IT to discuss the incident. The media outlet may ask a series of questions, such as:

- What happened?
- How did it happen?
- What is IT going to do about it?

All media response shall be handled by the Communication and Outreach Coordinator only. It is the responsibility of all other IT employees to direct media questions to the them.

Assumptions

Various scenarios were considered to form a basis for this IT Continuity Plan, and multiple assumptions were made.
The following assumptions were considered while developing the IT Continuity Plan:

- Backups of the application software and data are intact and available at the offsite storage facility.
- Data center equipment, including components supporting, are connected to an uninterruptible power supply (UPS) and Power Generator that provides 24 hours of electricity during a power failure.
- Equipment, connections are covered under AMC with vendors Key contacts are available to coordinate the recovery process.
- Key personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the IT Continuity and IT Continuity Plan.
- IT Continuity Plan personnel are available to perform the recovery activities and they are familiar with the procedures documented in this plan.
- Monthly Data Backup copy is available at offsite, can be used for any disaster.

Review

This policy is reviewed annually or as and when it required; however, control mechanisms exist to ensure compliance activities are built-in organizational policies and practices.

Annexure A:: Key Staff Person List

S.No.	Person	Role/ Responsibilities
1	Pawan Danwar	CFO
2	Parveen Juneja	CHRO (HR Head)
3	Sundar Mahalingam	CSO
4	Samrat Adlakha	Finance Head
5	Sunil Ahuja	IT Head
6	Rajesh Dawar	Data Centre Head
7	Deepak Kapoor	Fin ERP PMO
8	Ashish Dey	HR ERP PMO
9	Naveen Tyagi	Internal Applications & Cyber Security Lead
10	Deepak Agrawal	Data Centre Administrator
11	Adit Amar	IT Administrator A9 Sector 3 Noida Office
12	Neeraj Goyal	Admin Head A9 Sector 3 Noida Office

Annexure B:: Key Vendor Contact List

S.No.	Person	Role/ Responsibilities
1	Anil Dhayani	Fin ERP Partner SPOC
2	Vyas	HR ERP Partner SPOC
3	Nidhi Modi	IBS Fintech Partner SPOC
4	Prakhar Srivastava	JIO Account Manager
5	Saurav Rajpal	Airtel Account Manager