

IT Policies Handbook

This is I-STAY HOUSING PVT LTD - IT Policy document to help the Employees to know IT operational guidelines as well Process required in their day to day working. This IT Policy will be applicable to every employee in the I-STAY HOUSING PVT LTD. This IT Policy will also significantly impact on quality of IT Governance.

Purpose:

Purpose of this Policy is to issue guiding principal, process know-how and detailing about rule and regulation to be following in IT in individual day to day working.

Scope:

This Policy will be applicable to every individual who is working for I-STAY HOUSING PVT LTD. He / She may be direct employee of the organization - on role or off role or on contract or in any form connected to I-STAY HOUSING PVT LTD and operating directly or indirectly IT system, IT Infra of I-Stay Housing Pvt Ltd.

Table of Content:

- I. IT - General Operational Guidelines**
- II. IT - Equipment Policy**
- III. IT - Email Policy**
- IV. IT - Support Policy**
- V. IT - Internet Policy**
- VI. IT - Data Access & Security Policy**
- VII. IT - Backup Policy & Disaster Recovery**
- VIII. IT - Induction & Training Policy**
- IX. IT - Maintenance & Repair Policy**
- X. IT - Replacement & Upgrade Policy**

I. IT - General Operational Guidelines

Policy Name : I-STAY HOUSING PVT LTD - IT Policy

Policy Title : IT - General Operational Guidelines

Version number : 1

Contents

- 1. About Policy**
- 2. Communication on Social Media**
- 3. Internet / Network Usage**
- 4. Use of Email System**
- 5. Use of Company IT System**
- 6. General Password Guidelines**
- 7. IT Equipment Handling**
- 8. Intellectual property and Copyrights**
- 9. Disciplinary action**

1. About Policy

The purpose of this policy is to give clarity to end users of organization about General IT Operational Guidelines and responsibilities of end users in his day to day working. However; to get more clarity on every subject users are advised to go through the detailed Policy document.

2. Communication on Social Media

Social Media must be used only if your role requires and you have approval from Management. Social Media is extensively used by people. It has multiple benefits if it is used carefully. Employee must keep in mind following points while operating social media in his personal / professional life.

- Please make sure you are not mixing your personal and professional life on Social Media.

- Do not post anything about company / organization on social media without exclusive consent from Top Management.
- Beware that your identity on online social media network also represent the organization... So be careful while using the social media.
- Make sure your personal online activities don't interfere with your job profile.
- Use discretion. Take care not to publish information which is linked to organization policies, information or in any form linked to organization.
- There's no such thing as a truly "private" on social media site: so be careful before posting any comment.
- You are responsible for what you post so make sure dispute are not arising and you or organization are not being held liable for commentary deemed to be proprietary, copyrighted, defamatory, libellous or obscene.
- Please bring to management notice if you found any indecent comment / post about Organization in any form.
- Do not post offensive or disruptive messages including messages containing offensive comments gender, age, sexual orientation, pornography, religious or political belief etc

3. Internet / Network Usage

Internet has become primary system of the individual in day to day working However Internet has dark side as well so it must be used very carefully.

- The internet account must be used only for the purpose for which it is taken.
- It's the sole responsibility of the employee if he/she shares Internet account or laptop with any other person and misuse been observed.
- Use of Internet access for personal purpose, any un-solicited purpose, accessing the adult content, publishing / commenting on social media or any other external sites against org is strictly prohibited. Limited access is given to user as per management discretion.
- Don't attempt to open nonofficial, shopping & restricted sites.
- It is recommended not to download the heavy content during office time as it consumes lot of bandwidth which impact regular operation of other users.
- Contact IT-Support Engineer In case authorized Internet connection is not working.

4. Use of Email System

Email is “Must Have” system of any organization and being used by each employee in the organization. Company reserves the rights to monitor incoming and outgoing email or your mail box from any of the Mail ids without informing to the end user in the interest of Organization if required. Activities similar to mentioned below are strictly prohibited

- Sharing Organization data to Competitors or any other external agency / Domain without proper business objective and approval.
- Use of Id for personal work like Interview, CV Sharing, any other use which is purely in personal interest.
- Registering Mail id for personal use like; Community sites, Personal Site, Financial Sites and Adult Sites so on.
- Email system not be used for the creation or distribution of any offensive or disruptive messages including messages containing offensive comments gender, age, sexual orientation, pornography, religious or political belief etc. if any employees receives the email similar to this should immediately intimate to IT Department.
- Do not send email messages using another person’s email account.
- Do not disguise or attempt to disguise your identity when sending the email.
- The forwarding of chain letters, junk mails, jokes etc and executable is strictly forbidden.
- Avoid sending confidential information by email. If necessity , please ensure information is password protected in word or excel etc and inform the password to recipient by means of other communication method like phone.
- A prompt reply is to be given to all incoming mails in timely manner.

5. Use of Company IT System and Softwares

We have multiple IT system like ERP, CRM, and Various web system. Access to all these applications are given to Individual on need and role basis... Employee must strictly follow below mentioned guidelines.

- Access id and password must be kept confidentially. Any misuse by other person due to sharing ids and password will be sole responsibility of ID password holder.

- Any data from this system should not be shared with any other external agency / person in any form.
- User must monitor his usage in system; User must inform to IT if any unsolicited usage are Found
- Many authorization of the system like Salary slip, commercial info so on are given to employee as per need of his / her role. Employee must ensure that this information are being used strictly for official purpose.
- Any leakages of data, attempt to leakage is strictly prohibited.
- Employee is not permitted to delete Company data on the Laptop/desktop and maintain absolute Confidentiality about the data in total interest of the Company during tenure with the Company.

6. General Password Guidelines

Password is first security check. It is first line of defence for access of systems. Employee must maintain his password carefully. Following guidelines must be followed related to password. Everyone must use strong passwords with a minimum standard of:--

- At least six characters.
- Contain a mix of alpha and numeric, with at least one special character...
- More complex than a single word.
- Should not be any dictionary word.
- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password to access different company's information system or application.
- Users should change their password for every 6 months.

7. IT Equipment Handling

Company has provided IT asset to employee as per their Need / role like Laptop, Desktop, and Printer, Pen Drive or any other Storage Media so on. Company also installed IT equipment in Office for employee usage like Printer, Network devices, Scanning devices so on. Some IT equipment like Laptop is covered under Employee Laptop Policy.

- It is mandatory to the employee to handle IT equipment carefully. Take maximum precautions to avoid any physical or any kind of damages of these equipment.
- Authorized representatives can inspect Laptop, Desktop, Pen Drive or any other storage etc of Employee.
- Company representative can check its usage and data maintained at any time and the employee is required to readily submit this equipment for such inspections without hesitation...
- Misuse of the IT Equipment like visiting restricted sites, saving unauthorized data like songs / movies, unsolicited content etc. so on are strictly prohibited. Strict action will be initiated against employee if any such activities are found.
- Cost of repairs (spares +Service charges +any other charges) in case of damages in the company, Laptop, Desktop or any IT Equipment to be borne by concerned employee.
- In case of misplace / theft/ total damage due to mishandling of company laptop, Desktop or any IT Equipment; the cost to be paid back / settled by the employee will be decided by HR Department.
- Employee need to carry his / her Laptop or Tablet or Mobile Phone or allotted mobile IT equipment daily to the Office without fail and it should be strictly used for Official purpose in the interest of the organization's objectives and priorities.
- It is mandatory for the employee to deploy and adhere IT policies communicated and implemented by the IT time to time like Domain / Network policy, discipline of software installations defined by IT so on.
- Company has also provided data cards, Internet connectivity on Mobile Phone, Tablet so on... This connectivity strictly should be used for official purpose and as per management instruction issued time to time. HR Department has set usage and rent limit for such usage as per employee need and role which is published time to time to employee.
- It is sole responsibility of employee to use such connectivity as per usage limit and rent. Cost of any extra usage will be borne by employee.

- Return the company property while leaving the company on discharge / termination / resignation as per HR Department.
- Company encourage Green Environment and same applies to IT also... Employee must keep this in mind and according behave like—
 - Do not take print-out unless it is essential.
 - Take print on both the side of paper.
 - Switch off your Laptop, Desktop, and Printer when not in use and before leaving office strictly. So on.
 - Locking of devices, desktop & laptop when leaving the place for safety.

8. Intellectual property and Copyrights

- I-STAY HOUSING PVT LTD and its employees must respect the intellectual property rights of others and take care to protect and maintain its intellectual property.
- "Intellectual Property" includes creative works, the owners of which have legal rights to them and include copyrights, patents, trade secrets and trademarks. Violation can result in substantial liability and in some instances, may even be criminal in nature.
- Employee those are working in IT / ITES / R&D, Product Design, Industrial Design so on. must ensure any development done in company by them during their tenure in I-STAY HOUSING PVT LTD is not being taken while leaving and is not re-used in any form for any personal work or for any other external person or agency.
- Any misuse, whether inside the Company or outside, of the Corporate Logo, Channel Logos, Stationery formats etc., must be promptly reported to Legal.
- It is therefore very important that all I-STAY HOUSING PVT LTD personnel take care not only to protect our intellectual property rights, but also avoid violating the rights of others.

9. Disciplinary action

It is Mandatory to every employee for strict adherence of IT policies. The allegations of non compliance or reported violations with the Code of Conduct will be investigated whenever necessary and evaluated at proper level(s). Those found to be in violation of this Code of Conduct are subject to appropriate actions up to and including termination of employment / future

business with the company as per HR Department. Criminal misconduct may be referred to the appropriate legal authorities as per Law.

II. IT - EQUIPMENT POLICY

Contents

- 1. About Policy**
- 2. IT Equipment Eligibility (New User)**
 - a) Desktop**
 - b) Laptop**
 - c) Data Card**
 - d) Smart Devices**
- 3. Desktop Configuration**
- 4. Laptop Configuration (Company Paid)**
- 5. Laptop / Desktop Requirement Process (Existing User)**
- 6. Software Requirement Process (Existing User)**
- 7. User Data Backup & Security**
- 8. Data Card**
- 9. Smart Devices**
- 10. Printers Allocation**
- 11. Network Equipment**
- 12. Computer Usage & Operating Guidelines**

1. About Policy

IT Equipment Policy is designed to assist the Employees to understand the process to issue and use of the IT Equipment and comply with the business objectives even on field, and to access company application like Portals, Mails so on. Anywhere to comply with the work. In this policy it is also explained the Eligibility of getting IT Equipment as well as the approval process for getting the same issued to end user. All IT equipment / assets are recorded with proper tagging / stickers to maintain the record.

2. IT Equipment Eligibility (New User)

- a) **Desktop:** Any New Employee in Organization is Eligible getting Desktop if his Position requires. HR Department needs to send formal request “New Joinee Form” to I-STAY HOUSING PVT LTD - IT for issuing the desktop. HR Department has to mention that this desktop is being issued permanently to this Employee or on temporary basis. If temporary basis then they need to confirm approx number of days for using the desktop. For extension of the period user need to opt for additional approval from HR Department & I-STAY HOUSING PVT LTD - IT.
- b) **Laptop:** In our Organization Company Paid laptop is allowed as per management decision only. HR Department or HOD needs to give “IT Requisition Form” to I-STAY HOUSING PVT LTD – IT for issuing the Laptop to concerned employee. I-STAY HOUSING PVT LTD - IT will first issue laptop from Existing Stock if available. If Stock is not available then new laptop will be purchased with proper approval from management and issued to concerned user. New laptop Configuration will be same as per the I-STAY HOUSING PVT LTD – IT Policy.
- c) **Data Card:** As per management guidelines I-STAY HOUSING PVT LTD - IT will issue Data cards to concerned Employee on receipt of “IT Requisition Form” from HR Department.
- d) **Smart Devices:** As per management guidelines I-STAY HOUSING PVT LTD - IT will issue any Smart Devices like GPS/Handset/Tablet etc. to concerned Employee on receipt of “IT Requisition Form” from HR Department.
- e) **Accessories:** Any personal accessories brought for office use is to be inform to HR Department prior using.

3. Desktop Configuration

Minimum Configuration of Desktop:

Processor: Intel Corei3 /AMD

RAM: 8 GB

HDD: 1 TB

SCREEN: 18.5”

Warranty: 3 Yrs

OS: Microsoft Windows

Currently we are buying the entire desktop with above configuration only. Although we have old configuration desktop like Pentium 4 processor

with 1 GB or less Ram, 80 GB or less hard disk which is being used by Users. I-STAY HOUSING PVT LTD - IT keeps on replacing old Desktop machine which is hampering end users work on regular basis with approval of IT Head.

4. Laptop Configuration

Company Paid Laptop Minimum Configuration:

Processor: Intel Corei3 /AMD

RAM:8 GB

HDD: 1TB

Warranty: 1 Yrs

Screen Size: 15.6"

OS: Microsoft Windows

Currently we are buying all the Company paid laptops with above configuration only. Although we have old configuration laptops in working condition which is being either issued to user or kept in stock. Any Upgrade/downgrade in Configuration need to be approved from IT Head for purchasing the laptop.

As per policy only following software are allowed for I-STAY HOUSING PVT LTD Users on his Laptop /Desktop:

- a) Operating System: Windows
- b) Microsoft Office / Open Office
- c) Antivirus
- d) PDF Software Adobe Reader
- e) Google Chrome
- f) Zip Software 7 zip
- g) Adobe Flash Player Flash Player
- h) Remote Software Ultra Viewer
- i) Media Player VLC Media Player
- j) Java and other required plugins
- k) All I-STAY HOUSING PVT LTD Applications requires for business purpose

Note: This list will be updated time to time on requirement basis...

5. Laptop / Desktop Requirement Process (Existing User)

- The “IT Requisition Form” to be forwarded through HOD & HR Department to forward approved form to I-STAY HOUSING PVT LTD - IT for inspection of laptop / desktop Configuration. I-STAY HOUSING PVT LTD - IT will verify the details and return the form with their comment. Once the Configuration and other details is approved by IT and then send it to approval from management and if approved the process for Purchasing of Laptop / desktop.
- If Users Existing laptop / Desktop get damage (not repairable) / theft he needs to immediately inform HR Department / IT.
- Employee can ask a laptop / desktop on temp basis if his existing laptop is in repair or sent to service centre for repairing. HR Department has to approve the laptop / desktop request and forward to I-STAY HOUSING PVT LTD - IT.

6. Software Requirement Process (Existing User)

- If any User want to use any Software other than listed above in his/her laptop/desktop then he need to put that request to his Department Head/HOD.
- HOD need to study the justification of the requirement and if required then take approval from Respective Biz Unit Head with cost and forward it to IT for Installation of the same. IT will evaluate the need and accordingly installation will be done.
- Any violation/deviation from end user will lead to strict action from management. Users are advised to not add/remove any application from laptop/Desktop on his own.

7. User Data Backup & Security

- It is mandatory to the employee to handle the asset carefully. Take maximum precautions to avoid any physical damages to them.
- Employee is not permitted to delete the Company data on the Laptop/desktop and maintain absolute Confidentiality about the data in total interest of the Company during tenure with the Company.
- Authorized representatives can inspect the Laptop/Desktop, its usage and the data maintained at any time and the employee is required to readily submit the laptop/desktop for such inspections without hesitation.

- Misuse of the laptop/Desktop like visiting restricted sites, saving unauthorized data like songs/movies, unsolicited content etc. so on are strictly prohibited. Strict action will be initiated against employee if any such activities are found.
- In case of absconding of any employee HR Department need to impose the penalty and inform IT for block all the IT Equipment issued to him.

8. Data Card

- Data Card will be issued to user once the “IT Requisition Form” is duly filled by end user along with the approval from HOD & HR Department and submitted to IT. IT will issue the data cards to users as per management guidelines.
- While cessation concerned employee to submit the data card to IT along with “User Exit Form” failing which card will be discontinued and will intimate to HR Department for recovery of cost or any personal usage.
- Data card usage limit set while issuing the data card. Cost of any extra usage to be borne by employee.
- HR Department should ensure the deduction of extra usage from employee salary on monthly basis.
- HR Department will be deducted for reissuing New Data Card from Company in case of misplacement / damage of Existing Data Card. In case of misplacement - employee should immediately inform to IT to suspension of card to avoid any misuse however; employee will be responsible in case such misuse is being done. He has to bear the usage amount till the Data card is blocked from ISP END.
- In Case of misplacement / damage of Existing Data Card user can purchase blank data Card (without any monthly rental plan) from market on his own cost. In that case no recovery to be done for Hardware from Concerned Employee. Employee has to submit this working data card at the time of Exit.
- The employee should use the Data cards for official purposes only & in the interest of organization objectives & priorities. Employees are not allowed to use their data card in office... When Local Internet in offices is not working in that case same can be used.
- The Employee will be solely responsible for the upkeep/ maintenance and safe custody of the Data Card till his employment.
- The Employee will abide by all rules framed by the Company from time to time towards the usage of the Data Card.

- The Data Cards not to be used in any case for personal Internet Browsing. Any Violation in data card usages by end users will lead to strict action by management.

9. Smart Devices

- I-STAY HOUSING PVT LTD - IT Will issue the Smart Devices like GPS/Handset/Tablets etc. to Employees on the formal Approval of “IT Requisition Form” from HR Department as per business requirement. End Users need to take care of all the devices issued to them. Any damage or loss will be debited to concerned employee as per policy.
- In case of Lost/Damage of GPS/Handset or Other Smart Devices issued to user by Company deduction to be done from concerned employee as per Policy Published by HR Department. If device got damage out of warranty period employee to bear the cost of repairing +spares+ any other charges. Deduction to be done as per HR Department Policy from his F/F against tempered handset. Employee can carry the handset while separation in such cases with confirmation from HR Department.

10. Printers Allocation

- I-STAY HOUSING PVT LTD - IT has allocated sufficient Printers in order to facilitate users for their printing needs. Most of the locations have Company Owned printers.
- Common Printers is allotted in respective Corporate /Branches Units for printing purpose, if any user want separate printer he has to opt for approval of “IT Requisition Form” from HOD and HR Department respectively.

11. Network Equipment

Network Equipment is installed in all the Branches/Corporate Offices to facilitate end users with local Network Connectivity as well as Internet Connectivity. Although IT Engineers are responsible for maintaining the Devices but users need to ensure that no physical damage is being done to any of the devices. They need to support the respective IT support person to carry out any maintenance work to be done for the same.

12. Computer Usage & Operating Guidelines

- All users of the I-STAY HOUSING PVT LTD are allocated a unique username. The username is allocated when a person / staff is appointed.
- Most facilities of the I-STAY HOUSING PVT LTD that require authentication will use this username and password.
- Some facilities may have separate authentication methods and users of these systems may thus have separate usernames and passwords from their centrally provided credentials.
- User names should not be shared under any circumstances. Passwords should also be kept confidential and should not be divulged to anyone, not even IT staff.
- Users are responsible for all activity undertaken under their username and password including all material viewed, composed, sent and downloaded.
- Users are responsible for making sure any information stored locally on their desktop PC or a laptop is backed up on a regular basis. This is to ensure that in the event of a disk failure or accidental deletion of material that no vital data is lost.
- Users are advised to store important data/documents on their shared drive on a server if available.
- Users must take extra care when handling sensitive or confidential information, especially I-STAY HOUSING PVT LTD data & Users should avoid downloading such data to the hard drive of their PC. If this is necessary, then users should ensure that no unauthorised persons have access to the PC.
- Avoid copying data to portable devices such as pen -drives, laptops etc. If this is necessary then proper approval must be taken from their respected HOD. Local IT support staff can provide further advice and assistance.
- Avoid printing out such data and allowing the print out to be viewed by unauthorised persons.
- Printed data should be shredded or disposed of securely when it is no longer needed.
- Prevent unauthorised persons seeing the data when viewing it on screen.
- End users need to ensure cleanliness around the IT Equipment being issued or used by them.
- If any misuse of IT equipment's is observed, users should immediately inform to respective IT Support person. IT Engineer to take care of such

type of issues, if any regular misuse / mishandling of any IT equipment's like Printer/Scanners/observed they should immediately inform HR Department/HOD to take necessary action against concerned employee.

- Laptop/Desktop Users need to strictly follow the Hardware and Software compliance as per IT Policy.
- Any Change in compliance need to be approved first from IT, without IT approval no Hardware/Software can be changed in End Users laptop/Desktop.
- End Users to keep Antivirus application Updated. System scanning to be done at least once in a week. If any Virus alerts received immediately inform IT Engineer to get the issue resolved.
- End user to clean the temp files and unused file and folder from his respective laptop/desktop once in a month compulsorily to enhance the performance of the system.
- In case of Smart Devices user need to ensure not to connect the device with a machines having Virus infection that can cause the device OS or application malfunctioning. Always scan the devices for virus before connecting to any machine.
- It is recommended to get the Laptop Fully charged and then use still get completely drain. This cycle to be maintained to have best life of the batteries.
- User should always shut down their Laptop/Desktop/Monitor before leaving the office for the day to save energy and avoid damages in case of power failure this will save the energy as well as the device from any damage due to external power failure etc.
- Keep IT Equipment specially Network Devices/Smart Devices in cool place as these devices are very temperature sensitive. Excessive heat can damage the device or its components.

III. IT - EMAIL POLICY

Contents

- 1. About Policy**
- 2. About Product**
- 3. ID Creation/ Deletion/ Block/ Unblock**
- 4. Unused Mail ID Policy**
- 5. Email Quota Allocation and Traffic rule**
- 6. E-mail Password**
- 7. Group ids, Email Forwarding, Personal Emailing and Spam**
- 8. Global Address Book**
- 9. Mail Monitoring**
- 10.Outlook/ Webmail/ Blackberry/Smart Devices**
- 11.Operating Guidelines**

1. About Policy

The purpose of this policy is to ensure the proper use of Mail system and make users aware of what broader level guidelines and Rule to operate Mailing system. Amendments in this policy will be done as and when required basis.

2. About Product

We have installed below domains in our Mail Server as per business requirement.

Domain	:	I-stay.com
Webmail	:	www.gmail.com
IMAP Server:		imap.gmail.com
SMTP Server	:	smtp.gmail.com
Service Provider:		Google Inc.
Product	:	Corporate Mail
Infra	:	Shared Servers (Clustering)

3. ID Creation/ Deletion/ Block/ Unblock

- Respective HR Department representative will raise request for any addition, deletion, Block and unblock of id.
- All Mail ID Creation/Deletion Request need to register on mail communication will be entertained for said purpose. On receipt of Mail ID creation request it will be processed immediately. Mail ID creation request to be sent in proper format with all the correct details so on.
- I-STAY HOUSING PVT LTD - IT will not entertain any request for mail id creation other than the above said as approved by HR Department.
- Password reset request can be sent by End User other than HR Department, password reset can be done only on written request not on verbal communication.
- Common ID's can be created as per business requirement, respective HR Department representative as well as reporting manager of that particular user who is using common id's need to keep the track of such common id's to avoid any data leakages.
- In case Mail ID is not created within 12 working Hrs users can contact to below person for the escalation.

Sudesh Patil : support@itcaresolutions.in

4. Unused Mail ID Policy

- HR Department representative has to send request for Mail id deletion on Employee Exit/transfer. I-STAY HOUSING PVT LTD IT will also monitor the mail id's which is not been used since long. In coordination with HR Department those ids will be deleted.
- Mail Id's not being used for continuous 30 days will be Blocked / Disabled for period of seven days and then finally will be deleted if no request of activation.
- In case of User is on long leave due to any reason they need to intimate to HR Department and respective HR Department should forward the request to IT team for continuation of their mail id to avoid the deletion of mail ID.
- Once the ID is deleted then HR Department need to send fresh request for mail id creation as old id cannot be activated and any old mail data will not be provided to users in any case.

5. Email Quota Allocation and Traffic rule

- All IDs will be given a default quota of 15 GB.
- User to ensure sufficient free mail space to their id. If mail box is full up to 75% then inform IT team to increase the quota.
- Maximum number of recipients per message should not increase more than 100 recipients. If it is more, mails will bounce back.
- Ensure that mail size is less than 20 MB including message and Header. Bigger mail Size will lead into non-receipt of mail. One user can send a mail up to 20 MB as attachment if having limited text line in body of that mail. Similarly users cannot receive mails of having more than 25 MB size.

6. E-mail Password

- Password expiration duration: 90 Days. User need to change the password on regular interval to avoid Password expiry.
- User will be notified 3 days before the password is expired and will receive daily notification.
- Password Length: 6 to 16 Characters.
- Password Must Include: Letters and Numbers.
- When changing password last 3 passwords will not be accepted.
- Never share your password with anyone.
- Never Use password as any dictionary word.
- Don't keep password like pass@123, Abc@123, P@ssw0rd etc.

7. Group ids, Mass Mailing, Email Forwarding, Personal Emailing and Spamming

- Group ID: We can create a Group ID on mail server as per the business requirement. If any user or department wants to create a group id of a particular set of users then they need to take approval of HR Department for the same and forward the approval to IT. IT will evaluate and create in case of genuine requirement.
- Group Ids in mailing server will be available only for HOD's.
- Mass Mailing - Broadcasting of Mail to 50 users is not allowed as per policy. In case of Business requirement same should be routed through I-STAY HOUSING PVT LTD IT.
- Auto Email forwarding: Auto Email forwarding is disabled and this is to be routed through I-STAY HOUSING PVT LTD - IT.

- Personal Emailing & Spamming: Registering Mail id for personal use like. Community sites, Personal Site, Personal Messages, Greetings, Financial Sites and Adult Sites so on...is strictly prohibited. Strict action will be taken In case any such usages are found.

8. Global Address Book

- Existing Mail Server provides the facility of Global Address book which is updated once a month. All Mailing addresses are available on web mail with search facility.

9. Mail Monitoring

- Company reserves the rights to monitor incoming and outgoing email or your mail box from any of the Mail ids without informing to the end user in the interest of Organization if required.

10. Outlook/ Webmail/ Mobile/Smart Devices

- User can operate the Email through Outlook, Webmail, Blackberry & Any other Smart Devices.
- Outlook: IT-Engineer will create the Email account in Outlook express/Microsoft Outlook.
- Webmail : User can also access the Mails through web having URL : <http://www.gmail.com>
- Smart Devices: User can configure his Email in any of the Smart Devices like Smart Phones/Tablets etc...Using below settings of IMAP and SMTP Services.
- IMAP: imap.gmail.com & SMTP smtp.gmail.com

11. Operating Guidelines

- Ensure that your Mail password is not common like blank, or pass123, welcome so on... Do not Share your password with anyone.
- Delete junk mails from the inbox regularly.
- Do proper logout before closing system.
- Use Proper Signature in Email like your Name, Company Name, Logo and address, Job Function, Telephone and Mobile Number, Website and Corporate Slogan.

- Do not “Reply All” the mails. This leads into unwanted email traffic which slows the performance. Send the mail to only relevant people.
- Write well structured emails and use short, descriptive subjects.
- Do not access streaming sites or any other un-official sites and put official email id on the same.
- Better to send the attachment in zip format.
- Do not forward any personal message to others using official mail id.
- Don’t do mass mailing unnecessarily.
- Never publish official mail id to social networking sites.
- End Users not to share their mail id password with other users, failing to which will lead into strict disciplinary action against them.

IV. IT - SUPPORT POLICY

Contents

- 1. About Policy**
- 2. IT Support Request by User**
- 3. IT Support**
- 4. Software Requirement : Additional to Policy**
- 5. Preventive Maintenance**
- 6. Installation and Repair**
- 7. Support During Meeting and Conferences**
- 8. Blackberry & GPRS Mail**
- 9. IT Support Escalation Matrix**
- 10.IT Equipment Handling**

1. About Policy

The purpose of this policy is to ensure the proper IT support to all I-STAY HOUSING PVT LTD users. Detailed IT ENGINEER support as well as the IT Escalation Point for Infra & System is also provide in below policy. Amendments in this policy will be done as and when required basis.

2. IT Support

- I-STAY HOUSING PVT LTD - IT has deputed dedicated consultants for the IT support services.

- The IT Consultants including the Consultants for the installed software support will be responsible for providing below Support to end users:
 - a) All IT Support related Issues like Hardware issues, Software issues, Network connectivity, Coordination for implementation of Projects etc.
 - b) End user Communication on IT Matters.
 - c) Vendor Coordination for IT Matters.
 - d) Training to the end User on basic computer operation. So on...

3. Preventive Maintenance

- The IT Consultants has to make fix visit schedule for the head office as well as the site offices once in a week.
- All preventive Maintenance Should be completed quarterly basis.
- During the Preventive maintenance schedule of any particular branch every the IT Consultants need to cover following points in order to finish the said activity:
 - a) Proper Backup of All Networking Equipments like, Routers /Access points etc.
 - b) Monitoring of Dust Cleaning of All Network Equipment done by Housekeeping.
 - c) Monitoring of Dust Cleaning of All Laptop/ Desktop/Printer done by Housekeeping.
 - d) Network Rack dressing.
 - e) Earthing Check-up.
 - f) Formal Intimation will be given via email for maintenance by IT Department

4. Installation & Repair

- The IT Consultants will make sure all efforts have been taken to resolve all IT Issues to maximum possible extend and satisfaction however; any HW issue which cannot be repaired by The IT Consultants to be get resolved from local vendor with least quotation with prior approval from Biz Unit Head.
- Infra/Network Backup: IT ENGINEER has to take proper backup of Routers config, modem and other IT equipments every 30 days. This is part of preventive maintenance activity as well so that if that equipment goes down new equipment can be made up using the old backup of earlier working device.

5. Support during Meeting and Conference

- The IT Consultants has to ensure the proper connectivity and availability of IT facility to every meeting and conference as per business requirement. If equipments not available like projector/screen they need to arrange the on approval of respective HOD.

6. Mobile/GPRS Email

- Any personal Smart phone /GPRS Handset HW part is not under responsibility of The IT Consultants.
- User need to coordinate with Service Centre and get it repaired in case of failure.

7. IT Support Escalation Matrix for End User

Below is the Escalation Matrix for I-STAY HOUSING PVT LTD Employees in case of any pending issue which is not getting solved by the IT Consultants within 24 hrs can be escalated to next level as per the priority of the issue. I-STAY HOUSING PVT LTD - IT will ensure to solve the issue as soon as possible. Escalation Matrix for Infra related Issue:

Level 1

Name: IT Dept (Sudesh Patil))

Email:info@i-stay.com

8. IT Equipment Handling

- All IT Consultants are requested to maintain the working condition of IT Equipments issued to them or installed in Office premises. Any mishandling of IT equipments lead into strict action by management against the user and repairing/replacement cost will be debited from the concerned.
- Desktop/Laptop/Printer etc...IT Equipments need to be kept neat and clean. Power Condition and Earthling need to be checked on regular interval to avoid any damage to IT Equipments.

V. IT - INTERNET POLICY

Contents

1. About Policy
2. Types of Users
3. General User
4. CFS Policy
5. Do's & Don't
6. Internet Access Form

1. About Policy

The purpose of this policy is to ensure the proper use of Internet connectivity and guidelines and process to get the Internet Access to end users. This Policy is applicable for ALL I-STAY HOUSING PVT LTD Users including Sales, Service, Manufacturing so on... Amendments in this policy will be done as and when required basis as per business requirement.

2. Types of Users

- a) **Users:** These are common users those don't require much of the Internet access to perform their day to day job. Access of Default sites like erp.aorealty.com will be given without restrictions
- b) **HOD Users:** These are departmental Head who need specific categories of the websites...
 - Regular audit of Access will be done and result will be recorded.
 - Access to the category will be given as per the Web Filter policy.
- c) **Department / Specific Group:** These are the functional users who need specific websites to perform their day to day job... Like HR Department will have access of Job Portal, Finance will have access of banking site so on...

- d) **Other Group:** Any other users those don't fit into above category will be covered in this group... These users must give Proper Business Justification from HOD.

3. Web Filter Policy:

Below CFS policy for Internet is applicable in Head Office / Branch Offices. This CFS Policy is designed to cater the extra Internet Use of specific Department.

Web Filter Policy for Different Functions:

Name\Group	User	User+Gmail	HOD	HR
I-STAY HOUSING PVT LTDA	A	A	A	A
Gmail	F	A	A	A
Activex	F	F	F	F
AdultContent	F	F	F	F
Advertisements	A	A	A	A
AlcoholandTobacco	F	F	F	F
Applets	F	F	F	F
ArtsAndHistory	A	A	A	A
Astrology	F	F	F	F
AudioSearch	F	F	A	F
Blogs	A	A	A	A
BusinessAndEcoFmy	A	A	A	A
Chat	F	F	A	F
CommercialBanks	A	A	A	A
Communication	A	A	A	A
ComputerSecurity	F	F	F	F
Cookies	A	A	A	A
Cricket	F	F	F	F
CrimeandSuicide	A	A	A	A
CulturalInstitutions	A	A	A	A
DatingAndMatrimonials	F	F	F	F
DownloadFreewareAndShareware	F	F	F	F
Drugs	F	F	F	F
EducationAndReferenceMaterial	A	A	A	A
EducationalInstitutions	A	A	A	A
Electronics	A	A	A	A

Entertainment	F	A	A	A
FashionAndBeauty	F	F	A	F
Finance	A	A	A	A
Gambling	F	F	F	F
Games	F	F	F	F
Government	A	A	A	A
HTTPUpload	F	F	F	F
Hacking	F	F	F	F
HateAndRacism	F	F	F	F
HealthAndMedicines	A	A	A	A
HobbiesandRecreation	A	A	A	A
Homosexuality	F	F	F	F
HumanRightsAndLiberty	A	A	A	A
HumorComics	F	F	A	F
IPAddress	A	A	A	A
ISPWebHosting	F	F	A	F
IllegalUnethical	F	F	F	F
ImageBanks	A	A	A	A
ImageSearch	A	A	A	A
InformationTechFlogy	A	A	A	A
InstantMessaging	F	F	F	F
InternetRadioTV	F	F	F	F
InternetTelephony	F	F	F	F
JobsSearch	F	F	F	A
Kids	F	F	F	F
LegalOrganizations	A	A	A	A
MilitancyandExtremist	F	F	F	F
MobileEntertainment	F	F	F	F
Music	F	F	F	F
NatureAndWildLife	A	A	A	A
NewsAndMedia	A	A	A	A
FnGovernmentOrganizations	A	A	A	A
Fne	A	A	A	A
Nudity	F	F	F	F
P2P	F	F	F	F
ParkedDomain	F	F	F	F
PersonalAndBiographySites	F	F	F	F
PersonalStorage	F	F	A	F
PhishingandFraud	F	F	F	F

PhotoGalleries	F	F	A	F
Plagiarism	F	F	F	F
PoliticalOrganization	A	A	A	A
Porn	F	F	F	F
Portals	A	A	A	A
PropertyAndRealEstate	A	A	A	A
SPAMURL	F	F	F	F
Science	A	A	A	A
SearchEngines	A	A	A	A
SexHealthAndEducation	F	F	F	F
SharesAndStockMarket	F	F	F	F
Shopping	A	A	A	A
SocialNetworking	F	F	A	A
SocietyAndCulture	A	A	A	A
Spirituality	F	F	F	F
Sports	F	F	F	F
Spyware	F	F	F	F
SwimwearAndLingerie	F	F	F	F
TravelFoodAndImmigration	A	A	A	A
URLTranslationSites	F	F	F	F
Vehicles	A	A	A	A
VideoSearch	A	A	A	A
Violence	F	F	F	F
Weapons	F	F	F	F
WebBasedEmail	F	F	A	A

Note:

F= Forbidden

A= Allowed

4. DO'S & DON'T

- The internet account must be used only for the purpose for which it is taken.
- It's the sole responsibility of the applicant if he/she shares the Internet account or laptop with any other person and misuse been observed...
- Use of Internet access for personal purpose, any un-solicited purpose, accessing the adult content, publishing / commenting on social media or

any other external sites against org is strictly prohibited. Strict action will be initiated in case of any such usage are reported.

- Please check for Trojan's / Spyware in your computer from time to time. You may take help of IT Engineer.
- Don't attempt to open nonofficial & restricted sites.
- It is recommended not to download the heavy content during office time as it consumes lot of bandwidth which impact regular operation of other users.
- Contact IT-Support Engineer In case authorized Internet connection is not working.

***Any violation in above will lead into the block of internet access and strict disciplinary action against the concerned user as per HR department discretion.**

VI. IT - DATA ACCESS & SECURITY POLICY

Contents

- 1. About Policy**
- 2. Data classification**
- 3. Access to information**
- 4. Responsibilities**
- 5. Using personally owned devices**
- 6. Information on desks, screens and printers**
- 7. Exchanges of information**
- 8. Reporting losses**

1. About Policy

This policy defines the data management environment and assigned roles and responsibilities for protecting I-STAY HOUSING PVT LTD non-public information from unauthorized access, disclosure, or misuse. It is the responsibility of every I-STAY HOUSING PVT LTD employee who accesses non-public data and information to secure and protect that data. This policy is also designed to establish processes for ensuring the security and confidentiality of confidential information and

to establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information.

Such confidential information can be in any form including on printed media (e.g., forms, reports, memoranda, correspondence, microfilm, microfiche, books), computers, networks, magnetic or optical storage media (e.g., hard drive, zip drive, flash drive, memory card, diskette, tape, CD, DVD), physical storage environments (e.g., offices, filing cabinets, drawers), or in a person's memory.

2. Data classification

- a) **Public Data** – available to any member of the I-STAY HOUSING PVT LTD without restriction.
- b) **Open Data** – available to any authenticated member of the I-STAY HOUSING PVT LTD.
- c) **Confidential Data** – available only to specific I-STAY HOUSING PVT LTD members, with appropriate authorisation.
- d) **Strictly Confidential** – available to only a very small number of I-STAY HOUSING PVT LTD members.

3. Access to information

Members of the I-STAY HOUSING PVT LTD will be granted access to the information they need in order to fulfil their roles within the company. Members who have been granted access must not pass on information to others unless the others have also been granted access through appropriate authorisation.

The below responsibilities and obligations under this Policy shall survive the termination of employment with I-STAY HOUSING PVT LTD.

4. Responsibilities

a) General Principles

- All confidential information gathered and maintained by employees in the course of their duties and responsibilities for I-STAY HOUSING PVT LTD is considered company information and, as such, must be used, maintained and

handled by employees as specified by and consistent with the authorization and in a manner that appropriately safeguards and secures such confidential information.

- All confidential information in electronic media must reside and be stored on the network servers of I-STAY HOUSING PVT LTD, and not on local work stations, personal computers, laptops, flash drives, etc.
- All confidential information in print or paper media must be stored in file cabinets that are secured and locked.
- All confidential information containing company identifiable information must be accessed and used only by authorized employees of I-STAY HOUSING PVT LTD. Such confidential information shall be used for limited legitimate purposes.
- Such confidential information containing company identifiable information shall not be copied, stored, transferred, altered, destroyed or disclosed in any manner / form including on printed media (e.g., forms, reports, memoranda, correspondence, microfilm, microfiche, books), computers, networks, magnetic or optical storage media (e.g., hard drive, zip drive, flash drive, memory card, diskette, tape, CD, DVD), physical storage environments (e.g., offices, filing cabinets, drawers), or in a person's memory.
- Employees who are authorized to access and use such confidential information shall take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed in order to protect the confidentiality of such confidential information.
- All users of computers shall be responsible for adhering to all policies, standards and procedures for the use of information resources, including implementing security practices necessary to protect confidential data and information. Such computer users shall not access, acquire, use, copy, transfer or maintain confidential information on a personal computer and shall be held accountable for any loss or unauthorized disclosure of confidential information which is not on the I-STAY HOUSING PVT LTD's network servers.

b) Responsibilities of Authorized Users of Confidential Information

- Each authorized user of confidential information is responsible for understanding and complying with this Policy. Each authorized user accepts responsibility for the following:
 - i. Access only the information authorized and reasonably necessary to perform his/her duties as an employee of I-STAY HOUSING PVT LTD.
 - ii. Maintain, use and handle confidential information consistent with the principles and guidelines set forth in this Policy.
 - iii. Take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
 - iv. Safeguard the confidentiality of any security controls and passwords, e.g. physical key, ID card or computer/network account that allows access to confidential information.
 - v. Report any suspected activities that may compromise confidential information to his/her immediate supervisor, department head, Information Services or Director.

c) Responsibilities of HOD and Supervisors of Authorized Users of Confidential Information

- Department Heads and Supervisors are responsible for establishing and maintaining security for confidential information within their areas of responsibility consistent with this Policy including the following:
 - i. Require that only authorized users have access to confidential information and that he/she understands this Policy and his/her responsibilities in the handling of such information and materials.

- ii. Identify confidential information and materials and implementing adequate controls to secure confidential data and information.
- iii. Protect against the unauthorized disclosure of confidential information.

5. Using personally owned devices

- Company Data subject to the Data Protection Act must not be stored on personally owned devices. Data classified as sensitive under the Data Protection Act must neither be stored on nor processed using personally owned devices i.e., computers, networks, magnetic or optical storage media (e.g., hard drive, zip drive, flash drive, memory card, diskette, tape, CD, DVD).
- Personally owned devices should not be used for the storage or processing of any other information classified as strictly confidential or above without the explicit written permission of the I-STAY HOUSING PVT LTD.
- Appropriate security measures must be taken when using personally owned devices to process or store any company data.

6. Information on desks, screens and printers

- Members of staff who handle confidential paper documents should take appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.
- Care should also be taken when printing confidential documents to prevent unauthorised disclosure.
- Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended.

7. Exchanges of information

- Whenever significant amounts of confidential information are exchanged with other organisations, appropriate information security measures must be established to ensure the integrity and confidentiality of the data transferred. Regular exchanges must be covered by a formal written agreement with the third party.
- Information classified as strictly confidential may only be exchanged electronically both within the company and in exchanges with third parties if the information is strongly encrypted prior to exchange. Information classified as secret may not be transmitted electronically except with the explicit written permission of the information from I-STAY HOUSING PVT LTD.
- When exchanging information by email or fax, recipient addresses should be checked carefully prior to transmission.
- Unsolicited emails, faxes, telephone calls, instant messages or any other communication requesting information which is not classified as public should not be acted upon until and unless the authenticity and validity of the communication has been verified.
- Members of the I-STAY HOUSING PVT LTD must not disclose nor copy any information classified as confidential or above unless they are authorised to do so.

8. Reporting losses

- All members of the I-STAY HOUSING PVT LTD have a duty to report the loss, suspected loss or unauthorised disclosure of any Company information asset to IT or HR Department.

VII. IT - Backup Policy & Disaster Recovery

Contents

- 1. About Policy**
- 2. Backup Content**
- 3. Backup Schedule**
- 4. Data Restore**
- 5. Disaster recovery**

1. About Policy

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 Users. Information Technology recognizes that the backup and maintenance of data for servers are critical to the viability and operations of the respective departments. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

2. Backup Content

The 'data' backups covers all systems & servers managed by the IT department. Data held and managed locally in departments is excluded unless departments have entered into specific arrangements with IT. All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data must be stored on the network drives provided.

3. Backup Schedule

The service and hence this policy has been designed and implemented with disaster recovery/business continuity (i.e. the ability to recover recent live data in the event of a partial or total loss of data) as key deliverable and is not therefore designed as a method of archiving material for extended periods of time.

Below is the Backup Plan of I-Stay Housing Pvt Ltd.

Sr. No.	Server	Description	Type	Time
1	File Server	Backup of User Folder in C Drive	Append Backup	Daily
2	ERP App Server	Test DB Backup (FARVISIONDB_R2_Live & FARVISIONDB)	Full Backup	Daily
3	ERP DB Server	Live DB Backup (FARVISIONDB_R2_Live & FARVISIONDB)	Full Backup	Daily
5	ERP Server	Farvision Application Folder Backup	Full Backup	Daily

4. Data Restore

- Data is available for restore within a few minutes of a backup job completing on the daily schedule.
- Data will be available during the retention policy of each backup job – which is currently defined as 3 months.
- Recent data is available from this system on completion of the daily backup jobs, which means that there is potential data loss during a working day on some systems. The IT systems at RHUL have been specified to minimise data loss between backup windows by having elements of system redundancy.
- Requests for data recovery should be submitted to the IT Service desk.

5. Disaster recovery

- Currently in I-Stay Housing Pvt Ltd we are following Manual system of Disaster recovery where we take manual backup of All Databases

includes ERP, Tally etc. to an External HDD on fortnightly basis & keep at the safe location, as per management discretion.

- Other user data we take on NAS hard drive which is also detachable Device can be delink from the network immediately & take it away from the premises anytime.
- IT Department will be looking for the automated system of disaster recovery in new future.

VIII.

IX. IT - Induction & Training Policy

Contents

- 1. About Policy**
- 2. Induction & Training Program**

1. About Policy

Training helps in capacity and skill building of human resources and enables employees to achieve the organizational goals. Training also helps in inculcating a sense of teamwork and inter-team collaborations. The competence, skills and attitude of the employees have a great bearing on the quality of their output. Increased knowledge and skill set makes employees more productive in their workplace and thus enhance value in the organization in terms of efficiency. Training is one of the most effective and tested tools for performance enhancement. The IT Consultants has been providing IT training specific to the needs of the departments. The IT Consultants have been catering to the requirements of the departments in organizing tailor-made capacity building programs to develop IT skills of the employees to efficiently implement the IT projects. It is not only the capacity building of the departments but also upgradation of technical skills of the employees of the department.

2. Induction & Training Program

- As New User Joins after confirmation from HR Department, It Consultants provide them IT Induction & Necessary Training as per the Systems & Software in the organization.

- IT Induction Includes the IT Policy for Users about usage of IT Equipment, Software & Systems.
- Induction explains about the handling of Company Data & IT Assets.
- After accepting the IT Asset, User has to give his/her acceptance on IT Acceptance form with his feedback about the IT Staff.
- Over & Above the IT Induction, Necessary Training as per the Department/Function will be given to New User in I-Stay Housing Pvt Ltd ERP System.
- In depth Training on the go with actual work will be given with the Department Key User & IT Staff to New IT/ERP User.
- New IT User has to read the SOP & Understand the process of their respective module to understand the flow of Data & Processes already going on in I-Stay Housing Pvt Ltd ERP system.
- ERP Key user can explain the actual process in the Department/Function with the help of IT staff to new joinee.

IT - Maintenance & Repair Policy

Contents

- 1. About Policy**
- 2. Operational Definitions**
- 3. Planned System Maintenance**
- 4. Emergency or External System Maintenance**
- 5. Procedure for Repair or Replacement**

1. About Policy

IT Department is committed to ensuring reliable information technology services. In order to meet this objective, I-Stay Housing Pvt Ltd systems may need to be taken offline to maintain or improve system performance, safeguard data, or to respond to emergency situations. The goal of this policy is to explain those circumstances during which down time may occur, anticipated durations of down time events, and procedures for notifying affected users. This policy applies to I-Stay Housing Pvt Ltd hosted and run systems and services. Many services are also dependent on vendors and service providers that are outside the I-Stay Housing Pvt Ltd's control, and those specific dependencies are defined in each Service

Commitment. Planned down time is defined as periods when the system or service is or will be unavailable to the intended audience.

2. Operational Definitions

- Scheduled maintenance that occurs in the standard maintenance window will be announced at least 1 business day in advance
- Scheduled maintenance that occurs outside the standard maintenance window will be announced at least 1 week in advance
- **Change event:** A requested change that could potentially cause down time for Company production services.
- **Down time:** Periods when the system or service is or will be unavailable to its intended audience during the service's availability window.
- **Maintenance window:** Period of time during which system maintenance is expected to occur.
- **Service commitment:** Definition of how IT will support a particular service. Includes a description, the availability and maintenance windows, directions for reporting a problem, a description of the intended user, and definitions of prerequisites for using the service, dependencies on other services, and names and contact information for the service owner.
- **System maintenance:** Any change event that affects production systems or services, regardless of whether down time is expected or not.
- System maintenance occurs entirely during a maintenance window Time: 8:30AM to 10:00AM and there may or may not be down time during all or part of the maintenance window.

3. Planned System Maintenance

- From time to time, it will be necessary to make systems unavailable for the purpose of performing upgrades, maintenance, or housekeeping tasks. The goal of these tasks is to ensure maximum system performance and prevent future system failures. The following activities fall within the definition of planned system maintenance:
 - a) Application of patches to operating systems and other applications in order to fix vulnerabilities and bugs, add functionality, or improve performance.

- b) Monitoring and checking of system logs.
 - c) Security monitoring and auditing.
 - d) Required upgrades to system physical memory or storage capacity.
 - e) Installation or upgrade of applications or services.
 - f) System performance tuning.
 - g) Regular backup of system data for the purpose of disaster recovery.
- In the event that any of these activities will require down time to perform, every effort will be made to perform the procedure during off-hours in order to minimize the impact on those who use the affected systems or services. The following time periods will be used to carry out system maintenance activities: 8:30AM to 10:00AM
 - On occasion, it may be necessary to have system maintenance during regular business hours, especially if outside personnel are required to perform more elaborate procedures. Also, some changes to production systems are better performed outside the standard maintenance windows, due to availability of staff for testing and troubleshooting and other factors. If this is the case, then this maintenance window will be defined between IT and service owners of affected resources, using the Notification of System Maintenance mechanism described below.

4. Emergency or External System Maintenance

- Unexpected circumstances may arise where systems or services will be interrupted without prior notice. Every effort will be made to avoid such circumstances. However, incidences may arise involving a compromise of system security, the potential for damage to equipment or data, or emergency repairs. If the affected system(s) cannot be brought back online within 30 minutes, affected users will be contacted.

5. Procedure for Repair or Replacement

- If a computer system or related piece of equipment needs repair, IT department Consultants shall make the necessary repairs if possible.

- If IT department Consultants are unable to repair their computer systems, Outsourced Computer Services is called.
- Outsourced Computer Services returns the call to the problem site as soon as possible. The expected response time is four hours or less.
- Simple repairs: If the problem is simple, the equipment is repaired in premises or site.
- Parts required: If parts are required, the equipment is repaired in premises or site within 24 hours.
- Major repairs: If the repair problem is a major one and the equipment is expected to be down for longer than 24 hours, Computer Services provides a loaner (if available) and takes the equipment to the Maintenance Centre. Departments may lose data on their hard drives during repairs, in such case old data backup as per Backup Policy is restored.
- When Computer Services is unable to repair the equipment, it is sent to an authorized service centre and returned to the appropriate user.

X. IT - Replacement & Upgrade Policy

Contents

- 1. About Policy**
- 2. Roles & Responsibilities**
- 3. Replacement Timeframe**
- 4. Emergency or External System Maintenance**
- 5. Procedure for Repair or Replacement**

1. About Policy

Adequate computer and network hardware and software are essential to the delivery of instruction, learning, research and creative activities, and to the efficient and effective management of the company. Rapid changes in technology require that a well-managed company have a systematic plan for upgrading and replacing technology to ensure that it offers access to the most basic services.

This Policy applies to all I-Stay Housing Pvt Ltd owned workstations, laptop computers, desktop peripherals (printers, scanners, projectors, and interactive whiteboards), network hardware (servers, switches, routers,

bridges, and other key network devices), cable plant and physical infrastructure, and licensed software (Microsoft Operating System, Microsoft Office Suite, and any business specific applications) running on those devices.

2. Roles & Responsibilities

- Administration/Department Heads - Each department head is responsible for identifying any exceptions (earlier or delayed replacements/upgrades) necessary to ensure an employee can effectively perform his/her job duties. The Head of Department over the reporting line is responsible for reviewing and approving requested exceptions and divisional budgets.
- IT Department – This group is responsible for generating and monitoring inventories, budgeting for replacements and upgrades and executing equipment replacements and upgrades to business specific software according to the replacement cycle. This group also makes technical decisions on equipment and software standards and upgrades and replacements based on industry trends, software development cycles, costs and risks to systems stability.

3. Replacement Timeframe

- IT Department will maintain modern computer and network hardware and software capable of supporting its business activities. To accomplish this, technology hardware will be budgeted for replacement with management discretion through the IT budget and replaced and upgraded according to the schedule below:

Category	Description	Replacement Timeframe
High-performance Servers	This category encompasses all high-performance and high-use servers. These servers perform mission critical activities and/or provide access to critical services on a daily basis.	Fiscal year immediately after 3rd year of use
Laptop Computers	This category encompasses all laptop systems and includes all associated docking stations and monitors as a single unit.	Fiscal year immediately after 4th year

		of use
Workstation Computers	This category encompasses all desktop computer systems and includes the CPU and monitor as a single combined unit.	Fiscal year immediately after 5th year of use
General Use Servers	This category encompasses all servers not classified as "high-performance". These servers provide mission-essential services and perform activities supporting the academic, service and business goals of the institution.	Fiscal year immediately after 5th year of use
Network Hardware	Network hardware includes repeaters, routers, switches, bridges, access points and other communication devices.	Fiscal year immediately after 5th year of use
Desktop Peripherals	Desktop peripherals include printers, scanners, projectors, and interactive whiteboards.	Fiscal year immediately after 7th year of use
Cable Plant and Physical Infrastructure	The copper and fibre optic wires that connect data/information stations together and comprise the network infrastructure are the components identified in this last category.	Fiscal year immediately after 10th year of use

- If a hardware item is determined to be irreparable by IT or if the cost to repair exceeds the current market value of the item, the item may be replaced earlier than indicated in the table above with all costs for replacement covered by the I-Stay Housing Pvt Ltd IT budget.
- If a department elects to replace an item earlier than the identified replacement cycle, both the company budget and department head over the reporting line must approve the request and the IT department assumes all costs for replacing the item.
- Software Upgrades: Related to software, all systems should be running the current version or most recent prior (current -1) version of manufacturer-released software packages. If a I-Stay Housing Pvt Ltd owned system is found to be running an older version (current -2 or older) of any company-wide software package (Microsoft Operating System, Microsoft Office Suite, and any business specific

applications), it will be upgraded to the most recent version as soon as possible.

- Replacement Requirements: All replacements will adhere to a single standard for each equipment type. Departments must surrender a like device (computer, peripheral, etc.) for each device replaced. Departments may not repurpose existing devices to expand the number of technology devices supported. All enhancements to or changes from the standard resulting in a cost-higher than that of the standard will be added to the requesting department's budget.
- If a department keeps or maintains any special-purpose software or peripherals, they must be compatible with the new equipment and all company-wide software packages. Otherwise, the department is required to purchase the software or peripheral upgrade.