Sushant University

IT POLICY

Sushant University

INDEX (IT POLICY & PROCEDURE)

Sushant University

IT POLICY & PROCEDURE

Sushant University has a well defined IT policy which establishes guidelines for the use and maintenance of a university's IT infrastructure. The policy ensure's that the university's IT assets are protected and used appropriately and legally.

The policy establishes strategies and responsibilities for protecting the confidentiality, integrity, and availability of the university's IT assets. This includes data, computers, network devices, intellectual property, and documents

The policy provides guidelines for purchasing hardware to ensure it's appropriate, cost-effective, and integrates with university policy

The policy defines who can use the university's IT facilities and for what purposes. It also prohibits unauthorized access to IT resources

The policy outlines rules for the behavior of users and IT personnel, and identifies consequences for not following them

The policy ensures compliance with applicable laws and regulations

Sushant University

Erstwhile Ansal University Gurugram

Policies & Procedures

IT Department

09-February-2021

Disclaimer

Final Decision:

In Case of any differences of opinion or interpretation of Rules and Regulations or any other issue the decision of Vice-Chancellor / Registrar would be Final and Acceptable to all.
This Policy is valid till December-2025

Contents

Email and Instant Messaging IT_01

Objective:

Provide appropriate guidelines for productively utilizing the University's email system and instant messaging technology that protects the employee and University while benefiting our institution.

Applies to:

All Employees & Students (Active) wherever applicable

Key guidelines:

- The University has established this policy with regard to the acceptable use of University provided electronic messaging systems, including but not limited to email and instant messaging.
- Email and instant messaging is important and sensitive Operations tools. This policy applies to any and all electronic messages composed, sent or received by any Employee / Student or by any person using University provided electronic messaging resources.
- The University sets forth the following policies but reserves the right to modify them at any time in order to support our University:

General

- The University provides electronic messaging resources to assist in conducting University operations.
- All messages composed and/or sent using University provided electronic messaging resources must comply with University policies regarding acceptable communication.
- The University prohibits discrimination based on age, race, gender, sexual orientation or religious or political beliefs. Use of electronic messaging resources to discriminate for any or all of these reasons is prohibited.
- Upon termination or separation from the University, the University will remove all data of email, including any messages, Files stored in the system, regardless of sender or recipient. (DOC-PREPARE)
- Each employee will be assigned a unique email address that is to be used while conducting University Operations via email.

- Employees are prohibited from forwarding electronic messages sent through University provided systems to external messaging systems unless the job requires them for the benefit of the University.
- Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Any employee who discovers a violation of these policies should immediately notify their HOD / Dean or the Human Resources Department.
- Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.

Ownership

- The email/electronic messaging systems are University property. All messages stored in University provided electronic messaging system(s) or composed, sent or received by any employee or non-employee are the property of the University. Electronic messages are NOT the property of any employee.
- The University reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.
- The University reserves the right to alter, modify, re-route or block the delivery of messages as appropriate.
- The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of the University. Employees may use these identifiers only while employed by the University.

Confidentiality

- Messages sent electronically can be intercepted inside or outside the University and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.
- Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.

- Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.
- Employees are prohibited from unauthorized transmission of University trade secrets, confidential information, or privileged communications.
- Unauthorized copying and distribution of copyrighted materials is prohibited.

Security

- The University employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on University provided computer equipment.
- Although the University employs anti-virus software, some virus infected messages can enter the University's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:
  - Be suspicious of messages sent by people not known by you.
  - Do not open attachments unless they were anticipated by you. If you are not sure, always verify the sender is someone you know and that he or she actually sent you the email attachment.
  - Disable features in electronic messaging programs that automatically preview messages before opening them.
  - Do not forward chain letters. Simply delete them.
- The University considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links are often used as a means to verify that you exist.
- Internet message boards are a fertile source from which mass junk e-mailers harvest email addresses and email domains. Do not use University provided email addresses when posting to message boards.
- Upon passout /Withdrawal the emailid which was created as per request from schools / erp will be deleted.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM

Inappropriate use

- Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.
- University provided electronic messaging resources may not be used for the promotion or publication of one's political or religious views, the operation of our Operations or for any undertaking for personal gain.

Internet usage IT-02

Objective:

- Provide appropriate guidelines for accessing and utilizing the Internet through the University's network.

Applies to:

- All employees & Students with authorized access to Internet services

Key guidelines:

- Internet services are authorized to designated employees & Students by their HOD / Dean to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that the University must guard against. For that reason, employees and students are granted access only as a means of providing support in fulfilling their job responsibility.

General

- Internet is provided to employees and students as per IT Firewall policy
- Currently IT Department authorized to provide internet connectivity to all employees only on laptops and desktops as per **Firewall** IT policy.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Currently IT Department authorized to provide internet connectivity to all active student & Staff on their laptop only. It is mandatory to have reputed antivirus (Paid) and Legitimate Software on their laptop.
- Each individual is responsible for the account issued to him/her.
- Sharing Internet accounts or User-ID's is prohibited.
- Organizational use of Internet services must reflect the mission of the University and support the University's goals and objectives.
- These services must support legitimate, mission related activities of the University and be consistent with prudent operational, security, and privacy considerations.
- The Digital Marketting Team along with the respective content owners will take responsibility for all web site content (i.e., "the University web site") and format presentation to reflect the University's mission and in supporting University and departmental objectives, following are the content owner.

Content	Content Owner
School related	School Coordinator / Dean
Exam	COE
Digital	Admission / Marketting
Account	CFAO
Lab	IT
Library	Chief Librarian
HR	HR
Facility	Facility Office

- The University has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
- Any freeware or demo/trial applications/Softwares via the Internet into the University network will need **prior approval from the Individuals HOD / Dean counter signed by the IT-Head**, and then that becomes the property of the University. Any such software may be used only in ways that are consistent with their licenses or copyrights.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- IT-Team has already banned a few sites thru the Firewall,however these sites can be opened on a special request with **approval from "The Registrar" office and IT-Head**

Inappropriate use

- The following uses of University provided Internet access are not permitted:
  - To access, upload, download, or distribute pornographic or sexually explicit material
  - Violate and state, local, or federal law
    - Vandalize or damage the property of any other individual or organization
    - To invade or abuse the privacy of others
    - Violate copyright or use intellectual material without permission
    - To use the network for financial or commercial gain
  - To degrade or disrupt network performance
  - No employee & students may use University facilities knowingly to download or distribute pirated software or data. The use of file swapping software on University computers and University networks is prohibited.
  - No employee may use the University's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
- Specific Softwares which ease the use of downloading the large content is strictly prohibited. Any instances found for the same, can lead to permanent disablement of the said account and necessary action from the HR.

Password security IT 03

Objective:

- Provide guidelines in appropriate management of Operations passwords to maintain adequate security and integrity of all of the University's Operations systems.

Applies to:

- All employees & Students

Key guidelines:

- Maintaining security of the University's Operations applications, software tools, email systems, network facilities, and voice / Video mail are critical to providing data integrity and stability of our systems. Passwords are provided to limit access to these University assets on an as needed basis.
- The University provides access to network, electronic mail and voice mail resources to its employees in support of the University's mission. Passwords are assigned for access to each of these resources to authenticate a user's identity, to protect network users, and to provide security.
- It is the responsibility of each individual to protect and to keep private any and all passwords issued to him/her by the University.
- Although the University strives to manage a secure computing and networking environment, the University cannot guarantee the confidentiality or security of network, e-mail or voice mail passwords from unauthorized disclosure.

- Any employee passwords and changes must be requested by HR-HOD / Dean, post the approval from "The Registrar" Office. This helps monitor and manage the importance of protecting passwords in their distribution and use in such a way that reinforces the integrity of users accessing University systems.

SUSHANT UNIVERSITY * SECTOR-55, GURUGRAM *

- All the user to change the password at first login (Mandatory). Every individual is responsible for the security of his / her password and expected not to share with anyone.

- A network HOD / Dean must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.

- IT Support will handle requests from University HOD / Deans made in one of the following ways:
  - For emailed issue, the users can send an email to ithelpdesk@ansaluniversity.edu.in
- Password Changed requests must be verified by the employee's HOD / Dean.
- System administrators and users assume the following responsibilities:
  - System administrator must protect confidentiality of user's password.
  - User must manage passwords according to the Password Guidelines.
  - User is responsible for all actions and functions performed by his/her account.
  - Suspected password compromise must be reported to IT-Team immediately.
  - Only in case of Emergency or after 5.00pm till 8.00pm, team can reach to Mr Pradeep Lal (#9717295047) / Mr Manoj Kumar (9050470791)

Password Guidelines *Select a Wise Password*

- To minimize password guessing:
- Do not use any part of the account identifier (username, login ID, etc.).
- Use 8 or more characters. mixed alpha and numeric characters
- Use two or three short words that are unrelated. *Keep Your Password Safe*
- Do not let anyone observe you entering your password.
- Do not display your password in your work area or any other highly visible place.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Change your password periodically (every 3 months is recommended).
- Do not reuse old passwords. *Additional Security Practices*
- Ensure your workstation is reasonably secure in your absence from your office. Consider using a password-protected screen saver, logging off or turning off your monitor when you leave the room.

Software usage – IT-04

Objective:

- Provide guidelines on appropriate use of software products utilizing University equipment

Applies to:

All employees & Students

Key guidelines:

- This policy is intended to ensure that all University employees & Students understand that no computer software may be loaded onto or used on any computer owned or leased by the University unless the software is the property of or has been licensed by the University.

General

- Software purchased by the University or residing on University owned computers is to be used only within the terms of the license agreement for that software title.
- Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to the University's Software Usage Policy.
- To purchase software, users must obtain the approval of their department HOD / Dean who will follow the same procedures used for acquiring other University assets.
- All approved software will be purchased through the IT Department & Purchasing Committee.

- The IT - Head and designated members of the IT Department will be the sole governing body for defining appropriate software titles acceptable for use in the University.
- Under no circumstances will third party software applications be loaded onto University owned computer systems without the knowledge of and approval of the IT Department.
- Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any University user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.
- The University does not condone the illegal duplication of software in any form.

Compliance

- We will use all software in accordance with its license agreements.
- Under no circumstances will software be used on University computing resources except as permitted in the University's Software Usage Policy.
- Legitimate software will be provided to all users who need it. University users will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to termination.
- Each user of software purchased and licensed by the University must acquire and use that software only in accordance with the University's Software Usage Policy and the applicable Software License Agreement.
- All users acknowledge that software and its documentation are not owned by the University or an individual but licensed from the software publisher.
- Employees of the University are prohibited from giving University acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.
- All software used by a University entity for University owned computing devices, or purchased with University funds, will be acquired through the appropriate procedures as stated in the University Software Usage Policy.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Any user who determines that there may be a misuse of software within the organization will notify department HOD / Dean or IT-Head.

Registration of software

- Software licensed by the University will not be registered in the name of an individual.
- When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of the University with the job title or department name in which it is used.
- After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of the University. A copy of the license agreement will be filed and maintained by the IT Department's Software License Administrator.
- Once installed, the original installation media should be kept in a safe storage area designated by the IT Department.
- Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. The University's policy is to pay shareware authors the fee they specify for use of their products if the software will be used at the University. Installation and registration of shareware products will be handled the same way as for commercial software products.

Software Audit

- IT will conduct **quarterly** audits of all University owned PCs, including laptops, to ensure the University is in compliance with all software licenses.
- Audits will be conducted using an auditing software product or manual scanning of the machine.
- Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer.
- During these audits, the IT-Department will search for computer viruses and eliminate any that are found.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

PC software standards IT_05

Objective:
Provide guidelines for purchasing and installing software on University PC's

Applies to:
All employees

Key guidelines:
The purpose for this policy is to explain University software standards and to identify the levels of technical support available to the University employees from the IT Department.

Applicability

- This policy applies to all employees of the University requesting the purchase of new computer software and who desire computing support for that application from the IT technical support team.
- The following software standards have been established to ensure efficient and cost-effective use of University computing assets:
  - To help ensure compatibility between applications and releases
  - To provide more effective system administration
- To assist in the computer planning process and enable the realization of long-term goals and the future computing vision
- To ensure cost effective purchasing
- To enable effective tracking of software licenses
- To provide cost effective end user software training
- To facilitate efficient and effective technical support effort

Technical Support

- Software support is provided at several levels and is based on whether the software is the University enterprise standard or department specific.
- The IT Department will not provide support for evaluation software, personally purchased software, illegal copies of software, screen savers, shareware, and non-network software that is not included in the standard software list.

- Software applications determined by IT technical staff to cause computer problems with the University's standard network software will be removed.

IT Department's Role In The Purchase of Hardware And Software

- Assist departments with evaluating new Operations software solution.
- Act as liaison for departments when dealing with computing vendors.
- Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product.
- Assist with hardware and system requirements.
- Install the software as needed.
- Enforce University hardware and software standards.

Standard PC Equipment and Software List

- Standard PC hardware and software configurations are posted on the University's Intranet web site in the IT Department section.
- Contact the Systems Support of the IT Department for questions pertaining to University standards.

Requesting Standard PC Equipment and Software

- Equipment and software requests that are covered by the University's PC Equipment and Software Standards List will be provided quickly as long as appropriate approvals are granted.
- The steps that follow outlines the process for purchasing PC equipment and software:
  - Complete the PC Equipment and Software Request form. (See example in SAMPLES section)
  - Gain approval of the Department HOD / Dean
  - Submit request to IT Department.
  - The IT Department will review the order and forward to Purchasing or will contact Requestor for clarification as needed.
  - The IT Department or Purchasing Department are available for follow-up questions regarding your order as needed.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

Request for a Variance from the PC Hardware or Software Standard

- Complete the "Request for a Variance from the PC Hardware and Software Standard" form.
- Practical and sufficient justification is a key part so be concise in building your case for deviating from the standard.
- Gain approval of the request from your Department HOD / Dean.
- Submit the request to the IT Department's Systems Support for review.
- Your request will be reviewed and either approved or declined based upon justified reasons presented and the IT Department's ability to support the new configuration within the University's network.
- Pay close attention to the *Reason and justification* section. Variances from the University's standards are reviewed closely for compatibility and justification of need.

Inventory and equipment IT-06

Objective:

- Provide management guidelines for managing the use and security of University inventory and equipment

Applies to:

- All Employees & Temporary Staff

Key guidelines:

- PC's, equipment, and supplies are purchased for University employee use and productivity. It is the responsibility of all employees and HOD / Deans to manage the security of University equipment and supplies in order to cost effectively manage the University's expense in these areas.

Allocating equipment to employees

- Equipment is assigned to employees based upon their job function.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- HOD / Deans should maintain a list of equipment allocated to each of his/her employees
- Specific equipment should be tracked by employee includes, but is not limited to:
  - PC's (both desktop and laptop)
  - PC peripherals (scanners, printers, modems, etc.)

Employee Responsibilities

- One of the responsibilities of the HOD / Dean is to collect all allocated equipment issued to an employee who leaves the University and return to the IT-Department. Maintaining the Employee Inventory Allocation Log makes it a simple process.
- Employee to whom the IT Equipment has been issued will be solely responsible for its Repair / Consumables (Battery, Charger, Bag Etc) related to the Equipment issues to him / her till the Equipment is in his / her custody. After 1st January 2021, Official Laptops will be issued to VC Office, Registrar Office, Deans, Directors and HODs Only. Any other laptop to be issued after the special approval of the Registrar. Any use of personal laptops by the Faculty / Staff would require following IT Policy / Guidelines with respect to Antiviruses, Regular Audits, Use of Legitimate Software etc. Antivirus Software will be provided by Sushant University.
- Employees not able to return allocated equipment are responsible for reimbursing the University for the fair market value of the item.

Technology assets

- The IT Department will maintain an accurate inventory of all networked technology assets, laptops, and tangible technology equipment valued at over INR 5000.00 of the University to include the following information:
  - Item
  - Serial #
  - Basic configuration (i.e., HP PC Desktop -4GB RAM, 500GB FD, i3 Processor)
  - Physical location
  - Operating system release level
  - Date placed in service

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Original cost / Operating Lease Cost
- Vendor Detail
-

- Technology equipment will be tagged for easy identification.
- Periodic inventory audits will be conducted to validate the inventory and to identify maintenance issues needed for employee productivity.

PC standards IT-07

Objective:

Provide guidelines for maintaining a standard PC image for the University that addresses the needs of University employees

Applies to:

All employees

Key guidelines:

The University will maintain standard configurations of PC's and laptops in order to enhance employee productivity and supportability of the University's network.

General

- The IT Department will establish the standard configuration of PC hardware and software to be run on University PC's and laptops.
- Multiple configurations are maintained to provide stronger capabilities for employees that need more PC capabilities for their work. These users are called "Power users" and are determined to need the more capable PC's by their HOD / Dean.
- On an exception only basis, a PC may be requested that does not meet the standards configuration. To request a non-standard PC, see the PC Software Standards policy for the *Requesting a Variance from the Standard* request form.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

Network access

- All PC's are network enabled to access the University's network.
- It is the employee's responsibility to maintain appropriate security measures when accessing the network as defined in the University's Password Security policy.

PC Support

- The IT Department will maintain all PC's of the University or will direct you to appropriate measures for maintaining your PC.
- Standard configurations are defined to assist in providing responsive support and to assist in troubleshooting your issue or problem. Deviations from the standards are not permitted except in appropriately reviewed and approved situations.
- For assistance with your PC or peripheral equipment, contact the IT Help Desk.

Employee training

- Basic training for new employees on the use of PC's, accessing the network, and using applications software is held every week by the IT Department
- Training not listed on the IT Department's schedule may be requested or taken outside the University.

Backup procedures

- Network data and programs are backed up daily and archived off site in case of emergency.
- *Data and software on your PC are not backed up and IT Department is not responsible for any data stored on your machine*. If you want to protect data and files used on your PC, you should take one of the following measures:
  - Save the data onto Google Drive and File Server.
- Copy the data to the appropriate Google Drive **associated with email id** or Local Server specifically set up for this purpose. This will ensure your important data is saved and archived daily in our normal backup process.

Virus software

- The University maintains network virus software that will automatically scan your PC for possible viruses each time you log onto the network.
- Downloading or copying data files from external systems and the Internet are prohibited without the IT Department's review and approval in order to protect the integrity of the University network.

Applications software

- Standard software is maintained on all PC's and laptops. See the PC Software Standards policy for more information.
- Under no circumstances are additional software programs allowed to be loaded onto a PC without the review and approval of the IT Department. This is a protective measure to avoid network problems due to viruses and incompatibility issues.

Equipment requests (Adds, Changes, Deletes) IT-08

Objective:

Provide management guidelines on the proper steps and requirements for requesting equipment (adds, deletes, changes)

Applies to:

All Employees

Key guidelines:

Guidelines for ordering new technology equipment or making changes to existing equipment are provided to streamline the order process and to assist the IT Department in fulfilling the request.

General

- Capital equipment items (over INR 5,000/-) must be budgeted and approved for purchase.

- All technology capital requests are reviewed and approved by the IT Department and The Registrar's Office and Finance Departments for appropriate need even when budgeted in the University's annual Capital Budget.
- Only Department HOD / Deans may submit equipment requests.
- Appropriate lead time of at least three weeks should be taken into consideration when ordering new equipment, upgrades
- Equipment relocations, can be completed in 1 working day
- The IT Department will maintain a small inventory of standard PC's and other heavily used equipment to minimize the delay in fulfilling critical orders.
- It is the HOD / Dean's responsibility to provide enough lead time for new orders and change requests in managing his/her department effectively.

Procedures

- Complete the Equipment Request Form for the equipment or service you need.
- Have the Department HOD / Dean Review and approve the request.
- Submit the request to the IT Systems Support organization for review and follow-up.
- The IT Systems Support organization will review the request for appropriateness based upon standards and capital equipment purchasing guidelines of the University. The IT organization will follow-up in one of the following ways:
  - Forward the request to the Purchasing committee to order the equipment.
  - Fill the order if equipment is available in inventory.
  - Contact the requesting department for clarification.
  - Decline the request and forward the request form along with an explanation back to the originating department.

Approved equipment

- If the equipment exists in inventory, the equipment is prepared as needed and installed for the requesting department.
- If the equipment is ordered through Purchasing, the IT Department will either be notified of receipt at the requesting department or the

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

equipment will be sent directly to the IT Department for prep, staging, and installation.

Support

- For normal support of non-working technology equipment, contact support team as per email IDs mentioned below:

Student Support	ithelpdesk@ansaluniversity.edu.in
Staff / Faculty Support	it@ansaluniversity.edu.in

Information security IT-09

Objective:

Provide guidelines that protect the data integrity and proprietary nature of the University's information systems.

Applies to:

All employees

Key guidelines:

- By information security we mean protection of the University's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.
- The purpose of the information security policy is:
- To establish a University-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of University data, applications, networks, and computer systems.
- To define mechanisms that protect the reputation of the University and allow the University to satisfy its legal and ethical responsibilities regarding its networks' and computer systems' connectivity to worldwide networks.

- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.
- The University will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the University's data, network and system resources.
- Security reviews of servers, firewalls, routers, azsand monitoring platforms must be conducted on a regular basis. These reviews will include monitoring access logs and results of intrusion detection software.
- The IT Department must see to it that:
  - The information security policy is updated on a regular basis and published as appropriate.
  - Appropriate training is provided to data owners, data custodians, network and system administrators, and users.
  - Violation of the Information Security Policy may result in disciplinary actions as authorized by the University.

Data classification

- It is essential that all University data be protected. Different types of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.
- The University classifies data in the following three classes:
- High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure.
  - Payroll, personnel, and financial information are also in this class because of privacy requirements.
  - The University recognizes that other data may need to be treated as high risk because it would cause severe damage to the University if disclosed or modified.
  - The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.
- Confidential – Data that would not expose the University to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

(Schools consists /Dean, HODs) to implement the necessary security requirements.

- Public - Information that may be freely disseminated.
- All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the University.
- Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification level and University respective schools and depts.
- Data custodians are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or re-purposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Access control

- Data must have sufficient granularity to allow the appropriate authorized access.
- There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and addressed appropriately.
- The University will have a standard policy that applies to user access rights. This will suffice for most instances.
- Data owners or custodians may enact more restrictive policies for end-user access to their data.
- Access to the network and servers and systems will be achieved by individual and unique logins and will require authentication. Authentication includes the use of passwords other recognized forms of authentication.
- As stated in the Appropriate Use Policy, users must not share usernames and passwords, nor should they be written down or

SUSHANT UNIVERSITY ★★ SECTOR-55, GURUGRAM ★★

recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.

- All users of systems that contain high risk or confidential data must have a strong password, the definition of which will be established and documented by the IT Department.
- Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by the IT Department.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- Users are responsible for safe handling and storage of all University authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access the University's network or system resources.
- If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination.
- Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.
- Transferred employee access must be reviewed and adjusted as found necessary.
- Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

Virus prevention

- The willful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Intrusion detection

- Antivirus must be implemented on all servers and workstations containing data classified as high or confidential risk.
- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

Remote access IT-10

Objective:

Provide guidelines on appropriate use of remote access capabilities to the University's network, Operations applications, and systems

Applies to:

All employees

Key guidelines:

- The purpose of this policy is to define standards for connecting to the University network from a remote location outside the University.

SUSHANT UNIVERSITY ★★ SECTOR-55, GURUGRAM ★★

- These standards are designed to minimize the potential exposure to the University from damages that may result from unauthorized use of the University resources. Damages include the loss of sensitive or confidential University data, intellectual property, damage to critical University internal systems, etc.
- This policy applies to all the University employees, contractors, vendors and agents with a University owned or personally owned computer or workstation used to connect to the University network.
- This policy applies to remote access connections used to do work on behalf of the University, including reading or sending email and viewing Intranet web resources.
- It is the responsibility of the University employees, contractors, vendors and agents with remote access privileges to the University's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the University network.

Remote connection

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password phrases.
- At no time should any University employee provide his/her login or email password to anyone, not even family members.
- University employees and contractors with remote access privileges must ensure that their University owned or personal computer or workstation, which is remotely connected to the University's corporate network, is not connected to any other network at the same time.
- The University employees and contractors with remote access privileges to the University's corporate network must not use non University email accounts or other external resources to conduct the University Operations, thereby ensuring that official Operations is never confused with personal Operations.
- Internet configured for access to the University network must meet minimum authentication requirements established by the IT Department.
- All hosts that are connected to the University internal networks via remote access technologies must use the most up-to-date anti-virus software.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Personal equipment that is used to connect to the University's networks must meet the requirements of the University-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the University production network must obtain prior approval from the IT Department.

Enforcement

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- The IT Department is responsible for monitoring remote access and addressing inappropriate use of remote access priviliges.

Privacy IT-11

Objective:

Provide guidelines on appropriate management of employee and client privacy

Applies to:

All employees

Key guidelines:

This document describes the University's policy regarding the collection, use, storage, disclosure of and access to personal information in relation to the personal privacy of past and present staff, clients, and vendors of the University.

Handling personal information

- The following policy principles apply to the collection, use, storage, disclosure of and access to personal information:
- The collection and use of personal information must relate directly to legitimate purposes of the University.
- Individuals must be informed of the purpose for which personal information is obtained.

SUSHANT UNIVERSITY SECTOR-55 GURUGRAM

- The University will take all reasonable measures to ensure that the personal information it receives, and holds is up to date.
- The University will take all reasonable measures to store personal information securely.
- Individuals are entitled to have access to their own records, unless unlawful.
- Third party access to personal information may only be granted in accordance with the procedures made pursuant to this policy.
- This Policy does not apply to personal information that is:
    - In a publication available to the public
    - Kept in a library, art gallery or museum for reference, study or exhibition
    - This policy applies to all Institutional areas and is binding on all employees.

Personal Information

- Information obtained by the University which pertains to an individual's characteristics or affairs.
- The personal information can be recorded in any format - for example, in writing, online, digitally or by electronic means.

Complaints

- Any person, whether an employee of the University, who on reasonable grounds believes that a breach of this policy has occurred within the University, may complain to the University's IT Office
- The IT Office shall investigate complaints as expeditiously as practicable and shall provide a written copy of the findings of fact and recommendations made to both the University and to the individual filing the complaint.
- The Head of Human Resources or nominee will determine what action will be taken on any recommendation contained in the findings of the Privacy Officer.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

Contents

Email and Instant Messaging IT_01

Objective:

Provide appropriate guidelines for productively utilizing the University's email system and instant messaging technology that protects the employee and University while benefiting our institution.

Applies to:

All Employees & Students (Active) wherever applicable

Key guidelines:

- The University has established this policy with regard to the acceptable use of University provided electronic messaging systems, including but not limited to email and instant messaging.
- Email and instant messaging is important and sensitive Operations tools. This policy applies to any and all electronic messages composed, sent or received by any Employee / Student or by any person using University provided electronic messaging resources.
- The University sets forth the following policies but reserves the right to modify them at any time in order to support our University:

General

- The University provides electronic messaging resources to assist in conducting University operations.
- All messages composed and/or sent using University provided electronic messaging resources must comply with University policies regarding acceptable communication.
- The University prohibits discrimination based on age, race, gender, sexual orientation or religious or political beliefs. Use of electronic messaging resources to discriminate for any or all of these reasons is prohibited.
- Upon termination or separation from the University, the University will remove all data of email, including any messages, Files stored in the system, regardless of sender or recipient. (DOC-PREPARE)
- Each employee will be assigned a unique email address that is to be used while conducting University Operations via email.

- Employees are prohibited from forwarding electronic messages sent through University provided systems to external messaging systems unless the job requires them for the benefit of the University.
- Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Any employee who discovers a violation of these policies should immediately notify their HOD / Dean or the Human Resources Department.
- Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.

Ownership

- The email/electronic messaging systems are University property. All messages stored in University provided electronic messaging system(s) or composed, sent or received by any employee or non-employee are the property of the University. Electronic messages are NOT the property of any employee.
- The University reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.
- The University reserves the right to alter, modify, re-route or block the delivery of messages as appropriate.
- The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of the University. Employees may use these identifiers only while employed by the University.

Confidentiality

- Messages sent electronically can be intercepted inside or outside the University and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.
- Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.

- Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.
- Employees are prohibited from unauthorized transmission of University trade secrets, confidential information, or privileged communications.
- Unauthorized copying and distribution of copyrighted materials is prohibited.

Security

- The University employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on University provided computer equipment.
- Although the University employs anti-virus software, some virus infected messages can enter the University's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:
  - Be suspicious of messages sent by people not known by you.
  - Do not open attachments unless they were anticipated by you. If you are not sure, always verify the sender is someone you know and that he or she actually sent you the email attachment.
  - Disable features in electronic messaging programs that automatically preview messages before opening them.
  - Do not forward chain letters. Simply delete them.
- The University considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links are often used as a means to verify that you exist.
- Internet message boards are a fertile source from which mass junk e-mailers harvest email addresses and email domains. Do not use University provided email addresses when posting to message boards.
- Upon passout /Withdrawal the emailid which was created as per request from schools / erp will be deleted.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM

Inappropriate use

- Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.
- University provided electronic messaging resources may not be used for the promotion or publication of one's political or religious views, the operation of our Operations or for any undertaking for personal gain.

Internet usage IT-02

Objective:

- Provide appropriate guidelines for accessing and utilizing the Internet through the University's network.

Applies to:

- All employees & Students with authorized access to Internet services

Key guidelines:

- Internet services are authorized to designated employees & Students by their HOD / Dean to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that the University must guard against. For that reason, employees and students are granted access only as a means of providing support in fulfilling their job responsibility.

General

- Internet is provided to employees and students as per IT Firewall policy
- Currently IT Department authorized to provide internet connectivity to all employees only on laptops and desktops as per **Firewall** IT policy.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Currently IT Department authorized to provide internet connectivity to all active student & Staff on their laptop only. It is mandatory to have reputed antivirus (Paid) and Legitimate Software on their laptop.
- Each individual is responsible for the account issued to him/her.
- Sharing Internet accounts or User-ID's is prohibited.
- Organizational use of Internet services must reflect the mission of the University and support the University's goals and objectives.
- These services must support legitimate, mission related activities of the University and be consistent with prudent operational, security, and privacy considerations.
- The Digital Marketting Team along with the respective content owners will take responsibility for all web site content (i.e., "the University web site") and format presentation to reflect the University's mission and in supporting University and departmental objectives, following are the content owner.

Content	Content Owner
School related	School Coordinator / Dean
Exam	COE
Digital	Admission / Marketting
Account	CFAO
Lab	IT
Library	Chief Librarian
HR	HR
Facility	Facility Office

- The University has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
- Any freeware or demo/trial applications/Softwares via the Internet into the University network will need **prior approval from the Individuals HOD / Dean counter signed by the IT-Head**, and then that becomes the property of the University. Any such software may be used only in ways that are consistent with their licenses or copyrights.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- IT-Team has already banned a few sites thru the Firewall,however these sites can be opened on a special request with **approval from "The Registrar" office and IT-Head**

Inappropriate use

- The following uses of University provided Internet access are not permitted:
  - To access, upload, download, or distribute pornographic or sexually explicit material
  - Violate and state, local, or federal law
    - Vandalize or damage the property of any other individual or organization
    - To invade or abuse the privacy of others
    - Violate copyright or use intellectual material without permission
    - To use the network for financial or commercial gain
  - To degrade or disrupt network performance
  - No employee & students may use University facilities knowingly to download or distribute pirated software or data. The use of file swapping software on University computers and University networks is prohibited.
  - No employee may use the University's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
- Specific Softwares which ease the use of downloading the large content is strictly prohibited. Any instances found for the same, can lead to permanent disablement of the said account and necessary action from the HR.

Password security IT 03

Objective:

- Provide guidelines in appropriate management of Operations passwords to maintain adequate security and integrity of all of the University's Operations systems.

Applies to:

- All employees & Students

Key guidelines:

- Maintaining security of the University's Operations applications, software tools, email systems, network facilities, and voice / Video mail are critical to providing data integrity and stability of our systems. Passwords are provided to limit access to these University assets on an as needed basis.
- The University provides access to network, electronic mail and voice mail resources to its employees in support of the University's mission. Passwords are assigned for access to each of these resources to authenticate a user's identity, to protect network users, and to provide security.
- It is the responsibility of each individual to protect and to keep private any and all passwords issued to him/her by the University.
- Although the University strives to manage a secure computing and networking environment, the University cannot guarantee the confidentiality or security of network, e-mail or voice mail passwords from unauthorized disclosure.

- Any employee passwords and changes must be requested by HR-HOD / Dean, post the approval from "The Registrar" Office. This helps monitor and manage the importance of protecting passwords in their distribution and use in such a way that reinforces the integrity of users accessing University systems.

SUSHANT UNIVERSITY * SECTOR-55, GURUGRAM *

- All the user to change the password at first login (Mandatory). Every individual is responsible for the security of his / her password and expected not to share with anyone.

- A network HOD / Dean must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.

- IT Support will handle requests from University HOD / Deans made in one of the following ways:
  - For emailed issue, the users can send an email to ithelpdesk@ansaluniversity.edu.in
- Password Changed requests must be verified by the employee's HOD / Dean.
- System administrators and users assume the following responsibilities:
  - System administrator must protect confidentiality of user's password.
  - User must manage passwords according to the Password Guidelines.
  - User is responsible for all actions and functions performed by his/her account.
  - Suspected password compromise must be reported to IT-Team immediately.
  - Only in case of Emergency or after 5.00pm till 8.00pm, team can reach to Mr Pradeep Lal (#9717295047) / Mr Manoj Kumar (9050470791)

Password Guidelines *Select a Wise Password*

- To minimize password guessing:
- Do not use any part of the account identifier (username, login ID, etc.).
- Use 8 or more characters. mixed alpha and numeric characters
- Use two or three short words that are unrelated. *Keep Your Password Safe*
- Do not let anyone observe you entering your password.
- Do not display your password in your work area or any other highly visible place.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Change your password periodically (every 3 months is recommended).
- Do not reuse old passwords. *Additional Security Practices*
- Ensure your workstation is reasonably secure in your absence from your office. Consider using a password-protected screen saver, logging off or turning off your monitor when you leave the room.

Software usage – IT-04

Objective:

- Provide guidelines on appropriate use of software products utilizing University equipment

Applies to:

All employees & Students

Key guidelines:

- This policy is intended to ensure that all University employees & Students understand that no computer software may be loaded onto or used on any computer owned or leased by the University unless the software is the property of or has been licensed by the University.

General

- Software purchased by the University or residing on University owned computers is to be used only within the terms of the license agreement for that software title.
- Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to the University's Software Usage Policy.
- To purchase software, users must obtain the approval of their department HOD / Dean who will follow the same procedures used for acquiring other University assets.
- All approved software will be purchased through the IT Department & Purchasing Committee.

- The IT - Head and designated members of the IT Department will be the sole governing body for defining appropriate software titles acceptable for use in the University.
- Under no circumstances will third party software applications be loaded onto University owned computer systems without the knowledge of and approval of the IT Department.
- Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any University user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.
- The University does not condone the illegal duplication of software in any form.

Compliance

- We will use all software in accordance with its license agreements.
- Under no circumstances will software be used on University computing resources except as permitted in the University's Software Usage Policy.
- Legitimate software will be provided to all users who need it. University users will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to termination.
- Each user of software purchased and licensed by the University must acquire and use that software only in accordance with the University's Software Usage Policy and the applicable Software License Agreement.
- All users acknowledge that software and its documentation are not owned by the University or an individual but licensed from the software publisher.
- Employees of the University are prohibited from giving University acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.
- All software used by a University entity for University owned computing devices, or purchased with University funds, will be acquired through the appropriate procedures as stated in the University Software Usage Policy.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Any user who determines that there may be a misuse of software within the organization will notify department HOD / Dean or IT-Head.

Registration of software

- Software licensed by the University will not be registered in the name of an individual.
- When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of the University with the job title or department name in which it is used.
- After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of the University. A copy of the license agreement will be filed and maintained by the IT Department's Software License Administrator.
- Once installed, the original installation media should be kept in a safe storage area designated by the IT Department.
- Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. The University's policy is to pay shareware authors the fee they specify for use of their products if the software will be used at the University. Installation and registration of shareware products will be handled the same way as for commercial software products.

Software Audit

- IT will conduct **quarterly** audits of all University owned PCs, including laptops, to ensure the University is in compliance with all software licenses.
- Audits will be conducted using an auditing software product or manual scanning of the machine.
- Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer.
- During these audits, the IT-Department will search for computer viruses and eliminate any that are found.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

PC software standards IT_05

Objective:
Provide guidelines for purchasing and installing software on University PC's

Applies to:
All employees

Key guidelines:
The purpose for this policy is to explain University software standards and to identify the levels of technical support available to the University employees from the IT Department.

Applicability

- This policy applies to all employees of the University requesting the purchase of new computer software and who desire computing support for that application from the IT technical support team.
- The following software standards have been established to ensure efficient and cost-effective use of University computing assets:
  - To help ensure compatibility between applications and releases
  - To provide more effective system administration
- To assist in the computer planning process and enable the realization of long-term goals and the future computing vision
- To ensure cost effective purchasing
- To enable effective tracking of software licenses
- To provide cost effective end user software training
- To facilitate efficient and effective technical support effort

Technical Support

- Software support is provided at several levels and is based on whether the software is the University enterprise standard or department specific.
- The IT Department will not provide support for evaluation software, personally purchased software, illegal copies of software, screen savers, shareware, and non-network software that is not included in the standard software list.

- Software applications determined by IT technical staff to cause computer problems with the University's standard network software will be removed.

IT Department's Role In The Purchase of Hardware And Software

- Assist departments with evaluating new Operations software solution.
- Act as liaison for departments when dealing with computing vendors.
- Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product.
- Assist with hardware and system requirements.
- Install the software as needed.
- Enforce University hardware and software standards.

Standard PC Equipment and Software List

- Standard PC hardware and software configurations are posted on the University's Intranet web site in the IT Department section.
- Contact the Systems Support of the IT Department for questions pertaining to University standards.

Requesting Standard PC Equipment and Software

- Equipment and software requests that are covered by the University's PC Equipment and Software Standards List will be provided quickly as long as appropriate approvals are granted.
- The steps that follow outlines the process for purchasing PC equipment and software:
  - Complete the PC Equipment and Software Request form. (See example in SAMPLES section)
  - Gain approval of the Department HOD / Dean
  - Submit request to IT Department.
  - The IT Department will review the order and forward to Purchasing or will contact Requestor for clarification as needed.
  - The IT Department or Purchasing Department are available for follow-up questions regarding your order as needed.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

Request for a Variance from the PC Hardware or Software Standard

- Complete the "Request for a Variance from the PC Hardware and Software Standard" form.
- Practical and sufficient justification is a key part so be concise in building your case for deviating from the standard.
- Gain approval of the request from your Department HOD / Dean.
- Submit the request to the IT Department's Systems Support for review.
- Your request will be reviewed and either approved or declined based upon justified reasons presented and the IT Department's ability to support the new configuration within the University's network.
- Pay close attention to the *Reason and justification* section. Variances from the University's standards are reviewed closely for compatibility and justification of need.

Inventory and equipment IT-06

Objective:

- Provide management guidelines for managing the use and security of University inventory and equipment

Applies to:

- All Employees & Temporary Staff

Key guidelines:

- PC's, equipment, and supplies are purchased for University employee use and productivity. It is the responsibility of all employees and HOD / Deans to manage the security of University equipment and supplies in order to cost effectively manage the University's expense in these areas.

Allocating equipment to employees

- Equipment is assigned to employees based upon their job function.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- HOD / Deans should maintain a list of equipment allocated to each of his/her employees
- Specific equipment should be tracked by employee includes, but is not limited to:
  - PC's (both desktop and laptop)
  - PC peripherals (scanners, printers, modems, etc.)

Employee Responsibilities

- One of the responsibilities of the HOD / Dean is to collect all allocated equipment issued to an employee who leaves the University and return to the IT-Department. Maintaining the Employee Inventory Allocation Log makes it a simple process.
- Employee to whom the IT Equipment has been issued will be solely responsible for its Repair / Consumables (Battery, Charger, Bag Etc) related to the Equipment issues to him / her till the Equipment is in his / her custody. After 1st January 2021, Official Laptops will be issued to VC Office, Registrar Office, Deans, Directors and HODs Only. Any other laptop to be issued after the special approval of the Registrar. Any use of personal laptops by the Faculty / Staff would require following IT Policy / Guidelines with respect to Antiviruses, Regular Audits, Use of Legitimate Software etc. Antivirus Software will be provided by Sushant University.
- Employees not able to return allocated equipment are responsible for reimbursing the University for the fair market value of the item.

Technology assets

- The IT Department will maintain an accurate inventory of all networked technology assets, laptops, and tangible technology equipment valued at over INR 5000.00 of the University to include the following information:
  - Item
  - Serial #
  - Basic configuration (i.e., HP PC Desktop -4GB RAM, 500GB FD, i3 Processor)
  - Physical location
  - Operating system release level
  - Date placed in service

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Original cost / Operating Lease Cost
- Vendor Detail
-

- Technology equipment will be tagged for easy identification.
- Periodic inventory audits will be conducted to validate the inventory and to identify maintenance issues needed for employee productivity.

PC standards IT-07

Objective:

Provide guidelines for maintaining a standard PC image for the University that addresses the needs of University employees

Applies to:

All employees

Key guidelines:

The University will maintain standard configurations of PC's and laptops in order to enhance employee productivity and supportability of the University's network.

General

- The IT Department will establish the standard configuration of PC hardware and software to be run on University PC's and laptops.
- Multiple configurations are maintained to provide stronger capabilities for employees that need more PC capabilities for their work. These users are called "Power users" and are determined to need the more capable PC's by their HOD / Dean.
- On an exception only basis, a PC may be requested that does not meet the standards configuration. To request a non-standard PC, see the PC Software Standards policy for the *Requesting a Variance from the Standard* request form.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

Network access

- All PC's are network enabled to access the University's network.
- It is the employee's responsibility to maintain appropriate security measures when accessing the network as defined in the University's Password Security policy.

PC Support

- The IT Department will maintain all PC's of the University or will direct you to appropriate measures for maintaining your PC.
- Standard configurations are defined to assist in providing responsive support and to assist in troubleshooting your issue or problem. Deviations from the standards are not permitted except in appropriately reviewed and approved situations.
- For assistance with your PC or peripheral equipment, contact the IT Help Desk.

Employee training

- Basic training for new employees on the use of PC's, accessing the network, and using applications software is held every week by the IT Department
- Training not listed on the IT Department's schedule may be requested or taken outside the University.

Backup procedures

- Network data and programs are backed up daily and archived off site in case of emergency.
- *Data and software on your PC are not backed up and IT Department is not responsible for any data stored on your machine*. If you want to protect data and files used on your PC, you should take one of the following measures:
  - Save the data onto Google Drive and File Server.
- Copy the data to the appropriate Google Drive **associated with email id** or Local Server specifically set up for this purpose. This will ensure your important data is saved and archived daily in our normal backup process.

Virus software

- The University maintains network virus software that will automatically scan your PC for possible viruses each time you log onto the network.
- Downloading or copying data files from external systems and the Internet are prohibited without the IT Department's review and approval in order to protect the integrity of the University network.

Applications software

- Standard software is maintained on all PC's and laptops. See the PC Software Standards policy for more information.
- Under no circumstances are additional software programs allowed to be loaded onto a PC without the review and approval of the IT Department. This is a protective measure to avoid network problems due to viruses and incompatibility issues.

Equipment requests (Adds, Changes, Deletes) IT-08

Objective:

Provide management guidelines on the proper steps and requirements for requesting equipment (adds, deletes, changes)

Applies to:

All Employees

Key guidelines:

Guidelines for ordering new technology equipment or making changes to existing equipment are provided to streamline the order process and to assist the IT Department in fulfilling the request.

General

- Capital equipment items (over INR 5,000/-) must be budgeted and approved for purchase.

- All technology capital requests are reviewed and approved by the IT Department and The Registrar's Office and Finance Departments for appropriate need even when budgeted in the University's annual Capital Budget.
- Only Department HOD / Deans may submit equipment requests.
- Appropriate lead time of at least three weeks should be taken into consideration when ordering new equipment, upgrades
- Equipment relocations, can be completed in 1 working day
- The IT Department will maintain a small inventory of standard PC's and other heavily used equipment to minimize the delay in fulfilling critical orders.
- It is the HOD / Dean's responsibility to provide enough lead time for new orders and change requests in managing his/her department effectively.

Procedures

- Complete the Equipment Request Form for the equipment or service you need.
- Have the Department HOD / Dean Review and approve the request.
- Submit the request to the IT Systems Support organization for review and follow-up.
- The IT Systems Support organization will review the request for appropriateness based upon standards and capital equipment purchasing guidelines of the University. The IT organization will follow-up in one of the following ways:
  - Forward the request to the Purchasing committee to order the equipment.
  - Fill the order if equipment is available in inventory.
  - Contact the requesting department for clarification.
  - Decline the request and forward the request form along with an explanation back to the originating department.

Approved equipment

- If the equipment exists in inventory, the equipment is prepared as needed and installed for the requesting department.
- If the equipment is ordered through Purchasing, the IT Department will either be notified of receipt at the requesting department or the

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

equipment will be sent directly to the IT Department for prep, staging, and installation.

Support

- For normal support of non-working technology equipment, contact support team as per email IDs mentioned below:

Student Support	ithelpdesk@ansaluniversity.edu.in
Staff / Faculty Support	it@ansaluniversity.edu.in

Information security IT-09

Objective:

Provide guidelines that protect the data integrity and proprietary nature of the University's information systems.

Applies to:

All employees

Key guidelines:

- By information security we mean protection of the University's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.
- The purpose of the information security policy is:
- To establish a University-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of University data, applications, networks, and computer systems.
- To define mechanisms that protect the reputation of the University and allow the University to satisfy its legal and ethical responsibilities regarding its networks' and computer systems' connectivity to worldwide networks.

- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.
- The University will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the University's data, network and system resources.
- Security reviews of servers, firewalls, routers, azsand monitoring platforms must be conducted on a regular basis. These reviews will include monitoring access logs and results of intrusion detection software.
- The IT Department must see to it that:
  - The information security policy is updated on a regular basis and published as appropriate.
  - Appropriate training is provided to data owners, data custodians, network and system administrators, and users.
  - Violation of the Information Security Policy may result in disciplinary actions as authorized by the University.

Data classification

- It is essential that all University data be protected. Different types of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.
- The University classifies data in the following three classes:
- High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure.
  - Payroll, personnel, and financial information are also in this class because of privacy requirements.
  - The University recognizes that other data may need to be treated as high risk because it would cause severe damage to the University if disclosed or modified.
  - The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.
- Confidential – Data that would not expose the University to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

(Schools consists /Dean, HODs) to implement the necessary security requirements.

- Public - Information that may be freely disseminated.
- All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the University.
- Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification level and University respective schools and depts.
- Data custodians are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or re-purposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Access control

- Data must have sufficient granularity to allow the appropriate authorized access.
- There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and addressed appropriately.
- The University will have a standard policy that applies to user access rights. This will suffice for most instances.
- Data owners or custodians may enact more restrictive policies for end-user access to their data.
- Access to the network and servers and systems will be achieved by individual and unique logins and will require authentication. Authentication includes the use of passwords other recognized forms of authentication.
- As stated in the Appropriate Use Policy, users must not share usernames and passwords, nor should they be written down or

SUSHANT UNIVERSITY ★★ SECTOR-55, GURUGRAM ★★

recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.

- All users of systems that contain high risk or confidential data must have a strong password, the definition of which will be established and documented by the IT Department.
- Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by the IT Department.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- Users are responsible for safe handling and storage of all University authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access the University's network or system resources.
- If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination.
- Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.
- Transferred employee access must be reviewed and adjusted as found necessary.
- Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

Virus prevention

- The willful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Intrusion detection

- Antivirus must be implemented on all servers and workstations containing data classified as high or confidential risk.
- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

Remote access IT-10

Objective:

Provide guidelines on appropriate use of remote access capabilities to the University's network, Operations applications, and systems

Applies to:

All employees

Key guidelines:

- The purpose of this policy is to define standards for connecting to the University network from a remote location outside the University.

SUSHANT UNIVERSITY ★★ SECTOR-55, GURUGRAM ★★

- These standards are designed to minimize the potential exposure to the University from damages that may result from unauthorized use of the University resources. Damages include the loss of sensitive or confidential University data, intellectual property, damage to critical University internal systems, etc.
- This policy applies to all the University employees, contractors, vendors and agents with a University owned or personally owned computer or workstation used to connect to the University network.
- This policy applies to remote access connections used to do work on behalf of the University, including reading or sending email and viewing Intranet web resources.
- It is the responsibility of the University employees, contractors, vendors and agents with remote access privileges to the University's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the University network.

Remote connection

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password phrases.
- At no time should any University employee provide his/her login or email password to anyone, not even family members.
- University employees and contractors with remote access privileges must ensure that their University owned or personal computer or workstation, which is remotely connected to the University's corporate network, is not connected to any other network at the same time.
- The University employees and contractors with remote access privileges to the University's corporate network must not use non University email accounts or other external resources to conduct the University Operations, thereby ensuring that official Operations is never confused with personal Operations.
- Internet configured for access to the University network must meet minimum authentication requirements established by the IT Department.
- All hosts that are connected to the University internal networks via remote access technologies must use the most up-to-date anti-virus software.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

- Personal equipment that is used to connect to the University's networks must meet the requirements of the University-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the University production network must obtain prior approval from the IT Department.

Enforcement

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- The IT Department is responsible for monitoring remote access and addressing inappropriate use of remote access priviliges.

Privacy IT-11

Objective:

Provide guidelines on appropriate management of employee and client privacy

Applies to:

All employees

Key guidelines:

This document describes the University's policy regarding the collection, use, storage, disclosure of and access to personal information in relation to the personal privacy of past and present staff, clients, and vendors of the University.

Handling personal information

- The following policy principles apply to the collection, use, storage, disclosure of and access to personal information:
- The collection and use of personal information must relate directly to legitimate purposes of the University.
- Individuals must be informed of the purpose for which personal information is obtained.

SUSHANT UNIVERSITY SECTOR-55 GURUGRAM

- The University will take all reasonable measures to ensure that the personal information it receives, and holds is up to date.
- The University will take all reasonable measures to store personal information securely.
- Individuals are entitled to have access to their own records, unless unlawful.
- Third party access to personal information may only be granted in accordance with the procedures made pursuant to this policy.
- This Policy does not apply to personal information that is:
    - In a publication available to the public
    - Kept in a library, art gallery or museum for reference, study or exhibition
    - This policy applies to all Institutional areas and is binding on all employees.

Personal Information

- Information obtained by the University which pertains to an individual's characteristics or affairs.
- The personal information can be recorded in any format - for example, in writing, online, digitally or by electronic means.

Complaints

- Any person, whether an employee of the University, who on reasonable grounds believes that a breach of this policy has occurred within the University, may complain to the University's IT Office
- The IT Office shall investigate complaints as expeditiously as practicable and shall provide a written copy of the findings of fact and recommendations made to both the University and to the individual filing the complaint.
- The Head of Human Resources or nominee will determine what action will be taken on any recommendation contained in the findings of the Privacy Officer.

SUSHANT UNIVERSITY ★ SECTOR-55, GURUGRAM ★

IT POLICY (Details) OF CHANGES REQUIRED (2020)

SUSHANT UNIVERSITY

SECTOR – 55, GURGAON

Dated: October 29, 2020

Sub: IT Policy and Procedures - Revised
Ref: Approved IT Policy dated 17/04/2017.

As referred above, we have an approved IT Policy and Procedure which needs to be revised and updated as per the instructions received from Hon'ble Vice Chancellor's Office.

Few clauses of IT Policy are recommended from IT Department as per attached Summary (Annexure – Changes in IT policy and Procedure). Current IT Policy dated 17/04/2017 is attached herewith for the reference.

It is therefore requested to kindly go through and advise so that New IT Policy can be finalized and made available to all for their reference.

Submitted for kind consideration and necessary approvals please.

29/10/2020

(IT Department)

Sushant University
Erstwhile Ansal University Gurugram

Policies & Procedures

IT Department (Proposed Changes)

On

29/10/2020

Disclaimer

Final Decision:

In Case of any differences of opinion or interpretation of Rules and Regulations or any other issue the decision of Vice-Chancellor / Registrar would be Final and Acceptable to all.

Contents

Email and Instant Messaging IT_01

Objective:

Provide appropriate guidelines for productively utilizing the University's email system and instant messaging technology that protects the employee and University while benefiting our institution.

Applies to:

All Employees & Students (Active) wherever applicable

Key guidelines:

- The University has established this policy with regard to the acceptable use of University provided electronic messaging systems, including but not limited to email and instant messaging.
- Email and instant messaging is important and sensitive Operations tools. This policy applies to any and all electronic messages composed, sent or received by any Employee / Student or by any person using University provided electronic messaging resources.
- The University sets forth the following policies but reserves the right to modify them at any time in order to support our University:

General

- The University provides electronic messaging resources to assist in conducting University operations.
- All messages composed and/or sent using University provided electronic messaging resources must comply with University policies regarding acceptable communication.
- The University prohibits discrimination based on age, race, gender, sexual orientation or religious or political beliefs. Use of electronic messaging resources to discriminate for any or all of these reasons is prohibited.
- Upon termination or separation from the University, the University will remove all data of email, including any messages, Files stored in the system, regardless of sender or recipient. (DOC-PREPARE)
- Each employee will be assigned a unique email address that is to be used while conducting University Operations via email.

- Employees are prohibited from forwarding electronic messages sent through University provided systems to external messaging systems unless the job requires them for the benefit of the University.
- Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Any employee who discovers a violation of these policies should immediately notify their HOD / Dean or the Human Resources Department.
- Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.

Ownership

- The email/electronic messaging systems are University property. All messages stored in University provided electronic messaging system(s) or composed, sent or received by any employee or non-employee are the property of the University. Electronic messages are NOT the property of any employee.
- The University reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.
- The University reserves the right to alter, modify, re-route or block the delivery of messages as appropriate.
- The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of the University. Employees may use these identifiers only while employed by the University.

Confidentiality

- Messages sent electronically can be intercepted inside or outside the University and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.
- Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.

- Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.
- Employees are prohibited from unauthorized transmission of University trade secrets, confidential information, or privileged communications.
- Unauthorized copying and distribution of copyrighted materials is prohibited.

Security

- The University employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on University provided computer equipment.
- Although the University employs anti-virus software, some virus infected messages can enter the University's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:
  - Be suspicious of messages sent by people not known by you.
  - Do not open attachments unless they were anticipated by you. If you are not sure, always verify the sender is someone you know and that he or she actually sent you the email attachment.
  - Disable features in electronic messaging programs that automatically preview messages before opening them.
  - Do not forward chain letters. Simply delete them.
- The University considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links are often used as a means to verify that you exist.
- Internet message boards are a fertile source from which mass junk e-mailers harvest email addresses and email domains. Do not use University provided email addresses when posting to message boards.
- Upon passout /Withdrawal the emailid which was created as per request from schools / erp will be deleted.

Inappropriate use

- Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.
- University provided electronic messaging resources may not be used for the promotion or publication of one's political or religious views, the operation of our Operations or for any undertaking for personal gain.

Internet usage IT-02

Objective:

- Provide appropriate guidelines for accessing and utilizing the Internet through the University's network.

Applies to:

- All employees & Students with authorized access to Internet services

Key guidelines:

- Internet services are authorized to designated employees & Students by their HOD / Dean to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that the University must guard against. For that reason, employees and students are granted access only as a means of providing support in fulfilling their job responsibility.

General

- Internet is provided to employees and students as per IT Firewall policy
- Currently IT department authorized to provide internet connectivity to all employees only on Ansal University owned laptops and desktops as per **Firewall** IT policy. No Personal gadgets (laptop/mobile/tablets etc.) is allowed to connect campus network.

- Currently IT department authorized to provide internet connectivity to all active students on their laptop only. It is mandatory to have reputed antivirus (Paid) on their laptop and Legal Software and legitimate Software.
- Each individual is responsible for the account issued to him/her.
- Sharing Internet accounts or User-ID's is prohibited.
- Organizational use of Internet services must reflect the mission of the University and support the University's goals and objectives.
- These services must support legitimate, mission related activities of the University and be consistent with prudent operational, security, and privacy considerations.
- The Digital Marketting Team along with the respective content owners will take responsibility for all web site content (i.e., "the University web site") and format presentation to reflect the University's mission and in supporting University and departmental objectives, following are the content owner.

Content	Content Owner
School related	School Coordinator / Dean
Exam	COE
Digital	Admission / Marketting
Account	CFAO
Lab	IT
Library	Chief Librarian
HR	HR
Facility	Facility Office

- The University has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
- Any freeware or demo/trial applications/Softwares via the Internet into the University network will need **prior approval from the Individuals HOD / Dean counter signed by the IT-Head**, and then that becomes the property of the University. Any such software

may be used only in ways that are consistent with their licenses or copyrights.

- IT-Team has already banned a few sites thru the Firewall,however these sites can be opened on a special request with **approval from "The Registrar" office and IT-Head**

Inappropriate use

- The following uses of University provided Internet access are not permitted:
  - To access, upload, download, or distribute pornographic or sexually explicit material
  - Violate and state, local, or federal law
    - Vandalize or damage the property of any other individual or organization
    - To invade or abuse the privacy of others
    - Violate copyright or use intellectual material without permission
    - To use the network for financial or commercial gain
  - To degrade or disrupt network performance
  - No employee & students may use University facilities knowingly to download or distribute pirated software or data. The use of file swapping software on University computers and University networks is prohibited.
  - No employee may use the University's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
- Specific Softwares which ease the use of downloading the large content is strictly prohibited. Any instances found for the same, can lead to permanent disablement of the said account and necessary action from the HR.

Password security IT_03

Objective:

- Provide guidelines in appropriate management of Operations passwords to maintain adequate security and integrity of all of the University's Operations systems.

Applies to:

- All employees & Students

Key guidelines:

- Maintaining security of the University's Operations applications, software tools, email systems, network facilities, and voice / Video mail are critical to providing data integrity and stability of our systems. Passwords are provided to limit access to these University assets on an as needed basis.
- The University provides access to network, electronic mail and voice mail resources to its employees in support of the University's mission. Passwords are assigned for access to each of these resources to authenticate a user's identity, to protect network users, and to provide security.
- It is the responsibility of each individual to protect and to keep private any and all passwords issued to him/her by the University.
- Although the University strives to manage a secure computing and networking environment, the University cannot guarantee the confidentiality or security of network, e-mail or voice mail passwords from unauthorized disclosure.

- Any employee passwords and changes must be requested by a HR-HOD / Dean, post the approval from "The Registrar" Office. This helps monitor and manage the importance of protecting passwords in their distribution and use in such a way that reinforces the integrity of users accessing University systems.
- All the user to change the password at first login (Mandatory). Every individual is responsible for the security of his / her password and expected not to share with anyone.

- A network HOD / Dean must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.

- IT Support will handle requests from University HOD / Deans made in one of the following ways:
  - For emailed issue, the users can send an email to ithelpdesk@ansaluniversity.edu.in
- Password Changed requests must be verified by the employee's HOD / Dean.
- System administrators and users assume the following responsibilities:
  - System administrator must protect confidentiality of user's password.
  - User must manage passwords according to the Password Guidelines.
  - User is responsible for all actions and functions performed by his/her account.
  - Suspected password compromise must be reported to IT-Team immediately.
  - Only in case of Emergency or after 5.00pm till 8.00pm, team can reach to Mr Pradeep Lal (#9717295047) / Mr Manoj Kumar (9050470791)

Password Guidelines *Select a Wise Password*

- To minimize password guessing:
- Do not use any part of the account identifier (username, login ID, etc.).
- Use 8 or more characters. mixed alpha and numeric characters

- Use two or three short words that are unrelated. *Keep Your Password Safe*
- Do not let anyone observe you entering your password.
- Do not display your password in your work area or any other highly visible place.
- Change your password periodically (every 3 months is recommended).
- Do not reuse old passwords. *Additional Security Practices*
- Ensure your workstation is reasonably secure in your absence from your office. Consider using a password-protected screen saver, logging off or turning off your monitor when you leave the room.

Software usage – IT-04

Objective:

- Provide guidelines on appropriate use of software products utilizing University equipment

Applies to:

All employees & Students

Key guidelines:

- This policy is intended to ensure that all University employees & Students understand that no computer software may be loaded onto or used on any computer owned or leased by the University unless the software is the property of or has been licensed by the University.

General

- Software purchased by the University or residing on University owned computers is to be used only within the terms of the license agreement for that software title.
- Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to the University's Software Usage Policy.

- To purchase software, users must obtain the approval of their department HOD / Dean who will follow the same procedures used for acquiring other University assets.
- All approved software will be purchased through the IT Department & Purchasing Committee.
- The IT - Head and designated members of the IT Department will be the sole governing body for defining appropriate software titles acceptable for use in the University.
- Under no circumstances will third party software applications be loaded onto University owned computer systems without the knowledge of and approval of the IT Department.
- Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any University user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.
- The University does not condone the illegal duplication of software in any form.

Compliance

- We will use all software in accordance with its license agreements.
- Under no circumstances will software be used on University computing resources except as permitted in the University's Software Usage Policy.
- Legitimate software will be provided to all users who need it. University users will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to termination.
- Each user of software purchased and licensed by the University must acquire and use that software only in accordance with the University's Software Usage Policy and the applicable Software License Agreement.
- All users acknowledge that software and its documentation are not owned by the University or an individual but licensed from the software publisher.
- Employees of the University are prohibited from giving University acquired software to anyone who does not have a valid software

license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.

- All software used by a University entity for University owned computing devices, or purchased with University funds, will be acquired through the appropriate procedures as stated in the University Software Usage Policy.
- Any user who determines that there may be a misuse of software within the organization will notify department HOD / Dean or IT-Head.

Registration of software

- Software licensed by the University will not be registered in the name of an individual.
- When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of the University with the job title or department name in which it is used.
- After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of the University. A copy of the license agreement will be filed and maintained by the IT Department's Software License Administrator.
- Once installed, the original installation media should be kept in a safe storage area designated by the IT Department.
- Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. The University's policy is to pay shareware authors the fee they specify for use of their products if the software will be used at the University. Installation and registration of shareware products will be handled the same way as for commercial software products.

Software Audit

- IT will conduct **quarterly** audits of all University owned PCs, including laptops, to ensure the University is in compliance with all software licenses.
- Audits will be conducted using an auditing software product or manual scanning of the machine.

- Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer.
- During these audits, the IT-Department will search for computer viruses and eliminate any that are found.

PC software standards IT_05

Objective:
Provide guidelines for purchasing and installing software on University PC's

Applies to:
All employees

Key guidelines:
The purpose for this policy is to explain University software standards and to identify the levels of technical support available to the University employees from the IT Department.

Applicability

- This policy applies to all employees of the University requesting the purchase of new computer software and who desire computing support for that application from the IT technical support team.
- The following software standards have been established to ensure efficient and cost-effective use of University computing assets:
  - To help ensure compatibility between applications and releases
  - To provide more effective system administration
- To assist in the computer planning process and enable the realization of long-term goals and the future computing vision
- To ensure cost effective purchasing
- To enable effective tracking of software licenses
- To provide cost effective end user software training
- To facilitate efficient and effective technical support effort

Technical Support

- Software support is provided at several levels and is based on whether the software is the University enterprise standard or department specific.
- The IT Department will not provide support for evaluation software, personally purchased software, illegal copies of software, screen savers, shareware, and non-network software that is not included in the standard software list.

- Software applications determined by IT technical staff to cause computer problems with the University's standard network software will be removed.

IT Department's Role In The Purchase of Hardware And Software

- Assist departments with evaluating new Operations software solution.
- Act as liaison for departments when dealing with computing vendors.
- Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product.
- Assist with hardware and system requirements.
- Install the software as needed.
- Enforce University hardware and software standards.

Standard PC Equipment and Software List

- Standard PC hardware and software configurations are posted on the University's Intranet web site in the IT Department section.
- Contact the Systems Support of the IT Department for questions pertaining to University standards.

Requesting Standard PC Equipment and Software

- Equipment and software requests that are covered by the University's PC Equipment and Software Standards List will be provided quickly as long as appropriate approvals are granted.
- The steps that follow outlines the process for purchasing PC equipment and software:
  - Complete the PC Equipment and Software Request form. (See example in SAMPLES section)
  - Gain approval of the Department HOD / Dean
  - Submit request to IT Department.
  - The IT Department will review the order and forward to Purchasing or will contact Requestor for clarification as needed.
  - The IT Department or Purchasing Department are available for follow-up questions regarding your order as needed.

Request for a Variance from the PC Hardware or Software Standard

- Complete the "Request for a Variance from the PC Hardware and Software Standard" form.
- Practical and sufficient justification is a key part so be concise in building your case for deviating from the standard.
- Gain approval of the request from your Department HOD / Dean.
- Submit the request to the IT Department's Systems Support for review.
- Your request will be reviewed and either approved or declined based upon justified reasons presented and the IT Department's ability to support the new configuration within the University's network.
- Pay close attention to the *Reason and justification* section. Variances from the University's standards are reviewed closely for compatibility and justification of need.

Inventory and equipment IT-06

Objective:

- Provide management guidelines for managing the use and security of University inventory and equipment

Applies to:

- All Employees & Temporary Staff

Key guidelines:

- PC's, equipment, and supplies are purchased for University employee use and productivity. It is the responsibility of all employees and HOD / Deans to manage the security of University equipment and supplies in order to cost effectively manage the University's expense in these areas.

Allocating equipment to employees

- Equipment is assigned to employees based upon their job function.
- HOD / Deans should maintain a list of equipment allocated to each of his/her employees
- Specific equipment should be tracked by employee includes, but is not limited to:
  - PC's (both desktop and laptop)
  - PC peripherals (scanners, printers, modems, etc.)

Employee Responsibilities

- One of the responsibilities of the HOD / Dean is to collect all allocated equipment issued to an employee who leaves the University and return to the IT-Department. Maintaining the Employee Inventory Allocation Log makes it a simple process.
- Employee to whom the IT Equipment has been issued will be solely responsible for its Repair / Consumables (Battery, Charger, Bag Etc) related to the Equipment issues to him / her till the Equipment is in his / her custody. Also new faculty joining after 01/11/2020 will not be ssued any Laptop. Also the personal Laptops to be used by Faculty

would require to follow IT Policy / Guidelines with respect to antiviruses, regular audits etc.

- Employees not able to return allocated equipment are responsible for reimbursing the University for the fair market value of the item.

Technology assets

- The IT Department will maintain an accurate inventory of all networked technology assets, laptops, and tangible technology equipment valued at over INR 5000.00 of the University to include the following information:
  - Item
  - Serial #
  - Basic configuration (i.e., HP PC Desktop -4GB RAM, 500GB FD, i3 Processor)
  - Physical location
  - Operating system release level
  - Date placed in service
  - Original cost / Operating Lease Cost
  - Vendor Detail
  -
- Technology equipment will be tagged for easy identification.
- Periodic inventory audits will be conducted to validate the inventory and to identify maintenance issues needed for employee productivity.

PC standards IT-07

Objective:
Provide guidelines for maintaining a standard PC image for the University that addresses the needs of University employees

Applies to:

All employees

Key guidelines:
The University will maintain standard configurations of PC's and laptops in order to enhance employee productivity and supportability of the University's network.

General

- The IT Department will establish the standard configuration of PC hardware and software to be run on University PC's and laptops.
- Multiple configurations are maintained to provide stronger capabilities for employees that need more PC capabilities for their work. These users are called "Power users" and are determined to need the more capable PC's by their HOD / Dean.
- On an exception only basis, a PC may be requested that does not meet the standards configuration. To request a non-standard PC, see the PC Software Standards policy for the *Requesting a Variance from the Standard* request form.

Network access

- All PC's are network enabled to access the University's network.
- It is the employee's responsibility to maintain appropriate security measures when accessing the network as defined in the University's Password Security policy.

PC Support

- The IT Department will maintain all PC's of the University or will direct you to appropriate measures for maintaining your PC.

- Standard configurations are defined to assist in providing responsive support and to assist in troubleshooting your issue or problem. Deviations from the standards are not permitted except in appropriately reviewed and approved situations.
- For assistance with your PC or peripheral equipment, contact the IT Help Desk.

Employee training

- Basic training for new employees on the use of PC's, accessing the network, and using applications software is held every week by the IT Department
- Training not listed on the IT Department's schedule may be requested or taken outside the University.

Backup procedures

- Network data and programs are backed up daily and archived off site in case of emergency.
- ***Data and software on your PC is not backed up and IT Department is not responsible for any data stored on your machine***. If you want to protect data and files used on your PC, you should take one of the following measures:
  - Save the data onto Google Drive and File Server.
- Copy the data to the appropriate Google Drive **associated with email id** and store it within your personal file folder specifically set up for this purpose. This will ensure your important data is saved and archived daily in our normal backup process.
- Large amounts of data (over 2 GB) should be discussed with the IT Department before uploading to a Google Drive (Storage) associated with email id.

Virus software

- The University maintains network virus software that will automatically scan your PC for possible viruses each time you log onto the network.
- Downloading or copying data files from external systems and the Internet are prohibited without the IT Department's review and approval in order to protect the integrity of the University network.

Applications software

- Standard software is maintained on all PC's and laptops. See the PC Software Standards policy for more information.
- Under no circumstances are additional software programs allowed to be loaded onto a PC without the review and approval of the IT Department. This is a protective measure to avoid network problems due to viruses and incompatibility issues.

Equipment requests (Adds, Changes, Deletes) IT-08

Objective:
Provide management guidelines on the proper steps and requirements for requesting equipment (adds, deletes, changes)

Applies to:

All Employees

Key guidelines:
Guidelines for ordering new technology equipment or making changes to existing equipment are provided to streamline the order process and to assist the IT Department in fulfilling the request.

General

- Capital equipment items (over INR 5,000/-) must be budgeted and approved for purchase.
- All technology capital requests are reviewed and approved by the IT Department and The Registrar's Office and Finance Departments for appropriate need even when budgeted in the University's annual Capital Budget.
- Only Department HOD / Deans may submit equipment requests.
- Appropriate lead time of at least three weeks should be taken into consideration when ordering new equipment, upgrades
- Equipment relocations, can be completed in 1 working day
- The IT Department will maintain a small inventory of standard PC's and other heavily used equipment to minimize the delay in fulfilling critical orders.
- It is the HOD / Dean's responsibility to provide enough lead time for new orders and change requests in managing his/her department effectively.

Procedures

- Complete the Equipment Request Form for the equipment or service you need.

- Have the Department HOD / Dean Review and approve the request.
- Submit the request to the IT Systems Support organization for review and follow-up.
- The IT Systems Support organization will review the request for appropriateness based upon standards and capital equipment purchasing guidelines of the University. The IT organization will follow-up in one of the following ways:
    - Forward the request to the Purchasing committee to order the equipment.
    - Fill the order if equipment is available in inventory.
    - Contact the requesting department for clarification.
    - Decline the request and forward the request form along with an explanation back to the originating department.

Approved equipment

- If the equipment exists in inventory, the equipment is prepared as needed and installed for the requesting department.
- If the equipment is ordered through Purchasing, the IT Department will either be notified of receipt at the requesting department or the equipment will be sent directly to the IT Department for prep, staging, and installation.

Support

- For normal support of non-working technology equipment, contact support team as per email IDs mentioned below:

Student Support	ithelpdesk@ansaluniversity.edu.in
Staff / Faculty Support	it@ansaluniversity.edu.in

Information security IT-09

Objective:

Provide guidelines that protect the data integrity and proprietary nature of the University's information systems.

Applies to:

All employees

Key guidelines:

- By information security we mean protection of the University's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.
- The purpose of the information security policy is:
- To establish a University-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of University data, applications, networks, and computer systems.
- To define mechanisms that protect the reputation of the University and allow the University to satisfy its legal and ethical responsibilities regarding its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.
- The University will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the University’s data, network and system resources.
- Security reviews of servers, firewalls, routers, azsand monitoring platforms must be conducted on a regular basis. These reviews will include monitoring access logs and results of intrusion detection software.
- The IT Department must see to it that:
    - The information security policy is updated on a regular basis and published as appropriate.

- Appropriate training is provided to data owners, data custodians, network and system administrators, and users.
- Violation of the Information Security Policy may result in disciplinary actions as authorized by the University.

Data classification

- It is essential that all University data be protected. Different types of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.
- The University classifies data in the following three classes:
- High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure.
  - Payroll, personnel, and financial information are also in this class because of privacy requirements.
  - The University recognizes that other data may need to be treated as high risk because it would cause severe damage to the University if disclosed or modified.
  - The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.
- Confidential – Data that would not expose the University to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility (Schools consists /dean,HODs) to implement the necessary security requirements.
- Public - Information that may be freely disseminated.
- All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the University.
- Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification level and University respective schools and depts.

- Data custodians are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or re-purposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Access control

- Data must have sufficient granularity to allow the appropriate authorized access.
- There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and addressed appropriately.
- The University will have a standard policy that applies to user access rights. This will suffice for most instances.
- Data owners or custodians may enact more restrictive policies for end-user access to their data.
- Access to the network and servers and systems will be achieved by individual and unique logins and will require authentication. Authentication includes the use of passwords other recognized forms of authentication.
- As stated in the Appropriate Use Policy, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.
- All users of systems that contain high risk or confidential data must have a strong password, the definition of which will be established and documented by the IT Department.
- Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by the IT Department.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.

- Users are responsible for safe handling and storage of all University authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access the University's network or system resources.
- If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination.
- Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.
- Transferred employee access must be reviewed and adjusted as found necessary.
- Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

Virus prevention

- The willful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Intrusion detection

- Antivirus must be implemented on all servers and workstations containing data classified as high or confidential risk.

- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

Remote access IT-10

Objective:

Provide guidelines on appropriate use of remote access capabilities to the University's network, Operations applications, and systems

Applies to:

All employees

Key guidelines:

- The purpose of this policy is to define standards for connecting to the University network from a remote location outside the University.
- These standards are designed to minimize the potential exposure to the University from damages that may result from unauthorized use of the University resources. Damages include the loss of sensitive or confidential University data, intellectual property, damage to critical University internal systems, etc.
- This policy applies to all the University employees, contractors, vendors and agents with a University owned or personally owned computer or workstation used to connect to the University network.
- This policy applies to remote access connections used to do work on behalf of the University, including reading or sending email and viewing Intranet web resources.
- It is the responsibility of the University employees, contractors, vendors and agents with remote access privileges to the University's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the University network.

Remote connection

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password phrases.
- At no time should any University employee provide his/her login or email password to anyone, not even family members.

- University employees and contractors with remote access privileges must ensure that their University owned or personal computer or workstation, which is remotely connected to the University's corporate network, is not connected to any other network at the same time.
- The University employees and contractors with remote access privileges to the University's corporate network must not use non University email accounts or other external resources to conduct the University Operations, thereby ensuring that official Operations is never confused with personal Operations.
- Internet configured for access to the University network must meet minimum authentication requirements established by the IT Department.
- All hosts that are connected to the University internal networks via remote access technologies must use the most up-to-date anti-virus software.
- Personal equipment that is used to connect to the University's networks must meet the requirements of the University-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the University production network must obtain prior approval from the IT Department.

Enforcement

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- The IT Department is responsible for monitoring remote access and addressing inappropriate use of remote access priviliges.

Privacy IT-11

Objective:

Provide guidelines on appropriate management of employee and client privacy

Applies to:

All employees

Key guidelines:

This document describes the University's policy regarding the collection, use, storage, disclosure of and access to personal information in relation to the personal privacy of past and present staff, clients, and vendors of the University.

Handling personal information

- The following policy principles apply to the collection, use, storage, disclosure of and access to personal information:
- The collection and use of personal information must relate directly to legitimate purposes of the University.
- Individuals must be informed of the purpose for which personal information is obtained.
- The University will take all reasonable measures to ensure that the personal information it receives, and holds is up to date.
- The University will take all reasonable measures to store personal information securely.
- Individuals are entitled to have access to their own records, unless unlawful.
- Third party access to personal information may only be granted in accordance with the procedures made pursuant to this policy.
- This Policy does not apply to personal information that is:
    - In a publication available to the public
    - Kept in a library, art gallery or museum for reference, study or exhibition
    - This policy applies to all Institutional areas and is binding on all employees.

Personal Information

- Information obtained by the University which pertains to an individual's characteristics or affairs.
- The personal information can be recorded in any format - for example, in writing, online, digitally or by electronic means.

Complaints

- Any person, whether an employee of the University, who on reasonable grounds believes that a breach of this policy has occurred within the University, may complain to the University's IT Office
- The IT Office shall investigate complaints as expeditiously as practicable and shall provide a written copy of the findings of fact and recommendations made to both the University and to the individual filing the complaint.
- The Head of Human Resources or nominee will determine what action will be taken on any recommendation contained in the findings of the Privacy Officer.

Policies & Procedures

IT Department

17-Apr-2017

Disclaimer

Final Decision:

In Case of any differences of opinion or interpretation of Rules and Regulations or any other issue the decision of Vice-Chancellor / Registrar would be Final and Acceptable to all.

Policy Validity till December -2020

ANSAL UNIVERSITY * SECTOR-55, GURGAON *

Contents

ANSAL UNIVERSITY SECTOR-55, GURGAON

Email and Instant Messaging IT_01

Objective:

Provide appropriate guidelines for productively utilizing the University's email system and instant messaging technology that protects the employee and University while benefiting our institution.

Applies to:

All Employees & Students wherever applicable

Key guidelines:

- The University has established this policy with regard to the acceptable use of University provided electronic messaging systems, including but not limited to email and instant messaging.
- Email and instant messaging are important and sensitive Operations tools. This policy applies to any and all electronic messages composed, sent or received by any Employee / Student or by any person using University provided electronic messaging resources.
- The University sets forth the following policies but reserves the right to modify them at any time in order to support our University:

General

- The University provides electronic messaging resources to assist in conducting University operations.
- All messages composed and/or sent using University provided electronic messaging resources must comply with University policies regarding acceptable communication.
- The University prohibits discrimination based on age, race, gender, sexual orientation or religious or political beliefs. Use of electronic messaging resources to discriminate for any or all of these reasons is prohibited.
- Upon termination or separation from the University, the University will deny all access to electronic messaging resources, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.

ANSAL UNIVERSITY * SECTOR 55 * GURGAON

- Each employee will be assigned a unique email address that is to be used while conducting University Operations via email.
- Employees are prohibited from forwarding electronic messages sent through University provided systems to external messaging systems, unless the job requires them for the benefit of the University.
- Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Any employee who discovers a violation of these policies should immediately notify their HOD / Dean or the Human Resources Department.
- Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.

Ownership

- The email/electronic messaging systems are University property. All messages stored in University provided electronic messaging system(s) or composed, sent or received by any employee or non-employee are the property of the University. Electronic messages are NOT the property of any employee.
- The University reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received.
- The University reserves the right to alter, modify, re-route or block the delivery of messages as appropriate.
- The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of the University. Employees may use these identifiers only while employed by the University.

Confidentiality

- Messages sent electronically can be intercepted inside or outside the University and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.
- Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.

- Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.
- Employees are prohibited from unauthorized transmission of University trade secrets, confidential information, or privileged communications.
- Unauthorized copying and distribution of copyrighted materials is prohibited.

Security

- The University employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on University provided computer equipment.
- Although the University employs anti-virus software, some virus infected messages can enter the University's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:
    - Be suspicious of messages sent by people not known by you.
    - Do not open attachments unless they were anticipated by you. If you are not sure, **always verify** the sender is someone you know and that he or she actually sent you the email attachment.
    - Disable features in electronic messaging programs that automatically preview messages before opening them.
    - Do not forward chain letters. Simply delete them.
- The University considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links are often used as a means to verify that you exist.
- Internet message boards are a fertile source from which mass junk e-mailers harvest email addresses and email domains. Do not use University provided email addresses when posting to message boards.

Inappropriate use

- Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.

ANSAL UNIVERSITY * SECTOR-55, GURGAON *

- University provided electronic messaging resources may not be used for the promotion or publication of one's political or religious views, the operation of our Operations or for any undertaking for personal gain.

ANSAL UNIVERSITY ★ SECTOR-55, GURGAON ★

Internet usage IT-02

Objective:

- Provide appropriate guidelines for accessing and utilizing the Internet through the University's network.

Applies to:

- All employees & Students with authorized access to Internet services

Key guidelines:

- Internet services are authorized to designated employees by their HOD / Dean to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that the University must guard against. For that reason, employees are granted access only as a means of providing support in fulfilling their job responsibility.

General

- Internet accounts are approved for designated employees by their immediate HOD / Dean to provide tools that assist in their work.
- Each individual is responsible for the account issued to him/her.
- Sharing Internet accounts or User-ID's is prohibited.
- Organizational use of Internet services must reflect the mission of the University and support the University's goals and objectives.
- These services must support legitimate, mission related activities of the University and be consistent with prudent operational, security, and privacy considerations.
- The Digital Marketting Team along with the IT-Head led Internet Steering Committee will take responsibility for all web site content (i.e., "the University web site") and format presentation to reflect the University's mission and in supporting University and departmental objectives.
- The University has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
- Any freeware or demo/trial applications/Softwares via the Internet into the University network will need **prior approval from the Individuals HOD / Dean counter signed by the IT-Head**, and then that becomes

ANSAL UNIVERSITY * SECTOR-55, GURGAON *

the property of the University. Any such software may be used only in ways that are consistent with their licenses or copyrights.

- IT-Team has already banned a few sites thru the Firewall, however these sites can be opened on a special request with **approval from "The Registrar" office and IT-Head**

Inappropriate use

- The following uses of University provided Internet access are not permitted:
  - To access, upload, download, or distribute pornographic or sexually explicit material
  - Violate and state, local, or federal law
    - Vandalize or damage the property of any other individual or organization
    - To invade or abuse the privacy of others
    - Violate copyright or use intellectual material without permission
    - To use the network for financial or commercial gain
  - To degrade or disrupt network performance
  - No employee may use University facilities knowingly to download or distribute pirated software or data. The use of file swapping software on University computers and University networks is prohibited.
  - No employee may use the University's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
- Specific Softwares which ease the use of downloading the large content is strictly prohibited. Any instances found for the same, can lead to permanent disablement of the said account and necessary action from the HR.

ANSAL UNIVERSITY SECTOR-55, GURGAON

Password security IT 03

Objective:

- Provide guidelines in appropriate management of Operations passwords to maintain adequate security and integrity of all of the University's Operations systems.

Applies to:

- All employees & Students

Key guidelines:

- Maintaining security of the University's Operations applications, software tools, email systems, network facilities, and voice / Video mail are critical to providing data integrity and stability of our systems. Passwords are provided to limit access to these University assets on an as needed basis.
- The University provides access to network, electronic mail and voice mail resources to its employees in support of the University's mission. Passwords are assigned for access to each of these resources to authenticate a user's identity, to protect network users, and to provide security.
- It is the responsibility of each individual to protect and to keep private any and all passwords issued to him/her by the University.
- Although the University strives to manage a secure computing and networking environment, the University cannot guarantee the confidentiality or security of network, e-mail or voice mail passwords from unauthorized disclosure.
- New employee passwords and changes must be requested by a HR-HOD / Dean, post the approval from "The Registrar" Office. This helps monitor and manage the importance of protecting passwords in their distribution and use in such a way that reinforces the integrity of users accessing University systems.
- A network HOD / Dean must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.

ANSAL UNIVERSITY SECTOR-55, GURGAON

- IT Support will handle requests from University HOD / Deans made in one of the following ways:
  - Creating a Ticket on the ticketing tool: http://www.ansaluniversity.edu.in/ithelpdesk
  - Only in case of Emergency or after 5.00 PM till 8.00 PM team can be reached on ext 468.
- Password account requests must be verified by the employee's HOD / Dean.
- The IT Department will delete all passwords of exiting employees upon notification from Human Resources.
- System administrators and users assume the following responsibilities:
  - System administrator must protect confidentiality of user's password.
  - User must manage passwords according to the Password Guidelines.
  - User is responsible for all actions and functions performed by his/her account.
  - Suspected password compromise must be reported to IT-Team immediately.

Password Guidelines *Select a Wise Password*

- To minimize password guessing:
- Do not use any part of the account identifier (username, login ID, etc.).
- Use 8 or more characters.
- Use mixed alpha and numeric characters.
- Use two or three short words that are unrelated. *Keep Your Password Safe*
- Do not tell your password to anyone.
- Do not let anyone observe you entering your password.
- Do not display your password in your work area or any other highly visible place.
- Change your password periodically (every 3 months is recommended).
- Do not reuse old passwords. *Additional Security Practices*
- Ensure your workstation is reasonably secure in your absence from your office. Consider using a password-protected screen saver, logging off or turning off your monitor when you leave the room.

ANSAL UNIVERSITY SECTOR-55, GURGAON

Software usage – IT-04

Objective:

- Provide guidelines on appropriate use of software products utilizing University equipment

Applies to:

All employees & Students

Key guidelines:

- This policy is intended to ensure that all University employees & Students understand that no computer software may be loaded onto or used on any computer owned or leased by the University unless the software is the property of or has been licensed by the University.

General

- Software purchased by the University or residing on University owned computers is to be used only within the terms of the license agreement for that software title.
- Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to the University's Software Usage Policy.
- To purchase software, users must obtain the approval of their department HOD / Dean who will follow the same procedures used for acquiring other University assets.
- All approved software will be purchased through the IT Department & Purchasing Committee.
- The IT - Head and designated members of the IT Department will be the sole governing body for defining appropriate software titles acceptable for use in the University.
- Under no circumstances will third party software applications be loaded onto University owned computer systems without the knowledge of and approval of the IT Department.
- Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any University user who makes,

ANSAL UNIVERSITY ★ SECTOR-55, GURGAON

acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.

- The University does not condone the illegal duplication of software in any form.

Compliance

- We will use all software in accordance with its license agreements.
- Under no circumstances will software be used on University computing resources except as permitted in the University's Software Usage Policy.
- Legitimate software will be provided to all users who need it. University users will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to termination.
- Each user of software purchased and licensed by the University must acquire and use that software only in accordance with the University's Software Usage Policy and the applicable Software License Agreement.
- All users acknowledge that software and its documentation are not owned by the University or an individual, but licensed from the software publisher.
- Employees of the University are prohibited from giving University acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.
- All software used by a University entity for University owned computing devices, or purchased with University funds, will be acquired through the appropriate procedures as stated in the University Software Usage Policy.
- Any user who determines that there may be a misuse of software within the organization will notify department HOD / Dean or IT-Head.

Registration of software

- Software licensed by the University will not be registered in the name of an individual.
- When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher.

Software must be registered in the name of the University with the job title or department name in which it is used.

- After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of the University. A copy of the license agreement will be filed and maintained by the IT Department's Software License Administrator.
- Once installed, the original installation media should be kept in a safe storage area designated by the IT Department.
- Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. The University's policy is to pay shareware authors the fee they specify for use of their products if the software will be used at the University. Installation and registration of shareware products will be handled the same way as for commercial software products.

Software Audit

- IT will conduct periodic audits of all University owned PCs, including laptops, to ensure the University is in compliance with all software licenses.
- Audits will be conducted using an auditing software product or manual scanning of the machine.
- Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the user's computer.
- During these audits, the IT-Department will search for computer viruses and eliminate any that are found.
- The full cooperation of all users is required during software audits.

ANSAL UNIVERSITY SECTOR-55, GURGAON

PC software standards IT_05

Objective:
Provide guidelines for purchasing and installing software on University PC's

Applies to:
All employees

Key guidelines:
The purpose for this policy is to explain University software standards and to identify the levels of technical support available to the University employees from the IT Department.

Applicability

- This policy applies to all employees of the University requesting the purchase of new computer software and who desire computing support for that application from the IT technical support team.
- The following software standards have been established to ensure efficient and cost effective use of University computing assets:
  - To help ensure compatibility between applications and releases
  - To provide more effective system administration
- To assist in the computer planning process and enable the realization of long term goals and the future computing vision
- To ensure cost effective purchasing
- To enable effective tracking of software licenses
- To provide cost effective end user software training
- To facilitate efficient and effective technical support effort

Technical Support

- Software support is provided at several levels and is based on whether the software is the University enterprise standard or department specific.
- The IT Department will not provide support for evaluation software, personally purchased software, illegal copies of software, screen savers, shareware, and non-network software that is not included in the standard software list.

ANSAL UNIVERSITY * SECTOR-55, GURGAON *

- Software applications determined by IT technical staff to cause computer problems with the University's standard network software will be removed.

IT Department's Role In The Purchase of Hardware And Software

- Assist departments with evaluating new Operations software solution.
- Act as liaison for departments when dealing with computing vendors.
- Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product.
- Assist with hardware and system requirements.
- Install the software as needed.
- Enforce University hardware and software standards.

Standard PC Equipment and Software List

- Standard PC hardware and software configurations are posted on the University's Intranet web site in the IT Department section.
- Contact the Systems Support of the IT Department for questions pertaining to University standards.

Requesting Standard PC Equipment and Software

- Equipment and software requests that are covered by the University's PC Equipment and Software Standards List will be provided quickly as long as appropriate approvals are granted.
- The steps that follow outlines the process for purchasing PC equipment and software:
  - Complete the PC Equipment and Software Request form. (See example in SAMPLES section)
  - Gain approval of the Department HOD / Dean
  - Submit request to IT Department.
  - The IT Department will review the order and forward to Purchasing or will contact Requestor for clarification as needed.
  - The IT Department or Purchasing Department are available for follow-up questions regarding your order as needed.

Request for a Variance from the PC Hardware or Software Standard

- Complete the "Request for a Variance from the PC Hardware and Software Standard" form.
- Practical and sufficient justification is a key part so be concise in building your case for deviating from the standard.
- Gain approval of the request from your Department HOD / Dean.
- Submit the request to the IT Department's Systems Support for review.
- Your request will be reviewed and either approved or declined based upon justified reasons presented and the IT Department's ability to support the new configuration within the University's network.
- Pay close attention to the *Reason and justification* section. Variances from the University's standards are reviewed closely for compatibility and justification of need.

Inventory and equipment IT-06

Objective:

- Provide management guidelines for managing the use and security of University inventory and equipment

Applies to:

- All Employees & Temporary Staff

Key guidelines:

- PC's, equipment, and supplies are purchased for University employee use and productivity. It is the responsibility of all employees and HOD / Deans to manage the security of University equipment and supplies in order to cost effectively manage the University's expense in these areas.

Allocating equipment to employees

- Equipment is assigned to employees based upon their job function.
- HOD / Deans should maintain a list of equipment allocated to each of his/her employees
- Specific equipment should be tracked by employee includes, but is not limited to:
    - PC's (both desktop and laptop)
    - PC peripherals (scanners, printers, modems, etc.)
    - Cell phones
    - Building access keys and access cards

Employee termination

- One of the responsibilities of the HOD / Dean is to collect all allocated equipment issued to an employee who leaves the University and return to the IT-Department. Maintaining the Employee Inventory Allocation Log makes it a simple process.
- Employees not able to return allocated equipment are responsible for reimbursing the University for the fair market value of the item.

Technology assets

- The IT Department will maintain an accurate inventory of all networked technology assets, laptops, and tangible technology equipment valued at over INR 5000.00 of the University to include the following information:
  - Item
  - University ID# (Bar coded Tag ID)
  - Serial #
  - Basic configuration (i.e., HP PC Desktop -4GB RAM, 500GB FD, i3 Processor)
  - Physical location
  - Operating system release level
  - Date placed in service
  - Original cost / Operating Lease Cost
  - Vendor Detail
- Technology equipment will be tagged for easy identification.
- Periodic inventory audits will be conducted to validate the inventory and to identify maintenance issues needed for employee productivity.

ANSAL UNIVERSITY SECTOR-55, GURGAON

PC standards IT-07

Objective:

Provide guidelines for maintaining a standard PC image for the University that addresses the needs of University employees

Applies to:

All employees

Key guidelines:

The University will maintain standard configurations of PC's and laptops in order to enhance employee productivity and supportability of the University's network.

General

- The IT Department will establish the standard configuration of PC hardware and software to be run on University PC's and laptops.
- Multiple configurations are maintained to provide stronger capabilities for employees that need more PC capabilities for their work. These users are called "Power users" and are determined to need the more capable PC's by their HOD / Dean.
- On an exception only basis, a PC may be requested that does not meet the standards configuration. To request a non-standard PC, see the PC Software Standards policy for the *Requesting a Variance from the Standard* request form.

Network access

- All PC's are network enabled to access the University's network.
- It is the employee's responsibility to maintain appropriate security measures when accessing the network as defined in the University's Password Security policy.

PC Support

- The IT Department will maintain all PC's of the University or will direct you to appropriate measures for maintaining your PC.

- Standard configurations are defined to assist in providing responsive support and to assist in troubleshooting your issue or problem. Deviations from the standards are not permitted except in appropriately reviewed and approved situations.
- For assistance with your PC or peripheral equipment, contact the IT Help Desk.

Employee training

- Basic training for new employees on the use of PC's, accessing the network, and using applications software is held every week by the IT Department. Published schedules are available on the IT Department's Intranet site.
- Training not listed on the IT Department's schedule may be requested or taken outside the University.

Backup procedures

- Network data and programs are backed up daily and archived off site in case of emergency.
- ***Data and software on your PC is not backed up and IT Department is not responsible for any data stored on your machine***. If you want to protect data and files used on your PC, you should take one of the following measures:
    - Save the data onto network drives / pen drives.
- Copy the data to the appropriate network server and store it within your personal file folder specifically set up for this purpose. This will insure your important data is saved and archived daily in our normal backup process.
- Large amounts of data (over 2 GB) should be discussed with the IT Department before uploading to a network server.

Virus software

- The University maintains network virus software that will automatically scan your PC for possible viruses each time you log onto the network.
- Downloading or copying data files from external systems and the Internet are prohibited without the IT Department's review and approval in order to protect the integrity of the University network.

Applications software

- Standard software is maintained on all PC's and laptops. See the PC Software Standards policy for more information.
- Under no circumstances are additional software programs allowed to be loaded onto a PC without the review and approval of the IT Department. This is a protective measure to avoid network problems due to viruses and incompatibility issues.

Equipment requests(Adds, Changes, Deletes) IT-08

Objective:

Provide management guidelines on the proper steps and requirements for requesting equipment (adds, deletes, changes)

Applies to:

All Employees

Key guidelines:

Guidelines for ordering new technology equipment or making changes to existing equipment are provided to streamline the order process and to assist the IT Department in fulfilling the request.

General

- Capital equipment items (over INR 5,000/-) must be budgeted and approved for purchase.
- All technology capital requests are reviewed and approved by the IT Department and The Registrar's Office and Finance Departments for appropriate need even when budgeted in the University's annual Capital Budget.
- Only Department HOD / Deans may submit equipment requests.
- Published response times for various new equipment installations, changes, etc. is available within the SLA defined and approved by IT Head
- Appropriate lead time of at least three weeks should be taken into consideration when ordering new equipment, upgrades
- Equipment relocations, can be completed in 1 working day
- The IT Department will maintain a small inventory of standard PC's and other heavily used equipment to minimize the delay in fulfilling critical orders.
- It is the HOD / Dean's responsibility to provide enough lead time for new orders and change requests in managing his/her department effectively.

Procedures

- Complete the Equipment Request Form (see Sample) for the equipment or service you need.
- Have the Department HOD / Dean Review and approve the request.
- Submit the request to the IT Systems Support organization for review and follow-up.
- The IT Systems Support organization will review the request for appropriateness based upon standards and capital equipment purchasing guidelines of the University. The IT organization will follow-up in one of the following ways:
    - Forward the request to the Purchasing committee to order the equipment.
    - Fill the order if equipment is available in inventory.
    - Contact the requesting department for clarification.
    - Decline the request and forward the request form along with an explanation back to the originating department.

Approved equipment

- If the equipment exists in inventory, the equipment is prepared as needed and installed for the requesting department.
- If the equipment is ordered through Purchasing, the IT Department will either be notified of receipt at the requesting department or the equipment will be sent directly to the IT Department for prep, staging, and installation.

Support

- For normal support of non-working technology equipment, contact your IT Support Help Desk at #468.

Information security IT-09

Objective:

Provide guidelines that protect the data integrity and proprietary nature of the University's information systems.

Applies to:

All employees

Key guidelines:

- By information security we mean protection of the University's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.
- The purpose of the information security policy is:
- To establish a University-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of University data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of the University and allow the University to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.
- The University will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the University's data, network and system resources.
- Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews will include monitoring access logs and results of intrusion detection software.
- The IT Department must see to it that:
    - The information security policy is updated on a regular basis and published as appropriate.

- Appropriate training is provided to data owners, data custodians, network and system administrators, and users.
- Each department must appoint a person responsible for security, incident response, periodic user access reviews, and education of information security policies for the department.
- Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis.
- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data.
- Violation of the Information Security Policy may result in disciplinary actions as authorized by the University.

Data classification

- It is essential that all University data be protected. Different types of data require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance.
- The University classifies data in the following three classes:
- High Risk - Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure.
  - Payroll, personnel, and financial information are also in this class because of privacy requirements.
  - The University recognizes that other data may need to be treated as high risk because it would cause severe damage to the University if disclosed or modified.
  - The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.
- Confidential – Data that would not expose the University to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.
- Public - Information that may be freely disseminated.
- All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be

ANSAL UNIVERSITY * SEC 55, GURGAON *

consistent when the data is replicated and as it flows through the University.

- Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification level.
- No University owned system or network can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Data custodians are responsible for creating data repositories and data transfer procedures that protect data in the manner appropriate to its classification.
- High risk and confidential data must be encrypted during transmission over insecure channels.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or re-purposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Access control

- Data must have sufficient granularity to allow the appropriate authorized access.
- There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized and addressed appropriately.
- Where possible and financially feasible, more than one person must have full rights to any University owned server storing or transmitting high risk data.
- The University will have a standard policy that applies to user access rights. This will suffice for most instances.
- Data owners or custodians may enact more restrictive policies for end-user access to their data.
- Access to the network and servers and systems will be achieved by individual and unique logins, and will require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.

ANSAL UNIVERSITY * SECTOR-55, GURGAON *

- As stated in the Appropriate Use Policy, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system from unauthorized use.
- All users of systems that contain high risk or confidential data must have a strong password, the definition of which will be established and documented by the IT Department.
- Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by the IT Department.
- Passwords must not be placed in emails unless they have been encrypted.
- Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- Users are responsible for safe handling and storage of all University authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access the University's network or system resources.
- If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so that the device can be disabled.
- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination.
- Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.
- Transferred employee access must be reviewed and adjusted as found necessary.
- Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

ANSAL UNIVERSITY ★ SECTOR-55, GURGAON ★

- Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.
- There should be a documented procedure for reviewing system logs.

Virus prevention

- The willful introduction of computer viruses or disruptive/destructive programs into the University environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Intrusion detection

- Intruder detection must be implemented on all servers and workstations containing data classified as high or confidential risk.
- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

ANSAL UNIVERSITY ★ SECTOR-55, GURGAON ★

Remote access IT-10

Objective:
Provide guidelines on appropriate use of remote access capabilities to the University's network, Operations applications, and systems

Applies to:
All employees

Key guidelines:

- The purpose of this policy is to define standards for connecting to the University network from a remote location outside the University.
- These standards are designed to minimize the potential exposure to the University from damages that may result from unauthorized use of the University resources. Damages include the loss of sensitive or confidential University data, intellectual property, damage to critical University internal systems, etc.
- This policy applies to all the University employees, contractors, vendors and agents with a University owned or personally owned computer or workstation used to connect to the University network.
- This policy applies to remote access connections used to do work on behalf of the University, including reading or sending email and viewing Intranet web resources.
- Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, etc.
- It is the responsibility of the University employees, contractors, vendors and agents with remote access privileges to the University's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the University network.

Remote connection

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password phrases.

- At no time should any University employee provide his/her login or email password to anyone, not even family members.
- University employees and contractors with remote access privileges must ensure that their University owned or personal computer or workstation, which is remotely connected to the University's corporate network, is not connected to any other network at the same time.
- The University employees and contractors with remote access privileges to the University's corporate network must not use non University email accounts (i.e., Yahoo, AOL), or other external resources to conduct the University Operations, thereby ensuring that official Operations is never confused with personal Operations.
- Routers for dedicated ISDN lines configured for access to the University network must meet minimum authentication requirements established by the IT Department.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- All hosts that are connected to the University internal networks via remote access technologies must use the most up-to-date anti-virus software.
- Third party connections must comply with requirements defined by the IT Department.
- Personal equipment that is used to connect to the University's networks must meet the requirements of the University-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the University production network must obtain prior approval from the IT Department.

Enforcement

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- The IT Department is responsible for monitoring remote access and addressing inappropriate use of remote access priviliges.

ANSAL UNIVERSITY * SECTOR-55, GURGAON *

Privacy IT-11

Objective:

Provide guidelines on appropriate management of employee and client privacy

Applies to:

All employees

Key guidelines:

This document describes the University's policy regarding the collection, use, storage, disclosure of and access to personal information in relation to the personal privacy of past and present staff, clients, and vendors of the University.

Handling personal information

- The following policy principles apply to the collection, use, storage, disclosure of and access to personal information:
- The collection and use of personal information must relate directly to legitimate purposes of the University.
- Individuals must be informed of the purpose for which personal information is obtained.
- The University will take all reasonable measures to ensure that the personal information it receives and holds is up to date.
- The University will take all reasonable measures to store personal information securely.
- Individuals are entitled to have access to their own records, unless unlawful.
- Third party access to personal information may only be granted in accordance with the procedures made pursuant to this policy.
- This Policy does not apply to personal information that is:
    - In a publication available to the public
    - Kept in a library, art gallery or museum for reference, study or exhibition
    - This policy applies to all Institutional areas and is binding on all employees.

Personal Information

- Information obtained by the University which pertains to an individual's characteristics or affairs.
- The personal information can be recorded in any format - for example, in writing, online, digitally or by electronic means.

Privacy Officer

- A member of the University appointed to monitor compliance with this policy and to hear and determine complaints arising under the policy.
- The Privacy Officer's responsibilities will include: ☐ Receiving and investigating complaints
- Ongoing review of the University's practices and procedures to ensure that it complies with this Policy, current legislation and best practice
- Educating University employees on their responsibilities under this policy and the *Information Privacy Act*.
- The Privacy Officer will be appointed by the Vice-Chancellor / Registrar

Complaints

- Any person, whether or not an employee of the University, who on reasonable grounds believes that a breach of this policy has occurred within the University, may complain to the University's Privacy Officer.
- The Privacy Officer shall investigate complaints as expeditiously as practicable and shall provide a written copy of the findings of fact and recommendations made to both the University and to the individual filing the complaint.
- The Head of Human Resources or nominee will determine what action will be taken on any recommendation contained in the findings of the Privacy Officer.

ANSAL UNIVERSITY ★ SECTOR-55, GURGAON ★

Ansal University

Address: Golf Course Road, Sector 55, Gurugram, Haryana 122003

Phone: 0124 475 0400

Date.....

Name..... **EMP ID**.....

School..... **Department**.....

Contact No. ..... **Email Id**.....

Address .....

Laptop Specification

Brand..... **Model No**..... **Serial No**.....

RAM..... **HDD**..... **CPU**.....

Other Accessories.....

Cost of the Laptop (INR).....

UNDERTAKING

(All Faculty/Staff issued with a laptop/notebook are required to read and sign the following policy)

I_____presently faculty/Staff of _____ (Course)

_____(Department) do hereby affirm and undertakes as under:

1. That I have received the Laptop/Notebook along with all required software and power cable from my University/Department having following details:
   (a) Name (Laptop/Notebook)_____
   (b) Model No./Serial No._____
   (c) Bag/Carry Case: YES/NO

2. I acknowledge that laptop/notebook provided to me is to enhance my studies and learning in my College/Department. I will not allow anyone else to use this laptop. I will ensure that the laptop is available to me at College/Department on teaching days.

3. That if the hard disk is damaged or unusable or any other technical fault arises in the same, I will report the same to the Authorities in this regard without fail and I will not disable the antivirus software installed on the machine or alter system files or change hardware settings.

ANSAL UNIVERSITY SECTOR-55, GURGAON

4. That I am required to take reasonable precautions against loss, theft or damage of my laptop/notebook. I agree to safeguard the laptop by taking reasonable precautions against theft while my laptop is unattended at College/Department and other places.

5. That I will keep the machine away from food and drink at all times, and store it in a clean location. I will not leave the Laptop/Notebook, where it might be accidentally damaged. I will make sure the laptop is secure in its protective bag when travelling between locations.

6. That I undertake not to use unauthorised copies of software or pirated media, which are in breach of copyright. I also understand that the use of unauthorised software may damage the Laptop/Notebook. I undertake not to do this.

7. That If the Laptop/Notebook issued to me is lost or damaged, it will be my own responsibility and I will be liable to pay the compensation for the cost of repair/and if not repairable then the full cost of the device as decided by the competent authority.

8. That I will return the laptop/notebook to the College/Department at any time, when called upon to do by the College/Department.

9. That I will bring the notebook to my College/ Department for inspection at least once in three months during my course of study or as per the directives issued to me from time to time.

10. All equipment's (laptop, battery, charger & the cover box etc.) must be returned to the College at the end of the session.

WIRELESS NETWORK AND INTERNET ACCESS SERVICES:

11. That the network services provided by the College/Department/University reserves the right to monitor the use of the facilities and that the same may, in certain situations, be compelled to access and to disclose information such as e-mail and message, content and data relating to the use of Internet facilities.

12. That I undertake not to engage in any activity which:
    a) Disrupts the intended use of the resources.
    b) Wastes resources (people, capacity, computer, network, data etc.)
    c) Compromises the legal rights of others.
    d) Modifies, damages or destroys computing resources or the data on them.
    e) Jeopardize, in any way, the integrity, performance or reliability of the College's/Department's/University's computing resources by indulging in circumvent data protection schemes, to uncover security loopholes, to "hack" into systems or to interfere with the intended operation of the computer resources.

13. The Laptops are under five year's comprehensive warranty Hewlett Packard India Sales Pvt. Ltd. Any problem faced by me related to the working of Laptops, inform Ansal University's IT Department.

14. I have read and understood the above terms and conditions and I agree to abide by them.

Sign of Dean	Sign of Registrar	Sign of I.T. Head	Faculty/Staff Sign
.....	.....	.....	.....

ANSAL UNIVERSITY * SECTOR-55, GURGAON