shah investor's home ltd®
SERVICES THAT SECURE SMILES

CIN	:	U67120GJ1994PLC023257
MEMBER	:	NATIONAL STOCK EXCHANGE OF INDIA LTD. (ID-07590) BOMBAY STOCK EXCHANGE LTD. (ID-943)
DEPOSITORY	:	NATIONAL SECURITIES DEPOSITORY LTD. DPID : IN 300343
SEBI SINGLE REG. NO.	:	TRADING- INZ000167335 DEMAT- IN-DP-465-2020
CERTIFIED	:	ISO 9001 : 2015 Certified I ISO 27001 : 2022 Certified

DOCUMENT ON

INFORMATION SECURITY

POLICY AND PROCEDURES

SHAH INVESTOR'S HOME LTD. SIHL

Jinal A. Shah

April 01, 2025

Version: 1.0

Table of Contents

I. Introduction

Protection of SHAH INVESTOR"S HOME LTD„S information assets and the technology resources that support the over all activity of our company, is critical to the functioning of SIHL. Our Information assets are at risk from potential threats such as employee error, malicious or criminal action, system failure, and natural disasters. Such events could result in damage to or loss of information resources, corruption or loss of data integrity, interruption of the activities of the company or compromise to confidentiality or privacy of our members & clients.

These Electronic Information Security guidelines seek to reduce risks to electronic information resources through implementation of controls designed to detect and prevent errors or irregularities that may occur.

SIHL recognizes that absolute security of electronic information resources against all threats is an unrealistic expectation that would require the commitment of a prohibitively high level of resources. SIHL „s goals for risk reduction are based, therefore, on the principle that the level and type of security should reflect an assessment of

- the criticality of an Electronic Information Resource to our operation ;
- the sensitivity of the data residing in or accessible through the Electronic Information Resource;
- the cost of preventive measures and controls designed to detect errors or irregularities; and
- the amount of risk that company"s Board is willing to absorb.

Achieving a successful information security program has required management planning for preparedness, detection, response and recovery with respect to protection of the information enterprise.

These guidelines identify the set of measures that are part of company"s security programs. IS policy is a policy towards safe and secure environment and to achieve availability, integrity and confidentiality of the information while building Need – to- Know awareness.

Security policy and steps will undergo periodic evaluation of administrative, technical, and physical safeguards to ensure that they adequately address operational or environmental changes.

II. Scope

Fundamental reason of these detailed guideline on IS policy is to run our organization on a most Secure platform with the challenges of newer developments in a changing environment.

The power and convenience of information technology is, however, counterbalanced by the increasingly complex legislative framework which governs its use and by the wide range of threats to the security of electronic information.

On one hand the use of information and communication technology become inevitable for the organization and on the other hand there is urgent need of sound and efficient control procedure to create secure environment.

IS policy is made to respond effectively to any security incidents which may occur, to protect our business data and information in such a way that in case of any need of recovery, the same are available.

Our Assets include application systems, operating systems, tools, communications systems, data – in raw, summary, and interpreted form – and associated computer mainframe, server, desktop, communications and other hardware used to conduct activities of SHAH INVESTORE"S HOME LTD.

With these in mind, to safeguard our assets, maintain data integrity and to function with security, we have developed the following as a Policy and Procedures which is applicable across all the levels of employees including Managers and Directors.

III. Risk Assessment, Sensitivity and Criticality

Our company ensures that risk assessments were conducted to identify the Assets that require protection and to understand and document risks from security failures that may cause loss of confidentiality, integrity or availability; risk assessments have taken into account the potential adverse impact on SIHL reputation, operations and assets.
Risk assessments have been conducted by teams composed of appropriate administrators, managers, staff and other personnel associated with the activities subject to assessment.

We have determined the level of security required for an Electronic Information Resource, there are two basic risk characteristics to be assessed:
• The level of *sensitivity* of the Electronic Information Resource (Assets) and
• The level of *criticality* or overall importance of the same
-- to the continuing operation of our company.

The level of access controls required depends on the *sensitivity* of the Electronic Information Resource (Assets), as defined below.
The requirement to include a particular Electronic Information Resource in Disaster Recovery Plans as part of overall business continuity planning depends on the *criticality* of SIHL"s applications.

A. Electronic Information Resource Sensitivity

The sensitivity of an Electronic Information Resource, and therefore, the level of security required depend upon the sensitivity of the data retained by or accessible through the Electronic Information Resource.

Data falls into one of two levels of sensitivity: Restricted or Unrestricted. Sensitivity of data is based on:

The level of security required for protecting the data from unauthorized read-only access; and

The level of security required for protecting the data from unauthorized creation, deletion, or modification, collectively termed "modifications"

Restricted Data

Restricted data is data that is considered sensitive to some degree.

Unrestricted Data

Unrestricted data is the data for which access or modification is not restricted in principle and is permitted as per our Information Technology Act,

B. Electronic Information Resource (EIR) Criticality

Electronic Information Resource criticality is a measure of the importance of an Electronic Information Resource to the continuing operation of our company. The criticality of an Electronic Information Resource determines whether or not it must be included in a company"s Disaster Recovery Plan. EIR are classified into three levels of criticality as follows:

- Essential

  An Electronic Information Resource is designated as *Essential* if its failure to function correctly and on schedule could result in a major failure of company"s operation to perform mission-critical business functions, a significant loss of funds or a significant liability or other legal exposure.

  Assets at HO and all the Branches are as under:

  Connectivity with Exchanges and CTCL Manager
  Manager Server
  Admin server of CTCL
  LAN Switch: Dlink
  Router
  Leased Line Fiber MUX
  Power connections

- Required

  An Electronic Information Resource is designated as *Required* if it performs an important function, but the operation of the campus could continue for some designated period of time without the function provided by the Information Resource and there is time for recovery should the Information Resource not perform correctly or on schedule.

  Assets at HO and all the Branches are as under :

  Firewall
  Internal LAN nods
  Connectivity of client

- Deferrable

  An Electronic Information Resource should be designated *Deferrable* if company could continue operation for an extended period of time without the Information Resource performing correctly or on schedule.

C. Notification in Instances of Security Breaches

In the case of a security breach as defined in this policy, all the staff, managers and directors must follow these guidelines presented here to provide notification of the breach to the management.

Any person from SIHL, whose work / module / computer system / password, is reasonably believed to have been acquired by an unauthorized person has to notify to top level management and that notification must occur without delay.

Risk Assessment:

We define the following as:

Risk:	Potential of any action or event occurrence which will adversely affect business
Threat:	An action or event that will compromise desirable outcome of business process
Vulnerability:	Weakness in a system that can be exploited by a threat
Control:	Tools and techniques for mitigating risks
Exposure:	Risk – Control

We foresee the following are top threats which can adversely affect our functioning:

Virus	Inside abuse	Theft
System penetration	Unauthorized access	Denial of service
Sabotage	Fraud	Telecom fraud

Critical dependencies:

- Current Locational Setup :

Locations of HO and all the branches are under critical dependency . All our functions are performed and transmitted thorough these offices only.

- Vendors for the hardware and related software and their availability

  Shayona Hardware : All hardware

  Saral Information Technologies Pvt Ltd :

  NSE Exchange: NeatPlus

  BSE Exchange: BOLT

All the above vendors are available as and when required.

- Insurance coverage :

As per our latest insurance cover our below listed hardware and peripheral are covered for the insurance and the coverage is taken into consideration on devising this policy.

D. Electronic Information Resource (Assets): Inventory:

Electronic information resource inventory of all the assets and facilities which are critical considering non operation and which falls under the head of Essential as described above.

Connectivity with Exchanges and CTCL Manager
Manager Server
Admin server of CTCL
LAN Switch : Dlink ,Cisco
Routers
Leased Line Fiber MUX
Power connections
Firewall
Internal LAN nods
Connectivity of client
BOLT
Saral System (CTCL)
NeatXS

IV. Disaster Recovery Plan & Emergency Procedures

As part of ongoing business continuity planning, SIHL has prepared periodically updatable plan for recovering from a disaster that renders certain Electronic Information Resources unavailable for an unacceptable period of time.

Part (IV) Disaster recovery plan has to be referred and must be complied with for resources, action, tasks and data required to manage in the event of a disaster.

Recovery plans are addressing the failure of *Essential* Electronic Information Resources and are included in companies Disaster Recovery Plan.

The Disaster Recovery Plan include provisions for implementing and running Essential applications at an alternate site or provisions for equivalent alternate processing (possibly manual) in the event of a disaster or other interruption that renders normal processing inoperable for the period of time specified in the designation of the Electronic Information Resources as Essential.

Projected Disasters:

Earthquake
Fire
Riots
Human Malafide intent

Considering importance of activities and Essential resources, the DRP has been divided into following three parts.

A. Emergency Plan:

1. Urgent information to top management and police, fire fighters, doctor for occurance of disaster.
   The information to be given by any of the person from SIHL on knowing the disaster. Response time to be minimal.

2. Detachment of Servers and LAN nods.
   Termination of power supply, removal of important files, documents and shutting down of the whole network.
   The same to be done only by the System Administrator and in absence of him any of the staff from system developer team.

3. Emergency action plan team :

   Following are members of the fast action team on any of the disaster and they are responsible for all the transfers and secure removal of other staff, managers out of the affected location.

   IT Head: Jinal Shah
   System Administrator: Priyakant Vaghela
   Assistant to System Administrator: Apurva Shah

4. Except the members of action team, rest of the staff has to leave the premises urgently after shutting down of their related equipments and nods.

5. Emergency action plan team has to evaluate for removal of Essential assets and important file, document, hardware etc out of the disaster location.

6. This year we have set up Disaster Recovery Site at Mumbai location and for business continuity we have setup both Exchange's (NSE,BSE) connectivity over there now we are planning for Mock Drill for the same with the help of exchanges.

B. Back up & Recovery Plan :

1. As our DR site at Mumbai location is up and running routinely live backup of all the critical servers are synced with the help of MPLS and Internet bandwidth. So all the servers and data are safe remotely.
2. For recovery and business continuity we have to inform exchange regarding the event which occurs at Head office premises, so they will transfer our main userid to backup location and we could take login from over there and start our business activity.

C. Test Plan :

1. Every six month, both the above plans: Emergency and Back – Restoration has to be tested for the functionality and smooth operation.

2. The same is to be performed in the presence of Mr. Rajesh Punjabi (GM)

V. Logical Security

This section addresses security measures related to controlling access to Electronic Information Resources through logical measures (e.g., via software or network controls), controls related to software development and change control, security of data, communications security, and reduction of risk from Intrusive Computer Software.

When any Electronic Information Resource manages or contains Restricted data, appropriate measures must be in place to safeguard against unauthorized access to the data. This includes not only the primary operational copy of the information but also data extracts and backup copies.

A. **FireWall:**

A secure network is vital to a business. To secure a network SIHL has implanted firewall in its network, SIHL System Administrator has created a security policy that outlines all of the network resources within that business and the required security level for those resources. The policy applies the security rules to the transit traffic within a context (source zone and destination zone) and each policy is uniquely identified by its name. The traffic is classified by matching source and destination zones, source and destination addresses.
Firewall system implemented is: Sophos XGS2300

We have implemented an effective firewall policy to ensure better use of system memory and to optimize policy configuration:

1. Use least privilege policies - Make the firewall rules as tight as possible in terms of match criteria and permitting traffic. Only permit traffic that is allowed by your organizational policy and deny all other traffic. This is true for both ingress and egress traffic, meaning traffic from the Internet to internal resources and also traffic from internal resources to the Internet. A least privilege security policy helps to minimize the attack surface, making other controls more effective.

2. Segment logically - Zone-based firewalls allow you to place different interfaces into different zones. This allows you to design your network such that you can place resources in a manner where the firewall can enforce controls (interzone and intrazone policies).

Place specific firewall rules first - Place the most explicit firewall rules at the top of the rule base because traffic is matched starting at the top of the rulebase and going down with the first match.

3. Use address sets where possible - Address sets simplify administration of firewall policies. They allow you to group large sets of objects so that you can address them as a single object in a security policy. The more rules you can reference to the address sets, the easier it is to make changes because most organizations have logical objects that can be grouped.

4. Use explicit drop rules - To ensure that undesired traffic does not leak through a security policy, place an any-any-any drop rule at the bottom of each security zone context (for example, source zone to destination zone) along with a global policy. This does not mean that you should not define your firewall rules, it simply provides a catch-all mechanism for capturing unclassified traffic.

5. Use logging - We highly recommend that you log on all firewall policies. Logging provides you with an audit trail of all network activity, which helps in troubleshooting and diagnosis. Unless you are troubleshooting, it is best to use the Log on Session Close option instead of the Log on Session Initialization option. Session Close logs include a great deal more information about the session; this information is useful for diagnostic purposes.

6. Check memory utilization - Check your memory usage before and after compiling policies.

B. Malware Protection & Antivirus

SIHL has implemented Trend Micro Apex One on all required Desktops & Servers to protect them from Virus attack or Malware activity. System Administrator has also implemented following policy for the same:

1. Anti-virus software is mandatory.

2. Any system which is located in SIHL head office or branch office must have up-to-date antivirus software installed and operating. This includes laptop computers and computers owned by staff, visitors.

3. The AV product installed on desktops and servers must be configured to update on a daily or more frequent basis.

4. All Computers used solely as servers should have an Anti-Virus product installed and operating.

5. Only servers where a significant negative impact would result from operating anti-virus software, or servers running an Operating System with low likelihood of virus infection such as Linux, may be considered for exemption from this procedure.

6. All exemptions must be authorized by the Manager of Information Technology Services.

C. Access Controls

Access to Restricted Electronic Information Resources and data retained within or accessible through these Information Resources must be limited to *Authorized Users*. Authorized Users and their specific level of privilege are specified by the Electronic Information Resource Proprietor, unless otherwise defined by our companies policy.

Such access must be controlled with secure means of *authentication* and *authorization*. *Authentication* is the process of confirming that a known individual is correctly associated with a given credential, for example, by use of passwords to confirm correct association with a username or account name.3 *Authorization* is the process of determining whether or not the identified individual or class is authorized to gain access to an Information Resource, and determining what type of access is allowed, e.g., read-only, create, delete, and/or modify.

Once access to Electronic Information Resources is established, logical security mechanisms should be in place that prohibit or minimize the risk of unauthorized access to those resources by others who might gain control of the working session, for example, by accessing the authorized user"s computer if that user leaves it unattended.

These Guidelines do not require any specific technology to be employed for Logical Security, as long as the security functions of authentication and authorization are performed before access to Restricted or Essential Electronic Information Resources is granted to a User.

It is a violation of these Guidelines for Users to attempt to gain unauthorized access to any Electronic Information Resources or in any way damage, alter, or disrupt the operations of these Electronic Information Resources. It is also a violation of these Guidelines for Users to capture or otherwise obtain or tamper with passwords, encryption keys, or any other access control mechanism that could permit unauthorized access, except where expressly required in the performance of their duties, such as when systems personnel need to provide access to Electronic Information Resources when passwords or other keys have been lost or misplaced.

Our company has software vendors for the BSE and NSE operations and the software incorporates required access controls and the same are in parity with NEED TO KNOW – principles which our SIHL believes in.

When there is a need for shared passwords, additional measures should be implemented that record specifically who accessed the Electric Information Resource or other control mechanism that will provide an audit trail of the access.

Access controls are implemented to ensure that integrity, availability, privacy, and confidentiality of data are in compliance with rules and guidelines of NSE, BSE and SEBI.

Modifications to Restricted data should be performed according to established procedures like : System administrator has to document for the Change Request and the reason for need of change, Modifications are by approved person only etc.

SIHL has implemented these Guidelines with encouragement, where deemed appropriate, for use of system logs to assist in monitoring access to Electronic Information Resources and/or access to data retained within or accessible through such Resources.

a) Password Policy :

- Every fortnight there is compulsory changing of password for the CTCL client.
- Systems Administrator has to take password awareness programs for the benefit of all the users and staff of SIHL.
- It is highly prohibited to write password on the Desktop or on the table.
- No employee is allowed to share the password.
- Password is defined to be of minimum 8 characters. AND alphanumeric in nature
- Operating system is being configured considering Need to know basis for the access through passwords.

b) Policy on Database Access :

- Saral CTCL and Backoffice database has the internal access controls as per the application level security and the same is introduced by the respective approved vendors.

- The database access is available only to the Systems Administrator and not to any of the CTCL client nor to any of the top level management.

D. System Administration Access Controls

System administrators routinely require access to Electronic Information Resources to perform essential system administration functions critical to the continued operation of the Electronic Information Resource. Such privileged access is often termed "superuser access" and accounts that provide such privileges to system administrators are termed "superuser accounts." Privileged or superuser accounts enable vital system administration functions to be performed, such as establishing userid's or accounts, maintaining authorization for these accounts, terminating another user's session, correcting problems, doing Surveillance management and other broadly-defined system or other Electronic Information Resource privileges.

Such privileged accounts are especially sensitive and hence SIHL has established procedures, commensurate with the level of risk involved, to ensure that abuse will not occur. In particular, the number of privileged accounts is kept to a minimum, and only provided to those personnel whose job duties require them (currently to the Systems Administrator).

These personnel are advised not to use superuser accounts for other than authorized purposes. Activities performed using a superuser account is logged in detailed and be reviewed, on a regular basis by top level management.

E. Administrative System and Applications Software Development and Change Management Control:

Development and maintenance of any administrative systems, whenever performed by our SIHL personnel must follow the pattern of System Development Life cycle and all the stages of that must be planed, discussed, approved and documented and then after the software is to be checked for its functionality on a separate environment similar to the live environment. Access controls, Logs and report maintenance as per these guidelines must be implemented in that.

In case the software is purchased from the market, it must be purchased from approved vendor of NSE/BSE. Before any change to live software, detailed Change Request Form (CRF) explaining modifications and effects must be highlighted by the vendor and prior approval of top level management is required. Any change is to be done only by that vendor in presence of system administrator.

- Saral CTCL, BOLT or NEAT Plus trading software version changes are done only after necessary testing in exchange mock trading environment and thorough testing.

In general, the purpose of change controls is to ensure the accuracy, integrity, authorization, and documentation of all changes. Change procedures should include assignment of responsibilities to ensure adequate separation of duties, and may also include: confirmation of testing, authorization for moving the programs to production, user training requirements, and documentation requirements.
Change procedures should include backup of prior versions of application programs, so that a change may be "rolled back" if problems occur.

Change control offers an opportunity for organizations to manage the changes made to their systems. However, it also provides an ideal opportunity for internal auditors/ systems auditors to understand the changes that are made and why they are necessary. This could lead to focused audits where control issues are identified, significant systems are introduced, or major systems are changed.

Change control is a useful safety valve to ensure that all changes to systems and applications that may be put forward by people of user department within an organization are overseen by a dedicated group of people.

F. **Live Surveillance System against Undue Exposure Risk :**

Operational Risk of undue exposure of client in automated systems and high clientele is identified. To safeguard against the Undue Exposure by any of the Client of SIHL, company has a live surveillance system to track the client Exposure Limit and Restricting any of the client from making transaction beyond the particular exposure level per day and /or per script.

Each of these Exposure limit is being verified by the General Manager of our company and there is monthly scrutiny of Master Data Updations by System Admin in case of change in Exposure limits of clients. The system also prevents transactions wherein no trade is being

allowed temporarily or wherein the trade is required to be blocked due to norms of SEBI or exchange etc.

G. Policy for Dealing in Penny Stock :

Operational Risk of clients dealing in penny stock and to stop for manipulation of prices, IS policy has steps to mitigate the same. A Security that trades at a relatively low price (generally such securities are trading below face value of the security) and has small market capitalization, is called a penny stock. These types of stocks are generally considered to be highly speculative & high risk because of their lack of liquidity, large bid-ask spreads, small capitalization and limited following and disclosure. The Company recommends that its clients desist from trading in any penny stocks in view of the associated risk element while dealing in such stocks.

Depending on the market condition, applicable regulatory guidelines and applicable risk policy of the Company, the Company at its sole discretion, may impose certain restrictions and/ or conditions (on case to case basis) including but not limited to refusal, wholly or partly, for trading in penny stock. Company has decided to revise a list of penny stocks as per the exchange list and norms.

H. Data Backup and Retention :

Backup copies of data and software associated with Restricted or Essential Electronic Information Resources must be sufficient to satisfy Disaster Recovery Plan of these guideline, application processing requirements, and requirement of SEBI, NSE, BSE towards data backup and storage.

Backup copies of Essential data for Disaster Recovery purposes must be stored at a secure location that provides standard protection and at a non-commercial off-site providing equivalent protection.

SIHL undertakes the following back up procedures :

- Daily back ups for the following is required :
  Full CTCL Database & Back office database : to be done by System Administrator
- Loading of full back ups into the remote location

- Logs and reports are stored on the Hard disk and kept for almost 1 month.
- Every 2 months the kept back up is checked for the functionality by loading it on to the stand alone server.
- Version controls are to be kept with the detailed summery containing parameters and modules modified in the previous versions with the date of active usage.

VI. Physical Security

Shah Investor"s Home Ltd should establish procedures for the physical protection of its Electronic Information Resources. At a minimum, SIHL has developed procedures to protect physical access to Server Room, at Back office functions and CTCL operation taken place.

• Disaster Controls

Appropriate measures for the prevention, detection, early warning of, and recovery from emergency conditions, including earthquake, fire, water leakage or flooding, disruption or disturbance of power, air conditioning failures, and environmental conditions exceeding equipment limits.

• Physical Access Controls

Controls for limiting physical access to facilities housing Restricted or Essential Electronic Information Resources through the use of key locks, manual sign in/out logs, verification of identification, etc.

• There should be Maintenance records documenting repairs and modifications to physical components of the facility related to security, such as hardware, walls, doors, and locks.

- Policy on security of hardware and peripherals
  - AMC with Dell , Adit Microsys & Rubik Infotech : is available for almost all the Hardware & Softwares and peripherals.
  - No employee is allowed to have any tea or breakfast in the operational environment.
  - Office and Server room are locked except the operational hours.

- Policy on Network Security
  - Active router is being places for the security of remote access through Lease line and VPN connections.
  - Static IP Pool in the RAS server is defined restricting any remote access other than the defined IP addresses.
  - For radio frequency, transmission is done through router and signal receiver device. All the data are transmitted only in the encrypted form.

VII. Testing and Awareness Building

SIHL implementation of these Guidelines also include procedures for testing of these guidelines and norms.

We have established a timetable for regular review of the security plan to keep in step with the evolving needs, and with changes in local personnel and the external environment. Every quarter members of emergency action plan with compliance office of our company, will verify / observe about the implementation level of these guideline.

The basis aim of the same is to create awareness of security features and plans : among users of Electronic Information resources and to constant upgrade their knowledge with the developments of the Information technology environment adopted at our company : Shah Investor"s Home Ltd.

VIII. Responsibilities

It is the responsibility of the Top level management to devise the guidelines for IS policy and procedures and to maintenance, update and implement the same incompliance with the legal and regulatory norms of NSE/BSE and SEBI and Depositories.