D. Y. PATIL EDUCATION SOCIETY
INSTITUTION DEEMED TO BE UNIVERSITY,
KOLHAPUR

IT AND ICT POLICY

Contents

PREAMBLE

Objective:

To use the IT facility(s) / system(s) / infrastructure in a respectful, ethical, professional and legal manner.

Present IT infrastructure of D. Y. Patil Education Society (Institution Deemed to be University) consists of,

1. Hardware and software resources in University building, D. Y. Patil Hospital & Research Center Kadamwadi, Kolhapur and Nursing college campus at Kadamwadi, Kolhapur.

   The hardware resources include client desktop computing machines, printers, scanners, surveillance systems, network devices like switches, routers, access points etc. The intranet of the University consists of all the computing resources connected using CAT-6 cable and WiFi in University building serving various disciplines and departments. There is a separate local area network (LAN) built for Hospital at Kadamwadi and another LAN for Nursing college at Kadamwadi, these two networks and the University network is again interconnected using optical fiber and hence the complete network acts as a single local area network (LAN) of D. Y. Patil Education Society (Institution Deemed to be University). Apart from the computing machines there are surveillance systems installed at all the places to keep electronic eye on the movements happening at various places. All the resources mentioned above are configured to achieve the objective of their installation. As the LAN cannot work in isolation mode from WAN hence there is an internet connection of 1GBPS from National Knowledge Network serving all the Computers in the LAN with well-organized IP scheme and internet access speed. This is achieved using Virtual LAN ports configured at Firewall (SonicWall NSA 4600) with allocation of required bandwidth to each port. Apart from this, specific rules are set in firewall which helps in optimized usage of internet bandwidth. Firewall is helping users in University to block viruses coming from WAN and infecting computing devices into LAN. DDoS attack protection (UDP/ICMP/SYN flood), IPv4/IPv6 support and many other services including core network services are provided by firewall. Windows server 2012 R2 running on Dell power edge T420 server is used to capture all the biometric punched trigger times and employee / student ID's to mark attendance of staff and student. Biometric machines installed at various locations have auto push technology which are configured to push the punch triggers to WAN IP address 14.139.120.71. Port 5005 is configured for Real time make biometric machines and port 82 is configured for ESSL make biometric machines. Web applications (e-time tracker lite for ESSL and realsoft for Realtime) hosted for these machines are receiving the punch triggers and are storing that data into mysql database which intern is synched with JUNO ERP attendance module.

2. **Microsoft Office 365 - On cloud Software As A Service (SaaS)**

   Majority of the documents digitally created by the University are in the format of Word, Excel, and PowerPoint, some in PDF's are required to be shared with collogues or communicated to other authorities and hence there is a need of communication platforms and archive space for these files. All these facilities are available in Office 365 platform and gives lots of functional flexibility. O365 provides outlook with 50Gb space, One Drive with 1 Tb space, teams and many other applications to every account holder. University has started its teaching learning process online using Microsoft Teams since 10th April 2020 due to COVID-19 pandemic situations. Demonstration of practical's, Assignments, internal examination and final examination is also conducted in blended mode for which Teams has played a vital role in remote proctoring and communication.

3. **Juno ERP - On cloud Software As A Service (SaaS)**

   With more than 20 modules Juno ERP deployment started in 2017 and is now functional with Academics, Attendance, LMS, Faculty profile, Inventory, Fees modules implemented with their provided functionalities.

   All of the resources mentioned above are functioning to achieve goals of the University, but these resources are required to be used and maintained in respectful, ethical, professional and legal manner. As the IT is evolving with new dimensions, planning of the required resources is necessity of the time. IT resources are required to keep up and running all the time hence there is a need to have a policy which will frame every aspect while using IT.

4. **Hospital Management Information System**

   HMIS consists of more than 30 modules covering, Outpatient Department, Laboratory Information Service, Radiology Information Service, Inventory, Pharmacy, Inpatients, Billing, Nursing station, Operation Theatre etc.

5. **Picture Archiving and Communication System (PACS)**

   MEDSYNAPTIC PACS empowers the health care industry with effective & user-friendly image transmission system, it allows distribution of images within and outside the Hospital without any client software installation, can be operated directly from the browser providing unsurpassed ease of use from anywhere.

ACCEPTABLE USAGE POLICY FOR COMPUTER, INTERNET & INTRANET.

- University's computers, networks, and information systems exist to promote shared access for computing, communication, and information systems necessary to support the missions of teaching, work & research, Thus, all Users of information facilities have a responsibility to use these systems in a respectful, ethical, professional, and legal manner.

- University Acceptable Usage Policy applies to any individual (Director, faculty, staff, Students and guests) using University's owned or leased computers, networks, Internet connections, and communications systems transmitting data, voice, or video information. Activities involving these systems shall be in accordance with College policy and information technology ACT, 2000(IT ACT) and international laws.

- All Users of University's information facilities agree to demonstrate respect for (1) the privacy of others, (2) intellectual property rights (copyrights, trademarks, licenses, etc.) and ownership of information, (3) the operation and integrity of the various information systems.

- While respecting an individual employee's privacy, University cannot guarantee confidentiality. The IT Team has the right to monitor all aspects of college systems, including sites, instant messaging systems, chat or news groups visited by users, material downloaded or uploaded by users, and e-mail sent and/or received by users. Such information stored or transmitted on college/school systems by employees are considered college property and subject to disclosure to appropriate system administrators in a need-to-know situation, such as the investigation of a complaint. World Wide Web information located in designated web directories will be considered public information if read access is granted. The maintenance, operation, and security of computing resources require responsible System personnel to monitor and access the system. IT Team reserves the right to do periodic host scans to ensure there are no security holes on machines connected to the College/School network.

- All University/College/School employees are responsible for ensuring that permanent university/College/School records are stored on appropriate archival media. Designated Employee who fails to appropriately archive important university information may be subject to disciplinary action due to negligence.

All Users will abide by the following conditions:

- Users are responsible for all the activities that occur in or through their accounts and/or their computers.

- Account holders shall not share access to individual computer accounts.

- Account holders shall keep their passwords secret.

- Users may only access information that is their own, information to which they have been given explicit documentable authorization to access, or public information.

- Users, in respect of the operation and integrity of a shared system, shall not attempt to interfere with the normal operation, integrity, validity, or the security of any College or non-college information system.

- Users shall abide by the regulations posted in computer labs and on College Information systems and offices.

- ☐ Users shall not attempt to misappropriate or guess system passwords nor inappropriately use system accounts.

- ☐ Users shall not use other computers or programs to decode passwords, access restricted system control information, or monitor restricted system or network communications.

- ☐ Users shall not intentionally monopolize or waste resources such as Central Processing Unit (CPU) time, network bandwidth, disk storage (pen drive, CDs, DVDs, HDD), printers, paper, manuals, etc.

- ☐ Users shall report possible security violations and/or problems to appropriate systems administrators of respective college, offices only.

- ☐ Users shall not use College, Official systems to store or transmit obscene or Pornographic material in violation of state and Cyber law.

- ☐ College information systems shall not be used for non-University-affiliated work, on-going Commercial business enterprises or for any unauthorized mass mailings.

- ☐ Users shall not use College, offices systems to abuse, verbally assault, defame, Harass, intimidate, or otherwise annoy an individual or individuals.

- ☐ Users should not play games on college, office computers and should not engage in any form of chatting (voice or video) unless official.

- ☐ Staff and faculty members should restrain in storing personal data on college computers.
- ☐ Account holders shall abide by all relevant state and federal laws governing copyrights, trademarks, licensing terms for corporate software, ownership of information, and related material.

ANNUAL MAINTAINANCE CONTRACTS

- The new purchased material has standard company warranty as per the terms and condition discussed and mentioned in the purchase order. During the warranty period the company takes care of replacement of any faulty material.

- After warranty period is over, configuration is given to different vendors who quote for the charges for each system for annual maintenance of the system.

- After agreement on the terms and condition a Memorandum of Understanding is signed between the institute and the party.

- A copy of the MOU will be maintained in IT Team as well as in the respective Institute and offices.

- From the start date as in the memorandum the vendor takes care of internal cleaning of the system, replacing the faulty spares and routine maintenance check.

- The period for the routine checkup and cleaning is defined previously.

- If any breakdown or fault occurs in the working of the system, a complaint is immediately lodged with the vendor and a ticket is booked against the complaint.

- The complaint /ticket no. issued from the vendor is maintained in the Call Register.

- The vendor sends its service engineer to the concerned location to solve the problem. Either the problem is solved on site or the system is carried to the service center depending upon the nature of problem.

- On solving the problem the service engineer gives a service report stating the nature of problem and the action taken on it. This service report is maintained in the service report file and the call is closed for that ticket /complaint number.

- **Description of the Maintenance Work.**
  1. The maintenance services will consist of
     a) Attending complaints raised by various departments/individuals on daily basis.
     b) Onsite preventive and corrective maintenance of computers connected in LAN and peripherals where the system is installed as indicated from time to time.
     c) The maintenance contract will include necessary repairs to the installed systems and replacement of defective/damaged parts, components and other accessories included in the maintenance contract list without any extra cost.

- **Types of Maintenance Contracts**
  1. Server Maintenance. (Firewall, Biometric Web Server)

  2. Software Maintenance. (Required for customized software's & subscribed online software's)
     a. Office 365
     b. JUNO Systems Enterprise Resource Planning (ERP)

  3. Website Maintenance (Required for database and other features on web servers)

  4. Hardware Maintenance. (Active Components like routers, hardware firewalls, Printers, Desktops / Laptops, LCD Projectors, UPS)

- **Benefits of Maintenance Contracts**

- **Total support at a fixed price**

  One price covers the cost of spare parts and labor for a defined period, so in a way the expenses are known and predetermined.

- **Quick Response**

  Priority service for maintenance customers is guaranteed with a prompt service and reduced downtime.

- **On Site Service and Repair**

  Avoid the hassle and inconvenience of taking the broken-down hardware to a service center.

- **Preventative Maintenance**

  Delivers regular care for your hardware investment – reduces the frequency of breakdowns and improves performance.

- **Replacement equipment**

  For some hardware such as printers, if it cannot be repaired within a 24 hour period, the vendor will provide a replacement for the duration of repair.

- **Experienced Professional Technicians**

  Solve the problem causing minimum inconvenience with the help of experienced professional technical support through the vendor.

VIRUS PROTECTION POLICY

- University's IT infrastructure, data, files, and information systems must be protected from virus attack and other malicious code.
- Every computer, laptops and server in the University will have antivirus software installed.
- University will have nominated antivirus software applications.
- Central IT Dept. will ensure that the antivirus protection update is installed on all LAN connected computers every week after update is installed on Primary Server.
- Once a virus has infected a PC, it can rapidly spread to other PCs through the use of removable disks and via computer networks so USB ports will be disabled where ever applicable on all computers in University.
- The objective of this principle is to protect the University's computer systems from destruction or corruption of information and/or system processes. Hence Antivirus software on all computers and servers will be configured to examine all removable disks upon viewing / opening any file on the floppy disks.
- Computer viruses when discovered should be deleted or cleaned from the disk. No other option is to be made available.
- IT Dept. staff shall be notified whenever a virus is found.
- UNDER NO CIRCUMSTANCE anti-virus software should be disabled on any server, computer or laptop.
- All users in University will accept the antivirus software instructions for automated cleaning or quarantining of files with virus and will also notify the Network Administrator in writing by the ticketing system or email.
- IT Dept. shall ensure that antivirus software is always up-to-date with the latest virus signatures, which can be downloaded off the Server if an update to a computer has not occurred automatically.
- All networked computers antivirus applications will be configured to have the latest antivirus definition files (if not already installed on that computer) automatically sent to them from the server each time that computer is logged onto the Network.
- No freeware, pirated & trail antivirus software will be installed on a computers, laptops of the University.

COMPUTER USAGE

- ☐ All IT equipment owned by University will be made available for use by University personnel and other approved persons on the understanding that the Users abide by University IT Policies.
- ☐ University's computers are not 'owned' by any University personnel and as such will be made available for use by other University's personnel when requested to do so by University management.
- ☐ Sharing of University's Workstations is to be encouraged to increase the effective use of University IT resources and endeavor to reduce the overall number of computers that University uses and thus has to support and budget for in regards to maintenance and replacement.
- ☐ Users should not attempt to move, repair, reconfigure, modify, or attach external devices to University's computers, laptop's.
- ☐ No food or drink is allowed on or near any IT equipment in University.
- ☐ Users are instructed, not to use University IT equipment for recreational use (i.e. playing games, social web browsing or other activities that use the limited IT resources and budget of the University).
- ☐ Users are responsible for following any additional rules posted in computer facilities, offices or made known through other University communications channels.
- ☐ The owner of any personal machine brought into University campus is responsible for all Users of his/her machine.
- ☐ The owner of any personal machine brought into University campus is responsible for all network traffic to and from his/her machine.
- ☐ Private machines may not use the University's network for commercial gain or profit, or for personal use of any kind.
- ☐ Any staff member requiring University's computer Network access (not including Internet mail) from their allocated PC shall obtain a written authorization as per current Policies for Network Access.
- ☐ Access to unauthorized personal folders and Administration & Accounts folders is prohibited.
- ☐ Changes in access privileges for a file or folder will be documented and it should be approved by the head of Section/Division managing the relevant data, file or folder.
- ☐ No games are to be installed on any University's IT equipment. No personnel should at any time be allowed to play any games on any University's computers.
- ☐ The installing of software onto University computers or servers is prohibited at all times downloading software is strictly forbidden) and can jeopardize the IT Teams efforts to protect its systems. All downloading must be performed by IT Support staff, after written approval has been granted by IT management, and will then be acquired using University's antivirus checking procedures.
- ☐ No personal application software shall be installed on any of the University's computers.
- ☐ No copyright material shall be installed illegally on University's computers, or utilized in breach of its license agreement.

WI-FI ACCEPTABLE USE POLICY

- University WLAN Wi-Fi is the on-campus wireless network. It provides Internet and University WLAN Network access for the entire campus, including the hostels. The features of this service are a privilege and not a right. All students, faculty, staff, and guests are expected to practice responsible computing and to adhere to these requirements for acceptable use when accessing University WLAN Wi-Fi:

1. Policy Violations :
   Do not to use University WLAN Wi-Fi in a way that violates state law, federal law, or the established IT policies of University.
2. Responsibility :
   Use of University WLAN Wi-Fi is controlled by login with your user name and password / MAC ID. You are responsible for all activity conducted under your user name. You are expected to take reasonable precautions to prevent unauthorized and/or abusive use by other individuals.
3. Commercial Use :
   Your University WLAN Wi-Fi connection is for personal use only. Do not use University WLAN Wi-Fi for any commercial purpose or to host data services for other individuals or groups.
4. User Deception :
   Do not attempt to deceive others about your identity in electronic communications or other network traffic.
5. Improper Access :
   Do not access accounts, files, or other information belonging to other groups WLAN Wi-Fi users or Internet users without their knowledge and explicit consent.
6. Harassment:
   Do not use your group WLAN Wi-Fi connection to threaten, intimidate, or harass other individuals.
7. Copyrights :
   You are required to comply with Indian copyright law and the copyright policy of DYP University. Copying, downloading, or electronic transfer of copyrighted materials without the authorization of the copyright owner is against the law and may result in civil and criminal penalties, including fines and imprisonment.
8. Virus Protection :
   You are expected to comply with the University WLAN Virus Protection policy. If you connect your computer to University WLAN Wi-Fi, you must install licensed anti-virus software. You must also keep up-to-date with the latest security releases.
9. Personal Wireless Networks :
   Personal wireless networks in DYP University network are prohibited, in accordance with the Networking Policy.
10. Excess Usage or Abuse :
    If your University WLAN Wi-Fi connection uses excess bandwidth, sends disruptive signals, or violates any of the above policies, it will be subject to limitations or possible disconnection. Any other use or misuse of the connection that constitutes a violation of University Regulations could result in administrative or disciplinary procedures through the IT Team.

Network Security Monitoring

The University WLAN Wi-Fi network connection may be subject to monitoring, with cause, for security, legal, or troubleshooting purposes. This may include monitoring for bandwidth usage, security related incidents, or a request from legal/law enforcement authorities. In addition, the IT Team reserves the right to scan the network to assist in identifying and protecting against exploitable security vulnerabilities (e.g., viruses or worms) in efforts to preserve network integrity. Information gathered in such scans will be used only for the explicit purpose of monitoring network security.

Policy Updates

Due to the dynamic nature of technology and the Internet, the University WLAN Wi-Fi Acceptable Use policy is subject to change.

Wi-Fi Registration Policy

- ☐ Only registered handheld devices are allowed on Wi-Fi.
- ☐ Unknown device should not connect without registration on DYP University WLAN.
- ☐ Submit Registration form to system administrator to connect DYP University.
- ☐ System Admin will check & audit laptop.

  Checklist
  - ✓ Pirated software's not allowed.
  - ✓ Licensed Antivirus should be used.
  - ✓ Use Genuine Operating System.

- ☐ For Student & staff we will be provided Username & Password for Internet Authentication or MAC authentication will be followed.
  - ✓ Do not share your Username & Password with anyone.
  - ✓ Change your password often by contacting respective system administrators.
  - ✓ Use College E-mail ID for communication.
- ☐ By registering your Device, you accept personal responsibility for abiding by DYP University WLAN Computer.
- ☐ Before Registration Read carefully 'Information Technology Access Agreement' & other policy's & Notices. You have to abide by theses policy's while registration.
- ☐ Student/staff must have to sign declaration form if they are using institutes property.

Wi-Fi Internet Usage

- ☐ Illegal behavior such as unauthorized sharing of copyrighted music, movies, videos, games or software is strictly prohibited.
- ☐ Attempting to modify or tempering Network or laptop Settings or using personal unregistered devices on network will result in disciplinary measures.
- ☐ Not allowed to accessing without proper authorization network computers, software, information or networks to which the DYP University WLAN belongs.
- ☐ Using electronic communications to harass or threaten users in such a way as to create an atmosphere which unreasonably interferes with the education or the employment experience is subject to criminal penalties.
- ☐ Violating any software license or copyright, including copying or redistributing copyrighted software, without the written authorization of the software owner and is subject to civil and criminal penalties.
- ☐ Use Wi-Fi facility for academic, educational or official purpose only. Bypassing Firewalls, pornography, Excessive usage & downloading will lead to network disconnection.
- ☐ Infected devices (viruses, worms, Trojans, other network threatening programs) Wi-Fi services will be terminated immediately. Update Antivirus & O/S patches regularly.

Employee exit checklist Policy

- ✓ Inform Digital Library room.
- ✓ Handover procedure if laptop belongs to Institute.

- ☐ A failure to abide by the guidelines outlined in this document may result in the imposition of one or more of the following sanctions:
  - ✓ Denial of access to information resources and networks.
  - ✓ Disciplinary action by DYP University.
  - ✓ Civil action.
  - ✓ And/or criminal prosecution.

INTERNET & EMAIL USAGE POLICY

- All connections to the Internet from a Department / Division shall be implemented under strictly controlled means through the University's secure Internet infrastructure.
- The download of all application software (downloading software is strictly forbidden), can jeopardize the IT Team's efforts to protect its systems. All application software downloading must be performed by IT Team's staff and transported using the IT Teams anti-virus checking procedures identified previously, upon formal request and approval.
- Any staff member requiring full Internet access (not including Internet mail) from their allocated PC shall obtain a formal written/e-mailed authorization from the Director of their Division and it should be endorsed by the IT Officer, D Y Patil University.
- Internet services shall be accessed only through the University's Internet connection on all the devices pertaining to University.
- No personal Internet software shall be installed on any of the University's IT equipment's.
- No copyright material shall be downloaded illegally from the Internet, or utilized in breach of its license agreement.
- The University's Internet and network resources shall not be used to access for transfer any material containing:

  a. Derogatory remarks based on race, religion, gender, physical disability or sexual preference.
  b. Images or references that may be considered to be offensive or in breach of any law or regulation.

- Before sending or requesting a client to send urgent, sensitive or confidential messages via the Internet, preference shall be given to alternative, more appropriate and reliable methods.
- Using University's computer resources to access the Internet for personal purposes, without approval from the IT department, may be considered cause for disciplinary action up to and including termination.

WEBSITE REGISTRATION & UPDATING POLICY

Introduction:

The IT team is committed to deploy IT as an effective tool for catalyzing accelerated growth and efficient governance. The entire effort of developing and hosting websites of different Institutes, Programs & Curriculums needs to be streamlined and integrated. To achieve this, it is important to have common guidelines and policy for the Website Development, Hosting and Maintenance for various Institutes & Programs.

Applicability :

These guidelines are meant for all the institutes under University, programs of the University and their subordinate departments.

Guidelines for Design, Development and Hosting of Website :

The IT Team has been designated as the Key point for all websites of University. The IT Team has appointed a Web Administrator who is in charge of all the details of websites. The following guidelines will be followed:

1. Domain Name Conventions and Registration Authority.

   The domain names are the addresses on the web and certain set of naming conventions have been evolved to identify the web site. The Institutes will get a web site address after the domain name registration being done by IT Team and design & maintenance will be done thereafter.

2. Ownership Rights and Technical Control

   The ownership remains with the System Administrator of the respective institute, offices having the Administrative and Signatory rights. However, the Technical Contact remains with the IT Team as it is maintaining the Web Server on which the Web site is hosted.

3. Content Development

   The web content is entirely different from that of the print and audiovisual media and needs special care for drafting. The web content can serve multiple purposes and can be both brief as well as detailed. Two representatives / faculties will be deputed by the principal / head of the respective Institute, to go through the website and suggest any amendments/ updations. The contents for the website should be approved from the concerned representative of the Institute before handing it over to the Central IT department for designing the website.

4. Layout Planning and Designing

   The Web Administrator shall prepare the Layout / Templates of the site and shall design the entire web site as per site map duly approved by the IT Director & the concerned Director of the Institute. The IT Team shall ensure the uniformity and standardization in the layout and design of website and shall maintain a Library of Websites designed for various Institutes / Programs. A uniform pattern will be maintained so as to give an integrated look about the University. The final design shall be approved by concerned head and the site shall be uploaded on the net after approval.

5. Website Hosting of all the Institutes of the University.

   The websites / portals are hosted on the official Linux Virtual Private Server (LVPS) instance, hired for University. As per the revised guidelines pertaining to hosting of websites related to University, no one can now host website with a third party organization provided using their hosting servers.

6. Administration/ Maintenance/ Updation
   i. IT Team and Web Administrator will be responsible for overall supervision to ensure that authentic and updated information is available on the website.
   ii. Each Institute will appoint 2 representatives / faculties for the website.

iii. Deputed representatives will be responsible for timely updating of the website. Timely deletion of irrelevant and undesired information will also have to be ensured by him/her. The website projects the image of the University and hence it is very critical that whatever is hosted on the site is authentic and duly verified by concerned authorities, before uploading.

iv. IT Team and Web Administrator will visit the website at least twice a week. Any feedback or email received regarding the website would be treated as an official receipt and action will be taken as required.

7. Mailing Standards to be followed for every Domain.

contact@domain name is by default id created for all system mails related to that domain only, hence ideally this id should not be used by any institute and even if some institute is using following things needs to be taken care.

1. Assign/depute some representative for regular checking of these mails.

2. Any system related mail on info should be forwarded to system admin of that institute. Also to standardize the email communication all institute must have contact@domain id's related to their respective website , further that should also publish in all communications like website, brochures, advertisements, letter head etc. While sending a request for new email id creation to the IT Team, kindly insure to send name and designation of the person who will accessing mails so that ids can be configured on their respective outlook . Several times the e-mail id of an employee is continued even he/she has left the job and in that scenario chances of misuse of that id is very high, which needs to be taken care of by the concerned Department.

LICENSING & RENEWAL OF SOFTWARE

- The software procured by the organization, are of two types:

    i. The software having perpetual license validity (lifelong validity).
    ii. The software having license which needs to be renewed periodically (subscriptions).

- The software having perpetual license just needs to be purchased once and regularly updated.

- The software license which needs to be renewed on yearly basis are
    i. Microsoft Volume license
    ii. Antivirus and anti-spyware.
    iii. Firewall

- The License for all the software's is maintained centrally at IT-Department. According to the due date of the license renewal, Quotations are invited from various vendors and a comparison chart is prepared for the same. After negotiation and without compromising on the service, the vendor who has quoted the lowest price is selected for hiring the service. The quotation recommended by system administrator is forwarded to the IT Head for verification and approval. After the quotation is approved from Head, it is forwarded to the VC / Pro-VC / Dean for final approval.

- After the approval of quotation, a purchase order is raised in the name of the approved vendor stating the next validity period, terms and conditions and the amount for the same.

- Prior to raising the PO for license renewal the Central IT-Department provides the Accounts Department with the budgetary details which gives an insight of expenditure and make fund provisions according to the payment terms mentioned in the P.O.

NETWORK ACCESS & PERMISSIONS (Provided AD is implemented)

- ☐ Each User will have only one personal identification code (User ID).
- ☐ User IDs will be consistent in structure logic. It should consist of the first name and last name separated by dot delimiter, all in lower cases.
- ☐ Guidelines will be provided by IT Team for structure of passwords.
- ☐ At the beginning of each work session each User will be required to enter their individual ID and password.
- ☐ Users will be accountable for all actions performed with their User ID and will be responsible for preventing any other person from using their User ID. Agreements to these conditions will be a prerequisite to granting a User ID.
- ☐ Security systems will allow and encourage Users to protect their ID code from being used by any other person.
- ☐ Security systems will maintain a record of the use of data and files to satisfy privacy, legal requirements and the efficient management of data.
- ☐ Actions / Access allowed by Users will be determined by security information associated with their User ID.
- ☐ Only authorized personnel are allowed access to University computer resources including e-mail and Internet access.
- ☐ Users may not allow other personnel to use their password or share an account and are strictly forbidden to make known the password of any other User.
- ☐ Attempting to use others passwords or gain access to local or network resources is forbidden.
- ☐ No IT Infrastructure is to be connected to any part of the University Networks without written approval of IT Team.
- ☐ The IT Team has the right to access any User accounts and folders if there is reason to believe that an account or system has been breached.
- ☐ The IT Team has the right to access accounts if there is a complaint that a system is being used by an unauthorized User or to gain unauthorized access.
- ☐ The IT Team has the right to access accounts if there is reason to believe that a system is being used in violation of IT policy.
- ☐ Extension or development of the network is to be supported by full cost justification.
- ☐ To maximize the usability of workstations within its network, University will standardize on Windows 7 Professional, 10 as the base workstation operating system.
- ☐ No computer will have its operating system changed to any other than Windows 7 Professional, 10 without written approval of IT management and such approved changes will be completed by approved IT personnel.
- ☐ The Network Architecture must be established in such a way as to contain local traffic in discrete LAN configuration, utilizing LAN Bridges and Routers to direct traffic between configurations.
- ☐ While network versions of software should be employed wherever possible, commonly used applications are to be loaded on the individual workstations to minimize load on the network.
- ☐ A set of standards should be established for consistent identification of Users, workstations and other network objects.
- ☐ The network operating system will be supplemented by a standardized antivirus mechanism and a configuration management tool to control both hardware and software configurations.
- ☐ Network cabling must be CAT 6e with RJ45 connectors including installation of telephone cabling.
- ☐ Fiber-optic cabling implementations particularly for extending LAN in areas where installations are clustered are encouraged.
- ☐ Office cabling design particularly with regards to office layout should be based on 'Generally accepted standards' for networking in office areas.

NETWORK ADMINISTRATION POLICY

- A Network Administrator will be based in the IT management area. Any Network problems that can't be solved by IT Help Desk personnel will be referred to the Network Administrator / System Administrator.
- To maximize the usability of workstations within its network, University will standardize on hardware configuration, for memory, display, processor, disc, Operating System and Application software for common tasks and office services.
- The Network Architecture should be established in such a way as to contain local traffic in discrete LAN configuration, utilizing LAN Bridges and Switches to manage traffic over the network.
- While network versions of software should be employed wherever possible, commonly used applications should be distributed to and loaded on the individual workstations, to minimize load on the network.
- A corporate wide set of standards will be established for consistent identification of Users, workstations and other network objects. (first_name.last_name)
- The network operating system will be supplemented by a standardized antivirus mechanism (reflecting University's Antivirus Policies & Standards) and a configuration management tool to control both hardware and software configurations.
- Every Workstation in University (except in extreme situations of virus infections) must be connected to the University LAN.
- Adoption of a 'code of ethics' regarding the use of unlicensed software within University and regular software audits to check compliance.
- Standardization of system configuration, including directory structures, to simplify management.
- Establishment of a consistent and automated backup regime to preserve User data at a central point and assure recoverability in the event of accidental loss.
- Routine activities shall be formally documented and followed.
- Procedures for data backup, event logging and environment monitoring are necessary to ensure the integrity and availability of services.
- The IT Section shall keep a log of all media disks, consumables utilized for backup purpose, and printing jobs.
- Management shall maintain a log of all work carried out by third parties and those which have direct implication on systems availability.
- Environmental controls for Server Room and backup equipment shall be properly monitored to identify adverse conditions and enable prompt corrective action.
- All software on University's workstations shall be installed under strictly controlled means through the University's license agreements.
- The Administrator password for University servers will be changed frequently to ensure appropriate level of security.

EMPLOYEE CHECK-IN, CHECK – OUT PROCEDURE

Steps to be followed for Exit Check of Employee

- ☐ Change the password for Mail Box.
- ☐ Disable ERP / HRMS / FTP Login
- ☐ Backup Data from Server on User's Roaming Profile / Local disk to CD / DVD.
- ☐ Audit & prepare a report for the Desktop / Laptop for installed software's & Data.
- ☐ Take handover for the issued devices such as Laptops / IPAD / Data Card etc.
- ☐ Send a mail report to central server room / upload the complete exit report on mentioned One Drive.

Steps to be followed while inducing an Employee in University

- ☐ Create Mail Box on respective domain.
- ☐ Create User id on Domain for using Desktop.
- ☐ Get declaration signed while allotting the Desktop / Laptop for the user.
- ☐ Create ERP / HRMS user for the employee.
- ☐ Get the Handover form signed after handing over the device.

BACKUP, RECOVERY & DISASTER MANAGEMENT

- ☐ All computerized files in University are to be saved to the Primary Server (or other LAN connected Server where directed in writing by the IT Team) in the respective User's folder or Shared folder. Only files on the Primary Server (and other LAN-connected Servers nominated by the IT Team) will be backed up.

- ☐ It is the responsibility of the respective Users of any non LAN-connected computer / equipment (including laptops/notebooks) to arrange with the IT Team for the transfer of work files from the non LAN-connected equipment to the relevant folder on server for backup.

- ☐ No files on the local hard drives of any University's computers (including laptop/notebook computers) will be backed up by the IT Team (it is the responsibility of Users of laptop/notebook computers not connected to the Network to arrange with the Network Administrator for data/files to be transferred to the server every day).

- ☐ All systems software, application software, data and documentation shall be backed-up regularly to enable the system to be recovered with minimal data loss when required and without the loss of integrity.

- ☐ Each server must be backed up on a regular basis based on the incremental backup routine.

- ☐ Incremental daily backups of all data and systems considered being critical or important; Incremental weekly backups for all other data

- ☐ Monthly backup of all system, application, and data.

- ☐ No backup device or media shall ever be taken home by any staff member or other person.

- ☐ In addition to regular backup cycles, a system backup shall be performed before and after major changes to the operating system, network configuration, system software, or applications, at the discretion of the Network Administrator and IT Support management.
- ☐ Backup media are to be held in a location that provides adequate physical security to limit access to authorized personnel only.

- ☐ All-important data should be saved onto the appropriate server in specific location allocated to each Division or application. These servers will be backed up frequently to minimize data loss and ensure high availability of data to various Divisions.

- ☐ In case of any technical support required regarding the computer system, users are requested to kindly call the local tech support helpline number / contact points or raise ticket for their technical issues on the respective support system the institute. The complaint will be registered and a ticket will be generated accordingly. The ticket will be forwarded to the tech support executive who will handle the complaint.

IT AUDIT

Objective of and IT audit is to concentrate on substantiating that the internal controls exist and are functioning as expected to minimize business risk. These audit objectives include assuring compliance with legal and regulatory requirements, as well as the confidentiality, integrity, and availability of information systems and data.

The auditor will follow the procedure,

- Review IT organizational structure
- Review IT policies and procedures
- Review IT standards
- Review IT documentation
- Review the organization's Business Impact Analysis
- Interview the appropriate personnel
- Observe the processes and employee performance
- Examination, which incorporates by necessity, the testing of controls, and therefore includes the results of the tests.

In connection with Internal or External audit, following points may be considered,

- Identifying the significant application components; the flow of transactions through the application (system); and to gain a detailed understanding of the application by reviewing all available documentation and interviewing the appropriate personnel, such as system owner, data owner, data custodian and system administrator.
- Identifying the application control strengths and evaluating the impact, if any, of weaknesses you find in the application controls
- Developing a testing strategy
- Testing the controls to ensure their functionality and effectiveness
- Evaluating your test results and any other audit evidence to determine if the control objectives were achieved
- Evaluating the application against management's objectives for the system to ensure efficiency and effectiveness.

External IT Audit

Yearly - after the month of May

Internal IT Audit

Yearly - after the month of Feb

DOCUMENTATIONS & INFORMATION REQUEST

Standard format for Documentation and maintaining Files are followed to have a better accountability and to locate the resource when required for Audit. This Audit is carried out by IT Team and all documents of Individual institutes have to be submitted centrally duly signed by the respective heads of those institutes. The documentation includes maintaining the documents at two locations i.e.

1. Local IT Department in each campus.
2. Central IT Department governing all the local campuses.

The Types of documents needed to be maintained under the above locations are as follows:

a) Dead Stock Registers.
b) Consumable issue registers.
c) Requisition file.
d) Purchase order & Invoice file.
e) Quotation file.
f) AMC contract file
g) Service Report File
h) Website maintenance & updation file.
i) Wi-Fi Registration file.
j) Technical Staff profile.
k) Lab Registers.
l) Original Software License file.
m) Server maintenance.
n) Domain registration & renewal file.
o) Staff information & appraisal file.

IT E-WASTE & DISPOSAL POLICY

E-Waste getting generated from the University is to be disposed off or dismantled through the agency which will further dispose off the e-waste in an environment friendly manner and provide certificate of the same (Form 13) to the University for every delivery made. The entry of the same has to be made in the passbook issued by MPCB.