DPU

Dr. D. Y. PATIL VIDYAPEETH, PUNE

(DEEMED UNIVERSITY)

(Accredited by NAAC with 'A' grade)

DPU IT
POLICY DOCUMENT

DPU

Dr. D. Y. PATIL VIDYAPEETH, PUNE

(DEEMED UNIVERSITY)

(Accredited by NAAC with 'A' grade)

DPU IT
POLICY DOCUMENT

INDEX

Sr. No.	Title	Page No.
1	Introduction	1
2	Aims of IT Policy	3
3	IT Policy Statement	4
4	Email Policy	18
5	Campus ERP Policy	23
6	HIMS Policy	30

Introduction

IT Policy in Education is much more than the mere collection and distribution of knowledge. It offers intellectual hospitality, opportunities for innovation, creativity; power of thought and imagination. It envisages development of character and inculcation of a firmness of mind and zeal to offer one's best to the world. Education is the means of unfolding moral and spiritual potentialities of men.

The mission of the **Dr. D. Y. Patil Vidyapeeth, Pune**, is "To contribute to the socio-economic and ethical development of the nation, by providing high quality education through institutions that have dedicated faculty and state-of-the-art infrastructure, and are capable of developing competent professional and liberal-minded citizens".

Mission

Our Mission is to provide value added service in the field of information Technology. To achieve high level user satisfaction is our ultimate aim, for this we work hard to enhance our service and fetch user loyalty by considering them as equal business partners

Vision

We shall strive hard to create user oriented organization that focuses on IT solutions. We shall focus on user satisfaction by providing consistent & innovative IT solutions through continual improvements in organization processes and optimal utilization of human resources by building long-term relations through providing exciting & learning organization environment to explore their full potential

Why we require IT Policy?

- Rules for access to administrative data, including definitions explaining what it is and the rules for using it. Employees who access administrative data must use it according to the rules or risk disciplinary consequences.
- States the codes of practice with which the organization aligns its information technology security program to safeguard the institution’s computing assets in the face of growing security threats. This significant challenge requires a strong, persistent and coordinated program that leverages widely accepted, effective security practices appropriate for the higher education environment.
- Strictly limits the circumstances under which highly sensitive data may be stored on individual-use devices and media. It further mandates that strict security requirements be met when highly sensitive data must unavoidably be stored on individual-use electronic devices or electronic media.
- The Organizational Web pages must not be used for commercial purposes.
- Explains the conditions under which third parties (e.g., auditors, consultants) are allowed direct access to the network.
- Explains all users’ responsibilities for maintaining the security of their devices on the organizations network.
- Explains rules for maintaining privacy, confidentiality, and integrity of the computing environment while using resources appropriately
- Defines ban (and exemptions) on employee access to obscene materials & sexually explicit material via state equipment. Rules for using shared computing resources such as public labs.

Aims of IT Policy

DPU Information Security Policies are necessary to ensure that important data, Institution plans and other confidential information are protected from theft or unauthorized disclosure. If employees of any organization are not aware of these policies, they will not know what is expected of them when they handle such confidential information.

- Empowering citizens, managers and other stakeholders by enabling online teamwork for increased participation, collaboration and information sharing through the use of email, the Web and other remote collaboration tools.
- Enabling the rapid creation and inexpensive distribution of educational information and knowledge.
- Encouraging professional development, in service training, remote support and mentoring for lifelong learning for teachers, managers and other citizens.
- Facilitating fast and easy access to information and expertise around the world.
- Increasing motivation through the use of multimedia (sound, video, graphics, animation and text.)
- Allowing each student to learn at his/her level and speed thereby giving pupils greater control over their own learning.
- Enhancing the development of the abilities of mentally and physically challenged students.
- Promoting active rather than passive learning.
- Engaging students in research, data analysis and problem solving, thereby facilitating higher-order thinking processes such as synthesizing, interpreting and hypothesizing.

1. POLICY STATEMENT

"It shall be the responsibility of the I.T. Department to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorized members of staff, and to ensure the integrity of all data and configuration controls."

2. Benefits of Information Technology

1. Information Technology can affect in the spread of education and to enable greater access to it. IT increases flexibility so that students can access educational resources regardless of time and geographical barriers. They can affect the way that students are given instruction and how they learn. They enable collaborative development of skills and abilities to create knowledge. This as a result will bring a better preparation for students, lifelong learning and the opportunity to join industry.

2. Increase access, Flexibility of content and distribution Combination of education and work the methods are focused on the student.

3. High quality, cost-effective professional development in place of labor. Improve the skills of employees, increase of productivity. Developing a new culture of learning. Sharing of costs and timing of training among employees.

4. Increased capacity and cost effectiveness of the system education. Achievement of target groups that have limited access to traditional education. Support and improve the quality and relevance of existing structures of education. Provide links to education institutions and curricula with the networks.

5. IT can also help improve the performance of knowledge workers and enhance organizational learning. Externally, it can improve the performance of knowledge workers in customer, supplier and partner organizations; add information value to existing products and services; create new information-based products and services.

6. In terms of Functionality and Flexibility, internally IT can help improve infrastructure performance thus increasing functionality and the range of options that can be pursued. Externally, it can help create an efficient, flexible online/offline platform for doing coordination with educational Organizations.

3. Limitations of IT use in Education

1. IT as a modern technology that simplifies and facilitates human activities is not only Advantageous in many respects, but also has many limitations. Many people from inside and outside the education system, think of IT as "Panacea" or the most important solution to institution problems and improvements. However, many conditions can be considered as limitations of IT use in education. The limitations can be categorized as teacher related, student related, and technology related. All of them potentially limit the benefits of IT to education.

2. The other limitation of IT use in education is technology related. The high cost of the technology and maintenance of the facilities, high cost of spare parts, virus attack of software and the computer, interruptions of internet connections, and poor supply of electric power are among the technology related limitations of IT use in education.

Summary of Main Security Policies

1. Confidentiality of all data is to be maintained through discretionary and mandatory access controls, and wherever possible these access controls should meet with security functionality.

2. Internet and other external service access are restricted to authorized personnel only.

3. Access to data on all laptop computers is to be secured through encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.

4. Only authorized and licensed software may be installed, and installation may only be performed by I.T. Department staff.

5. The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it will be removed from the workstation immediately.

6. Data may only be transferred for the purposes determined in the Organizations' data-protection policy.

7. All diskette drives and removable media from external sources must be virus checked before they are used within the Organization.

8. Passwords must consist of a mixture of at least 4 alphanumeric characters, and must be changed every 30 days and must be unique.

9. Workstation configurations may only be changed by I.T. Department staff.

10. The physical security of computer equipment will conform to recognized loss prevention guidelines.

11. To prevent the loss of availability of I.T. resources measures must be taken to backup data, applications and the configurations of all workstations.

2. VIRUS PROTECTION

1. The I.T. Department will have available up to date virus scanning software for the scanning and removal of suspected viruses.

2. Corporate file-servers will be protected with virus scanning software.

3. Workstations will be protected by virus scanning software.

4. All workstation and server anti-virus software will be regularly updated with the latest anti-virus patches by the I.T. Department.

5. No disk that is brought in from outside the Organization is to be used until it has been scanned.

6. All systems will be built from original, clean master copies whose write protection has always been in place. Only original master copies will be used until virus scanning has taken place.

7. All removable media containing executable software (software with .EXE and .COM extensions) will be write protected wherever possible.

8. All demonstrations by vendors will be run on their machines and not the Organizations'.

9. Shareware is not to be used, as shareware is one of the most common infection sources. If it is absolutely necessary to use shareware it must be thoroughly scanned before use.

10. New commercial software will be scanned before it is installed as it occasionally contains viruses.

11. All removable media brought in to the Organization by field engineers or support personnel will be scanned by the IT Department before they are used on site.

12. To enable data to be recovered in the event of virus outbreak regular backups will be taken by the I.T. Department.

13. Management strongly endorses the Organizations' anti-virus policies and will make the necessary resources available to implement them.

14. Users will be kept informed of current procedures and policies.

15. Users will be notified of virus incidents.

16. Employees will be accountable for any breaches of the Organizations' anti-virus policies.

17. Anti-virus policies and procedures will be reviewed regularly.

18. In the event of a possible virus infection the user must inform the I.T. Department immediately. The I.T. Department will then scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

4. ACCESS CONTROL

1. Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.

2. Users requiring access to systems must make a written application on the forms provided by the I.T Department.

3. Where possible no one person will have full rights to any system. The I.T. Department will control network/server passwords and system passwords will be assigned by the system administrator in the end-user department.

4. The system administrator will be responsible for the maintaining the data integrity of the end-user department's data and for determining end-user access rights.

5. Access to the network/servers and systems will be by individual username and password, or by smartcard and PIN number/biometric.

6. Usernames and passwords must not be shared by users.

7. Usernames and passwords should not be written down.

8. Usernames will consist of initials and surname.

9. All users will have an alphanumeric password of at least 4 characters.

10. Passwords will expire every 30 days and must be unique.

11. Intruder detection will be implemented where possible. The user account will be locked after 5 incorrect attempts.

12. The I.T. Department will be notified of all employees leaving the Organizations’ employment. The I.T. Department will then remove the employee’s rights to all systems.

13. Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster, for example a fire safe in the I.T. Department.

14. Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.

15. I.T. Department staff will not login as root on to UNIX, Linux systems, but will use the SU command to obtain root privileges.

16. Use of the admin username on Novell systems and the Administrator username on Windows is to be kept to a minimum.

17. Default passwords on systems such as Oracle and SQL Server will be changed after installation.

18. On UNIX and Linux systems, rights to RLOGIN, FTP, TELNET, SSH will be restricted to I.T. Department staff only.

19. Where possible users will not be given access to the UNIX, or Linux shell prompt.

20. Access to the network/servers will be restricted to normal working hours. Users requiring access outside normal working hours must request such access in writing on the forms provided by the I.T. Department.

21. File systems will have the maximum security implemented that is possible. Where possible users will only be given Read and

Files scan rights to directories, files will be flagged as read only to prevent accidental deletion.

5. LAN Security

Routers & Switches

1. LAN equipment, hubs, bridges, repeaters, routers, switches will be kept in secure hub rooms. Hub rooms will be kept locked at all times. Access to hub rooms will be restricted to I.T. Department staff only. Other staff and contractors requiring access to hub rooms will notify the I.T. Department in advance so that the necessary supervision can be arranged.

Workstations

1. Users must logout of their workstations when they leave their workstation for any length of time. Alternatively Windows workstations may be locked.
2. All unused workstations must be switched off outside working hours.

Wiring

1. All network wiring will be fully documented.

2. All unused network points will be de-activated when not in use.

3. All network cables will be periodically scanned and readings recorded for future reference.

4. Users must not place or store any item on top of network cabling.

5. Redundant cabling schemes will be used where possible.

6. Monitoring Software will be used.

7. The use of LAN analyzer and packet sniffing software is restricted to the I.T. Department.

8. LAN analyzers and packet sniffers will be securely locked up when not in use.

9. Intrusion detection systems will implemented to detect unauthorized access to the network

Servers

1. All servers will be kept securely under lock and key.
2. Access to the system console and server disk/tape drives will be restricted to authorized I.T. Department staff only.

Electrical Security

1. All servers will be fitted with UPS's that also condition the power supply.

2. All hubs, bridges, repeaters, routers, switches and other critical network equipment will also be fitted with UPS's.

3. In the event of a mains power failure, the UPS's will have sufficient power to keep the network and servers running until the generator take over.

4. Software will be installed on all servers to implement an orderly shutdown in the event of a total power failure.

5. All UPS's will be tested periodically.

Inventory Management

1. The I.T. Department will keep a full inventory of all computer equipment and software in use throughout the Company.

2. Computer hardware and software audits will be carried out periodically via the use of a desktop inventory package. These audits will be used to track unauthorized copies of software and unauthorized changes to hardware and software configurations.

6. Server Specific Security

This section applies to Windows, UNIX, & Linux servers.

1. The operating system will be kept up to date and patched on a regular basis.

2. Servers will be checked daily for viruses.

3. Servers will be locked in a secure room.

4. Where appropriate the server console feature will be activated.

5. Remote management passwords will be different to the Admin/Administrator/root password.

6. Users possessing Admin/Administrator/root rights will be limited to trained members of the I.T. Department staff only.

7. Use of the Admin/Administrator/root accounts will be kept to a minimum.

8. Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.

9. User’s access to data and applications will be limited by the access control features.

10. Intruder detection and lockout will be enabled.

11. The system auditing facilities will be enabled.

12. Users must logout or lock their workstations when they leave their workstation for any length of time.

13. All unused workstations must be switched off outside working hours.

14. All accounts will be assigned a password of a minimum of 8 characters.

15. Users will change their passwords every 30 days.

16. Unique passwords will be used.

17. The number of grace logins will be limited to 5.

18. The number of concurrent connections will be limited to 3.

19. Network login time restrictions will be enforced preventing users from logging in to the network outside normal working hours.

20. In certain areas users will be restricted to logging in to specified workstations only.

7. UNIX & Linux Specific Security

1. Direct root access will be limited to the system console only.

2. I.T. Department staff requiring root access must make use of the SU command.

3. Use of the root account will be kept to a minimum.

4. All UNIX and Linux system accounts will be password protected, lP etc.

5. RLOGIN facilities will be restricted to authorize I.T. Department staff only.

6. FTP facilities will be restricted to authorize I.T. Services staff only.

7. TELNET facilities will be restricted to authorized users.

8. SSH facilities will be restricted to authorized users.

9. User’s access to data and applications will be limited by the access control features.

10. Users will not have access to the $ prompt.

11. All accounts will be assigned a password of a minimum of characters.

12. Users will change their passwords every 30 days.

8. Wide Area Network Security

1. Wireless LAN's will make use of the most secure encryption and authentication facilities available.

2. Users will not install their own wireless equipment under any circumstances.

3. Dial-in modems will not be used if at all possible. If a modem must be used dial-back modems should be used. A secure VPN tunnel is the preferred option.

4. Modems will not be used by users without first notifying the I.T. Department and obtaining their approval.

5. Where dial-in modems are used, the modem will be unplugged from the telephone network and the access software disabled when not in use.

6. Modems will only be used where necessary, in normal circumstances all communications should pass through the Organizations’ router and firewall.

7. Where leased lines are used, the associated channel service units will be locked up to prevent access to their monitoring ports.

8. All bridges, routers and gateways will be kept locked up in secure areas.

9. Unnecessary protocols will be removed from routers.

10. The preferred method of connection to outside Organizations is by a secure VPN connection, using IPSEC or SSL.

11. All connections made to the Organizations’ network by outside organizations will be logged.

9. TCP/IP & Internet Security

1. Permanent connections to the Internet will be via the means of a firewall to regulate network traffic.

2. Permanent connections to other external networks, for offsite processing etc., will be via the means of a firewall to regulate network traffic.

3. Where firewalls are used, a dual homed firewall (a device with more than one TCP/IP address) will be the preferred solution.

4. Network equipment will be configured to close inactive sessions.

5. Where modem pools or remote access servers are used, these will be situated on the DMZ or non-secure network side of the firewall.

6. Workstation access to the Internet will be via the Organizations' proxy server and website content scanner

7. All incoming e-mail will be scanned by the Organizations' e-mail content scanner.

10. Email Policy

The purpose of this policy is to ensure the proper use of Dr. D.Y. Patil Vidyapeeth, Pune’s email system and make users aware of what Dr. D.Y. Patil Vidyapeeth, Pune deems as acceptable and unacceptable use of its email system. The Dr. D.Y. Patil Vidyapeeth, Pune reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

Legal RISKS

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of e-mail:

- If you send emails with any defamatory, offensive, racist or obscene remarks, you and Dr. D.Y. Patil Vidyapeeth, Pune can be held liable.

- If you forward emails with any defamatory, offensive, racist or obscene remarks, you and Dr. D.Y. Patil Vidyapeeth, Pune can be held liable.

- If you unlawfully forward confidential information, you and Dr. D.Y. Patil Vidyapeeth, Pune can be held liable.

- If you unlawfully forward or copy messages without permission, you and Dr. D.Y. Patil Vidyapeeth, Pune can be held liable for copyright infringement.

- If you send an attachment that contains a virus, you and Dr. D.Y. Patil Vidyapeeth, Pune can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of e-mail. If any user disregards the rules set out in this Email Policy, the user will be fully liable and Dr. D.Y. Patil Vidyapeeth, Pune will disassociate itself from the user as far as legally possible.

Legal requirements

The following rules are required by law and are to be strictly adhered to:

- It is strictly prohibited to send or forward emails containing defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify webmaster.
- Do not forward a message without acquiring permission from the sender first.
- Do not send unsolicited email messages.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person’s email account.
- Do not copy a message or attachment belonging to another user without permission of the originator.
- Do not disguise or attempt to disguise your identity when sending mail.

Best practices

Dr. D.Y. Patil Vidyapeeth, Pune considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Therefore Dr. D.Y. Patil Vidyapeeth, Pune wishes users to adhere to the following guidelines:

- Writing emails:
    - Write well-structured emails and use short, descriptive subjects.
    - Dr. D.Y. Patil Vidyapeeth, Pune’s email style is informal. This means that sentences can be short and to

the point. You can start your e-mail with ‘Hi’, or ‘Dear’, and the name of the person. Messages can be ended with ‘Best Regards’. The use of Internet abbreviations and characters such as smileys however, is not encouraged.

- Signatures must include your name, designation and department name. A disclaimer will be added underneath your signature (see Disclaimer)
- Use the spell checker before you send out an email.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.
- Do not write emails in capitals.
- Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.
- If you forward mails, state clearly what action you expect the recipient to take.
- Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).
- Only mark emails as important if they really are important.

- Replying to emails:

  - Emails should be answered within at least 8 working hours, but users must endeavour to answer priority emails within 4 hours.

  - Priority emails are emails from Principals, Deans, Directors, Registrars, Vice-Chancellor, Chancellor and Secretary.

Personal Use

Although Dr. D.Y. Patil Vidyapeeth, Pune's email system is meant for business use, Dr. D.Y. Patil Vidyapeeth, Pune allows the reasonable use of email for personal use if certain guidelines are adhered to:

- Personal use of email should not interfere with work.
- Personal emails must also adhere to the guidelines in this policy.
- Personal emails are kept in a separate folder, named 'Private'.
- The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.
- On average, users are not allowed to send more than 2 personal emails a day.
- Do not send mass mailings.
- All messages distributed via the DPU's email system, even personal emails, are Dr. D.Y. Patil Vidyapeeth, Pune's property.

Confidential information

Avoid sending confidential information by e-mail. If you do, you must secure the information by including it in a Microsoft Word or Excel file and protecting it with a password. Then provide the recipient with the password by means of other communication, for instance by telephone.

Disclaimer

The following disclaimer will be added to each outgoing email:

'This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify us on webmaster@dpu.edu.in. Please note that any views or opinions

presented in this email are solely those of the author and do not necessarily represent those of Dr. D.Y. Patil Vidyapeeth, Pune. Finally, the recipient should check this email and any attachments for the presence of viruses. Dr. D.Y. Patil Vidyapeeth, Pune, accepts no liability for any damage caused by any virus transmitted by this email.'

System Monitoring

You must have no expectation of privacy in anything you create, store, send or receive on the DPU's computer system. Your emails can be monitored without prior notification if Dr. D.Y. Patil Vidyapeeth, Pune deems this necessary. If there is evidence that you are not adhering to the guidelines set out in this policy, the Dr. D.Y. Patil Vidyapeeth, Pune reserves the right to take disciplinary action, including termination and/or legal action.

Email accounts

Dr. D.Y. Patil will issue email ID to the employees on request. The format of the email Id will be *FirstName.Surname@dpu.edu.in*. The request for creation of new email ID has to be sent to webmaster@dpu.edu.in by any one of these: Registrar/ Principal/ Dean/ Director/ HOD.

All email accounts maintained on our email systems are property of Dr. D.Y. Patil Vidyapeeth, Pune. Passwords should not be given to other people and should be changed once a month. Email accounts not used for 60 days will be deactivated and possibly deleted.

Questions

If you have any questions or comments about this IT Policy, please contact Mr. Jai Ram Choudhary, Incharge, Software Development Cell, 8007252735, webmaster@dpu.edu.in and Mr. Gaurav Pandey , IT Incharge Central IT Department, 02027805637, itincharge@dpu.edu.in If you do not have any questions Dr. D.Y. Patil Vidyapeeth, Pune presumes that you understand and are aware of the rules and guidelines in this IT Policy and will adhere to them.

Campus ERP Policy

Introduction

An ERP is an Enterprise Resource Planning system -- a software system that processes institution-wide transactions on a single software system and a single data base. These multi-functional systems are designed to streamline almost every aspect of how institutions operate. Simply put, an ERP integrates -institutional data and processes through one system.

Among other things, an ERP will:

1. Integrate information across all functions (examples include registration, financial aid, human resources).

2. Facilitate the flow of information among the institution's functions.

3. Track a wide range of institutional events in an integrated fashion, and facilitate planning future activities based on these events.

4. Support analysis of trends and thus improve the performance of the institution.

5. Allow users to:
   a) Input data into one system to enable it to be processed with other data
   b) Access data as information reports in a real-time environment
   c) Share common data and practices across the entire institution
   d) Re-engineer business practices

In this context, ERP refers to the use of commercial solutions for both administrative and academic purposes by university and its constituent colleges. Typical administrative functions may include human resources, accounting, payroll, and billing. Academic functions include recruitment, admissions, registration, and all aspects of student records.

An ERP system has been developed for the University and its constituent Institutes by the Software Development Cell. It has been named CampusERP.

Salient Features

The silent features of the systems are

- **Reducing the repeated work of data entry**. Data once entered at any location is available throughout the system.
- **Reducing the wastage of paper.** As a step towards paperless office, online transactions will greatly help in reducing the use of paper.
- **Fast, Timely and Accurate Information**. Since the data is entered only once, the chances of mistakes are minimized.
- **Centralized Data and Information.** The data of all the colleges is being stored at one location. This will facilitate easy information retrieval, data security and database maintenance.

Implementation

The system is hosted on the servers in the Data Centre of DPU. All the Institutes are connected to the Data Centre through Fiber Optic cable.

The system has been hosted on a separate domain named **dpuerp.in**. There are sub-domains defined for each Institute. Below is the list of sub-domains of various Institutes through which they can access the CampusERP system.

SrNo	Institute Name	Sub-Domain Name
1.	Dr. D.Y. Patil Vidyapeeth, Pune	university.dpuerp.in
2.	Padmashree Dr. D. Y. Patil Medical College, Hospital and Research Centre, Pimpri	medical.dpuerp.in
3.	Dr. D. Y. Patil Dental College & Hospital	dental.dpuerp.in
4.	Dr. D.Y. Patil Institute of Biotechnology and Bioinformatics	biotech.dpuerp.in
5.	Padmashree Dr. D.Y. Patil College of Physiotherapy	physio.dpuerp.in
6.	Global Business School & Research Centre	gbsrc.dpuerp.in
7.	Padmashree Dr. D. Y. Patil College of Nursing	nursing.dpuerp.in
8.	Dr. D. Y. Patil Institute of Optometry and Visual Sciences	optom.dpuerp.in
9.	Institute of Distance Learning	idl.dpuerp.in

Modules

Student Section

- Upon admission confirmation, the staff in student section will enter the complete data of the student into the CampusERP system.

- CampusERP will generate and assign a unique StudentID to the student. This ID will be used by the student to log into the CampusERP.

- Staff will allocate proper class, batch, course and rollno to the student.

- Once the exams are over for a semester, the student can be promoted to next class.

- If the student requires, different type of certificates can be given to him/ her through appropriate menus. Examples are Bonafide certificate, Transfer Certificate, Migration Certificate etc.

- Upon receipt of mark list, the staff will enter the marks into the system so that these marks are visible in the Student Dashboard.

- Online request for printing and issuing ID cards to the students should be made within first seven days to the Software Development Cell.

- All the notices and circulars related to the students should be created using CampusERP so that they are present for the Students on their Dashboards.

Academic Section

- All the teaching staff will create their respective lesson plans into the system.

- Authorized staff will create the time table and allocate mentors before the start of the new semester.

- After completion of a lecture, the staff will feed the details of the topic covered along with resources, if any, in the CampusERP. Attendance of the students who attended the lecture needs to be entered as well.

- Staff can upload subject wise reference books list, syllabus and notes to benefit the students.

HR Module

- When a staff joins the Institute, authorized person from HR will enroll the staff into the CampusERP system filling in all the details. The system will generate a StaffID for the newly enrolled staff. This StaffID will be used by the staff to login into the CampusERP.

- Authorised staff will allocate leaves to the staff and also define the flow of the Leave Application.

- Each staff member needs to fill online Leave Application in the CampusERP. The HR staff will decide the type of the leave that has to be given against the application.

- Proper training and registration of the enrolled staff with the Biometrics Attendance System

- HR Staff will create the Attendance voucher for salary in the CampusERP system. All the attendance

- Staff should be provided with Institute ID Card. The request for ID Card printing has to be given through the option available in CampusERP.

- When a Staff member resigns from the service, an entry needs to be made into the CampusERP system. This will ensure that the staff

Hostel Management

- Any student who wants to take admission in Hostel needs to be enrolled in Hostel module.

- Hostel staff will allocate the room and bed to the students.

- All the notices and circulars related to the Hostel Activities may be given through this Module.

Library Management

- This Library staff will use this module to manage its day-to-day activities.

- All the books need to be barcoded. The stickers with barcode are available from Software Development Cell on request.

- Staff needs to put entries of the new arrivals so that all the members of the library are aware.

- The members can use the OPAC module from their own dashboard to search for various titles and also to view their transactional history of the library.

Communication

- All the notices and circulars should be made online through the use of this module.

- The notices can be typed directly or can be uploaded after scanning the original document.

Security

All the users of the CampusERP system have been provided with an ERPID and password. This ERPID is printed on the ID Cards of both the faculty and Students. The users can change their password at any time. If they forget their password, a utility has been provided to recover the password.

The system uses Secure Hash Algorithm (SHA-2) to encrypt the user passwords. SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256) designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS).SHA-2 currently consists of a set of six hash functions with digests that are 224, 256, 384 or 512 bits.

SHA-512 is being used by us to encrypt the password. It has novel hash functions computed with 64-bit words.

HIMS (Hospital Information Management System) Policy

Introduction

A Hospital information system is a comprehensive, integrated information system designed to manage all the aspects of a hospital operation, such as medical, administrative, financial, legal and the corresponding service processing. Hospital Information Systems can be defined as massive, integrated systems that support the comprehensive information requirements of hospitals, including patient, clinical, ancillary and financial management. Hospitals are extremely complex institutions with large departments and units coordinate care for patients. Hospitals are becoming more reliant on the ability of hospital information system (HIS) to assist in the diagnosis, management and education for better and improved services and practices.

Hospital Information Systems provide a common source of information about a patient's health history. The system has to keep data in secure place and controls who can reach the data in certain circumstances. These systems enhance the ability of health care professionals to coordinate care by providing a patient's health information and visit history at the place and time that it is needed. Patient's laboratory test information also visual results such as X-ray may reachable from professionals. HIS provide internal and external communication among health care providers.

Benefits of HIS

- Easy access to doctors' data to generate varied records, including classification based on demographic, gender, age, and so on. It is especially beneficial at ambulatory (out-patient) point, hence enhancing continuity of care. As well as, Internet-based access improves the ability to remotely access such data.

- It helps as a decision support system for the hospital authorities for developing comprehensive health care policies.

- Efficient and accurate administration of finance, diet of patient, engineering, and distribution of medical aid. It helps to view a broad picture of hospital growth

- Improved monitoring of drug usage, and study of effectiveness. This leads to the reduction of adverse drug interactions while promoting more appropriate pharmaceutical utilization.

- Enhances information integrity, reduces transcription errors, and reduces duplication of information entries.

- Hospital software is easy to use and eliminates error caused by handwriting. New technology computer systems give perfect performance to pull up information from server or cloud servers.

Implementation

The system is hosted on the servers in the Data Centre of DPU. All the Institutes are connected to the Data Centre through Fiber Optic cable.

The system has been implemented in parts in Medical College and Dental College. The following subdomains are used to host the HIMS:

- hismedical.dpuerp.in : Online HIMS for Medical Hospital

- hisdental.dpuerp.in : Online HIMS for Dental Hospital.

Medical Hospital Modules

Registration Counter

- All the patients need to register themselves at the Registration Counter. If the patient is visiting for the first time, his complete data is entered into the HIMS and a new OPD number is allotted to the patient.

- Follow-up status is used if the patient is visiting for follow-up.
- Appropriate OPD Unit is selected while entering the OPD no.

Central Clinical Laboratory

- All the lab tests that are need to be carried out in labs should be done so.
- Upon receipt of the sample, the Data Operator will create a CCL Requisition. This requisition will have the detailed info of the patient and details of the tests to be conducted.
- Once the test has been conducted, the results have to be entered into the system. These results are available to all the concerned doctors.

Medical Record Department

- All the patient records are available in this department.
- Many summary reports have been created to have statistical view of the patients.

Dental Hospital Modules

Registration Counter

- Whenever a new patient visits the hospital, his complete details are entered into the system.
- The patient then proceeds to OMDR department where his/ her complete history is entered into the HIMS.

Departments

- All the departments have separate logins to view and edit the patient information.
- The login user can view the complete history of the patient.
- If some treatment is specified, the patient makes payment on the cash counter.
- Cash Counter will receive payment against the specified treatment and the record will be updated in the departments.

The system is a combination of desktop and Web-based technologies in order to get maximum usage. The web-based system is developed in such a way that it can be opened on any available device (android smartphones, windows smartphones, laptops, other touchscreen devices).