DPU

Dr. D. Y. PATIL VIDYAPEETH, PUNE
(Deemed to be University)

(Accredited (3rd Cycle) by NAAC with a CGPA of 3.64 on four point scale at 'A++' Grade)
(Declared as Category - I University by UGC under Graded Autonomy Regulations, 2018)
(An ISO 9001:2015, ISO 14001:2015 Certified University)

DPU IT POLICY DOCUMENT

(Amended upto March, 2024)

DPU

Dr. D. Y. PATIL VIDYAPEETH, PUNE
(Deemed to be University)
(Accredited (3rd Cycle) by NAAC with a CGPA of 3.64 on four point scale at 'A++' Grade)
(Declared as Category - I University by UGC Under Graded Autonomy Regulations, 2018)
(An ISO 9001:2015 and 14001:2015 Certified University and Green Education Campus)

Dr. Narendra M. Kadu
Registrar (Offg)

Ref. No. : DPU/24(j)/iii/2024
Date : 04/04/2024

NOTIFICATION

In pursuance of the resolutions passed by the **Academic Council** at its meeting held on **15th March, 2024** vide **Resolution No. AC-14(iii)-24** and the **Executive Council** at its meeting held on **22nd March 2024** vide **Resolution No. EC-14(iii) -24**.

It is hereby notified for information of all concerned that Dr. D. Y. Patil Vidyapeeth, Pimpri, Pune has published **"DPU IT Policy Document (Amended upto March, 2024)"** for information to all the concerned.

The **DPU IT Policy** comprises of the following parts:

1. Introduction
2. Mission
3. Vision
4. Requirement
5. Aims of the Policy
6. Policy Statements
7. Email Policy
8. Campus ERP Policy
9. HMS (Hospital Information Management System) Policy
10. Data Privacy Policy
11. Digital Readiness Strategy Document
12. Student Record Security Policy
13. Digital and Blended Learning Document
14. IT Security Policy
15. Tech Governance Policy
16. Learning Systems Roadmap
17. IT Infrastructure Roadmap

The **"DPU IT Policy Document (Amended upto March, 2024)"** will serve as a detailed guideline and will be useful to all the concerned. This will come into force with immediate effect.

Dr. D. Y. PATIL VIDYAPEETH PIMPRI, PUNE-18. Deemed to be University

(Dr. Narendra M. Kadu)
Registrar

Copy to;
1. P.S. to Chancellor for the Kind information of Hon'ble Chancellor, Dr. D. Y. Patil Vidyapeeth Pune.
2. P.S. to Vice Chancellor for the Kind information of Hon'ble Vice Chancellor, Dr. D.Y. Patil Vidyapeeth, Pune.
3. P.S. to Pro Vice Chancellor for the Kind information of Hon'ble Pro Vice Chancellor, Dr. D.Y. Patil Vidyapeeth, Pune.
4. Director (IQAC), Dr. D.Y. Patil Vidyapeeth, Pune.
5. Director (Administration: Quality Assurance, Faculty Development & Research), Dr. D. Y. Patil Vidyapeeth, Pune
6. Director (Research), Dr. D.Y. Patil Vidyapeeth, Pune.
7. Controller of Examinations, Dr. D.Y. Patil Vidyapeeth, Pune.
8. Finance Officer, Dr. D.Y. Patil Vidyapeeth, Pune.
9. All the Heads of the Colleges / Institutes of DPU
10. Web master for uploading on DPU website.

Encl: As above

Sant Tukaram Nagar, Pimpri, Pune - 411018, Maharashtra (India)
Phone : + 91-20-27805000, 27805001, Email : registrar@dpu.edu.in

Dr. D. Y. Patil Vidyapeeth, Pune

(Deemed University)
(Accredited by NAAC with 'A' grade)

Ref.No.: DPU /26 /2015 Date: 12/01/2015
16

NOTIFICATION

In pursuance of the resolution passed by the Board of Management at its meeting held on 26th December 2014, vide it resolution no. BM-42-14 and the decision taken by the Vidyapeeth Authorities.

It is hereby notified for information of all concerned that the Dr. D V Patil Vidyapeeth. Pune has published **IT Policy Document of the Vidyapeeth** for rules for access to administrative data, codes of practice, storage of sensitive data on individual use devices, etc. for your information and record.

This Policy will serve as a guideline for measures to be adopted by Vidyapeeth and all its Constituent Colleges / Institutions / Offices. The Policy will be helpful to all the concerned.

This Policy will come into force with immediate effect.

Suryakar

(Dr. A. N. Suryakar)
Registrar

Copy to:

I. P.S. to Chancellor for the Kind information of Hon'ble Chancellor, Dr. D. Y Patil Vidyapeeth, Pune.
2. P. S. to Vice Chancellor for the Kind information of Hon'ble Vice Chancellor, Dr. D. Y. Patil Vidyapeeth, Pune.
3 All the Heads of the Institutes.

Sant Tukaram Nagar, Pimpri, Pune – 411 018, Maharashtra, India. Ph. 91-20-27420069 / 27420156. Fax 91-20 -27420010.
E-mail – vc@dpu.edu.in / info@dpu.edu.in Website – www.dpu.edu.in

Contents

1 DPU IT Policy 9
1.1 Introduction 9
1.2 Mission 9
1.3 Vision 9
1.4 Requirement 9
1.5 Aims of IT Policy 10
1.6 Policy Statement 10
1.6.1 Benefits of Information Technology 10
1.6.2 Limitations of IT use in Education 11
1.6.3 Summary of Main Security Policies 11
1.6.4 Virus Protection 12
1.6.5 Access Control 13
1.6.6 LAN Security 14
1.6.7 Server Specific Security 15
1.6.8 UNIX & Linux Specific Security 15
1.6.9 Wide Area Network Security 16
1.6.10 TCP/IP & Internet Security 16
1.7 Email Policy 17
1.7.1 Legal Risks 17
1.7.2 Legal requirements 17
1.7.3 Best practices 17
1.7.4 Personal Use 18
1.7.5 Confidential information 19
1.7.6 Disclaimer 19
1.7.7 System Monitoring 19
1.7.8 Email Accounts 19
1.7.9 Questions 19
1.8 Campus ERP Policy 19
1.8.1 Introduction 19
1.8.2 Salient Features 20
1.8.3 Implementation 20
1.8.4 Modules 21

1.8.5 Security 22
1.9 HIMS (Hospital Information Management System) Policy 23
1.9.1 Introduction 23
1.9.2 Benefits of HIS 23
1.9.3 Implementation 24
1.9.4 Medical Hospital Modules 24
1.9.5 Dental Hospital Modules 24
2 Data Privacy Policy 25
2.1 Introduction 25
2.2 Objective 25
2.3 Vision 25
2.4 Mission 25
2.5 Definitions 25
2.6 Legal and Regulatory Framework 25
2.7 Principles of Data Privacy 26
2.8 Scope of Data Collection and Processing 27
2.9 Data Collection Practices 27
2.10 Data Use and Sharing 28
2.10.1 Data Use: 28
2.10.2 Data Sharing 28
2.10.3 Transparency and Control 29
2.10.4 Data Security 29
2.11 Data Retention and Disposal 29
2.11.1 Data Retention Periods 29
2.11.2 Data Disposal Procedures 30
2.11.3 Data Minimization 30
2.12 Data Security Measures 30
2.12.1 Access Controls and User Authentication 30
2.12.2 Data Encryption 30
2.12.3 Regular Security Assessments and Audits 30
2.12.4 Incident Response and Data Breach Notification Procedures 31
2.12.5 Secure Storage and Backups 31
2.12.6 Additional Security Measures 31

2.12.7 Your Role in Data Security 31
2.13 Data Subject Rights 31
2.13.1 Your Rights 31
2.13.2 Exercising Your Rights 32
2.14 Data Breach Notification 32
2.14.1 Our Data Breach Response Process 32
2.14.2 How We Will Notify You 33
2.14.3 What You Can Do 33
2.15 Compliance and Accountability 33
2.16 Training and Awareness 33
2.17 Contact Information 34
3 Digital Readiness Strategy Document 35
3.1 Vision 35
3.2 Mission 35
3.3 Purpose 35
3.4 Digital Readiness Goals 35
3.5 Implementation Strategies 36
4 Student Record Security Policy 37
4.1 Introduction 37
4.1.1 Purpose of the Policy 37
4.1.2 Vision 37
4.1.3 Mission 37
4.1.4 Scope and Applicability 37
4.1.5 Legal and Regulatory Compliance 37
4.2 Definitions 38
4.2.1 Student Records 38
4.2.2 Confidentiality 38
4.2.3 Integrity 38
4.2.4 Availability 38
4.2.5 Personal Data 38
4.2.6 Sensitive Personal Data 38
4.3 Policy Statement 39
4.3.1 Commitment to Security 39

4.3.2 Roles and Responsibilities 39
4.3.3 Compliance 39
4.4 Access Control 39
4.4.1 Authentication and Authorization 39
4.4.2 Access Privileges 39
4.4.3 Monitoring and Audit Trails 39
4.4.4 Data Access Requests 40
4.5 Data Collection and Storage 40
4.5.1 Lawful Basis for Data Collection 40
4.5.2 Secure Storage 40
4.5.3 Encryption and Data Masking 40
4.5.4 Data Minimization 40
4.5.5 Data Classification 41
4.5.6 Data Retention 41
4.6 Data Handling and Transmission 41
4.6.1 Secure Handling 41
4.6.2 Secure Transmission 41
4.6.3 Data Sharing 41
4.6.4 Student Rights Regarding Data Sharing 41
4.7 Data Retention and Disposal 42
4.7.1 Retention Periods 42
4.7.2 Secure Disposal of Student Data 42
4.7.3 Record of Destruction 42
4.8 Monitoring and Auditing 42
4.8.1 Monitoring Mechanisms 42
4.8.2 Regular Audits 43
4.8.3 Incident Response 43
4.9 Training and Awareness 43
4.9.1 Staff Training 43
4.9.2 Student Awareness 43
4.9.3 Phishing Awareness 43
4.10 Compliance and Enforcement 43
4.10.1 Compliance Requirements 43

5 Digital and Blended Learning Document 45
5.1 Introduction 45
5.2 Objective 45
5.3 Vision 45
5.4 Mission 45
5.5 Organizational Context 45
5.6 DPU Central IT Department Leadership Structure 46
5.6.1 Central IT Department 47
5.6.2 Software Development Cell 48
5.7 Digital and Blended Learning Strategy 51
5.8 Educational Quality Assurance 52
5.9 Support and Infrastructure 52
5.10 Collaboration and Partnerships 53
5.11 Policy Compliance and Review 53
6 IT Security Policy 54
6.1 Introduction and Purpose 54
6.2 Summary of Main Security Policies 54
6.2.1 Confidentiality of Data 54
6.2.2 Virus Protection 54
6.2.3 Access Control 54
6.2.4 LAN Security 55
6.2.5 Electrical Security 55
6.2.6 Inventory Management 55
6.2.7 Server Specific Security 55
6.2.8 Email Policy 55
7 Tech Governance Policy 57
7.1 Introduction 57
7.2 Scope 57
7.3 Objectives 57
7.4 Governance Structure 57
7.4.1 Technology Governance Committee (TGC): 57
7.4.2 Technology Operations Team (TOT): 57
7.4.3 Technology User Groups: 57

7.5 Policy Framework 58
7.5.1 Technology Strategy and Planning: 58
7.5.2 Technology Procurement and Vendor Management: 58
7.5.3 Data Management and Security: 58
7.5.4 Compliance and Risk Management: 58
7.5.5 Innovation and Continuous Improvement: 58
7.6 Communication and Training 58
7.7 Monitoring and Evaluation 59
8 Learning Systems Roadmap 60
8.1 Introduction 60
8.2 Vision and Objectives 60
8.2.1 Vision 60
8.2.2 Objectives: 60
8.3 The Roadmap 60
8.3.1 Phase 1 (Year 1): 60
8.3.2 Phase 2 (Year 2-3): 61
8.3.3 Phase 3 (Year 4-5): 62
8.3.4 Phase 4 (Year 6-7): 63
8.3.5 Phase 5: Future Plans 65
9 IT Infrastructure Roadmap. 68
9.1 Introduction 68
9.2 Evolution of IT Infrastructure at Dr. D. Y. Patil Vidyapeeth, Pune: 68
9.2.1 Initial Phase (Foundation): 68
9.2.2 Expansion and Upgrades: 68
9.2.3 Investment in Human Resources and Software: 68
9.2.4 Hardware Upgrades and Network Expansion: 68
9.3 Future Roadmap: 69
9.3.1 Ring-Shaped Network Connectivity: 69
9.3.2 Innovative Healthcare Solutions: 69
9.4 Future Vision and Goals 69
9.5 Proposed Changes and Enhancements 70
9.6 IT Infrastructure Roadmap 70
9.7 Risk Management and Contingency Plans 70

9.8 Monitoring and Evaluation Framework 71
9.9 Conclusion 71
9.10 Appendices 71

1 DPU IT Policy

1.1 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".

1.2 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.

1.3 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.

1.4 Requirement

- 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.

1.5 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.

1.6 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."

1.6.1 Benefits of Information Technology

- 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.

- Increase access, Flexibility of content and distribution Combination of education and work the methods are focused on the student.
- High quality, cost-effective professional development in place of labour. Improve the skills of employees, increase of productivity. Developing a new culture of learning. Sharing of costs and timing of training among employees.
- 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.
- 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.
- 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.

1.6.2 Limitations of IT use in Education

- 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.
- 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.

1.6.3 Summary of Main Security Policies

- 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.
- Internet and other external service access are restricted to authorized personnel only.
- 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.
- Only authorized and licensed software may be installed, and installation may only be performed by I.T. Department staff.
- The use of unauthorized software is prohibited. In the event of unauthorized software being discovered it will be removed from the workstation immediately.

- Data may only be transferred for the purposes determined in the Organizations' data-protection policy.
- All diskette drives and removable media from external sources must be virus checked before they are used within the Organization.
- Passwords must consist of a mixture of at least 4 alphanumeric characters and must be changed every 30 days and must be unique.
- Workstation configurations may only be changed by I.T. Department staff.
- The physical security of computer equipment will conform to recognized loss prevention guidelines.
- To prevent the loss of availability of I.T. resources measures must be taken to backup data, applications, and the configurations of all workstations.

1.6.4 Virus Protection

- The I.T. Department will have available up to date virus scanning software for the scanning and removal of suspected viruses.
- Corporate file-servers will be protected with virus scanning software.
- Workstations will be protected by virus scanning software.
- All workstation and server anti-virus software will be regularly updated with the latest anti-virus patches by the I.T. Department.
- No disk that is brought in from outside the Organization is to be used until it has been scanned.
- 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.
- All removable media containing executable software (software with .EXE and .COM extensions) will be write protected wherever possible.
- All demonstrations by vendors will be run on their machines and not the Organizations'.
- 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.
- New commercial software will be scanned before it is installed as it occasionally contains viruses.
- All removable media brought into the Organization by field engineers or support personnel will be scanned by the IT Department before they are used on site.
- To enable data to be recovered in the event of virus outbreak regular backups will be taken by the I.T. Department.
- Management strongly endorses the Organizations' anti-virus policies and will make the necessary resources available to implement them.
- Users will be kept informed of current procedures and policies.
- Users will be notified of virus incidents.
- Employees will be accountable for any breaches of the Organizations' anti-virus policies.
- Anti-virus policies and procedures will be reviewed regularly.

- 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.

1.6.5 Access Control

- 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.
- Users requiring access to systems must make a written application on the forms provided by the I.T Department.
- 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.
- 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.
- Access to the network/servers and systems will be by individual username and password, or by smartcard and PIN number/biometric.
- Usernames and passwords must not be shared by users.
- Usernames and passwords should not be written down.
- Usernames will consist of initials and surname.
- All users will have an alphanumeric password of at least 4 characters.
- Passwords will expire every 30 days and must be unique.
- Intruder detection will be implemented where possible. The user account will be locked after 5 incorrect attempts.
- 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.
- 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.
- Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all systems.
- I.T. Department staff will not login as root on to UNIX, Linux systems, but will use the SU command to obtain root privileges.
- Use of the admin username on Novell systems and the Administrator username on Windows is to be kept to a minimum.
- Default passwords on systems such as Oracle and SQL Server will be changed after installation.
- On UNIX and Linux systems, rights to RLOGIN, FTP, TELNET, SSH will be restricted to I.T. Department staff only.
- Where possible users will not be given access to the UNIX, or Linux shell prompt.
- 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.

- 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.

1.6.6 LAN Security

1.6.6.1 Routers & Switches

- 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.

1.6.6.2 Workstations

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

1.6.6.3 Wiring

- All network wiring will be fully documented.
- All unused network points will be de-activated when not in use.
- All network cables will be periodically scanned, and readings recorded for future reference.
- Users must not place or store any item on top of network cabling.
- Redundant cabling schemes will be used where possible.
- Monitoring Software will be used.
- The use of LAN analyzer and packet sniffing software is restricted to the I.T. Department.
- LAN analyzers and packet sniffers will be securely locked up when not in use.
- Intrusion detection systems will implemented to detect unauthorized access to the network.

1.6.6.4 Servers

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

1.6.6.5 Electrical Security

- All servers will be fitted with UPS's that also condition the power supply.
- All hubs, bridges, repeaters, routers, switches, and other critical network equipment will also be fitted with UPS's.
- 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.
- Software will be installed on all servers to implement an orderly shutdown in the event of a total power failure.
- All UPS's will be tested periodically.

1.6.6.6 Inventory Management

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

1.6.7 Server Specific Security

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

- The operating system will be kept up to date and patched on a regular basis.
- Servers will be checked daily for viruses.
- Servers will be locked in a secure room.
- Where appropriate the server console feature will be activated.
- Remote management passwords will be different to the Admin/Administrator/root password.
- Users possessing Admin/Administrator/root rights will be limited to trained members of the I.T. Department staff only.
- Use of the Admin/Administrator/root accounts will be kept to a minimum.
- Assigning security equivalences that give one user the same access rights as another user will be avoided where possible.
- User's access to data and applications will be limited by the access control features.
- Intruder detection and lockout will be enabled.
- The system auditing facilities will be enabled.
- Users must logout or lock their workstations when they leave their workstation for any length of time.
- All unused workstations must be switched off outside working hours.
- All accounts will be assigned a password of a minimum of 8 characters.
- Users will change their passwords every 30 days.
- Unique passwords will be used.
- The number of grace logins will be limited to 5.
- The number of concurrent connections will be limited to 3.
- Network login time restrictions will be enforced preventing users from logging in to the network outside normal working hours.
- In certain areas users will be restricted to logging in to specified workstations only.

1.6.8 UNIX & Linux Specific Security

- Direct root access will be limited to the system console only.
- I.T. Department staff requiring root access must make use of the SU command.
- Use of the root account will be kept to a minimum.
- All UNIX and Linux system accounts will be password protected, lP etc.
- RLOGIN facilities will be restricted to authorize I.T. Department staff only.
- FTP facilities will be restricted to authorize I.T. Services staff only.

- TELNET facilities will be restricted to authorized users.
- SSH facilities will be restricted to authorized users.
- User's access to data and applications will be limited by the access control features.
- Users will not have access to the $ prompt.
- All accounts will be assigned a password of a minimum of characters.
- Users will change their passwords every 30 days.

1.6.9 Wide Area Network Security

- Wireless LAN's will make use of the most secure encryption and authentication facilities available.
- Users will not install their own wireless equipment under any circumstances.
- 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.
- Modems will not be used by users without first notifying the I.T. Department and obtaining their approval.
- Where dial-in modems are used, the modem will be unplugged from the telephone network and the access software disabled when not in use.
- Modems will only be used where necessary; in normal circumstances all communications should pass through the Organizations' router and firewall.
- Where leased lines are used, the associated channel service units will be locked up to prevent access to their monitoring ports.
- All bridges, routers and gateways will be kept locked up in secure areas.
- Unnecessary protocols will be removed from routers.
- The preferred method of connection to outside Organizations is by a secure VPN connection, using IPSEC or SSL.
- All connections made to the Organizations' network by outside organizations will be logged.

1.6.10 TCP/IP & Internet Security

- Permanent connections to the Internet will be via the means of a firewall to regulate network traffic.
- Permanent connections to other external networks, for offsite processing etc., will be via the means of a firewall to regulate network traffic.
- Where firewalls are used, a dual homed firewall (a device with more than one TCP/IP address) will be the preferred solution.
- Network equipment will be configured to close inactive sessions.
- Where modem pools or remote access servers are used, these will be situated on the DMZ or non-secure network side of the firewall.
- Workstation access to the Internet will be via the Organizations' proxy server and website content scanner.
- All incoming e-mail will be scanned by the Organizations' e- mail content scanner.

1.7 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.

1.7.1 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 are 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.

1.7.2 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.

1.7.3 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:

1.7.3.1 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.

1.7.3.2 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.

1.7.4 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.

1.7.5 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.

1.7.6 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.'

1.7.7 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.

1.7.8 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.

1.7.9 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.

1.8 Campus ERP Policy

1.8.1 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:

- Integrate information across all functions (examples include registration, financial aid, human resources).
- Facilitate the flow of information among the institution's functions.
- Track a wide range of institutional events in an integrated fashion and facilitate planning future activities based on these events.
- Support analysis of trends and thus improve the performance of the institution.
- 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.

1.8.2 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.

1.8.3 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.

Sr. No.	Institute Name	Sub-Domain Name
1.	Dr. D.Y. Patil Vidyapeeth, Pune	university.dpuerp.in
2.	Dr. D. Y. Patil Medical College, Hospital & Research Centre, Pimpri	medical.dpuerp.in

Sr. No.	Institute Name	Sub-Domain Name
3.	Dr. D. Y. Patil Dental College & Hospital, Pimpri	dental.dpuerp.in
4.	Dr. D. Y. Patil Biotechnology and Bioinformatics Institute, Tathawade	biotech.dpuerp.in
5.	Global Business School & Research Centre, Tathawade	gbsrc.dpuerp.in
6.	Center for Online Learning, Pimpri	col.dpuerp.in
7.	Dr. D. Y. Patil College of Nursing, Pimpri	nursing.dpuerp.in
8.	Dr. D. Y. Patil College of Physiotherapy, Pimpri	physio.dpuerp.in
9.	Dr. D. Y. Patil Institute of Optometry and Visual Sciences, Pimpri	optom.dpuerp.in
10.	Dr. D. Y. Patil College of Ayurved & Research Centre, Pimpri	ayurved.dpuerp.in
11.	Dr. D. Y. Patil Homoeopathic Medical College & Research Centre, Pimpri	homoeopathy.dpuerp.in
12.	Dr. D. Y. Patil School of Design, Tathawade	sod.dpuerp.in
13.	Dr. D. Y. Patil School of Liberal Arts, Pimpri	liberalarts.dpuerp.in
14.	Dr. D. Y. Patil School of Science & Technology, Tathawade	sst.dpuerp.in
15.	Dr. D. Y. Patil School of Allied Health Sciences, Pimpri	sahs.dpuerp.in

1.8.4 Modules

1.8.4.1 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.

1.8.4.2 Academic Section

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

1.8.4.3 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.

1.8.4.4 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.

1.8.4.5 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.

1.8.4.6 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.

1.8.5 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.

1.9 HIMS (Hospital Information Management System) Policy

1.9.1 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.

1.9.2 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.

1.9.3 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.

1.9.4 Medical Hospital Modules

1.9.4.1 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.

1.9.4.2 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.

1.9.4.3 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.

1.9.5 Dental Hospital Modules

1.9.5.1 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.

1.9.5.2 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).

2 Data Privacy Policy

2.1 Introduction

Dr. D. Y. Patil Vidyapeeth, Pune (the "Vidyapeeth"), is committed to protecting the privacy and confidentiality of the personal data entrusted to us by our students, faculty, staff, and other stakeholders. We operate within the legal framework of the Information Technology Act, 2000 (the "IT Act") and the Personal Data Protection Act, 2023 (the "DPDPA"), along with any guidelines or regulations issued by the Data Protection Authority (DPA) established under the DPDPA. This Data Privacy Policy outlines our practices for collecting, using, storing, and protecting your personal data.

2.2 Objective

To establish and maintain a framework for protecting the privacy and confidentiality of personal data at Dr. D. Y. Patil Vidyapeeth, Pune, ensuring compliance with relevant data protection laws and regulations.

2.3 Vision

To create a culture of transparency, accountability, and trust regarding the handling of personal data, fostering confidence among students, faculty, staff, and other stakeholders.

2.4 Mission

To implement robust data privacy practices guided by principles of transparency, purpose limitation, data minimization, accuracy, integrity, confidentiality, and accountability, while providing mechanisms for data subjects to exercise their rights and ensuring continuous improvement through training, awareness, and policy review.

2.5 Definitions

- **Personal Data:** As defined under Section 2(v) of the IT Act and Clause (t) of the DPDPA, it refers to any information relating to an identified or identifiable individual, including but not limited to name, address, email address, phone number, identification number, biometric data, location data, online identifiers (e.g., IP address, cookies), and financial information.
- **Processing:** As defined under Section 2(f) of the IT Act, it refers to any operation or set of operations performed on personal data, such as collection, recording, organization, storage, retrieval, consultation, use, disclosure, dissemination, erasure, or destruction.
- **Data Controller:** As defined under Section 4(1)(b) of the IT Act, it is the entity responsible for determining the purposes and means of processing personal data. The Vidyapeeth is the Data Controller for personal data collected through its activities.
- **Data Subject:** As defined under Section 11(1) of the IT Act, it refers to an identified or identifiable individual to whom personal data relates. You are the data subject if your personal data is processed by the Vidyapeeth.

2.6 Legal and Regulatory Framework

Dr. D. Y. Patil Vidyapeeth, Pune, operates within a robust legal and regulatory framework governing data protection in India. This includes compliance with:

- **The Information Technology Act, 2000 (India):** This legislation governs electronic transactions, cybersecurity, and the protection of digital data in India. While the IT Act provides a foundation for data protection, the DPDPA supersedes it in many aspects. We will comply with the relevant provisions of the IT Act.
- **The Personal Data Protection Act, 2023 (India):** This Act establishes a comprehensive framework for the processing of personal data in India. It outlines the principles, rights, obligations, and procedures for handling personal data. The Vidyapeeth adheres to the principles and fulfills the obligations set forth in the DPDPA.
- **Guidelines issued by the Data Protection Authority (DPA) (if applicable):** The DPA is an independent regulatory body established under the DPDPA. We will comply with any guidelines, regulations, or advisories issued by the DPA to ensure adherence to the evolving data protection landscape.

2.7 Principles of Data Privacy

Dr. D. Y. Patil Vidyapeeth is committed to upholding the following core principles of data privacy:

- **Transparency:** We strive for transparency in our data processing activities. We provide clear and accessible information to data subjects about how their personal data is collected, used, stored, and disclosed. This includes information about the purposes of processing, the legal basis for processing, and the rights of data subjects.
- **Lawfulness, Fairness, and Purpose Limitation:** We collect and process personal data only for specified, explicit, and legitimate purposes aligned with our educational and administrative functions. We rely on a lawful basis for processing under the DPDPA, such as consent, contract, legal obligation, or public interest. We collect only the minimum amount of personal data necessary to achieve those purposes and do not further process it in a manner incompatible with those purposes.
- **Data Minimization:** We believe in collecting only the personal data essential to fulfill the specific purposes for which it is collected. We avoid collecting excessive data and implement processes to regularly review and remove unnecessary data.
- **Accuracy:** We take reasonable steps to ensure that the personal data we hold is accurate, complete, and up-to-date. We encourage data subjects to keep their information updated and provide mechanisms for them to correct any inaccuracies.
- **Storage Limitation:** We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, considering legal, regulatory, and administrative requirements. We have established data retention schedules and procedures to ensure data is not retained longer than necessary.
- **Integrity and Confidentiality:** We implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful access, accidental loss, destruction, or damage. This includes measures such as access controls, encryption, and regular security assessments.
- **Accountability:** We are accountable for complying with the DPDPA and other applicable data protection laws and regulations. We have established data governance policies and procedures to ensure compliance and maintain a data protection program.

2.8 Scope of Data Collection and Processing

Dr. D. Y. Patil Vidyapeeth, Pune, collects and processes personal data for various purposes related to its educational and administrative functions. This includes:

- **Admission and Enrollment Processes:** Personal data collected during the registration, admission and enrollment process includes but is not limited to name, date of birth, contact information, educational background, and medical history (if applicable).
- **Academic Activities and Assessments:** Personal data collected for academic purposes includes student records, grades, attendance records, and research data.
- **Student Support Services:** Personal data may be collected to provide student support services such as counseling, disability support, and career services.
- **Human Resources Management:** Personal data of faculty, staff, and other employees is collected for human resources management purposes, including recruitment, payroll, and performance evaluation.
- **Alumni Relations:** Personal data of alumni may be collected for alumni relations and fundraising purposes.
- **Research Activities:** Personal data may be collected for research purposes, subject to ethical and legal requirements.
- **Compliance with Legal and Regulatory Requirements:** Personal data may be collected and processed to comply with legal and regulatory requirements, such as reporting obligations to government authorities.

2.9 Data Collection Practices

Dr. D. Y. Patil Vidyapeeth collects personal data through various channels to fulfill its educational and administrative functions. We prioritize transparency and ensure data subjects are informed about the collection process. Here are some common methods we use:

- **Application Forms:** Online or paper-based application forms for prospective students collect information like name, date of birth, contact details, educational background, and potentially medical history (with explicit consent).
- **Registration Forms:** Online or in-person registration forms for courses, programs, or events may collect data from enrolled students, such as program selection and additional contact information.
- **Online Portals and Platforms:** Learning Management Systems (LMS), student portals, and other online platforms used for educational purposes may collect data related to your activity and progress. This could include course materials accessed, assignments submitted, and interaction with online learning tools.
- **Correspondence:** We may collect personal data through email, letters, or other communication channels with students, faculty, staff, and other stakeholders. This might include inquiries, feedback submissions, or requests for specific services.
- **Surveys and Feedback Forms:** Surveys and feedback forms used to gather your opinions or experiences may collect personal data relevant to the topic at hand. Participation in these activities is usually voluntary.

Before collecting your personal data, we will provide clear information about:

- **The purpose(s) of data collection:** We will explain why your data is needed and how it will be used.
- **The legal basis for processing:** We will identify the lawful justification under the DPDPA for processing your data (e.g., consent, contract, legal obligation).
- **Your rights as a data subject:** We will inform you of your rights under the DPDPA, such as the right to access, rectify, or erase your personal data.

In many cases, we will obtain your explicit consent for collecting and processing your data. However, there may be instances where processing is necessary to fulfill a contractual obligation (e.g., student enrollment) or comply with legal requirements.

We are committed to respecting your privacy and ensuring you have control over your personal data. If you have any questions about our data collection practices or wish to exercise your data subject rights, please refer to the section “contact information”.

2.10 Data Use and Sharing

Dr. D. Y. Patil Vidyapeeth uses and shares personal data only for specific, lawful purposes outlined in "Scope of Data Collection and Processing" and with a justified basis under the DPDPA. We prioritize data privacy and security, and we will never sell or lease your personal data to third parties for marketing purposes.

Here's a breakdown of how we use and share your data:

2.10.1 Data Use:

- **Fulfilling Educational and Administrative Functions:** We primarily use personal data to fulfill our core functions as an educational institution. This includes processing data for activities such as:

    a) Admission and enrollment processes
    b) Academic activities and assessments (including grading and progress tracking)
    c) Providing student support services (e.g., counseling, career guidance)
    d) Human resources management (e.g., payroll, performance evaluation)
    e) Alumni relations and communication
    f) Conducting research activities (subject to ethical and legal requirements)

- **Compliance with Legal Obligations:** We may use personal data to comply with legal and regulatory requirements, such as reporting obligations to government authorities.

2.10.2 Data Sharing

We share personal data with third parties only when necessary and lawful. In such cases, we enter into strict contractual agreements to ensure these third parties maintain an adequate level of data protection and security. Here are some scenarios where data sharing may occur:

- **Service Providers and Vendors:** We may share data with service providers and vendors who assist us in delivering our services. These may include companies providing IT support, cloud storage, payment processing, or other services.
- **Educational Partners and Affiliates:** Personal data may be shared with educational partners and affiliates for academic collaborations, research projects, or exchange programs. This will only be done with your consent (where required by the DPDPA) and subject to data protection agreements.
- **Regulatory Authorities and Government Agencies:** We may share personal data with regulatory authorities and government agencies as required by law, such as reporting obligations or investigations.

2.10.3 Transparency and Control

We are committed to transparency regarding data sharing. Whenever possible, we will inform you in advance if we plan to share your data with a third party. We will also strive to provide you with choices about how your data is shared, where applicable.

2.10.4 Data Security

We implement robust security measures to protect your personal data from unauthorized access, disclosure, alteration, or destruction. Please refer to "Data Security Measures" for more details on how we secure your information.

If you have any questions about how your data is used or shared, please don't hesitate to contact us using the information provided in “Contact Information”.

2.11 Data Retention and Disposal

Dr. D. Y. Patil Vidyapeeth recognizes the importance of retaining personal data only for as long as necessary and disposing of it securely when it's no longer required. We comply with the data retention periods outlined in the DPDPA and implement secure disposal practices to protect your privacy.

2.11.1 Data Retention Periods

We retain personal data for a defined period based on the purpose for which it was collected and in accordance with legal or regulatory requirements. Here are some general guidelines:

- **Admission and Enrollment Data:** Retained for a specific period after enrollment or application closure, as mandated by the Vidyapeeth or relevant regulations.
- **Academic Records:** Maintained for a longer duration as mandated by accreditation bodies or for historical and reference purposes.
- **Student Support Service Records:** Retained for a specific period after the completion of the service or as required by regulations.
- **Human Resource Data:** Retained for the duration of employment and for a specified period after termination, as mandated by labour laws or for potential legal disputes.
- **Alumni Relations Data:** Maintained for a longer period unless the alumnus/alumna requests deletion.

- **Research Data:** Retained according to research protocols, ethical guidelines, and any funder requirements.

2.11.2 Data Disposal Procedures

When personal data reaches the end of its retention period or is no longer required, we securely dispose of it using appropriate methods. These methods may include:

- **Secure Overwriting:** Electronic data is overwritten with random characters to render it unrecoverable.
- **Physical Destruction:** Physical media containing personal data (e.g., paper documents, hard drives) is shredded or destroyed using secure methods to prevent unauthorized access.

2.11.3 Data Minimization

We implement data minimization practices to reduce the amount of personal data collected and stored. We regularly review the data we hold and delete any information that is no longer necessary.

We are committed to responsible data management and ensuring the security and privacy of information throughout its lifecycle. If you have any questions about our data retention or disposal practices, please contact us using the information provided in Section “Contact Information”.

2.12 Data Security Measures

Dr. D. Y. Patil Vidyapeeth prioritizes the security and confidentiality of your personal data. We implement robust technical and organizational measures to protect your information from unauthorized access, disclosure, alteration, or destruction. Here's an overview of our data security measures:

2.12.1 Access Controls and User Authentication

- We restrict access to personal data to authorized personnel only. This includes implementing strong password policies, user authentication mechanisms (e.g., multi-factor authentication), and access control lists to limit access based on job roles and permissions.
- Regular training is provided to staff on data security best practices and procedures to ensure they handle personal data responsibly.

2.12.2 Data Encryption

- Sensitive personal data, such as financial information or medical records, is encrypted at rest and in transit. This adds an extra layer of security by scrambling the data using encryption algorithms, making it unreadable to unauthorized individuals even if they gain access.

2.12.3 Regular Security Assessments and Audits

- We conduct regular security assessments and audits to identify and address any vulnerabilities in our systems and processes. These assessments help us maintain a strong security posture and proactively mitigate potential security risks.
- We stay updated on emerging cybersecurity threats and implement appropriate security measures to address them.

2.12.4 Incident Response and Data Breach Notification Procedures

- We have established incident response and data breach notification procedures to effectively respond to security incidents. These procedures include identifying and containing the breach, notifying affected individuals and relevant authorities as required by law, and taking steps to prevent future incidents.

2.12.5 Secure Storage and Backups

- Personal data is stored on secure servers with industry-standard security measures in place. We maintain regular backups of data to ensure information recovery in case of disasters or system failures.

2.12.6 Additional Security Measures

- We may implement additional security measures depending on the type of personal data collected and the associated risks. This may include firewalls, intrusion detection/prevention systems, and data loss prevention (DLP) tools.

2.12.7 Your Role in Data Security

While we strive to implement robust security measures, data security is a shared responsibility. We encourage you to practice good security hygiene by:

- Choosing strong and unique passwords for your accounts.
- Being cautious about opening suspicious emails or clicking on unknown links.
- Reporting any suspected security incidents to the appropriate authorities.

By working together, we can create a secure environment for your personal data.

We are committed to continuously improving our data security practices to protect your information. If you have any questions about our data security measures, please don't hesitate to contact us using the information provided in Section “Contact Information”.

2.13 Data Subject Rights

The Dr. D. Y. Patil Vidyapeeth recognizes your right to control your personal data under the Personal Data Protection Act, 2023 (DPDPA). This section outlines the data subject rights available to you and how you can exercise them.

2.13.1 Your Rights

Under the DPDPA, you have the following rights regarding your personal data:

- **Right to Access:** You have the right to request access to the personal data we hold about you. This includes the right to:

    a) Be informed about the categories of personal data we collect, process, and store.
    b) Obtain a copy of your personal data in a structured, commonly used, and machine-readable format.

c) Know the purposes for which your data is processed and the legal basis for such processing.

- **Right to Rectification:** You have the right to request that we rectify any inaccuracies or update any incomplete personal data we hold about you.
- **Right to Restriction of Processing:** You have the right to request the restriction of processing of your personal data under certain circumstances, such as when you contest the accuracy of the data or object to its processing.
- **Right to Data Portability:** You have the right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit the data to another controller (if technically feasible).
- **Right to Object:** You have the right to object to the processing of your personal data for certain purposes, such as direct marketing or automated decision-making processes that significantly affect you.

2.13.2 Exercising Your Rights

To exercise any of your data subject rights, please submit a written request to the designated Incharge, Software Development Cell using the following methods:

- Email: webmaster@dpu.edu.in

Your request should include:

- Your full name and contact information.
- A clear description of the right you wish to exercise.
- Specific details regarding the personal data you are requesting access to, rectification of, erasure of, or restriction on processing of

We will respond to your request within a reasonable timeframe.

2.14 Data Breach Notification

Dr. D. Y. Patil Vidyapeeth is committed to protecting the privacy and security of your personal data. In the unfortunate event of a data breach, we will take swift action to contain the incident, assess the risks, and notify affected individuals and relevant authorities as required by the Personal Data Protection Act, 2023 (DPDPA).

2.14.1 Our Data Breach Response Process

In the event of a data breach, we will follow a comprehensive response process that includes:

- **Containment:** We will take immediate steps to contain the breach and prevent further unauthorized access to personal data. This may involve isolating affected systems, resetting passwords, and implementing additional security measures.
- **Assessment:** We will conduct a thorough assessment of the breach to identify the nature and scope of the incident, the types of personal data affected, and the potential risks to individuals.

- **Notification:** We will notify affected individuals as soon expeditingly as practicable and in accordance with the requirements of the DPDPA. The notification will describe the nature of the breach, the types of personal data affected, and the steps we are taking to address the incident. We will also provide information on how affected individuals can protect themselves.
- **Reporting:** We will report the data breach to the Data Protection Authority (DPA) as required by law, depending on the severity of the breach and the risk it poses to individuals.
- **Review and Improvement:** We will conduct a review of the data breach incident to identify any weaknesses in our security measures and implement corrective actions to prevent similar incidents from occurring in the future.

2.14.2 How We Will Notify You

In the event of a data breach, we may notify you through one or more of the following methods, depending on the nature of the breach and the contact information we have on file:

- **Website:** We may post a notice on our website about the data breach.

2.14.3 What You Can Do

If you receive a notification from us about a data breach, we encourage you to take the following steps:

- Review the notification carefully to understand the nature of the breach and the types of personal data affected.
- Change your passwords for any accounts that may have been affected by the breach.
- Be cautious about phishing emails or calls that may attempt to exploit the data breach.
- Contact us if you have any questions or concerns.

We understand that a data breach can be a concerning event. We are committed to protecting your privacy and will take all necessary steps to address any data breaches that may occur.

2.15 Compliance and Accountability

Dr. D. Y. Patil Vidyapeeth, Pune, is committed to complying with data protection laws and regulations and holds itself accountable for ensuring the confidentiality, integrity, and security of personal data. Compliance with this policy is monitored through regular audits, assessments, and reviews conducted by our designated data protection officer or privacy team. Any violations of this policy or data protection laws and regulations will be promptly investigated and addressed, and appropriate disciplinary action will be taken against individuals found to be in breach of their obligations.

2.16 Training and Awareness

Employees and stakeholders receive training and awareness programs on data privacy and protection to ensure understanding and compliance with this policy and relevant laws and regulations. Training programs cover topics such as data protection principles, security best practices, incident response procedures, and data subject rights. Employees are required to complete data privacy training upon hire and periodically thereafter to stay informed about updates to policies and procedures.

2.17 Contact Information

For inquiries, concerns, or requests related to data privacy, please contact:

IT Incharge,

Dr. D. Y. Patil Vidyapeeth,

Sant Tukaram Nagar, Pimpri,

Pune – 411018

Email – webmaster@dpu.edu.in

3 Digital Readiness Strategy Document

3.1 Vision

Empowering students through innovative digital technologies to excel in their respective fields, fostering holistic development and global competitiveness.

3.2 Mission

To create a digitally enabled ecosystem that enhances learning experiences, facilitates seamless collaboration, and promotes research excellence across all institutes under Dr. D.Y. Patil Vidyapeeth, Pune.

3.3 Purpose

The purpose of this document is to outline the digital readiness goals, vision, and strategies to effectively serve student community utilizing modern technologies and processes across various disciplines including Medicine, Dentistry, Biotechnology, Nursing, Physiotherapy, Homoeopathy, Ayurveda, Science and Technology, Liberal Arts, and Management.

3.4 Digital Readiness Goals

- **Enhanced Learning Experience:** Implement digital tools and platforms to augment traditional teaching methods, providing interactive and personalized learning experiences tailored to individual student needs.
- **Seamless Collaboration:** Foster collaboration among students, faculty, and researchers through digital platforms, facilitating knowledge sharing, project collaboration, and interdisciplinary learning opportunities.
- **Research Excellence:** Enable research initiatives by providing access to cutting-edge digital resources, data analytics tools, and collaborative platforms to facilitate innovative research projects and publications.
- **Accessibility and Inclusivity:** Ensure accessibility and inclusivity by adopting universal design principles in digital content and platforms, catering to diverse learning styles and needs of all students including those with disabilities.
- **Data-driven Decision Making:** Utilize data analytics and business intelligence tools to analyse student performance, engagement metrics, and feedback data, enabling evidence-based decision-making to improve teaching methodologies and student support services.
- **Cybersecurity and Data Privacy:** Implement robust cybersecurity measures and data privacy protocols to safeguard sensitive student information and intellectual property, ensuring compliance with relevant regulations and standards.
- **Professional Development:** Provide training and professional development opportunities for faculty and staff to enhance digital literacy skills, pedagogical techniques, and technology integration strategies to effectively utilize digital tools in teaching, research, and administrative tasks.
- **Infrastructure and Technical Support:** Invest in modern infrastructure including high-speed internet connectivity, digital classrooms, laboratories, and IT support services to ensure seamless functioning of digital initiatives and technology-enabled learning environments.

- **Student Engagement and Support:** Develop digital platforms for student engagement, academic counseling, career guidance, and mental health support services, fostering a supportive learning community and holistic student development.
- **Continuous Improvement:** Establish mechanisms for continuous feedback and evaluation of digital initiatives, incorporating student and stakeholder input to iteratively improve digital readiness strategies and enhance overall effectiveness.

3.5 Implementation Strategies

- Develop a comprehensive digital roadmap outlining specific initiatives, timelines, and responsibilities for implementation across all institutes.
- Establish a dedicated Digital Transformation Committee comprising representatives from each institute to oversee planning, execution, and monitoring of digital readiness initiatives.
- Collaborate with industry partners, technology vendors, and educational institutions to leverage best practices, expertise, and resources in implementing digital solutions.
- Conduct regular assessments and audits to evaluate the effectiveness and impact of digital initiatives on student learning outcomes, faculty engagement, and institutional performance.
- Promote a culture of innovation and experimentation, encouraging faculty and students to explore emerging technologies and pedagogical approaches to enhance teaching and learning experiences.
- Foster strategic partnerships with government agencies, funding bodies, and industry associations to secure funding support for digital infrastructure development, research projects, and capacity-building initiatives.
- Communicate regularly with students, faculty, staff, and other stakeholders to ensure transparency, alignment, and engagement throughout the digital transformation journey.
- Establish mechanisms for knowledge sharing and dissemination of best practices through workshops, seminars, conferences, and publications to promote peer learning and collaboration within the academic community.

By embracing digital transformation and leveraging modern technologies, Dr. D.Y. Patil Vidyapeeth, Pune aims to create a dynamic and future-ready educational ecosystem that empowers students to thrive in a rapidly evolving global landscape while upholding its commitment to excellence, integrity, and social responsibility.

4 Student Record Security Policy

4.1 Introduction

4.1.1 Purpose of the Policy

The purpose of this policy is to establish comprehensive guidelines and procedures for safeguarding the confidentiality, integrity, and availability of student records maintained by Dr. D. Y. Patil Vidyapeeth, Pune, in accordance with the Digital Personal Data Protection Act, 2023 (DPDPA) and other applicable Indian laws and regulations governing the privacy and security of student data, including but not limited to the University Grants Commission (UGC) Regulations and the All India Council for Technical Education (AICTE) Guidelines. This policy aims to ensure that student personal data is processed lawfully, ethically, and transparently.

4.1.2 Vision

Dr. D. Y. Patil Vidyapeeth, Pune aspires to be a leader in student data privacy and security within the Indian educational landscape. We envision a future where student information is consistently protected with the utmost care, fostering a culture of trust and transparency with our student body. Through robust data governance practices and unwavering commitment to the Digital Personal Data Protection Act (DPDPA) and other relevant regulations, we aim to empower students by ensuring their personal data is used responsibly and solely for legitimate educational and administrative purposes.

4.1.3 Mission

Dr. D. Y. Patil Vidyapeeth, Pune is dedicated to safeguarding the confidentiality, integrity, and availability of student records. We strive to achieve this mission by implementing comprehensive data security policies and procedures that adhere to the highest ethical and legal standards. Our commitment extends to fostering a culture of data security awareness among staff, faculty, and students. By prioritizing student privacy and employing cutting-edge data protection measures, we ensure the responsible management of student information, allowing them to focus on their academic pursuits with confidence.

4.1.4 Scope and Applicability

This policy applies to all staff, faculty, contractors, and third-party vendors who have access to student records, whether in electronic or physical format, at Dr. D. Y. Patil Vidyapeeth, Pune. It encompasses all academic programs and disciplines offered by the institution, including Medicine, Dentistry, Nursing, Physiotherapy, Optometry, Biotechnology, Management, Ayurveda, Homeopathy, Design, Allied Health Sciences, Liberal Arts, Science & Technology, and the Online Learning Center.

4.1.5 Legal and Regulatory Compliance

This policy complies with relevant Indian laws and regulations governing the privacy and security of student data, including but not limited to:

- The Digital Personal Data Protection Act, 2023 (DPDPA)
- The University Grants Commission (UGC) Regulations on Minimum Standards and Procedure for Award of M.Phil./Ph.D. Degrees, as amended.
- The All India Council for Technical Education (AICTE) Approval Process Handbook

- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

4.2 Definitions

4.2.1 Student Records

Student records refer to any information or data related to students enrolled at Dr. D. Y. Patil Vidyapeeth, Pune, including but not limited to:

- Academic transcripts
- Enrollment information
- Financial aid records
- Disciplinary records
- Personally identifiable information (PII) such as names, addresses, and identification numbers

4.2.2 Confidentiality

Confidentiality refers to the protection of student records from unauthorized access, disclosure, or use. It ensures that only authorized individuals have access to student information and that sensitive data is not disclosed to unauthorized parties.

4.2.3 Integrity

Integrity refers to the accuracy, completeness, and reliability of student records. It ensures that student information is not altered or tampered with unlawfully and that it remains trustworthy and reliable for its intended purpose.

4.2.4 Availability

Availability refers to the accessibility of student records to authorized users when needed for legitimate purposes. It ensures that student information is accessible and usable by those who have the right to access it, without undue delay or hindrance.

4.2.5 Personal Data

Information relating to a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

4.2.6 Sensitive Personal Data

A subset of personal data that requires a higher level of protection due to its sensitive nature. This may include information such as financial data, health records, religious beliefs, caste, biometrics, and sex life.

4.3 Policy Statement

4.3.1 Commitment to Security

Dr. D. Y. Patil Vidyapeeth, Pune is committed to protecting the privacy and security of student data in accordance with the Digital Personal Data Protection Act, 2023 (DPDPA) and all other applicable laws and regulations. We recognize the importance of safeguarding student personal information and are dedicated to ensuring that all staff, faculty, and stakeholders adhere to the policies and procedures outlined in this document.

4.3.2 Roles and Responsibilities

All staff, faculty, contractors, and third-party vendors who have access to student records are responsible for ensuring the security of this information. Specific roles and responsibilities related to student record security are outlined in departmental policies and procedures and may include:

- Designating data custodians responsible for the collection, storage, and maintenance of student records.
- Appointing data stewards responsible for overseeing compliance with data security policies, and procedures.
- Providing training and awareness programs to staff and faculty on data security best practices, student rights, and their obligations regarding lawful data processing.

4.3.3 Compliance

Compliance with this policy and the principles of the DPDPA is mandatory for all individuals and entities associated with Dr. D. Y. Patil Vidyapeeth, Pune. Failure to comply with this policy or the Act may result in disciplinary action, including but not limited to reprimands, suspension, termination of employment, or legal consequences, depending on the severity of the violation.

4.4 Access Control

4.4.1 Authentication and Authorization

Access to student records is restricted to authorized personnel with a legitimate need to know, based on their role and responsibilities within the institution. Authentication mechanisms, such as unique usernames and strong passwords, are used to verify the identity of users accessing student records. Role-based access control (RBAC) is employed to limit access to student information according to job function and level of authority.

4.4.2 Access Privileges

Access privileges are granted based on the principle of least privilege, with individuals only given access to the minimum amount of information necessary to perform their duties. Access to sensitive student information, such as financial aid records or disciplinary records, is restricted to authorized personnel designated by the data custodian or data steward.

4.4.3 Monitoring and Audit Trails

Monitoring mechanisms are implemented to track access to student records and detect any unauthorized or suspicious activity. Audit trails are maintained to record access attempts,

modifications, or deletions of student information. Regular audits are conducted to assess compliance with access control policies and procedures and to identify any vulnerabilities or weaknesses in the system. This information is used for security purposes and may also be required for compliance with the DPDPA's audit trail requirements.

4.4.4 Data Access Requests

Procedures are established for handling requests for access to student records from authorized individuals within the institution. This may involve a formal request process and verification of the requester's identity and legitimate need for access.

4.5 Data Collection and Storage

4.5.1 Lawful Basis for Data Collection

Dr. D. Y. Patil Vidyapeeth, Pune collects student data only for legitimate educational and administrative purposes. We will collect the minimum amount of personal data necessary for these purposes and will always strive to obtain consent from students before processing their data unless a lawful basis for processing exists without consent.

Examples of lawful bases for processing student data may include:

- Consent from the student.
- Contractual necessity (e.g., processing data to fulfill enrollment requirements)
- Legal obligation (e.g., reporting certain data to government agencies)

Students will be informed about the purposes for which their data is being collected, the lawful basis for processing, and how long the data will be retained.

4.5.2 Secure Storage

Student records are stored in a secure manner to prevent unauthorized access, disclosure, or use. Physical records are stored in locked cabinets or rooms accessible only to authorized personnel. Electronic records are stored on secure servers with access controls, encryption, and regular backups to prevent data loss or unauthorized access.

4.5.3 Encryption and Data Masking

Sensitive student information, such as personally identifiable information (PII) or financial data is encrypted both in transit and at rest to protect it from unauthorized access or interception. Data masking techniques may be employed to obfuscate certain elements of student records, such as Aadhar card, to further enhance security.

4.5.4 Data Minimization

The principle of data minimization is followed, ensuring that only the minimum amount of student information necessary for academic and administrative purposes is collected and stored. Unnecessary or redundant data is not retained to reduce the risk of exposure in the event of a security breach.

4.5.5 Data Classification

Student records are classified based on their sensitivity and importance, with different levels of security measures applied accordingly. For example, highly sensitive personal data such as health records, financial aid applications, or biometric information may be subject to stricter access controls, encryption protocols, and anonymization techniques where possible.

4.5.6 Data Retention

Student records are retained only for as long as necessary to fulfill their intended purpose and in compliance with legal and regulatory requirements, including retention periods. Retention periods for different types of student records are determined based on the nature of the information and its significance to the academic or administrative functions of the institution.

4.6 Data Handling and Transmission

4.6.1 Secure Handling

Procedures are in place to ensure that student records are handled securely at all times. Authorized personnel are trained on proper data handling procedures, including the use of secure communication channels, encryption methods, and physical security measures. Records are protected from loss, theft, or unauthorized access during transportation or handling.

4.6.2 Secure Transmission

Student records are transmitted securely both internally and externally to prevent interception or unauthorized access. Secure communication channels, such as encrypted email or virtual private networks (VPNs), are used to transmit sensitive information. Data encryption protocols are employed to protect student records during transmission over unsecured networks.

4.6.3 Data Sharing

Procedures for sharing student data internally and externally are governed by data sharing agreements and protocols established by Dr. D. Y. Patil Vidyapeeth, Pune. These agreements will be drafted with the requirements of the DPDPA in mind, ensuring:

- **Lawful Basis for Sharing:** Data is only shared with authorized individuals or entities who have a legitimate need to know and a lawful basis for processing the data under the Act. This may involve obtaining consent from students or relying on another permitted basis for processing.
- **Data Minimization:** Only the minimum amount of student data necessary for the specific purpose of sharing is disclosed.
- **Security Measures:** Data sharing agreements will specify the security measures that the receiving party must implement to protect the confidentiality and integrity of the student data.

4.6.4 Student Rights Regarding Data Sharing

Students will be informed about how their data is shared and will have the right to object to such sharing in certain circumstances. The policy will explain the process for students to exercise these rights.

4.7 Data Retention and Disposal

4.7.1 Retention Periods

Dr. D. Y. Patil Vidyapeeth, Pune will retain student records only for as long as necessary to fulfill their intended purpose and in accordance with legal and regulatory requirements.

Here's how we will determine retention periods:

- **Academic Records:** Academic transcripts, course registration information, and other academic achievement data will be retained for a minimum period as required by accreditation agencies or government regulations. The institution may choose to retain this data for longer periods for historical or research purposes, but anonymization techniques will be applied where feasible to minimize the use of personal data.
- **Enrollment Information:** Basic enrollment information such as name, contact details, and program details may be retained for longer periods for administrative or alumni relations purposes. However, we will strive to minimize the amount of personal data retained and ensure it is only used for these specific purposes.
- **Financial Aid Records:** Financial aid such as fee waiver or DPU Merit scholarship records containing sensitive financial data will be retained in accordance with relevant financial regulations.
- **Disciplinary Records:** Disciplinary records will be retained for a specific period as determined by the severity of the offense and institutional policies. After the retention period expires, these records will be securely disposed of in accordance with the procedures outlined below.

4.7.2 Secure Disposal of Student Data

At the end of their retention period, student records will be disposed of securely in a manner that prevents unauthorized access, reconstruction, or use. The specific disposal methods will depend on the format of the data:

- **Electronic Records:** Electronic records will be permanently deleted from storage devices using data sanitization techniques that overwrite the data with random characters.

4.7.3 Record of Destruction

A record of destruction is maintained for all student records that are disposed of, including the date of disposal, method of destruction, and the individual responsible for overseeing the process. This record serves as evidence of compliance with data retention and disposal policies and may be subject to audit or review.

4.8 Monitoring and Auditing

4.8.1 Monitoring Mechanisms

Dr. D. Y. Patil Vidyapeeth, Pune implements monitoring mechanisms to detect and prevent unauthorized access to student data. This includes logging access attempts, monitoring data activity, and using intrusion detection systems.

4.8.2 Regular Audits

Regular audits are conducted to assess compliance with the Student Record Security Policy, data security best practices. These audits may be internal, conducted by designated IT security personnel or internal audit teams. Audits may focus on various aspects, including:

- Access controls and user permissions
- Data security practices
- Incident response procedures
- Data retention and disposal practices

4.8.3 Incident Response

Procedures are in place for responding to security incidents or breaches involving student records. An incident response team is designated to assess the severity of the incident, contain the breach, mitigate any damage, and notify affected individuals or authorities as required by law. Lessons learned from security incidents are used to improve security practices and prevent future breaches.

4.9 Training and Awareness

Dr. D. Y. Patil Vidyapeeth, Pune recognizes the importance of staff and faculty awareness regarding data protection and their obligations in handling student records securely. We are committed to providing training and awareness programs to ensure everyone understands their roles and responsibilities in complying with this policy.

4.9.1 Staff Training

Training programs are provided to staff and faculty on data security best practices and procedures, including the importance of safeguarding student information and the consequences of non-compliance. Training sessions may cover topics such as data handling, access control, encryption, and incident response.

4.9.2 Student Awareness

Awareness campaigns are conducted to educate students about their rights and responsibilities regarding their own records and to promote a culture of security awareness within the institution. Students are informed about the importance of protecting their personal information and are provided with guidance on how to safeguard their records from unauthorized access or disclosure.

4.9.3 Phishing Awareness

Training programs include awareness about phishing attacks and social engineering tactics used by cybercriminals to trick users into revealing sensitive information or credentials. Staff and faculty are educated on how to recognize and report phishing attempts to prevent unauthorized access to student records.

4.10 Compliance and Enforcement

4.10.1 Compliance Requirements

Dr. D. Y. Patil Vidyapeeth, Pune will maintain a comprehensive data protection compliance program that includes:

- Regularly reviewing and updating policies and procedures to reflect any changes.
- Conducting internal audits to assess compliance and identify areas for improvement.
- Implementing appropriate technical and organizational safeguards to protect student data.
- Providing ongoing training and awareness programs to staff and faculty.
- Maintaining accurate records of data processing activities.

5 Digital and Blended Learning Document

5.1 Introduction

Dr. D. Y. Patil Vidyapeeth, Pune, recognizes the transformative potential of digital and blended learning in enhancing educational outcomes and fostering student success. As we embark on this journey, it's imperative to acknowledge the rapid evolution of technology and its profound impact on the educational landscape. This document serves as a comprehensive guide to our institution's Digital and Blended Learning Policy, outlining our strategies, principles, and goals for leveraging technology to create engaging, accessible, and effective learning experiences for all students.

5.2 Objective

The Digital and Blended Learning Policy at Dr. D. Y. Patil Vidyapeeth, Pune, has a multi-pronged objective. It aims to leverage technology to create engaging learning experiences, seamlessly integrate technology into teaching, and promote data-driven decision making to improve the digital learning ecosystem. Quality assurance is ensured through regular review and assessment.

5.3 Vision

Dr. D. Y. Patil Vidyapeeth, Pune aspires to be a leader in harnessing the transformative potential of digital and blended learning. The vision is to create a dynamic and engaging educational landscape that leverages technology to empower students and foster their success. This includes embracing innovative pedagogical approaches, seamless technology integration, and data-driven decision making to ensure students are well-equipped for the demands of the digital age.

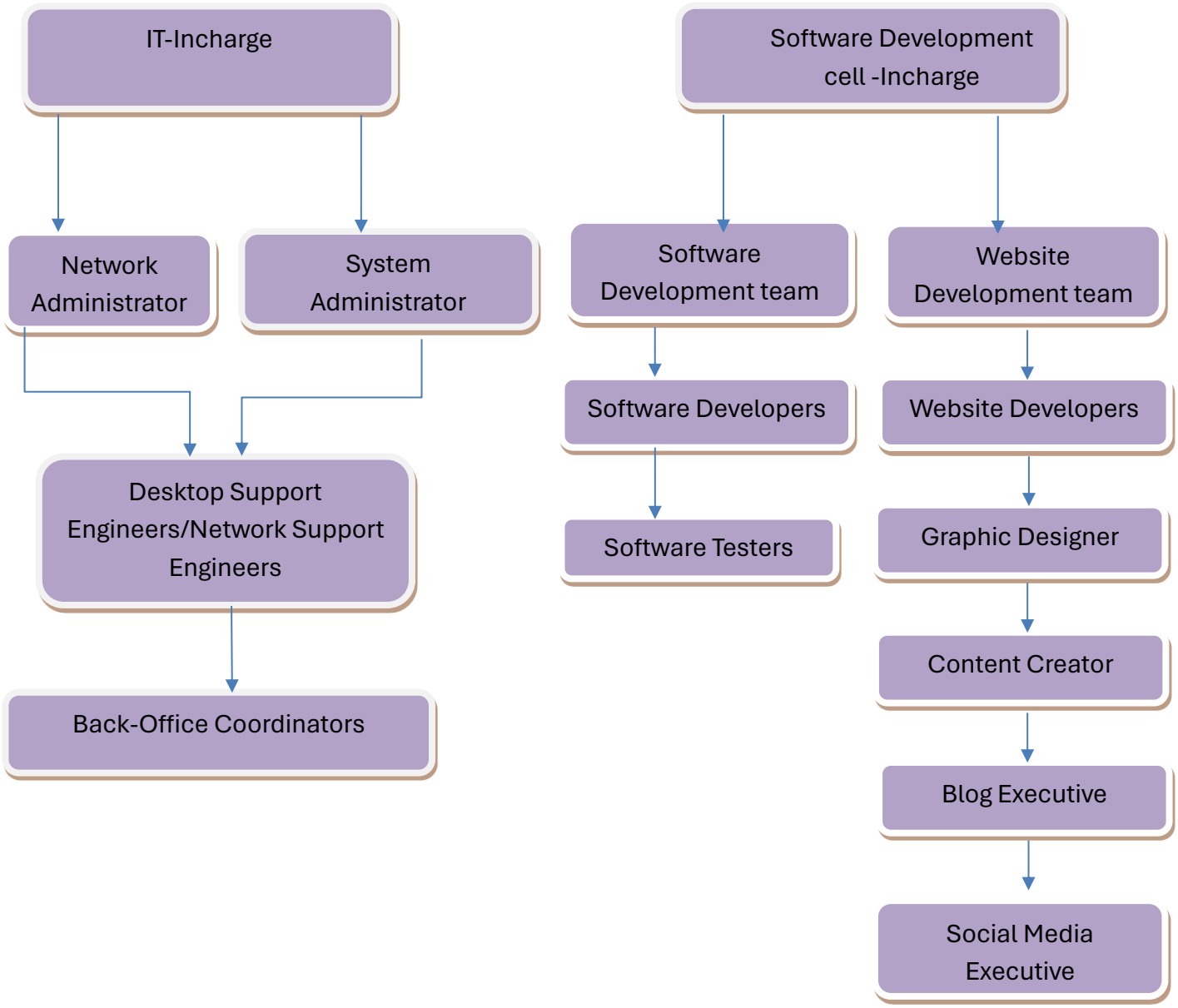
5.4 Mission

The mission of the digital and blended learning policy is to provide a comprehensive framework for the strategic implementation of technology in education. This framework prioritizes quality by establishing mechanisms for regular review, assessment, and data analysis. It fosters inclusivity by ensuring accessibility features and support services are available to all students. Through robust infrastructure, technical support, and collaboration with external partners, the mission is to create a sustainable and thriving digital learning ecosystem that empowers students to become lifelong learners and future leaders.

5.5 Organizational Context

Our institution's rich history and tradition of excellence provide a solid foundation for our digital and blended learning initiatives. With a legacy spanning decades and a reputation for academic excellence, Dr. D. Y. Patil Vidyapeeth, Pune, is well-positioned to lead the charge in embracing digital transformation in education. Our commitment to innovation and continuous improvement drives us to explore new frontiers in teaching and learning, guided by the principles of inclusivity, accessibility, and quality.

5.6 DPU Central IT Department Leadership Structure



5.6.1 Central IT Department

5.6.1.1 Central IT Incharge

The Head of Department (IT Incharge) is responsible for overseeing the administration and technical operations of the IT department within the university. They are entrusted with various duties and authorities to ensure the effective functioning of IT systems and services across the institution.

- The entire administration of the department.
- To Design and analysis and propose the IT systems (Hardware / Software) for various working in the University.
- To propose the budget for the purchase of IT equipment, consumables, upgradation work and other related work.
- To organize the meeting of TAC for suggestion/approval of new technologies and technical specification of IT related equipment.
- To convey the technical specification to purchase section for further purchase procedure.
- To supervise co-curricular and extracurricular activity within the department.
- To ensure that the allocated budget is properly utilized in the department.
- To supervise the smooth functioning of Computer, Printers, Scanners, Network services etc.
- To supervise the smooth functioning of internet facilities made available to various departments of DPU.
- To conduct departmental meetings from time to time.
- To monitor the achievement of Quality Objectives.
- Any other work assigned by Hon'ble Vice-Chancellor, Pro-Vice-Chancellor, and Registrar of the University from time to time.
- Work allocation to subordinate staff (Manpower management).
- To make recommendation of subordinate staff for knowledge up gradation.

5.6.1.2 Network Administrator

The Network Administrator is responsible for managing and maintaining the network infrastructure of the organization, ensuring its smooth operation and optimal performance. Their duties encompass various aspects of network setup, configuration, monitoring, and planning.

- Installation & Maintenance of Various L3 & L2 Switches.
- Configuration of Firewall, Core switches with Virtual LAN.
- Monitoring & Maintain Internet speed.
- Designing & planning new network technologies with existing network.
- Assist with IT Incharge for Networking related purchasing and decisions.

5.6.1.3 System Administrator

The System Administrator plays a crucial role in maintaining the stability, security, and efficiency of the organization's IT infrastructure. They are tasked with various responsibilities related to server management, troubleshooting, and technological innovation.

- To assist IT Incharge to full utilization of IT resources.

- Installation & Maintenance of All the servers,
- Periodically checking the logs of Servers such as Webserver, Antivirus server, Squid server, etc.
- Guide the Helpdesk Engineers regarding IT related issues.
- Periodically checking Data Backups schedule, it for Critical Systems.
- Finding the new technologies and implement in the existing IT Infrastructure.

5.6.1.4 Helpdesk Engineers

Helpdesk Engineers play a vital role in providing technical support and assistance to end-users within the organization. Their responsibilities encompass a range of tasks related to hardware maintenance, technical support, and facilitating communication services.

- Installation and maintenance of Computer, Printer & its related hardware and computer network.
- To carry out various work assigned by HOD.
- To help to start the Video Conferencing services.
- Provide Helpdesk Support to end users.

5.6.1.5 UPS Engineer

UPS Engineers are responsible for ensuring the reliable operation and maintenance of uninterruptible power supply (UPS) systems within the organization. Their duties involve installation, maintenance, troubleshooting, and documentation related to UPS equipment.

- Installation and preventive maintenance of UPS.
- Load study of the ups for the new requirement and calculate how much kva ups is required.
- Maintain Service Reports of installation and repairing of ups and arrange engineer for AMC/CMC and repairing.
- Repairing and troubleshooting of UPS.

5.6.2 Software Development Cell

5.6.2.1 Software Development Cell Incharge

The Software Development Cell Incharge serves as the primary leader and coordinator of the Software Development Cell. He is responsible for providing strategic direction, overseeing operations, and ensuring the successful implementation of digital and blended learning initiatives.

- Develop and implement the digital and blended learning strategy in alignment with institutional goals and objectives.
- Lead and mentor the members of the Software Development Cell, fostering a culture of innovation, collaboration, and continuous improvement.
- Liaise with key stakeholders, including faculty, staff, students, and administrators, to gather input, address concerns, and ensure alignment with organizational priorities.
- Monitor and evaluate the effectiveness of digital learning initiatives, gathering feedback and data to inform decision-making and drive improvement efforts.

- Collaborate with internal and external partners to leverage resources, expertise, and opportunities for enhancing digital and blended learning experiences.
- Stay abreast of emerging trends, technologies, and best practices in digital education, advocating for innovation and advancement within the institution.

5.6.2.2 Software Developers

Software Developers are responsible for designing, developing, and maintaining digital platforms, tools, and resources to support teaching and learning activities.

- Design and develop user-friendly and scalable software solutions, including learning management systems (LMS), educational apps, and digital learning resources.
- Collaborate with faculty, instructional designers, and other stakeholders to gather requirements and specifications for digital learning projects.
- Implement coding best practices and quality assurance measures to ensure the functionality, usability, and security of digital applications and platforms.
- Conduct regular maintenance and updates to address bugs, glitches, and performance issues, ensuring the smooth operation of digital learning tools and resources.
- Provide technical support and troubleshooting assistance to faculty, staff, and students, resolving issues, and optimizing user experiences.
- Stay current with programming languages, frameworks, and development methodologies, continuously enhancing skills and knowledge in software development.

5.6.2.3 Software Tester

The Software Tester ensures the quality and functionality of digital applications and platforms through rigorous testing and evaluation.

- Develop and execute test plans, test cases, and test scripts to verify the functionality, performance, and reliability of digital learning applications and platforms.
- Identify and document defects, bugs, and issues, working closely with software developers to troubleshoot and resolve issues in a timely manner.
- Conduct regression testing to ensure that fixes and updates do not adversely affect existing functionality or introduce new issues.
- Collaborate with stakeholders to gather feedback and user insights, incorporating user feedback into testing processes and product improvements.
- Participate in quality assurance reviews and audits, ensuring compliance with established standards and guidelines for software development and testing.
- Stay informed about industry trends, best practices, and emerging technologies in software testing, continuously improving skills and techniques.

5.6.2.4 Website Designers

Website Designers are responsible for creating and maintaining an intuitive and user-friendly interface for the institution's website.

- Design visually appealing and responsive website layouts, incorporating best practices in user experience (UX) and user interface (UI) design.

- Collaborate with stakeholders to gather requirements and specifications for website design projects, ensuring alignment with institutional branding and goals.
- Develop wireframes, mock-ups, and prototypes to visualize website designs and gather feedback from stakeholders.
- Implement website designs using HTML, CSS, JavaScript, and other relevant technologies, ensuring compatibility across devices and browsers.
- Conduct usability testing and user research to identify opportunities for improvement and optimize the user experience.
- Monitor website performance and analytics, identifying trends and opportunities for enhancement, and making recommendations for optimization and improvement.

5.6.2.5 Graphic Designer

Graphic Designers create visually compelling educational materials, presentations, and promotional materials to enhance the learning experience.

- Design engaging and informative graphics, illustrations, and visual assets for educational materials, presentations, and digital learning resources.
- Collaborate with faculty and instructional designers to create visually appealing and pedagogically effective learning materials, ensuring alignment with learning objectives and instructional goals.
- Develop branding guidelines and templates for consistent visual identity across digital learning platforms, courses, and materials.
- Utilize graphic design software and tools to create and manipulate images, layouts, and typography, optimizing visual communication and readability.
- Incorporate principles of accessibility and inclusivity into graphic design projects, ensuring that visual content is accessible to all learners, including those with disabilities.
- Stay informed about graphic design trends, techniques, and best practices, continuously improving skills and knowledge in visual communication and design.

5.6.2.6 Content Creator

Content Creators develop engaging and informative educational content for digital platforms, including videos, articles, and interactive modules.

- Develop educational content for digital platforms, including written articles, video lectures, interactive quizzes, and multimedia presentations.
- Collaborate with subject matter experts, faculty, and instructional designers to research, plan, and develop content that aligns with learning objectives and instructional goals.
- Create scripts, storyboards, and outlines for multimedia content, ensuring accuracy, clarity, and engagement.
- Produce high-quality multimedia content using video editing software, animation tools, and other multimedia production technologies.
- Optimize content for search engines and accessibility, incorporating keywords, metadata, and alternative text to enhance discoverability and usability.

- Monitor content performance and user engagement metrics, gathering feedback and insights to inform content strategy and development priorities.

5.6.2.7 Blog Executive

Blog Executive manage and update the institution's blog with relevant articles, news, and insights related to digital learning and education.

- Develop a content strategy and editorial calendar for the institution's blog, identifying topics, themes, and target audiences.
- Research and write engaging and informative blog posts, articles, and news updates related to digital learning, educational technology, and institutional initiatives.
- Collaborate with content creators, faculty, and subject matter experts to gather input, insights, and contributions for blog content.
- Edit and proofread blog posts for clarity, accuracy, and adherence to editorial standards and style guidelines.
- Publish blog posts on the institution's website and promote them through social media channels, email newsletters, and other distribution channels.
- Monitor blog performance metrics, including traffic, engagement, and conversions, and use data insights to optimize content strategy and improve blog effectiveness.

5.6.2.8 Social Media Executive

Social Media Executives manage the institution's social media channels to promote digital learning initiatives, engage with stakeholders, and disseminate information.

- Develop and implement a social media strategy and content calendar for the institution's social media channels, including Facebook, Twitter, LinkedIn, Instagram, and YouTube.
- Create engaging and informative social media posts, graphics, and videos to promote digital learning initiatives, share educational content, and showcase institutional achievements.
- Monitor social media channels for mentions, comments, and messages, responding promptly and professionally to inquiries and engaging with followers.
- Collaborate with other departments and stakeholders to gather content and insights for social media posts and campaigns.
- Analyze social media performance metrics, including reach, engagement, and conversion rates, and use data insights to optimize content strategy and improve social media effectiveness.
- Stay informed about social media trends, algorithms, and best practices, continuously adapting strategies, and tactics to maximize impact and reach.

5.7 Digital and Blended Learning Strategy

In alignment with national and international best practices, our digital and blended learning strategy prioritizes the following areas:

- **Pedagogical Innovation:** We embrace pedagogical approaches that leverage technology to enhance student engagement, critical thinking, and collaboration. Blended learning models,

flipped classrooms, and project-based learning experiences are integrated into our curriculum to promote active learning and student-centered instruction.

- **Technology Integration:** Our strategy emphasizes the seamless integration of technology into teaching and learning processes. From learning management systems (LMS) to virtual reality (VR) simulations, we leverage a wide range of digital tools and platforms to create immersive and interactive learning experiences that transcend traditional boundaries.
- **Data-Driven Decision Making:** We harness the power of data analytics and learning analytics to inform decision-making and drive continuous improvement. By analyzing student performance data, engagement metrics, and feedback, we gain valuable insights into the effectiveness of our digital learning initiatives and identify areas for enhancement.

5.8 Educational Quality Assurance

Ensuring the quality of our digital and blended learning experiences is a top priority. We employ a variety of mechanisms to assess, monitor, and improve the quality of our digital learning initiatives, including:

- **Regular Review and Evaluation:** We conduct regular reviews and evaluations of our digital learning materials and platforms to ensure alignment with learning objectives, standards, and best practices. Feedback from students, faculty, and stakeholders is solicited and used to inform ongoing improvement efforts.
- **Assessment and Feedback:** We utilize a variety of assessment and feedback mechanisms to gather input from students and faculty on the effectiveness of our digital learning initiatives. Surveys, focus groups, and interviews are conducted to gather insights into student engagement, satisfaction, and learning outcomes.
- **Monitoring and Analysis:** We monitor student performance data to identify trends, patterns, and areas for improvement. Analytics tools are used to track student progress, participation, and achievement, allowing us to make data-driven decisions to enhance the quality of our digital learning experiences.

5.9 Support and Infrastructure

Providing robust support and infrastructure is essential to the success of our digital and blended learning initiatives. We invest in the following areas to ensure that faculty, staff, and students have the resources they need to thrive in our digital learning environment:

- **Technical Support Services:** We provide comprehensive technical support services to assist faculty, staff, and students with troubleshooting, problem-solving, and assistance with digital tools and platforms. Help desks, online resources, and training sessions are available to address technical issues and provide guidance on using digital resources effectively.
- **Accessibility Accommodations:** We are committed to promoting accessibility and inclusivity in our digital learning environment. Accessibility features such as closed captioning, screen readers, and alternative text are integrated into our digital platforms and resources to accommodate students with disabilities or special needs. Furthermore, we collaborate with campus accessibility services and disability support offices to provide personalized accommodations and support services to students as needed.

- **Infrastructure Investments:** We invest in infrastructure upgrades and maintenance to ensure the reliability, security, and scalability of our digital learning systems. This includes investments in hardware, software, networking, and cybersecurity measures to safeguard sensitive data and ensure uninterrupted access to digital resources and platforms.

5.10 Collaboration and Partnerships

Our institution actively engages with industry partners, educational organizations, government agencies, and non-profit entities to advance our digital and blended learning agenda. Through strategic partnerships and collaborative initiatives, we leverage collective expertise, resources, and networks to drive innovation, share best practices, and address common challenges in digital education. Joint research projects, technology transfer agreements, and knowledge exchange programs are examples of the collaborative opportunities pursued to enhance our digital learning ecosystem.

5.11 Policy Compliance and Review

In accordance with Indian laws and regulations, we place paramount importance on data privacy and security. Our institution adheres strictly to data protection protocols and industry best practices to safeguard sensitive information. We ensure compliance with relevant data privacy regulations, including the Personal Data Protection Bill, which is India's comprehensive legislation aimed at protecting personal data and upholding individuals' privacy rights.

Regular audits, assessments, and compliance checks are conducted to evaluate our adherence to data privacy and security standards. These measures help us identify any areas for improvement and ensure that our data handling practices remain in line with legal requirements and ethical principles.

As we navigate the complexities of the digital age, our commitment to excellence, innovation, and student success remains unwavering. By embracing digital and blended learning, we position ourselves at the forefront of educational innovation, poised to meet the evolving needs of our students and society. With a steadfast dedication to quality, accessibility, and inclusivity, we are confident that our digital learning initiatives will empower learners to thrive in an increasingly digital world.

6 IT Security Policy

6.1 Introduction and Purpose

This security policy is established to ensure the confidentiality, integrity, and availability of data and resources within Dr. D Y Patil Vidyapeeth Pune. The policy aims to outline the necessary measures and procedures to safeguard the organization's assets and interests.

6.2 Summary of Main Security Policies

6.2.1 Confidentiality of Data

- Maintain confidentiality through discretionary and mandatory access controls. Access controls should meet security functionality standards.
- Restrict internet and external service access to authorized personnel only to prevent unauthorized access to sensitive data.
- Secure data on laptop computers through encryption or other means to maintain confidentiality in case of loss or theft.
- Prohibit unauthorized software installation and usage to prevent security vulnerabilities.
- Implement data transfer restrictions as per the organization's data-protection policy to ensure data confidentiality is maintained during transmission.

6.2.2 Virus Protection

- Utilize up-to-date virus scanning software for scanning and removal of suspected viruses to prevent malware infections.
- Protect corporate fileservers and workstations with virus scanning software to detect and eliminate viruses.
- Regularly update anti-virus software with the latest patches to ensure protection against new threats.
- Scan all removable media for viruses before use to prevent malware spread within the organization.
- Conduct regular backups to enable data recovery in the event of a virus outbreak and minimize data loss.

6.2.3 Access Control

- Grant users' sufficient rights only for their job function, following the principle of least privilege, to minimize the risk of unauthorized access.
- Users must apply for access to systems through written applications provided by the IT Department to ensure proper authorization.
- Implement individual username and password access, with passwords meeting specified criteria, to prevent unauthorized access.
- Enforce password expiration and uniqueness policies, with intruder detection and account lockout mechanisms, to enhance password security.
- Maintain audit logs for login attempts, failures, and changes made to systems to track and investigate security incidents.

6.2.4 LAN Security

- Keep LAN equipment in secure hub rooms with restricted access to prevent unauthorized tampering.
- Ensure users logout or lock their workstations when not in use to prevent unauthorized access to network resources.
- Document and periodically scan network wiring to identify and address any vulnerabilities.
- Implement monitoring software and restrict the use of LAN analyzers and packet sniffing software to authorized personnel only to prevent unauthorized network monitoring.

6.2.5 Electrical Security

- Equip servers and critical network equipment with UPS's to ensure uninterrupted power supply and protect against power surges.
- Install software for orderly shutdown during total power failure to prevent data loss and system damage.
- Test UPS's periodically to ensure functionality and readiness for emergency situations.

6.2.6 Inventory Management

- Maintain a full inventory of computer equipment and software to track assets and identify any unauthorized devices or software.
- Conduct periodic hardware and software audits to track unauthorized copies and changes and ensure compliance with licensing agreements.

6.2.7 Server Specific Security

- Keep server operating systems patched and up to date to address known security vulnerabilities.
- Perform daily virus checks on servers to detect and remove any malware infections.
- Secure servers in locked rooms and restrict access to authorized personnel only to prevent unauthorized access to sensitive data.
- Limit users possessing Admin/root rights to trained IT staff to minimize the risk of unauthorized system changes.
- Enable intruder detection, system auditing, and user logout policies to enhance server security and detect unauthorized access attempts.

6.2.8 Email Policy

- Ensure proper use of the email system in a responsible, effective, and lawful manner to prevent data breaches and legal issues.
- Notify users of legal risks associated with email communication, including defamation, copyright infringement, and dissemination of confidential information.
- Strictly adhere to legal requirements and best practices outlined in the policy to ensure compliance with relevant laws and regulations.
- Maintain professional email etiquette and timely responses to improve communication efficiency and professionalism.

- Allow reasonable personal use of email with adherence to guidelines to balance productivity and security.

Conclusion: Dr. D Y Patil Vidyapeeth Pune is committed to upholding the highest standards of security to protect its data, systems, and stakeholders. This policy serves as a guideline for all employees and stakeholders and will be regularly reviewed and updated to adapt to evolving security threats and best practices.

7 Tech Governance Policy

7.1 Introduction

Dr. D.Y. Patil Vidyapeeth recognizes the critical role technology plays in delivering high-quality education, facilitating research, and managing administrative operations. The Tech Governance Policy outlines the framework for overseeing and managing technology within the university, ensuring alignment with the institution's mission, compliance with regulatory requirements, and effective risk management.

7.2 Scope

This policy applies to all technology-related activities within Dr. D.Y. Patil Vidyapeeth, including IT infrastructure, software systems, data management, cybersecurity, procurement, and technology services. It encompasses all university stakeholders, including faculty, staff, students, contractors, and third-party vendors.

7.3 Objectives

- Establish a clear structure for technology governance, including roles and responsibilities.
- Ensure that technology decisions align with the university's strategic goals and values.
- Promote best practices for technology management, data security, and compliance.
- Encourage innovation and adaptability in the use of technology.
- Foster effective communication and collaboration among stakeholders.

7.4 Governance Structure

The university's technology governance structure includes the following components:

7.4.1 Technology Governance Committee (TGC):

- The TGC is responsible for overseeing technology governance at the university level.
- It comprises representatives from academic and administrative departments, IT leadership, risk management, compliance, and other relevant stakeholders.
- The TGC is responsible for setting technology policies, approving major technology projects, and providing strategic guidance.

7.4.2 Technology Operations Team (TOT):

- The TOT is responsible for implementing technology policies and managing day-to-day operations.
- It includes IT managers, system administrators, cybersecurity specialists, and other technical staff.
- The TOT reports to the TGC and ensures compliance with governance policies.

7.4.3 Technology User Groups:

- These groups consist of faculty, staff, and students who use technology for teaching, research, and administrative purposes.

- They provide feedback and recommendations to the TGC regarding technology needs and user experiences.

7.5 Policy Framework

The technology governance policy framework encompasses the following key areas:

7.5.1 Technology Strategy and Planning:

- The TGC develops a technology strategy that aligns with the university's overall strategic plan.
- Technology projects and initiatives are evaluated for their impact, benefits, and alignment with the university's mission.

7.5.2 Technology Procurement and Vendor Management:

- The TOT establishes procurement guidelines to ensure that technology acquisitions meet university standards.
- Vendor management practices are implemented to maintain accountability and compliance with contracts.

7.5.3 Data Management and Security:

- The university adopts data governance practices to ensure data accuracy, integrity, and security.
- Policies are established for data privacy, access controls, and data retention.
- The TOT implements cybersecurity measures to protect against unauthorized access, breaches, and other threats.

7.5.4 Compliance and Risk Management:

- The university ensures compliance with applicable laws, regulations, and industry standards related to technology.
- Risk management practices are implemented to identify and mitigate technology-related risks.

7.5.5 Innovation and Continuous Improvement:

- The university encourages innovation in technology use and supports pilot projects and research initiatives.
- Continuous improvement processes are established to evaluate technology effectiveness and identify opportunities for enhancement.

7.6 Communication and Training

The TGC ensures that technology policies are communicated to all stakeholders in a clear and accessible manner.

- Training programs are provided to faculty, staff, and students to ensure awareness of technology policies and best practices.

- Feedback mechanisms are established to collect input from stakeholders and incorporate it into policy updates.

7.7 Monitoring and Evaluation

- The TOT is responsible for monitoring compliance with technology policies and conducting regular audits to ensure adherence to governance standards.
- The TGC evaluates the effectiveness of technology governance through metrics and performance indicators.
- The policy is reviewed periodically to ensure it remains current and aligned with the university's strategic goals.

8 Learning Systems Roadmap

8.1 Introduction

Dr. D.Y. Patil Vidyapeeth is committed to delivering high-quality education and fostering an environment that encourages continuous learning and innovation. This Learning Systems Roadmap outlines the strategic plan for implementing and enhancing technology-driven learning systems at the university. It includes the development, integration, and maintenance of learning technologies to support the university's educational objectives.

8.2 Vision and Objectives

8.2.1 Vision

To create a learning environment that is flexible, accessible, and adaptive, empowering students and faculty with advanced technology tools.

8.2.2 Objectives:

- Enhance the quality of teaching and learning through technology.
- Provide flexible and personalized learning experiences for students.
- Facilitate collaboration and knowledge sharing among faculty and students.
- Ensure the security and privacy of learning-related data.
- Foster a culture of continuous learning and professional development.

8.3 The Roadmap

The roadmap includes the following key initiatives to achieve the outlined objectives:

8.3.1 Phase 1 (Year 1):

During the initial stage of the project, a detailed comparative analysis was conducted to determine the most effective strategy for addressing the software needs of the organization. This study aimed to evaluate whether it would be more advantageous to establish and train an internal team to develop custom software or to source and acquire a ready-made software solution from the market. The analysis considered various factors such as cost, time, scalability, flexibility, and long-term maintenance requirements to identify the optimal approach for meeting the organization's software objectives.

Given that the university encompassed numerous institutes within its domain, it became clear that maintaining an in-house development team would yield greater benefits. This decision was based on several key factors:

- **Customization:** An internal team would have the flexibility to tailor software solutions to meet the unique needs of each institute, ensuring a more cohesive and integrated system.
- **Cost-Effectiveness:** Over time, the costs of developing and maintaining software in-house would likely be lower than purchasing and customizing third-party products.
- **Agility:** An in-house team could respond swiftly to changing requirements and priorities, providing a more agile and adaptive approach to software development.

- **Knowledge Retention:** By having a dedicated internal team, the university would retain valuable institutional knowledge, fostering innovation and continuity in software solutions.
- **Inter-Institute Collaboration:** With an in-house team, there would be enhanced opportunities for collaboration across different institutes, promoting a consistent technological infrastructure throughout the university.

Consequently, it was determined that building an internal development team was the most suitable path for fulfilling the university's software requirements and ensuring long-term sustainability.

A dedicated team was assembled, and the necessary infrastructure was established to begin developing the systems. This process involved several key steps:

- Team Recruitment
- Infrastructure Development
- Development Tools and Software
- Training and Onboarding
- Project Planning and Strategy

With these foundational elements in place, the team was ready to commence work on the software systems, aiming to create solutions that would meet the evolving needs of the university and its constituent institutes. A strategy was developed to prioritize the needs of different institutes and ensure a smooth rollout of new systems.

8.3.2 Phase 2 (Year 2-3):

The team conducted a comprehensive study of various learning systems available in the market, evaluating their features, functionality, and compatibility with the university's requirements. The goal was to identify key features that would best support the university's unique educational environment, with a focus on providing an effective blended learning experience. Here's how the process unfolded:

8.3.2.1 Market Research and Feature Shortlisting:

The team explored a range of learning systems, assessing each for its user interface, content delivery methods, integration capabilities, and support for blended learning.

Features like virtual classrooms, course management, assessment tools, collaboration platforms, and mobile accessibility were evaluated to understand what a comprehensive learning system should offer.

A list of the most valuable features was created to guide the in-house development process, ensuring the university's system would be competitive with leading market offerings.

8.3.2.2 Collaboration with Teaching Staff:

To ensure the system would meet the practical needs of educators, the team held several meetings with the teaching staff across various departments.

These sessions gathered input on current teaching methods, challenges in delivering content, and expectations for the new system.

Faculty members shared insights on specific functionalities they required, such as interactive content, flexible assessment options, and real-time feedback mechanisms.

8.3.2.3 Adoption of Blended Learning Approach:

As a medical university, classroom teaching is essential for hands-on training and practical skills development. However, the team recognized the benefits of integrating technology to enhance the learning experience.

A blended learning approach was proposed, combining traditional classroom instruction with online resources, virtual simulations, and interactive tools.

This approach allowed for greater flexibility, enabling students to access learning materials online while still participating in mandatory classroom sessions for clinical and practical training.

8.3.2.4 Customized System Development:

The team's goal was to develop a learning system that accommodated the unique requirements of a medical university, focusing on a blend of in-person and virtual learning experiences.

Features were designed to support various aspects of medical education, including anatomy simulations, virtual lab exercises, and collaborative case studies.

The system was intended to be scalable, allowing the university to add new modules and functionalities as needed to keep pace with evolving educational demands.

With this comprehensive groundwork, the university was poised to implement a learning system tailored to its specific context, enhancing the educational experience for both faculty and students. The collaborative approach ensured that the system would be well-received by those who would be using it daily, leading to greater adoption and success.

8.3.3 Phase 3 (Year 4-5):

The Learning Management System (LMS) was developed as an integral component of the larger Campus wide ERP system, designed to manage and streamline various academic and administrative processes across the university. In its initial phase, the LMS focused on core features that would support the day-to-day operations of the university, while also laying the foundation for further enhancements in the future.

8.3.3.1 Core Components of the Initial LMS

8.3.3.1.1 Timetables

- A centralized timetable management system was developed to allow faculty and students to access course schedules easily.
- This feature enabled real-time updates and notifications to ensure that all parties were informed of changes or adjustments to class timings.

8.3.3.1.2 Lecture Entry System:

- The lecture entry system was designed to allow faculty to upload lecture plans, materials, and other relevant information for their courses.
- This feature provided a digital platform for organizing course content and preparing for upcoming lectures.

8.3.3.1.3 Lecture Attendance System:

- A digital attendance system was implemented, allowing faculty to record student attendance electronically.
- The system included features like automated reports and analytics to track attendance trends and ensure compliance with university policies.

8.3.3.1.4 E-Resource and Learning Material Sharing:

- This component provided a platform for faculty to share e-resources, such as lecture notes, presentations, videos, and supplementary materials, with students.
- The system supported various file formats and offered features like searchability and categorization for easy access to learning materials.

8.3.3.2 Integration with DPU-ERP

The LMS was seamlessly integrated with the broader DPU-ERP system, allowing data to flow between different modules, such as the student information system, academic records, and administrative functions.

This integration facilitated comprehensive data management and ensured that all stakeholders had access to the information they needed.

8.3.4 Phase 4 (Year 6-7):

To keep pace with evolving technology and to meet the changing needs of the academic environment, the Learning Management System (LMS) within the DPU-ERP system underwent a significant upgrade. The upgrade introduced a variety of new features and improvements, with a strong emphasis on mobile accessibility and enhanced interaction between students, faculty, and mentors.

8.3.4.1 Mobile App Development

8.3.4.1.1 Mobile Compatibility:

- The LMS was developed to work as a mobile application, allowing students and faculty to access the system on smartphones and tablets.
- The mobile app provided a user-friendly interface, enabling quick navigation through different modules, such as timetables, learning materials, and assessments.

8.3.4.1.2 Cross-Platform Support:

- The app was designed to be cross-platform, ensuring compatibility with both iOS and Android devices.
- This approach facilitated broader adoption among students and faculty, who could now access the system from anywhere at any time.

8.3.4.2 Enhanced Academic Features

8.3.4.2.1 Internal Assessments:

- The system incorporated tools for creating and administering internal assessments, allowing teachers to evaluate student performance throughout the academic term.
- Teachers could set up various types of assessments, such as quizzes, tests, and exams, with automated scoring and analytics.

8.3.4.2.2 Quizzes and Assignments:

- The addition of quizzes and assignments provided a flexible method for teachers to gauge student understanding and track progress.
- These features supported multiple question formats, including multiple-choice, short answer, and essay, with customizable grading rubrics.

8.3.4.2.3 Assignment Submission:

- Students could submit assignments directly through the app, enabling teachers to review and grade them electronically.
- The system supported collaborative assignments, allowing group submissions and peer reviews.

8.3.4.3 Feedback and Interaction

8.3.4.3.1 Feedback Systems:

- The upgraded system included a robust feedback mechanism, allowing teachers to provide personalized feedback on assessments, quizzes, and assignments.
- Students could also submit feedback on courses and teaching methods, providing valuable insights for continuous improvement.

8.3.4.3.2 Mentor-Mentee Interactions:

- A dedicated section was developed for mentor-mentee interactions, facilitating regular communication between students and their academic mentors.
- Mentors could track the progress of their mentees, set goals, and offer guidance on academic and career-related matters.

8.3.4.4 User Experience and Customization

8.3.4.4.1 Intuitive User Interface:

- The mobile app's interface was designed to be intuitive and easy to navigate, with clear menus and icons for different functions.
- Customization options allowed users to personalize their dashboards, setting preferences for notifications and updates.

8.3.4.5 Integration and Security

8.3.4.5.1 Seamless Integration:

- The mobile app remained integrated with the larger DPU-ERP system, allowing data to sync across different modules in real time.
- This integration ensured continuity of information and avoided data silos.

8.3.4.5.2 Data Security:

- Enhanced security measures were implemented to protect sensitive data, including encryption for data transmission and secure authentication for user access.
- Regular security audits and vulnerability assessments ensured that the system remained secure against emerging threats.

With these upgrades, the LMS provided a comprehensive platform for the university's academic operations, supporting both traditional and blended learning approaches. The new features and enhancements enabled teachers to assess student performance more effectively, while the feedback and mentor-mentee interactions promoted a collaborative and supportive learning environment. The mobile app format allowed for greater flexibility and convenience, aligning with the needs of a modern educational institution.

8.3.5 Phase 5: Future Plans

Looking ahead, the Learning Management System (LMS) at Dr. D.Y. Patil Vidyapeeth is poised for further enhancements, aiming to create an even more robust and versatile platform for both educators and students. Here's a roadmap outlining key features and improvements planned for the future:

8.3.5.1 Advanced Analytics and Reporting

8.3.5.1.1 Learning Analytics:

- The LMS will integrate advanced learning analytics to provide deeper insights into student performance, engagement, and learning outcomes.
- Teachers and administrators will be able to track student progress in real-time, identify at-risk students, and customize learning paths based on individual needs.

8.3.5.1.2 Comprehensive Reporting:

- The system will support comprehensive reporting, allowing faculty and administrators to generate custom reports for academic analysis, accreditation, and compliance.
- Data visualization tools will be incorporated to make it easier to interpret and present complex data.

8.3.5.2 Enhanced Collaboration and Communication

8.3.5.2.1 Social Learning Features:

- Social learning features, such as discussion boards, collaborative projects, and peer-to-peer interaction, will be added to foster a sense of community among students.
- These features will encourage knowledge sharing and collaborative problem-solving.

8.3.5.2.2 Advanced Communication Tools:

- The LMS will include enhanced communication tools, such as integrated video conferencing and instant messaging, allowing teachers to interact with students remotely.
- These tools will support virtual office hours, group discussions, and team projects.

8.3.5.3 Adaptive Learning and Personalization

8.3.5.3.1 Adaptive Learning Paths:

- The system will implement adaptive learning technology to create personalized learning paths based on individual student performance and preferences.
- This will enable students to progress at their own pace and focus on areas where they need additional support.

8.3.5.3.2 Intelligent Tutoring Systems:

- Intelligent tutoring systems, powered by AI, will be developed to offer automated assistance and feedback to students as they work through course materials and assessments.
- This will enhance student engagement and provide instant support when needed.

8.3.5.4 Integration with Emerging Technologies

8.3.5.4.1 Virtual Reality (VR) and Augmented Reality (AR):

- The LMS will incorporate VR and AR technologies to create immersive learning experiences, particularly for medical simulations and practical training.
- These technologies will offer a hands-on approach to learning, enhancing understanding and retention of complex concepts.

8.3.5.4.2 Artificial Intelligence (AI) and Machine Learning (ML):

- AI and ML will be used to automate administrative tasks, streamline grading, and provide predictive analytics for student performance.
- These technologies will also support intelligent content recommendations, guiding students to relevant resources based on their interests and learning history.

8.3.5.5 Expanded Resource Library

8.3.5.5.1 Comprehensive E-Resource Library:

- The LMS will develop an expanded e-resource library, offering a wide range of digital learning materials, including e-books, research papers, videos, and interactive content.
- The resource library will be searchable and categorized for easy access by students and faculty.

8.3.5.5.2 Open Educational Resources (OER):

- The system will integrate Open Educational Resources, allowing the university to access high-quality, publicly available educational content.
- This will support cost-effective learning and encourage the sharing of knowledge across the academic community.

8.3.5.6 Enhanced Security and Compliance

8.3.5.6.1 Advanced Security Measures:

- The LMS will implement state-of-the-art security measures, including biometric authentication, multi-factor authentication, and encrypted data storage, to protect sensitive information.

- Regular security audits and compliance checks will ensure the system adheres to the latest data protection regulations.

8.3.5.6.2 Compliance with Educational Standards:

- The system will be designed to meet educational standards and accreditation requirements, facilitating smooth audits and regulatory reviews.
- Compliance features will include secure data retention, audit trails, and robust privacy controls.

With these planned enhancements, the future LMS at Dr. D.Y. Patil Vidyapeeth will offer a comprehensive, flexible, and innovative learning platform. It will cater to the needs of students and educators while incorporating the latest technological advancements to create a dynamic and engaging educational environment.

9 IT Infrastructure Roadmap

9.1 Introduction

In the dynamic landscape of Indian higher education, the effective utilization of technology is paramount to ensuring academic excellence and operational efficiency. Dr. D. Y. Patil Vidyapeeth, Pune, is dedicated to embracing digital transformation to meet the evolving needs of its stakeholders and maintain its position as a leading educational institution in India. This document presents the IT Infrastructure Roadmap designed to enhance the organization's digital capabilities and propel it towards achieving its strategic objectives.

9.2 Evolution of IT Infrastructure at Dr. D. Y. Patil Vidyapeeth, Pune:

9.2.1 Initial Phase (Foundation):

- In the early stages, the institution started with a modest IT infrastructure.
- Internet connectivity was provided through a 300Mbps line, catering to the needs of approximately 400 computers across the campus.
- Basic Wi-Fi devices were deployed to offer limited wireless connectivity to students and staff.

9.2.2 Expansion and Upgrades:

- Recognizing the growing demand for digital resources and services, the institution embarked on a journey of expansion and upgrades.
- Internet bandwidth was gradually increased as right now we are having 2000Mbps leased line from Tata Communications, with additional connections from reputable providers such as BSNL NKN line which is 1000Mbps.
- Wi-Fi infrastructure underwent significant enhancement, with the deployment of advanced wireless access points WIFI-6 from leading manufacturers such as Grand Stream, and Mojo.
- Storage capacity was augmented with the deployment of EMC Unity 210TB Storage, offering substantial storage capabilities to accommodate the increasing data requirements.

9.2.3 Investment in Human Resources and Software:

- To effectively manage the expanding IT infrastructure, the institution invested in human resources, establishing a central IT cell comprising 25 skilled professionals.
- In-house software development capabilities were developed to create customized solutions tailored to institutional requirements.
- Licensing agreements were established to ensure compliance and efficient management of software resources.

9.2.4 Hardware Upgrades and Network Expansion:

- The hardware infrastructure received significant upgrades, with the addition of high-end servers such as Dual Xeon processors with 4GHz, high frequency 128*2 ram & RAID redundant SSDs from reputable manufacturers such as Dell, Intel, and IBM.
- Likewise, we upgraded/procured 3000+ user Desktop to a Corei5 12th generation SSD based system from Dell & HP.

- Network architecture was redesigned to implement a structured 3-tier approach, enhancing scalability, performance, and security.
- Advanced network equipment, including Juniper SRX-1500 Firewall and QFX-5100 series switches, was deployed to bolster network security and efficiency.

9.3 Future Roadmap:

Inter-Building Communication at 10000 Mbps on the campus: The institution will upgrade inter-building communication links to 10000 Mbps, ensuring high-speed data transfer between campus buildings. High-speed inter-building communication will enhance productivity and collaboration among faculty, staff, and students, enabling them to access resources and collaborate effectively across campus locations.

9.3.1 Ring-Shaped Network Connectivity:

Dr. D. Y. Patil Vidyapeeth, Pune, will implement a ring-shaped network topology connecting every campus within its network. The ring-shaped network will facilitate seamless communication and data exchange between campuses, fostering collaboration and efficiency across the institution.

9.3.2 Innovative Healthcare Solutions:

9.3.2.1 App-Based Appointments:

- Dr. D. Y. Patil Vidyapeeth, Pune, has introduced app-based appointment scheduling for its Hospital, Medical, Dental, and Ayurveda institutions.
- Patients can conveniently schedule appointments using a dedicated mobile application, reducing wait times, and improving patient satisfaction.

9.3.2.2 Electronic Patient Records:

- The institution has implemented a comprehensive electronic health record (EHR) system to digitize and manage patient medical records across its healthcare facilities.
- Patient health information, including medical history, diagnostic reports, treatment plans, and medications, is securely stored in a centralized database for easy access and retrieval.
- Future initiatives may include the adoption of emerging technologies, such as cloud data synchronization and artificial intelligence, to drive greater efficiency and innovation across the campus.

9.3.2.3 5G Lab's setup in Institutions. (Ministry of Telecommunications of India Initiative)

- To build competencies and engagement in 5G technologies in students and academic fraternity.
- To enable projects at under-graduation and post-graduation level for students using 5G environment.
- To Encourage academia-industry engagement to ideate and develop 5G use cases.
- To Provide local access to 5G test setup for Startups and MSMEs around the institution.

9.4 Future Vision and Goals

The future vision of Dr. D. Y. Patil Vidyapeeth, Pune, revolves around leveraging technology to enhance teaching, learning, and administrative processes. Key goals include enhancing network scalability,

improving data storage and retrieval capabilities, optimizing software licensing arrangements, and strengthening cybersecurity measures. By prioritizing these objectives, the organization aims to enhance operational efficiency, improve service delivery, and foster a culture of innovation.

In the context of Indian higher education, where the digital landscape is rapidly evolving, Dr. D. Y. Patil Vidyapeeth, Pune, seeks to position itself as a leader in leveraging technology to address the needs of diverse stakeholders. The institution aims to provide a modern and flexible learning environment that empowers students to succeed in an increasingly digital world.

9.5 Proposed Changes and Enhancements

To realize its vision for leveraging technology, Dr. D. Y. Patil Vidyapeeth, Pune, proposes several changes and enhancements to its IT infrastructure. These include upgrading internet bandwidth to accommodate increasing data demands, deploying additional WiFi access points to ensure comprehensive coverage, expanding storage capacity to accommodate growing data volumes, and streamlining software licensing arrangements to optimize costs. Furthermore, the organization plans to invest in cybersecurity measures to safeguard sensitive information and mitigate risks.

The proposed changes and enhancements align with the institution's strategic priorities and regulatory requirements in the Indian higher education landscape. By investing in modernizing its IT infrastructure, Dr. D. Y. Patil Vidyapeeth, Pune, aims to enhance its competitiveness, improve operational efficiency, and deliver a superior experience to its stakeholders.

9.6 IT Infrastructure Roadmap

The IT Infrastructure Roadmap delineates a detailed timeline for implementing the proposed changes and enhancements. Phase 1 focuses on upgrading internet bandwidth and expanding Wi-Fi coverage, followed by Phase 2, which entails enhancing storage capacity and optimizing software licensing arrangements. Phase 3 prioritizes cybersecurity enhancements, including the implementation of advanced threat detection systems and employee training initiatives. Each phase is accompanied by specific tasks, responsible parties, and milestones to ensure timely execution and accountability.

The IT Infrastructure Roadmap reflects the institution's commitment to continuous improvement and innovation in its IT infrastructure. By adopting a phased approach, Dr. D. Y. Patil Vidyapeeth, Pune, aims to minimize disruptions, manage resources effectively, and achieve measurable outcomes aligned with its strategic objectives.

9.7 Risk Management and Contingency Plans

The organization acknowledges potential risks and challenges associated with infrastructure upgrades, such as technical failures, budget overruns, and resistance to change. To mitigate these risks, contingency plans have been developed, including regular risk assessments, stakeholder communication strategies, and backup and recovery protocols. Additionally, the organization remains committed to fostering a culture of innovation and adaptability to navigate unforeseen challenges effectively.

In the Indian context, where regulatory compliance and data security are paramount concerns, risk management assumes heightened importance. Dr. D. Y. Patil Vidyapeeth, Pune, is committed to

ensuring compliance with relevant regulations and standards while proactively addressing emerging threats and vulnerabilities.

9.8 Monitoring and Evaluation Framework

Effective monitoring and evaluation mechanisms are essential for measuring the success of the IT Infrastructure Roadmap. Key performance indicators (KPIs), such as network uptime, WiFi coverage, storage utilization, and cybersecurity incidents, will be tracked regularly to assess progress and identify areas for improvement. Quarterly reviews and annual assessments will facilitate ongoing optimization of the IT infrastructure and ensure alignment with the organization's strategic objectives.

The monitoring and evaluation framework will provide valuable insights into the effectiveness of the proposed changes and enhancements. By leveraging data-driven insights, Dr. D. Y. Patil Vidyapeeth, Pune, aims to identify opportunities for further improvement and innovation in its IT infrastructure.

9.9 Conclusion

The IT Infrastructure Roadmap outlined in this document represents a strategic initiative to enhance the digital capabilities of Dr. D. Y. Patil Vidyapeeth, Pune. By prioritizing improvements to its internet bandwidth, Wi-Fi network, storage solutions, software licensing arrangements, and cybersecurity measures, the organization aims to achieve operational excellence and deliver enhanced services to its stakeholders. Through effective implementation and continuous monitoring, the organization is poised to elevate its digital maturity and establish itself as a leader in the field of higher education.

9.10 Appendices

- Technical specifications
- Escalation Matrix for Maintenance of IT Infrastructure

9.11 Infrastructure:

- **Internet Bandwidth:** Internet and LAN. Wi-Fi / optic fiber network Internet broadband connectivity is through 2000 Mbps 1:1 lease line of Tata comm.; 1000Mbps through NKN, BSNL; 1500 Mbps though MPLS VPN HUB connectivity from Tata; 1-10 Gbps ring shape OFC from DPU Data Center to the Institutes.
- **WIFI Devices:** Grand Stream Wireless Access point Model: GWN7660/ GWN7664LR Juniper Wireless Access point. Model: - WLA322-WW and Mojo Wireless Access point Model: -C-110 (Total Active 626 Wireless Access point).
- **Storage:** EMC Unity 300 Storage (Solud-D31D24AF25) 210 TB. Based on the powerful new family of Intel E5-2600 processors, Dell EMC Unity Hybrid storage systems implement an integrated architecture for block, file, and VMware VVols with concurrent support for native NAS, iSCSI, and Fiber Channel protocols. Each system leverages dual storage processors, full 12 Gb SAS back-end connectivity and Dell EMC’s patented multicore architected operating environment to deliver unparalleled performance & efficiency. Additional storage capacity is added via Disk Array Enclosures (DAEs) and for additional performance, online controller upgrades are available.

- **Manpower:** A central IT cell (ITC) with 25 qualified personnel takes care of planning and designing, creation, evaluation, implementation, and maintenance of IT facilities as per DPU's IT policy framework. They are also responsible for procurement of professional software from outside agencies. ITC is responsible for developing a state-of-art Data Centre that caters to all the Institutes under DPU. There is also a central Software Development Cell (SDC) of DPU to design, develop and maintain customized software. All the hardware (servers, firewalls, router, switches) and software are of international standard.
- **Software Licenses:** Windows Datacenter Server 2016 & 2019, SQL Server 2017, Windows 10 Pro & 11 Pro, office 365. The Volume Licensing Service Center (VLSC) is an online platform made to make managing your Microsoft Volume Licensing agreements simple. Within the VLSC, you can access your licensing information, view agreements and purchases for your organization, and access licensing summaries of all entitlements by product and version, as well as view all assigned product keys and download products in the VLSC.
- **Hardware:** Central Data Centre includes 21 central servers (Dell /Intel / IBM). The servers are dedicated for specific functions namely - proxy, Database, AD, PACS, ERP, Antivirus, Tally, Web, HMIS, File, SCM, FTP (mainly IT Security).
- **Wi-Fi Users:** Concurrent users per access points: 60. 5000+ Student having Wi-Fi facility.
- **Network Plan:** DPU's IT has 3 tier architecture core distribution and access. User gets connected to IT service and security management servers via dedicated LAN through Internet / Intranet (Currently 250 VLAN, extendable to 1500 VANS**) Juniper SRX-1500 Firewall, Juniper QFX – 5100 Fiber Switch, Juniper QFX – 5100 Copper Switch**
- **SRX1500 Firewall Features:** HA based (Clustering firewall Cum Router). It's carter's 2 million concurrent sessions. Offers high onboard port densities with the flexibility of multiple Ethernet interface speeds. Provides fault tolerance through redundant hardware and components such as power supplies. Carrier-class reliability stems from the system and network resiliency of the Junos OS. Gives users on- and off-box automation capabilities and centralized network security management to simplify deployment and maintenance across geographically dispersed locations. Offers comprehensive protection, including multigigabit firewall capability, security intelligence via Spotlight Secure, policy enforcement, UTM, application security, antivirus, antispam, and Web filtering), NAT, DoS, and QoS.
- **Juniper QFX – 5100-48 Port Fiber/Copper Switch Features:** Fiber and Copper switch both in virtual stack chassis. Centrally all VLAN Configuration. Up to 2.56 Tbps sustains wire-speed switching with low latency and jitter, along with full Layer 2 and Layer 3 performance. Dual hot-swappable AC or DC power supplies provide 1+1 redundancy, while five hot-swappable fan trays maintain high system availability. Independent planes maximize system availability and throughput. Independent planes maximize system availability and throughput. Software-programmable infrastructure helps you make the most of your network resources and adapt quickly to changing needs. Contrail Networking enables you to provision and automate data center fabrics and Data Center Interconnect (DCI). Low power consumption reduces your carbon footprint and operational expenses.

- **Attendance System:** Centrally Attendance Management System with the help of RFID base K990 attendance system. Integrated with ERP. (RFID, Finger, Photo capture)
- **CCTV:** Campus under CCTV surveillance.(IP Based and Analog Technology, Wide Dynamic Range (WDR), PoE (Power Over Ethernet), PTZ Technology)
- **Media Center:** DPU Equipped with capacity to create and produce LMS Data such as E-content, video lecture, graphic design, images, animations. We have a workstation computer system enhanced with the latest technology in hardware and software. Our media center uses Adobe professional production software for the editing of all visual contents. Regular backup of all LMS data in storage server available with centralized data storage system for any data loss prevention.