INDIA HOME
LOAN LTD.

INFORMATION TECHNOLOGY POLICY & PROCEDURES

Revision 2.0

Change Management

Policy No:	**Effective:**
Information Technology / 2018-12 / 02	**1st April 2025**
Original Internal Approval Date:	**Next Revision:**
1st February 2025	April 2026
Management Approval by:	**Prepared by:**
Mitesh Pujara	Vinod Prajapati
Board Approval Date	
Waiting	**Preparation Date**
	24th November 2024
Board Approval by:	**Recommended By**
Waiting	Mitesh Pujara

INTRODUCTION

The India Home Loan LTD General Information Technology (IT) Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the business. Same needs to be followed by all staff. It also provides guidelines which organisation will use to administer these policies, with the correct procedure to follow.

India Home Loan Limited (IHLL) will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply for all IT related process to be adhered to by all IHLL Employees.

TECHNOLOGY HARDWARE PURCHASING POLICY

Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners.

PURPOSE OF THE POLICY

This policy provides guidelines for the purchase of hardware for the business to ensure that all hardware technology for the business is appropriate, value for money and where applicable integrates with other technology for the business. The objective of this policy is to ensure that there is minimum diversity of hardware within the business.

PROCEDURES

PURCHASE OF HARDWARE

Guidance: The purchase of all desktops, servers, portable computers, computer peripherals and mobile devices must adhere to this policy.

PURCHASING DESKTOP COMPUTER SYSTEMS

The desktop computer systems purchased must run at Windows 7 or above version and integrate with existing Dell power edge T430 & Hp ML10 server's hardware.

The desktop computer systems must be purchased as standard desktop system bundle and must be only of HP, Dell, Acer, Lenovo brand.

The desktop computer system bundle must include:

a) Desktop tower

- Keyboard and mouse You may like to consider stating if these are to be wireless
- Desktop screen of 18-inch minimum
- Windows 7, or above version, And software Office 2013 or above version.
- No purchase for speakers, microphone, webcam, printers aligned single user.

b) The minimum capacity of the desktop must be:

- Core I3 (3.00GH) Minimum
- 4 GB (RAM) Minimum
- USB Port not to be activated any employee's, except key management executives.

Any change from the above requirements must be authorised by Executive Director / Chief Finance Officer

All purchases of desktops must be supported by minimum warranty of 3 years for Desktop and Laptop and be compatible with the business's server system.

PURCHASING PORTABLE COMPUTER SYSTEMS

The purchase of portable computer systems includes notebooks, laptops.

Portable computer systems purchased must run a Windows7 or above version and integrate with existing hardware dell PowerEdge & HP ML 10.

The portable computer systems purchased must be must be Only from HP, Dell, Acer, Lenovo brand.

The minimum capacity of the portable computer system must be:

- Core I3 (3.00GH) Minimum
- 4 GB (RAM) Minimum
- USB Port not to be activated any employee's, except key management executives.

Any change from the above requirements must be authorised by ED and CFO

All purchases of all portable computer systems must be supported by 3 years, warranty and be compatible with the business's server system.

PURCHASING SERVER SYSTEMS

Server systems can only be purchased by IT Personnel / IT Head.

Server systems purchased must be compatible with all other computer hardware in the business.

All purchases of server systems must be supported by minimum of three years' warranty and be compatible with the business's server systems.

Any change from the above requirements must be authorised jointly by two of CFO / ED / Managing Director. And same has to be mandatorily recommended only by IT personnel

PURCHASING COMPUTER PERIPHERALS

Computer system peripherals include printers, scanners, external hard drives etc.

Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software in the business.

The purchase of computer peripherals can only be authorised by ED/CFO.

All purchases of computer peripherals must be supported by 3 years' warranty and be compatible with the business's other hardware and software systems.

Any change from the above requirements must be authorised by ED & CFO.

POLICY FOR GETTING SOFTWARE

PURPOSE OF THE POLICY

This policy provides guidelines for the purchase of software for the business to ensure that all software used by the business is appropriate, value for money and where applicable integrates with other technology for the business. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

PROCEDURES

Request for Software

All software, including open source, freeware, etc. must be approved by IT Head prior to the use or download of such software.

Purchase of software

The purchase of all software must adhere to this policy.

All purchased software must be purchased by ED/CFO

All purchases of software must be supported by warranty requirements and be compatible with the business's server and/or hardware system.

Any changes from the above requirements must be authorised by ED/CFO.

Obtaining open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval from **IT Head** must be obtained prior to the download or use of such software.

All open source or freeware must be compatible with the business's hardware and software systems.

Any change from the above requirements must be authorised by ED / CFO.

IT requisition form to be used for all Software / Hardware related purchase

IT form.xlsx

POLICY FOR USE OF SOFTWARE

PURPOSE OF THE POLICY

This policy provides guidelines for the use of software for all employees within the business to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

PROCEDURES

SOFTWARE LICENSING

All computer software copyrights and terms of all software licences will be followed by all employees of the business.

ED/CFO is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and licence agreements are adhered to.

SOFTWARE INSTALLATION

All software must be appropriately registered with the supplier where this is a requirement.

Mr. Mitesh Pujara is to be the registered owner of all software.

Only software obtained in accordance with the getting software policy is to be installed on the business's computers.

All software installation is to be carried out by IT Team.

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

SOFTWARE USAGE

Only software purchased in accordance with the getting software policy is to be used within the business.

Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of ED/CFO.

Employees are prohibited from bringing software from home and loading it onto the business's computer hardware.

Unless express approval from IT Head is obtained, software cannot be taken home and loaded on a employees' home computer

Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation from ED/CFO is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the business and must be recorded on the software register by IT head.

Unauthorised software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to ED/ CFO for such as further consultation, reprimand action etc. The illegal duplication of software or other copyrighted works is not condoned within this business and IT head is authorised to undertake disciplinary action where such event occurs.

Breach of Policy

Where there is a breach of this policy by an employee, that employee will referred to ED/EFO for such as further consultation, reprimand action.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify IT Head immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee will be referred to ED/CFO for such as further consultation, reprimand action.

BRING YOUR OWN DEVICE POLICY

At India Home Loan Limited we acknowledge the importance of mobile technologies in improving business communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to India Home Loan's network and equipment. We encourage you to read this document in full and to act upon the recommendations. This policy should be read and carried out by all staff.

PURPOSE OF THE POLICY

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and other types of mobile devices for business purposes. All staff who use or access India Home Loan's technology equipment and/or services are bound by the conditions of this Policy.

PROCEDURES

CURRENT MOBILE DEVICES APPROVED FOR BUSINESS USE

The following personally owned mobile devices are approved to be used for business purposes:

- Type of approved mobile devices such as notebooks, smart phones, tablets, iPhone, removable media.

REGISTRATION OF PERSONAL MOBILE DEVICES FOR BUSINESS USE

Guidance: You will need to consider if the business is to have any control over the applications that are used for business purposes and/or used on the personal devices.

Employees when using personal devices for business use will register the device with HR department.

HR will record the device and all applications used by the device.

Personal mobile devices can only be used for the following business purposes:

- Each type of approved use such as email access, business internet access, business telephone calls.

Each employee who utilises personal mobile devices agrees:

- Not to download or transfer business or personal sensitive information to the device. Sensitive information includes business or personal information that you consider sensitive to the business, for example intellectual property, other employee details.
- Not to use the registered mobile device as the sole repository for India Home Loan's information. All business information stored on mobile devices should be backed up
- To make every reasonable effort to ensure that India Home Loan's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected
- To maintain the device with current operating software, current security software.

- Not to share the device with other individuals to protect the business data access through the device
- To abide by India Home Loan's internet policy for appropriate use and access of internet sites etc.
- To notify India Home Loan Limited immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to India Home Loan's equipment.

All employees who have a registered personal mobile device for business use acknowledge that the business:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data
- Will regularly back-up data held on the device
- Will delete all data held on the device in the event of loss or theft of the device
- Has first right to buy the device where the employee wants to sell the device
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
- Has the right to deregister the device for business use at any time.

Keeping mobile devices secure

The following must be observed when handling mobile computing devices such as notebooks and iPads:

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended
- Mobile devices should be carried as hand luggage when travelling by aircraft.

BREACH OF THIS POLICY

Any breach of this policy will be referred to ED/CFO who will review the breach and determine adequate consequences, which can include such as confiscation of the device and or termination of employment.

INDEMNITY

India Home Loan Limited bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify India Home Loan Limited against any and all damages, costs and expenses suffered by India Home Loan Limited arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by India Home Loan Limited.

CYBER SECURITY (FIREWALL RULE)

PREAMBLE

The purpose of this IT Standard is to provide guidance on the use of network firewalls and Intrusion Prevention System (IPS) in order to protect the company’s IT infrastructure and data against unauthorised access or potential malicious attack. The IT Standard will assist in minimising the risk of incorrectly configured network security devices, which could result in exploitable vulnerabilities.

Firewalls and Intrusion Prevention System are a vital part of any information system’s defence against attack. These devices are designed to detect and block unwanted traffic traversing the network and to minimise the adverse effects of intrusion should it occur. Firewalls and Intrusion Prevention System may be hardware or software-based and are deployed in various locations within the IT architecture.

STANDARD

NETWORK FIREWALLS AND IPS

All Network Firewalls and IPS must be properly installed, configured and managed as per this standard. Failure of a network firewall or IPS to conform to this standard may create an exploitable vulnerability within the Company’s IT infrastructure. A successful exploit could compromise the Company’s networks, IT systems or data and consequently damage the Company’s reputation.

STANDARD RULES

1 Network Zoning

Segregation of the network via separate security zones is to be defined and used to segregate assets.

2 Deny by Default

Company has configured below firewalls at server to manage internet traffic:

a) Fortigate 60E (Host Name: FGT60E4Q16011011)
b) Fortigate 60E (Host Name: FGT60E4Q16010655): Backup Firewall as part of BCP strategy

Firewalls block all non-permitted incoming traffic not allowed by the Company's default firewall configuration, defined below. Access to Company network and assets is set to deny all inbound traffic by default and any permitted inbound network traffic is only allowed based on approved business requirements.

3- Internet Protocol (IP) Addresses

Firewalls and IPS will only allow appropriate source and destination IP addresses and are required to block all traffic that is addressed to or appears to come from invalid or malformed IP addresses. All IP address should be minimum at IPV4

3.1 IP Protocols

Only authorised protocols will be permitted through the firewall. IT head at regular frequency are reviewing authorised protocols.

3.2 Ports

Virtual Private Network (VPN) with below configuration is an authorised port under current firewall.

a) VPN –L2TP
b) Site-To-Site

3.3 Logging

All network based firewalls and IPS are to be configured to record traffic and event logs, which must be transmitted and stored in the same way as other security-related logs. All Firewall and IPS traffic and event logs must be maintained for a minimum of 30 days.

3.4 Device Configuration and Backup

All network Firewall configuration backup is kept at every change and it has to be kept for at least 12 months.

4 -Variations

Any variations to the default standard rule sets must be authorised by the ED/CFO.

INFORMATION TECHNOLOGY SECURITY POLICY

PURPOSE OF THE POLICY

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets.

PHYSICAL SECURITY

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through key lock.

It will be the responsibility of ED & CFO to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify ED & CFO immediately.

All security and safety of all portable technology, such as laptop, will be the responsibility of the employee who has been issued with the laptop, mobile phones. Each employee is required to use locks, passwords. and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, ED & CFO will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

INFORMATION SECURITY

In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out. The responsibility for backing up the information located in shared access servers is of the network administrators (which has to be managed by IT personnel). It must be borne in mind that not only are hard disks inclined to fail, but also magnetic tapes are quite prone to errors that destroy their contents, so we need to do the restoration testing time to time basis.

- **General Rule:** Daily incremental copying of all important business data is happening on two different servers on real time basis through an automated process. To prevent data loss, the data is stored at Ahmedabad office outside IHLL Head Office and the data is maintained on Ahmedabad office 'servers'.

- Backup of Tally Data will occur alternate day after regular business hours in Ahmedabad office 'server'.

Special backups may be made for longer retention periods during special situations such as system upgrades and major projects.

It is the responsibility of IT Head to ensure that data back-ups are conducted weekly and the backed up data is kept in Ahmedabad office server, and tally data also.

All technology that has internet access must have anti-virus software installed. It is the responsibility of IT Head to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any employee breaching this will be Severe Reprimand / Suspension of Service.

PASSWORD POLICY

Every employee will be issued with a unique identification code to access the business technology and will be required to set a password for access.

Each password is to be number of alpha and numeric ext. and is not to be shared with any employee within the business.

IT Head is responsible for the issuing of the identification code and initial password for all employees.

Where an employee forgets the password or is 'locked out' after three attempts, then IT Head is authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

It is the responsibility of ED & CFO to keep all procedures for this policy up to date.

E – MAIL POLICY

Each employee is responsible for the contents of his/her e-mail and all actions performed using his/her email logon credentials.

Email should be used only for business purposes. Personal or non-business use of the Systems is not permitted.

Only the email client authorized for use by IT Department should be used.

User should use only their own IHLL E-Mail account and should not allow anyone else to access their account. Users should identify themselves by their name; pseudonyms that are not readily attributable to actual users should not be allowed. Users should not represent themselves as another user. Each user should take precautions to prevent unauthorized use of the E-mail account. Forging of header information in E-Mail account. Forging of header information in E-Mail (including source address, destination address, and timestamps) is not permitted.

Users should not provide other unauthorized persons with their E-Mail ID and password.

Users should not send confidential or restrictive information via E-mail, unless the information is encrypted using approved encryption technique.

E-Mail should not be used to transmit or receive statement that contain any material that is offensive, defamatory, or threatening to others.

Employees may either communicate with the originator of the offensive E-mails, asking him/her to stop sending such messages, or report such offensive E-mails directly to Information Security Officer.

Users should not post server or network configuration information about IHLL information resources to public newsgroup or mailing lists. This includes internal machine addresses, server names, server types, or software version numbers.

Users who cannot access their email for long periods (due to vacation, outstation work etc.) should use “Out of Office” feature in IHLL email system.

Users must not employ a scanned version of a hand-rendered signature to give the impression that the sender signed an E-mail message or other electronic communications, as another person could misuse the signature.

Users should not modify the security parameters within IHLL E-Mail system.

Users should not send unsolicited bulk mail messages. This practice includes, but is not limited to, bulk mailing of commercial advertising and religious or political tracts. Malicious E-Mail, including but not limited to “mail bombing”, is prohibited.

At any time, with or without notice, this information may be monitored, searched, reviewed, disclosed, or intercepted by IHLL for any legitimate purpose, including the following:

EMAIL CONTROL POLICY:

All mails sent through IHLL server should be routed with a default copy to vinod@indiahomeloan.co.in, except senior management executives.

INFORMATION TECHNOLOGY ADMINISTRATION POLICY

PURPOSE OF THE POLICY

This policy provides guidelines for the administration of information technology assets and resources within the business.

PROCEDURES

All software installed and the licence information for organisation must be on Register available with the IT Head. It is the responsibility of ED & CFO to ensure that this registered is maintained. The register must record the following information:

- What software is installed on every machine
- What licence agreements are in place for each software package
- Renewal dates if applicable.

IT head is responsible for the maintenance and management of all service agreements for the business technology. Any service requirements must first be approved by ED & CFO.

IT Head is responsible for maintaining adequate technology spare parts and other requirements including toners, printing paper, etc.

Any unspecified technology administration requirements should be directed to ED & CFO

WEBSITE POLICY

PURPOSE OF THE POLICY

This policy provides guidelines for the maintenance of all relevant technology issues related to the business website.

PROCEDURES

WEBSITE REGISTER

The website register must record the following details:

- List of domain names registered to the business
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

The keeping the register up to date will be the responsibility of IT Head.

IT Head will be responsible for any renewal of items listed in the register.

WEBSITE CONTENT

All content on the business website is to be accurate, appropriate and current. This will be the responsibility of MD, ED, CFO, CS

The content of the website has to be reviewed frequently.

The following persons are authorised to make changes to the business website:

Mrs. Jaymala Jain (GM –Finance & Accounts)

Ms. Akash Das (Company Secretary)

Mr. Mitesh Pujara (Executive Director)

Mr. Mahesh Pujara (Managing Director)

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the business.

IT SERVICE AGREEMENTS POLICY

PURPOSE OF THE POLICY

This policy provides guidelines for all IT service agreements entered into on behalf of the business.

PROCEDURES

The following IT service agreements can be entered into on behalf of the business:

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of business software
- Provision of mobile phones and relevant plans
- Website design, maintenance etc.

All IT service agreements must be reviewed by recommended solicitor before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by ED / CFO

Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorised by ED / CFO.

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to IT Head who will be responsible for the settlement of such dispute.

IT head will be responsible as custodian for all service agreements

EMERGENCY MANAGEMENT OF INFORMATION TECHNOLOGY

PURPOSE OF THE POLICY

This policy provides guidelines for emergency management of all information technology within the business.

PROCEDURES

IT Hardware Failure

Where there is failure of any of the business's hardware, this must be referred to IT Head immediately.

It is the responsibility of IT head to undertake tests on planned procedures in the event of IT hardware failure.

It is the responsibility of IT Head to undertake tests on planned emergency procedures each three months to ensure that all planned emergency procedures are appropriate and minimise disruption to business operations.

VIRUS OR OTHER SECURITY BREACH

In the event that the business's information technology is compromised by software window defender such breaches are to be reported to IT head immediately.

WEBSITE DISRUPTION

In the event that business website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified
- ED & CFO must be notified immediately

DATA BACKUP POLICY AND PROCEDURES

Purpose

The unprecedented growth in data volumes has necessitated an efficient approach to data backup and recovery. This document is intended to provide details on the stipulations of data backup and retrieval operations to the client.

Tally Backup Mechanism

Backup of Tally Data will occur weekly after regular business hours Ahmedabad office 'server'.

It is the responsibility of IT Head to ensure that data back-ups are conducted weekly and the backed up data is kept in Ahmedabad office server, and tally data also.

All technology that has internet access must have anti-virus software installed. It is the responsibility of IT Head to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any employee breaching this will be Severe Reprimand / Suspension of Service.

Restoration.

Users who need files restored must submit a request to IT head via a Business Email Request. They will need to include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

OmniFin Backup Mechanism

OmniFin Backup Mechanism OmniFin Application is no longer in use; however, the application is still hosted. Data was backed up weekly on the local server at Ahmedabad to prevent data loss. Incremental backup was performed for all OmniFin business data on the same servers at an agreed frequency through an automated procedure.

----End---