IT POLICY FOR EMPLOYEE

1. Applicability

This Policy applies to everyone who accesses SUAS resources, whether a part of SUAS or not, whether on campus or from remote locations. By accessing SUAS resources, the user of the resources agrees to comply with this Policy. This policy is thus applicable to the following users / individuals / entities, on or off SUAS campus –

2. Eligibility

- **Laptops:**
  - **Faculty:** Associate Professors, and Professors/Dean/Director/VC
  - **Non-Teaching Staff:** Managers and above.
- **Notebooks:**
  - **Faculty:** Assistant Professor
- **Desktop**: - Non-teaching below Manager Level. (Depends upon nature of work)
- **Emergency Allocation:**
  - Non-teaching staff of grades below manager may receive laptops or notebooks based on job priority, upon approval from their reporting authority in case of an emergency.

3. Usage Guidelines

- All provided laptops, desktops and notebooks are university property and should be used primarily for academic and administrative purposes.
- Users are responsible for maintaining the equipment in good condition.

4. Damage and Repair Costs of Laptop and Notebook

1. **Reporting Damage:**
   - Any damage, malfunction, or loss of equipment must be reported to the IT department immediately.
2. **Minor Damage:**
   - **Examples:** Screen scratches and touch pad (external/ peripheral device)
   - **Cost:** The University will cover costs for minor repairs.
3. **Major Damage:**
   - **Examples:** Broken screens, broken hinch, Damage of Keyboard, Liquid damage and damage of cabinet (external/ peripheral device).
   - **Cost:** Faculty and staff are responsible for repair or replacement costs for major damage after confirmation of the cost by the IT department.
   - **Procedure:** The IT department will assess and confirm the cost. Users will be informed of the cost before any repair or replacement is undertaken.

5. Damage and Repair Costs of Desktop: Cost Responsibility:

- **User Negligence**: If damage is deemed to be caused by user negligence or misuse (e.g., spilling liquid, physical damage), the user may be responsible for repair or replacement costs.
- **Cost Calculation**: IT Support will provide an estimate of repair or replacement costs.

- **Payment**: The user will be notified of the cost and payment procedure. Costs will be deducted from the user's paycheck or invoiced as per company policy.

4. **Replacement Costs:**
   - **Laptops /Desktops and Notebooks:** In cases of loss or irreparable damage due to negligence, users may be required to cover the cost of replacement.

6. Return of Equipment

- All issued equipment must be returned to the IT department upon resignation, retirement, or termination of employment.
- Failure to return equipment may result in a deduction of the replacement cost from any pending dues or salary. (HR should not release the salary without confirmation from IT department)

7. Essential Guidelines for User:

A. Usage of Institute Systems / Computers / Laptops and /or Information / Data.

1) SUAS provides the Personal computers, Laptops, Internet, Electronic mail and other communication/processing devices to the above listed stakeholders for business purposes only. SUAS is the sole owner of all the data/information and SUAS may access, disclose all data or messages stored on its systems or sent over its electronic mail system.
2) Wherever desktop/laptop is required, HR will send a new user login form to IT dept. IT dept. will create a login ID and email ID for the new joinee as per the IT GUIDELINES defined for the purpose. IT GUIDELINES 's for Laptop allocation and User creation and resource allocation are already defined for the purpose.
3) The users are not authorized to retrieve or read any e-mail messages that are not sent to them and cannot use a password, access a file, or retrieve any stored information unless authorized to do so.
4) SUAS reserves the right to monitor communications and data at any time, with or without notice, to ensure that the Institute property is being used only for business purposes and to ensure that the use of the said property is not compromised in any manner.
5) SUAS also reserves the right to disclose the contents of messages for any purpose at its sole discretion. No monitoring or disclosure will occur without the direction of SUAS Senior Management, unless otherwise noted.
6) SUAS holds every right to retain the electronic data, information or any file or folder downloaded, copied or extracted by the employees at any time during the course of employment.
7) SUAS also holds the right to use such a retained data, information or file or folder downloaded, copied or extracted by the employee as an evidence against the employee.
8) Before a user accesses the facilities or computer resources of SUAS, a notice will be displayed that warns against unauthorized use of the IT resources or system.
9) All the new joinees will be trained with the IT procedures, security policies, and its implementation either by HR department or by the concerned Department Head.
10) All the users are required to log a support ticket using the Helpdesk portal for any kind of support required from the IT dept. IT GUIDELINES for Using the Helpdesk portal for Support already defined for the purpose, will be followed.
11) IT dept. will perform maintenance of desktops, printers, servers, etc. as per their predefined

schedule. IT GUIDELINES for Maintenance including Monitoring and Control processes, already defined for the purpose, will be followed.

B. Usage of Electronic Mail

1) SUAS will provide e-mail IDs to individuals who are authorized to carry out internal and external communications and are designated on a particular job position based on their roles and responsibilities. Such named or role specific generic email ids will be assigned to the said stakeholders which will be used for all internal and external communications.
2) The E-mail system is allowed to be accessed by the stakeholders within SUAS premises only. In special cases, designated stakeholders may be provided external access to the email system, with prior permission and approval of Senior Management.
3) Access to email using personal mobile devices is not permitted unless authorized and approved by Senior Management.
4) Group email-ids may be created for operational convenience. Similarly function specific email-ids may be created for official response and necessary actions. SUAS HR Department shall ensure that such an email account is inactive when an individual separate from SUAS.
5) Users should note that any data and information on the system will not be deemed personal or private. In addition, the e-mail system may not be used to send or receive copyrighted materials, confidential information related to SUAS and its students, proprietary financial information, or similar materials without prior authorization and approvals.
6) The e-mail system is not to be used to solicit for personal gains, commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations. The system is not to be used to create any offensive or disruptive messages.
7) Information sent by individuals via the electronic mail system may be used in legal proceedings, if need be. Electronic mail messages are considered written communications and are potentially the subject of subpoena in litigation. SUAS Management may inspect the contents of electronic mail messages in the course of an investigation, will respond to the legal process and will fulfill any legal obligations to third parties, as and when needed.
8) SUAS also reserves every right to sue any staff member who sends or posts any unauthorized comments or contents on behalf of SUAS or any authority in SUAS using infrastructure owned by SUAS.
9) Any individual posting any unauthorized comments on behalf of SUAS or commenting anything against the name, repute or any policy decision of SUAS will be subjected to legal consequences and proceedings.
10) The individuals will be liable under the Information Technology (Amendments) Act, 2008 for any illegal acts, contravention or any offences if they commit any such prohibited acts under the Information Technology (Amendments) Act, 2008.
11) Sending, receiving, transmitting and retrieving the obscene material through any computer resources owned by the SUAS will be treated as gross indiscipline and the individual found guilty for such an act will be legally prosecuted.
12) Users should open attachments only from trusted or known email Ids. If any unknown person has sent any attachments without any proper information on the body of the mail then those attachments should not be opened as they may contain virus or malware.
13) All the SUAS computer resources, will be equipped with licensed anti-virus software which get auto-updates periodically. However, in the event of breaches, IT department will provide the necessary guidance and technical support.
14) Users are not allowed to take the backup of their mailbox. This activity will be carried out

by personnel from the IT department only.

15) User not allowed to use other Email ID Like Gmail, Hotmail, Rediff mail etc only official email permitted. If require Gmail for official use, so take approval of Higher Authorities.

C. Usage of University Logo

1) Logos of all SUAS institutes, whether in electronic form or otherwise, are the trademark of the Institute and should be used only by the authorized officials designated for work that requires communication to be done using University logo and letter heads.
2) No user is allowed to use University logo or soft copies of Institute letter head without prior approval of HR and SUAS Senior Management.
3) Any individual using the logo of the SUAS without the lawful authority and prior sanction of the authorities and / or Heads of the Institute / department will face severe legal consequences. SUAS reserves every right to take strict and rigorous punitive action against such an individual.

D. Usage of Physical Assets

1) Physical assets allocated to users like computer, laptop etc. are to be used within SUAS premises only. In special conditions, laptops can be taken out and used outside SUAS with prior approval of HR department and SUAS Senior Management.
2) Physical assets allocated to users will be secured by Admin passwords which will not be shared with the users. However, the user will be allowed to set-up and configure his own user id and password for use of the computer resource.
3) If a user is allocated a laptop then he/she need to adhere to the Laptop Policy defined.
4) The individual concerned to whom a SUAS owned asset is allocated is responsible for the safety and should contact the IT department in case of issues related to upkeep of the computing and related equipment (including laptops) and all the accessories associated with the concerned equipment.
5) SUAS reserves every right to take legal and/or punitive action against individual if he/she introduces any virus, worm or any kind of computer contaminant, inadvertently or purposefully, in any of the computer resources owned by the SUAS. The employee will be held responsible for any physical or virtual loss caused to the computer resources owned by SUAS in the event of any clause/s mentioned in this policy.
6) At the time of separation of an employee, arising out of his resignation, retirement, dismissal, transfer, or termination, the employee must hand over the allotted equipment along with its full set of accessories in good working condition to the IT Department or SUAS Senior Management.
7) HR or Department Head should inform IT department immediately when any staff separates from SUAS so that the access can be removed or blocked. IT GUIDELINES for User Management including User id creation and resource allocation already defined for the purpose, will be followed. Equipment which is to be removed from SUAS campus must be approved in advance by Senior Management. The move to be done by the Admin department along with the IT department and an inventory of this equipment maintained by the IT department. All equipment removal from the premises by an individual must be supported by the necessary documentation and approvals.
8) Physical access to departments / institutes will be controlled using access cards and only the users of that department / institutes will be provided access on request received from HR

department. The access can be provided to others on specific request and necessary approvals from HR department.

9) Access to server rooms will be provided to members of IT staff for the carrying out their designated activities and duties. The server rooms will be secured at all times by physical access controls. Any illegal entry in the server room will invite legal and punitive action against such employee.
10) Users are not allowed to connect their personal devices such as laptops, desktops, USB drives, mobile phones to SUAS network.
11) If any login or email ID of a former user who is not presently serving SUAS needs to be activated for a certain duration then IT department will need approval from Senior Management and the login ID will be made active for a limited period.
12) Users will lock their desktops or laptops when they are away from their desks. The user to whom a computer resource is allocated will be solely responsible for all the activity happening on the said computer resource.

E. Usage of Software Assets

1) Only authorized and licensed software will be installed on the machines of the users, as per their requirements. The installation of such software will be carried out by authorized IT staff only, subject to receiving approvals from concerned authorities. Freeware, if needed for official work, will be installed by authorized IT department personnel, subject to receiving the necessary approvals.
2) The use of unauthorized software in SUAS is strictly prohibited. In the event of cases of installation and usage of unauthorized software is noticed, it will be removed from the workstation immediately and necessary action may be initiated against the employee, as needed.
3) SUAS holds every right to confiscate any personal digital add-ons (such as pen drive, memory card or any portable memory device) of the user in case he/she uses it for any illegal acts.

F. Internet Usage

1. Access to Internet will be given on need basis and will be restricted strictly to the job requirements of the said user. This is applicable to all individuals who represent SUAS on the internet through web pages, blogs and any other social media.
2. SUAS's internet facility or its equipment should not be used for any unrelated commercial purpose.
3. While using the internet for such relevant communications, it is the sole responsibility of the sender or receiver as case may be, to validate the content of the outgoing and incoming communications.
4. Use of internet facility to access objectionable content is strictly prohibited and violation of the same may invite legal punitive actions Objectionable content will involve but not restricted to the following - pornography, racial or religious comments, gender specific comments, criminal and / or terror related matter, drugs, trafficking, sects and cults and gambling.
5. Any download of large or massive data files including video or audio, on SUAS network may be carried out only by the IT department or with prior arrangement made by the IT

department personnel without disturbing the normal course of work. Such downloads may be carried out for academic or IT administration purposes only.

6. The use of social networking sites such as Twitter, LinkedIn, Facebook, Instagram, Pinterest, Google Hangouts etc. is not permitted as per SUAS policy. In special cases, designated stakeholders may be provided access to such sites with prior permission and approval of Senior Management.
7. Gaming sites or any site which the anti-virus mechanism connotes as dangerous will be strictly prohibited from use in the SUAS. Any employee using the computer resources for games or online games or any non-safe sites as categorized by the anti-virus used in SUAS will be facing strict disciplinary actions.
8. Internet usage for the following activities such as illegal or criminal activities, military / security violations, use of offensive or sexually objectionable content, spam promotions, unauthorized access, online gambling, ethical or unethical hacking is strictly prohibited.
9. Employees are not allowed to download illegal software such as music, films, movies, games via file-sharing or other freeware technologies.
10. Internet usage by the employees should be such that it does not in any way compromise the reputation and standing of SUAS.
11. Any violations of the above, may result in a disciplinary action as per SUAS HR policy. In such an eventuality, the access to the individual will be shall blocked. Violators may also be subject to civil or criminal liability under the applicable Cyber laws.

G. Wireless LAN Usage

1) Wi-Fi networks at SUAS will be set-up to provide internet access in cases wherein SUAS internet is not available.
2) The IT department shall implement encryption, strong authentication, and other security methods as per industry norms. Wi-Fi access will be provided only upon HR and / or Senior Management approvals and will be activated by IT department.
3) Use of Wi-Fi network in illegal and unauthorized manner is strictly prohibited.
4) The access to Wi-Fi for any unlawful purpose or with any unlawful authority will be dealt with legal punitive actions.
5) The breaking into the secured systems of SUAS will be dealt with strict punishments as per the policy of the SUAS in accordance with the provisions of the Information Technology (Amendments) Act, 2008 or any other suitable penal statute.

H. Data Security

1) All information available in the computer network including reports / documents / designs prepared by the employees is the property of SUAS and should not be taken out in the form of an outgoing email, pen drives or CD or any other medium by any employee, unless specifically authorized in writing by the Senior Management.
2) All confidential data shall be maintained separately and should be accessible only to the authorized users. All critical data should be handled with restricted access. Only persons designated by the Senior Management should be allowed to view and work on the same. Any data required for statutory purposes shall be maintained appropriately for the prescribed period. Care should be taken so as to ensure that such historical data is accessible as and when required to individuals with proper access.
3) IT department will configure all workstations with virus protection software, which should

not be removed or disabled. Each employee is responsible for protecting their computer against virus attacks by following IT guidelines for scanning all incoming communications and media.

4) No employee is permitted to disable the anti-virus application installed on his / her workstations.
5) All CD, DVDs and removable media from external sources must be virus checked before they are used within the organization.
6) All users will log out of the network and turn their computers off before leaving the office at the end of the day. Users should log off of the network when they will be away from their desk for an extended period.
7) All the important business-related data should be stored in shared drives assigned to users; so that it gets backed up at predefined frequency. It is user's responsibility to store business data in proper folders and confirm from IT department that it is getting backed up. IT department will not be responsible for any data loss stored on local hard drives.
8) Each department will have access to shared folder(s) in the file server (currently called "EARTH"). Such folder(s) will have limitations on the size. Each department head must ensure that no duplicate data or personal data exists on the shared folder. This will avoid duplication of the data and will help optimally utilize the disk space. Some of the users may have access to Interdepartmental folder on the file server. Users should ensure that once the usage of the files have been complete, the files should be removed from the inter-departmental folder. Users should not copy any un-wanted data on the file server.
9) System logon Password must consist of a combination of minimum 8 alphanumeric characters and is expected to be changed every 30 days, and must be unique.
10) Any employee breaching into any secured system, secured data or information will face severe legal action, if found guilty.
11) Employees will not directly store SUAS's sensitive data on laptops, mobiles devices such as tablets or smartphones. If data is stored on removable media (zip drives, CD's or DVDs), the same should be locked away securely.
12) Documents containing sensitive data should be disposed off securely or shredded.
13) Sensitive data if transferred or transmitted electronically should be in encrypted format only.
14) IT department will schedule periodic backups of data based on the Data Backup IT GUIDELINES. The backups will be maintained by an authorized IT person, the details of which will be maintained in a register. Historic data will be archived as per the policy and stored securely.

I. Network Security

1) The IT department will monitor and be responsible for security of SUAS network.
2) The IT department will monitor the SUAS Local Area Network and also have liaison with service providers for internet connectivity or for connectivity with cloud partner sites where SUAS software applications are hosted.
3) IT department will implement and maintain procedures to provide adequate protection from intrusion into SUAS computer systems and network from external sources.
4) The IT Network Administrator shall monitor the quality of service of the internet provided by the vendor on a daily basis. The quality of service should meet the SLA agreed by the vendors such as Leased line providers, Cloud service partners etc.
5) On a daily basis, the IT Network Administrator will check if all the critical components of

the network are performing satisfactorily and in case of exception take necessary steps to ensure that the network is fully operational. Regular monitoring of the network shall be carried out at predetermined times.

6) SUAS reserves every right to prosecute an individual employee found guilty for any breach of any network security.

7) Any employee may be asked to depose or give a statement in case of any judicial proceeding or any investigation authority if some employee is found guilty in any illegal activity as per the provisions of the Information Technology (Amendments) Act, 2008 or any other suitable law for the time being in force.

8) Every dispute subjected to any security breach within the premises of SUAS or outside breaches by the employee or any other person will be subjected to the jurisdiction of the Pune Court as per the provisions of the Information Technology (Amendments) Act, 2008.

9) The employees of SUAS may be asked to assist the authorities of SUAS in case of investigation of any matter related to cyber security within or outside SUAS. Any existing employee not complying with this provision will be facing disciplinary action for non-compliance to the IT policy of the SUAS.

8. Refreshment of Laptop/Notebook. Desktop (E-Waste)

- Laptop/Notebook/desktop along with additional accessories will be refreshed within the fiscal year in which they are determined to be end-of-life, i.e. at the end of 7 years for laptop/notebook and 10 years for desktop from the date of purchase, based on the actual condition of laptop/notebook, like in good condition, but not possible to upgrade configuration then only below points will be follows:
- Such assets would be disposed in the following manner; subject to Management Approval.
- a) offered to the employee (user) on the book value;
- b) if the employee not willing to buy, the asset would be put up for e-waste;
- c) else the asset would be considered for buyback while procuring new asset;

9. Audit Review:

IT Department should properly maintain the physical stock of laptops/notebook/desktop which will be audited by on quarterly basis by the external engineer/agencies.

IT POLICY FOR STUDENTS

1. Applicability

This Policy applies to everyone who accesses SUAS resources, whether a part of SUAS or not, whether on campus or from remote locations. By accessing SUAS resources, the user of the resources agrees to comply with this Policy. This policy is thus applicable to the following users / individuals / entities, on or off SUAS campus –

2. Usage Guidelines

- All provided laptops, desktops and notebooks are university property and should be used primarily for academic and administrative purposes.
- Users are responsible for maintaining the equipment in good condition.

3. Damage and Repair Costs of Laptop and Notebook

1. **Reporting Damage:**
   - Any damage, malfunction, or loss of equipment must be reported to the IT department immediately.
2. **Minor Damage:**
   - **Examples:** Screen scratches and touch pad (external/ peripheral device)
   - **Cost:** The University will cover costs for minor repairs.
3. **Major Damage:**
   - **Examples:** Broken screens, broken hinch, Damage of Keyboard, Liquid damage and damage of cabinet (external/ peripheral device).
   - **Cost:** Faculty and staff are responsible for repair or replacement costs for major damage after confirmation of the cost by the IT department.
   - **Procedure:** The IT department will assess and confirm the cost. Users will be informed of the cost before any repair or replacement is undertaken.

4. Damage and Repair Costs of Desktop : Cost Responsibility:

- **User Negligence**: If damage is deemed to be caused by user negligence or misuse (e.g., spilling liquid, physical damage), the user may be responsible for repair or replacement costs.
- **Cost Calculation**: IT Support will provide an estimate of repair or replacement costs.
- **Payment**: The user will be notified of the cost and payment procedure. Costs will be deducted from the user’s paycheck or invoiced as per company policy.

4. **Replacement Costs:**
   - **Laptops /Desktops and Notebooks:** In cases of loss or irreparable damage due to negligence, users may be required to cover the cost of replacement.

5. Return of Equipment

- All issued equipment must be returned to the IT department upon resignation, retirement, or termination of employment.

- Failure to return equipment may result in a deduction of the replacement cost from any pending dues or salary. (HR should not release the salary without confirmation from IT department)

6. Essential Guidelines for User:

A. Usage of Institute Systems / Computers / Laptops and /or Information / Data.

1) SUAS provides the Personal computers, Laptops, Internet, Electronic mail and other communication/processing devices to the above listed stakeholders for business purposes only. SUAS is the sole owner of all the data/information and SUAS may access, disclose all data or messages stored on its systems or sent over its electronic mail system.
2) Wherever desktop/laptop is required, HR will send a new user login form to IT dept. IT dept. will create a login ID and email ID for the new joinee as per the IT GUIDELINES defined for the purpose. IT GUIDELINES 's for Laptop allocation and User creation and resource allocation are already defined for the purpose.
3) The users are not authorized to retrieve or read any e-mail messages that are not sent to them and cannot use a password, access a file, or retrieve any stored information unless authorized to do so.
4) SUAS reserves the right to monitor communications and data at any time, with or without notice, to ensure that the Institute property is being used only for business purposes and to ensure that the use of the said property is not compromised in any manner.
5) SUAS also reserves the right to disclose the contents of messages for any purpose at its sole discretion. No monitoring or disclosure will occur without the direction of SUAS Senior Management, unless otherwise noted.
6) SUAS holds every right to retain the electronic data, information or any file or folder downloaded, copied or extracted by the Students at any time during the course of employment.
7) SUAS also holds the right to use such a retained data, information or file or folder downloaded, copied or extracted by the Student as an evidence against the Student.
8) Before a user accesses the facilities or computer resources of SUAS, a notice will be displayed that warns against unauthorized use of the IT resources or system.
9) All the new joinees will be trained with the IT procedures, security policies, and its implementation either by HR department or by the concerned Department Head.
10) All the users are required to log a support ticket using the Helpdesk portal for any kind of support required from the IT dept. IT GUIDELINES for Using the Helpdesk portal for Support already defined for the purpose, will be followed.
11) IT dept. will perform maintenance of desktops, printers, servers, etc. as per their predefined schedule. IT GUIDELINES for Maintenance including Monitoring and Control processes, already defined for the purpose, will be followed.

B. Usage of Electronic Mail

1) SUAS will provide e-mail IDs to individuals who are authorized to carry out internal and external communications and are designated on a particular job position based on their roles and responsibilities. Such named or role specific generic email ids will be assigned to the said stakeholders which will be used for all internal and external communications.
2) The E-mail system is allowed to be accessed by the stakeholders within SUAS premises only. In special cases, designated stakeholders may be provided external access to the email system,

with prior permission and approval of Senior Management.

3) Access to email using personal mobile devices is not permitted unless authorized and approved by Senior Management.
4) Group email-ids may be created for operational convenience. Similarly function specific email-ids may be created for official response and necessary actions. SUAS HR Department shall ensure that such an email account is inactive when an individual separate from SUAS.
5) Users should note that any data and information on the system will not be deemed personal or private. In addition, the e-mail system may not be used to send or receive copyrighted materials, confidential information related to SUAS and its students, proprietary financial information, or similar materials without prior authorization and approvals.
6) The e-mail system is not to be used to solicit for personal gains, commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations. The system is not to be used to create any offensive or disruptive messages.
7) Information sent by individuals via the electronic mail system may be used in legal proceedings, if need be. Electronic mail messages are considered written communications and are potentially the subject of subpoena in litigation. SUAS Management may inspect the contents of electronic mail messages in the course of an investigation, will respond to the legal process and will fulfill any legal obligations to third parties, as and when needed.
8) SUAS also reserves every right to sue any staff member who sends or posts any unauthorized comments or contents on behalf of SUAS or any authority in SUAS using infrastructure owned by SUAS.
9) Any individual posting any unauthorized comments on behalf of SUAS or commenting anything against the name, repute or any policy decision of SUAS will be subjected to legal consequences and proceedings.
10) The individuals will be liable under the Information Technology (Amendments) Act, 2008 for any illegal acts, contravention or any offences if they commit any such prohibited acts under the Information Technology (Amendments) Act, 2008.
11) Sending, receiving, transmitting and retrieving the obscene material through any computer resources owned by the SUAS will be treated as gross indiscipline and the individual found guilty for such an act will be legally prosecuted.
12) Users should open attachments only from trusted or known email Ids. If any unknown person has sent any attachments without any proper information on the body of the mail then those attachments should not be opened as they may contain virus or malware.
13) All the SUAS computer resources, will be equipped with licensed anti-virus software which get auto-updates periodically. However, in the event of breaches, IT department will provide the necessary guidance and technical support.
14) Users are not allowed to take the backup of their mailbox. This activity will be carried out by personnel from the IT department only.
15) User not allowed to use other Email ID Like Gmail, Hotmail, Rediff mail etc only official email permitted. If require Gmail for official use, so take approval of Higher Authorities.

C. Usage of University Logo

1) Logos of all SUAS institutes, whether in electronic form or otherwise, are the trademark of the Institute and should be used only by the authorized officials designated for work that requires communication to be done using University logo and letter heads.
2) No user is allowed to use University logo or soft copies of Institute letter head without prior approval of HR and SUAS Senior Management.
3) Any individual using the logo of the SUAS without the lawful authority and prior sanction of

the authorities and / or Heads of the Institute / department will face severe legal consequences. SUAS reserves every right to take strict and rigorous punitive action against such an individual.

D. Usage of Physical Assets

1) Physical assets allocated to users like computer, laptop etc. are to be used within SUAS premises only. In special conditions, laptops can be taken out and used outside SUAS with prior approval of HR department and SUAS Senior Management.
2) Physical assets allocated to users will be secured by Admin passwords which will not be shared with the users. However, the user will be allowed to set-up and configure his own user id and password for use of the computer resource.
3) If a user is allocated a laptop then he/she need to adhere to the Laptop Policy defined.
4) The individual concerned to whom a SUAS owned asset is allocated is responsible for the safety and should contact the IT department in case of issues related to upkeep of the computing and related equipment (including laptops) and all the accessories associated with the concerned equipment.
5) SUAS reserves every right to take legal and/or punitive action against individual if he/she introduces any virus, worm or any kind of computer contaminant, inadvertently or purposefully, in any of the computer resources owned by the SUAS. The Student will be held responsible for any physical or virtual loss caused to the computer resources owned by SUAS in the event of any clause/s mentioned in this policy.
6) At the time of separation of a Student, arising out of his resignation, retirement, dismissal, transfer, or termination, the Student must hand over the allotted equipment along with its full set of accessories in good working condition to the IT Department or SUAS Senior Management.
7) HR or Department Head should inform IT department immediately when any staff separates from SUAS so that the access can be removed or blocked. IT GUIDELINES for User Management including User id creation and resource allocation already defined for the purpose, will be followed. Equipment which is to be removed from SUAS campus must be approved in advance by Senior Management. The move to be done by the Admin department along with the IT department and an inventory of this equipment maintained by the IT department. All equipment removal from the premises by an individual must be supported by the necessary documentation and approvals.
8) Physical access to departments / institutes will be controlled using access cards and only the users of that department / institutes will be provided access on request received from HR department. The access can be provided to others on specific request and necessary approvals from HR department.
9) Access to server rooms will be provided to members of IT staff for the carrying out their designated activities and duties. The server rooms will be secured at all times by physical access controls. Any illegal entry in the server room will invite legal and punitive action against such Student.
10) Users are not allowed to connect their personal devices such as laptops, desktops, USB drives, mobile phones to SUAS network.
11) If any login or email ID of a former user who is not presently serving SUAS needs to be activated for a certain duration then IT department will need approval from Senior Management and the login ID will be made active for a limited period.
12) Users will lock their desktops or laptops when they are away from their desks. The user to

whom a computer resource is allocated will be solely responsible for all the activity happening on the said computer resource.

E. Usage of Software Assets

1) Only authorized and licensed software will be installed on the machines of the users, as per their requirements. The installation of such software will be carried out by authorized IT staff only, subject to receiving approvals from concerned authorities. Freeware, if needed for official work, will be installed by authorized IT department personnel, subject to receiving the necessary approvals.
2) The use of unauthorized software in SUAS is strictly prohibited. In the event of cases of installation and usage of unauthorized software is noticed, it will be removed from the workstation immediately and necessary action may be initiated against the Student, as needed.
3) SUAS holds every right to confiscate any personal digital add-ons (such as pen drive, memory card or any portable memory device) of the user in case he/she uses it for any illegal acts.

F. Internet Usage

1. Access to Internet will be given on need basis and will be restricted strictly to the job requirements of the said user. This is applicable to all individuals who represent SUAS on the internet through web pages, blogs and any other social media.
2. SUAS's internet facility or its equipment should not be used for any unrelated commercial purpose.
3. While using the internet for such relevant communications, it is the sole responsibility of the sender or receiver as case may be, to validate the content of the outgoing and incoming communications.
4. Use of internet facility to access objectionable content is strictly prohibited and violation of the same may invite legal punitive actions Objectionable content will involve but not restricted to the following - pornography, racial or religious comments, gender specific comments, criminal and / or terror related matter, drugs, trafficking, sects and cults and gambling.
5. Any download of large or massive data files including video or audio, on SUAS network may be carried out only by the IT department or with prior arrangement made by the IT department personnel without disturbing the normal course of work. Such downloads may be carried out for academic or IT administration purposes only.
6. The use of social networking sites such as Twitter, LinkedIn, Facebook, Instagram, Pinterest, Google Hangouts etc. is not permitted as per SUAS policy. In special cases, designated stakeholders may be provided access to such sites with prior permission and approval of Senior Management.
7. Gaming sites or any site which the anti-virus mechanism connotes as dangerous will be strictly prohibited from use in the SUAS. Any Student using the computer resources for games or online games or any non-safe sites as categorized by the anti-virus used in SUAS will be facing strict disciplinary actions.
8. Internet usage for the following activities such as illegal or criminal activities, military / security violations, use of offensive or sexually objectionable content, spam promotions, unauthorized access, online gambling, ethical or unethical hacking is strictly prohibited.
9. Students are not allowed to download illegal software such as music, films, movies, games

via file-sharing or other freeware technologies.

10. Internet usage by the Students should be such that it does not in any way compromise the reputation and standing of SUAS.
11. Any violations of the above, may result in a disciplinary action as per SUAS HR policy. In such an eventuality, the access to the individual will be shall blocked. Violators may also be subject to civil or criminal liability under the applicable Cyber laws.

G. Wireless LAN Usage

1) Wi-Fi networks at SUAS will be set-up to provide internet access in cases wherein SUAS internet is not available.
2) The IT department shall implement encryption, strong authentication, and other security methods as per industry norms. Wi-Fi access will be provided only upon HR and / or Senior Management approvals and will be activated by IT department.
3) Use of Wi-Fi network in illegal and unauthorized manner is strictly prohibited.
4) The access to Wi-Fi for any unlawful purpose or with any unlawful authority will be dealt with legal punitive actions.
5) The breaking into the secured systems of SUAS will be dealt with strict punishments as per the policy of the SUAS in accordance with the provisions of the Information Technology (Amendments) Act, 2008 or any other suitable penal statute.

H. Data Security

1) All information available in the computer network including reports / documents / designs prepared by the Students is the property of SUAS and should not be taken out in the form of an outgoing email, pen drives or CD or any other medium by any Student, unless specifically authorized in writing by the Senior Management.
2) All confidential data shall be maintained separately and should be accessible only to the authorized users. All critical data should be handled with restricted access. Only persons designated by the Senior Management should be allowed to view and work on the same. Any data required for statutory purposes shall be maintained appropriately for the prescribed period. Care should be taken so as to ensure that such historical data is accessible as and when required to individuals with proper access.
3) IT department will configure all workstations with virus protection software, which should not be removed or disabled. Each Student is responsible for protecting their computer against virus attacks by following IT guidelines for scanning all incoming communications and media.
4) No Student is permitted to disable the anti-virus application installed on his / her workstations.
5) All CD, DVDs and removable media from external sources must be virus checked before they are used within the organization.
6) All users will log out of the network and turn their computers off before leaving the office at the end of the day. Users should log off of the network when they will be away from their desk for an extended period.
7) All the important business-related data should be stored in shared drives assigned to users; so that it gets backed up at predefined frequency. It is user’s responsibility to store business data in proper folders and confirm from IT department that it is getting backed up. IT department will not be responsible for any data loss stored on local hard drives.

8) Each department will have access to shared folder(s) in the file server (currently called "EARTH"). Such folder(s) will have limitations on the size. Each department head must ensure that no duplicate data or personal data exists on the shared folder. This will avoid duplication of the data and will help optimally utilize the disk space. Some of the users may have access to Interdepartmental folder on the file server. Users should ensure that once the usage of the files have been complete, the files should be removed from the inter-departmental folder. Users should not copy any un-wanted data on the file server.

9) System logon Password must consist of a combination of minimum 8 alphanumeric characters and is expected to be changed every 30 days, and must be unique.

10) Any Student breaching into any secured system, secured data or information will face severe legal action, if found guilty.

11) Students will not directly store SUAS's sensitive data on laptops, mobiles devices such as tablets or smartphones. If data is stored on removable media (zip drives, CD's or DVDs), the same should be locked away securely.

12) Documents containing sensitive data should be disposed off securely or shredded.

13) Sensitive data if transferred or transmitted electronically should be in encrypted format only.

14) IT department will schedule periodic backups of data based on the Data Backup IT GUIDELINES. The backups will be maintained by an authorized IT person, the details of which will be maintained in a register. Historic data will be archived as per the policy and stored securely.

I. Network Security

1) The IT department will monitor and be responsible for security of SUAS network.

2) The IT department will monitor the SUAS Local Area Network and also have liaison with service providers for internet connectivity or for connectivity with cloud partner sites where SUAS software applications are hosted.

3) IT department will implement and maintain procedures to provide adequate protection from intrusion into SUAS computer systems and network from external sources.

4) The IT Network Administrator shall monitor the quality of service of the internet provided by the vendor on a daily basis. The quality of service should meet the SLA agreed by the vendors such as Leased line providers, Cloud service partners etc.

5) On a daily basis, the IT Network Administrator will check if all the critical components of the network are performing satisfactorily and in case of exception take necessary steps to ensure that the network is fully operational. Regular monitoring of the network shall be carried out at predetermined times.

6) SUAS reserves every right to prosecute an individual Student found guilty for any breach of any network security.

7) Any Student may be asked to depose or give a statement in case of any judicial proceeding or any investigation authority if some Student is found guilty in any illegal activity as per the provisions of the Information Technology (Amendments) Act, 2008 or any other suitable law for the time being in force.

8) Every dispute subjected to any security breach within the premises of SUAS or outside breaches by the Student or any other person will be subjected to the jurisdiction of the Pune Court as per the provisions of the Information Technology (Amendments) Act, 2008.

9) The Students of SUAS may be asked to assist the authorities of SUAS in case of investigation of any matter related to cyber security within or outside SUAS. Any existing Student not complying with this provision will be facing disciplinary action for non-compliance to the IT policy of the SUAS.

7. Refreshment of Laptop/Notebook. Desktop (E-Waste)

- Laptop/Notebook/desktop along with additional accessories will be refreshed within the fiscal year in which they are determined to be end-of-life, i.e. at the end of 7 years for laptop/notebook and 10 years for desktop from the date of purchase, based on the actual condition of laptop/notebook, like in good condition, but not possible to upgrade configuration then only below points will be follows:
- Such assets would be disposed in the following manner; subject to Management Approval.
- a) offered to the Student (user) on the book value;
- b) if the Student not willing to buy, the asset would be put up for e-waste;
- c) else the asset would be considered for buyback while procuring new asset;

8. Audit Review:

IT Department should properly maintain the physical stock of laptops/notebook/desktop which will be audited by on quarterly basis by the external engineer/agencies.