

Information Technology Policy of Osmania University

Preface

In the ever-evolving landscape of education and research, Osmania University embraces the transformative potential of Information Technology (IT). As a cornerstone for effective teaching, learning, research, administration, and organizational development, IT plays a pivotal role in shaping our academic and operational pursuits. This IT Policy is a testament to our commitment to harness the power of IT while ensuring its responsible and secure use.

The policy establishes a framework comprising principles, guidelines, and responsibilities that encompass the entirety of our IT resources. It applies to every member of our esteemed Osmania University community, including faculty, staff, students, contractors, and all individuals or entities entrusted with access to our IT assets.

We recognize that responsible and ethical use of IT is paramount in an interconnected world. This policy upholds core principles of secure access, acceptable use, data protection, and adherence to software and hardware standards. It outlines the roles and responsibilities of users and the IT department, setting clear expectations for both.

We are dedicated to conduct training and awareness programs that equip our community with the knowledge to safeguard our digital ecosystem. Additionally, we maintain a rigorous incident reporting and response mechanism, ensuring timely and effective action in the face of security challenges.

Disaster recovery and business continuity planning are integral components of our approach to IT. We strive to ensure uninterrupted access to essential systems and data, regardless of unforeseen disruptions. We embrace collaboration and partnerships with external entities, recognizing that shared knowledge enhances the security of all.

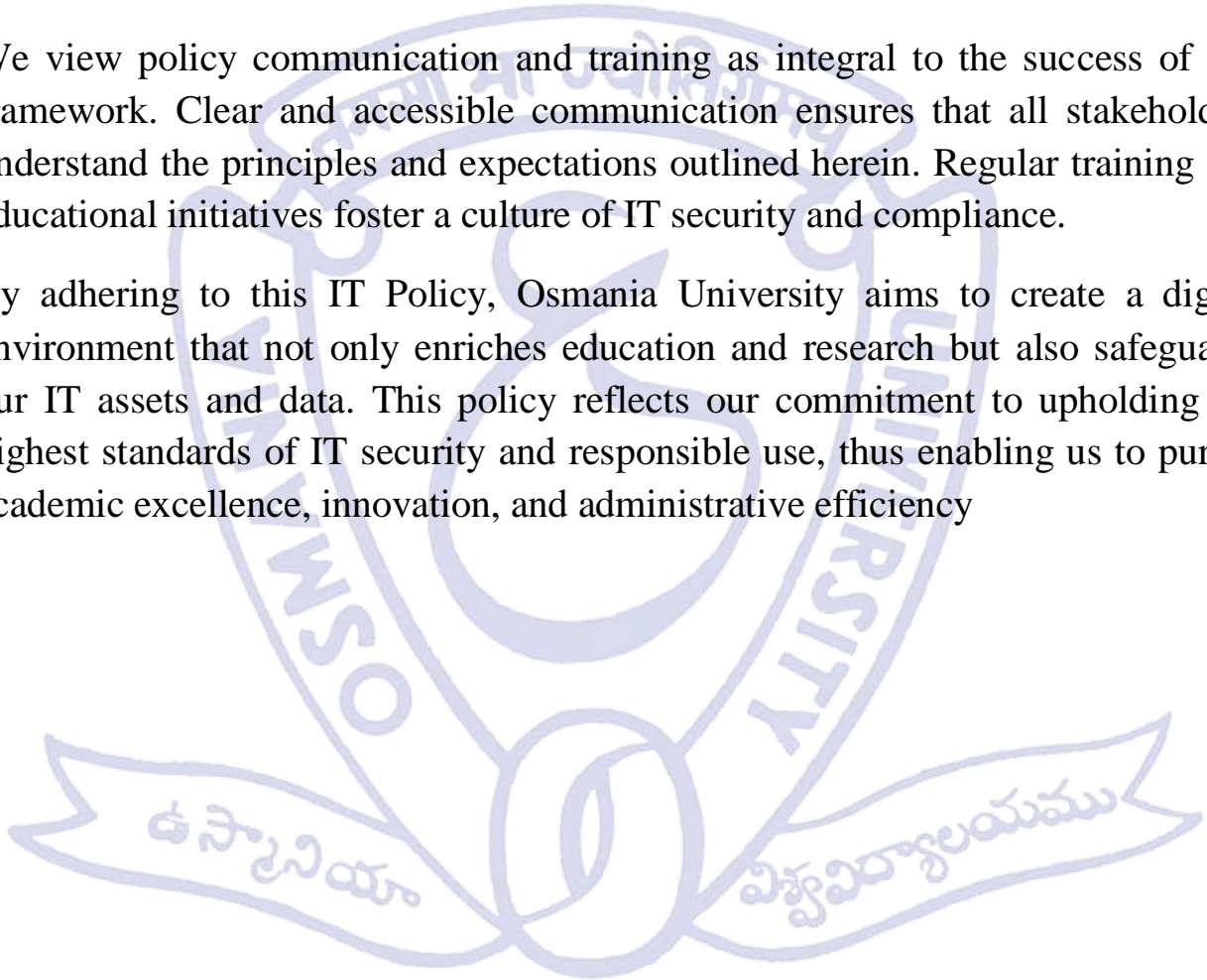
Compliance with legal and regulatory requirements is non-negotiable. Osmania University pledges to stay current with evolving laws and standards, adjusting

our policies accordingly. We allocate resources judiciously to guarantee the stability, performance, and growth of our IT infrastructure.

Network and internet usage, software and application utilization, mobile device policies, data management, and privacy guidelines are thoroughly addressed in this policy. Through comprehensive data classification, we are committed to preserving the confidentiality and integrity of sensitive information.

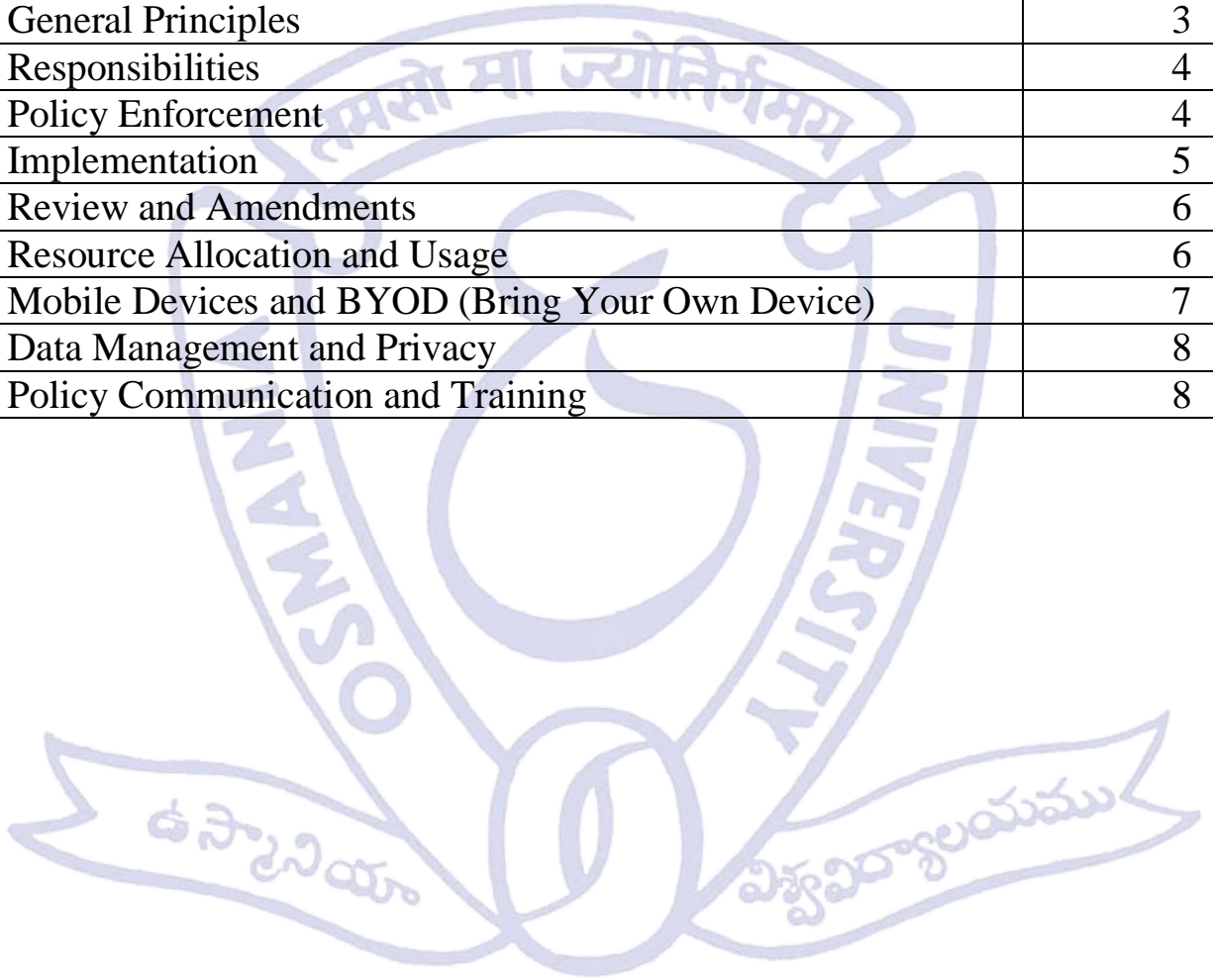
We view policy communication and training as integral to the success of this framework. Clear and accessible communication ensures that all stakeholders understand the principles and expectations outlined herein. Regular training and educational initiatives foster a culture of IT security and compliance.

By adhering to this IT Policy, Osmania University aims to create a digital environment that not only enriches education and research but also safeguards our IT assets and data. This policy reflects our commitment to upholding the highest standards of IT security and responsible use, thus enabling us to pursue academic excellence, innovation, and administrative efficiency



Title:	Information Technology Policy of Osmania University	
Effective year:	2023	
Issuing Authority:	Registrar, Osmania University, Hyderabad	
Drafting Committee		
Prof. E. Vidyasagar, Head, Department of Electrical Engineering, UCE, OU		Chairman
Prof. B. Vijayalakshmi, Dean, Faculty of Law, UCL, OU		Member
Prof. M. Kumar, Dean, Faculty of Engineering, UCE, OU		Member
Prof. P. Naveen Kumar, Director, Infrastructure, OU		Member
Prof. B. Sireesha, Director, IQAC, OU		Member
Dr. A. Vijaya Bhasker Reddy, Coordinator, IQAC, OU		Member
Dr. D. Suman, Department of Biomedical Engineering, UCE, OU		Convener
Purpose of this Policy:		
<p>The purpose of this IT Policy at Osmania University is to ensure responsible and secure use of information technology resources, protect data and systems, promote compliance with regulations, enhance collaboration, provide training, establish incident response protocols, ensure business continuity, and foster data privacy within the university community.</p>		

S.no	Contents	Page Nos
	Preface	(i)
	Drafting Committee	(iii)
	Contents	(iv)
1.	Preamble	1
2.	Introduction	2
3.	Scope	3
4.	General Principles	3
5.	Responsibilities	4
6.	Policy Enforcement	4
7.	Implementation	5
8.	Review and Amendments	6
9.	Resource Allocation and Usage	6
10.	Mobile Devices and BYOD (Bring Your Own Device)	7
11.	Data Management and Privacy	8
12.	Policy Communication and Training	8



Information Technology Policy of Osmania University

1. Preamble

In the age of information and technology, Osmania University acknowledges the indispensable role of Information Technology (IT) in reshaping the landscape of education, research, and administrative processes. As we navigate the dynamic currents of the digital era, this IT Policy serves as a guiding light, illuminating the path to secure, ethical, and efficient utilization of IT resources within our esteemed institution.

Osmania University, founded on a legacy of academic excellence and research innovation, stands as a testament to the transformative power of knowledge. As we delve into the digital realm, it is incumbent upon us to embrace IT as an enabler of our mission. This policy encapsulates our commitment to leverage IT as a catalyst for progress while upholding the principles of integrity, responsibility, and security. Recognizing the universality of technology, this policy extends its reach to encompass every member of the Osmania University community. Whether they be faculty, staff, students, or partners, all individuals entrusted with access to our IT resources bear a collective responsibility to safeguard and utilize these assets judiciously.

At its core, this policy champions the principles of responsible access, ethical use, data protection, and adherence to software and hardware standards. Through clear delineation of roles and responsibilities, we establish a foundation upon which our digital ecosystem thrives. Our commitment to IT extends beyond the written word. We pledge to invest in education and training programs that empower our community with the knowledge and skills to navigate the digital realm securely. We stand ready with a comprehensive incident reporting and response mechanism to address emerging challenges swiftly and effectively.

Disaster recovery and business continuity planning are not mere contingencies but integral facets of our IT strategy. We are unwavering in our

commitment to ensure uninterrupted access to critical systems and data, irrespective of external disruptions. In recognition of the global nature of technology, we embrace collaboration and partnerships, actively seeking to share knowledge and insights with external entities. Together, we fortify the bulwarks of our digital defenses.

Compliance with legal and regulatory frameworks is sacrosanct. Osmania University will keep a vigilant eye on evolving laws and standards, aligning our policies accordingly. We allocate resources thoughtfully, ensuring the stability, growth, and security of our IT infrastructure. From network and internet usage to software and application management, from mobile device policies to data privacy guidelines, this policy leaves no stone unturned in its pursuit of comprehensive IT governance. Through robust data classification, we commit ourselves to preserving the sanctity and confidentiality of sensitive information.

As we pledge allegiance to this IT Policy, Osmania University seeks to forge a digital environment that not only enriches education and research but also protects our IT assets and data. This policy epitomizes our dedication to upholding the highest standards of IT security and ethical use, empowering us to stride confidently towards academic excellence, innovation, and administrative efficiency

2. Introduction

Osmania University recognizes the critical role of information technology (IT) in enabling effective teaching, learning, research, administration, and overall organizational development. This IT policy outlines the principles, guidelines, and responsibilities for the secure and efficient use of IT resources within Osmania University.

3. Scope

This policy applies to all members of the Osmania University community, including faculty, staff, students, contractors, and any other individuals or entities granted access to the university's IT resources.

4. General Principles

4.1. IT Resource Access

- i. Access to IT resources (internet services) shall be granted to authorized individuals only, based on their roles and responsibilities.
- ii. Users must protect their login credentials and not share them with others. Individual accounts are non-transferable.
- iii. Any unauthorized use, access, or attempt to access IT resources is strictly prohibited.

4.2. Acceptable Use

- i. IT resources shall be used in a responsible, ethical, and legal manner, and in accordance with all applicable laws and regulations.
- ii. Users shall respect the intellectual property rights of others and not engage in any unauthorized copying, distribution, or use of copyrighted materials.
- iii. Users shall not use IT resources for personal gain, commercial activities, or any activities that could disrupt or compromise the university's operations.

4.3. Security and Data Protection

- i. Users shall take appropriate measures to protect IT resources from unauthorized access, loss, damage, or theft.
- ii. Users shall not attempt to compromise the security of IT resources or engage in any activities that could jeopardize the confidentiality, integrity, or availability of data or systems.
- iii. All users shall comply with the university's data protection policies and guidelines when handling sensitive or personal data.

4.4. Software and Hardware

- i. Users shall use licensed software and hardware in accordance with the respective software licenses and applicable copyright laws.
- ii. Users shall not install or use unauthorized software or hardware that may pose security risks or violate any policies or regulations.

5. Responsibilities

5.1. Users

- i. Users are responsible for familiarizing themselves with this IT policy and complying with its provisions.
- ii. Users must report any suspected security incidents or policy violations to the appropriate university authorities.
- iii. Users shall undergo training and awareness programs to enhance their understanding of IT policies and best practices.

5.2. IT Department

- i. The IT department shall provide necessary infrastructure, technical support, and expertise to ensure the secure and efficient operation of IT resources.
- ii. The IT department shall regularly monitor and evaluate the university's IT systems for vulnerabilities, threats, and compliance with policies and regulations.
- iii. The IT department shall collaborate with other university departments to develop and enforce IT security protocols and standards.

6. Policy Enforcement

6.1. Violations

- i. Violations of this IT policy may result in disciplinary action, including but not limited to, warnings, temporary or permanent suspension of IT resource access, or legal prosecution as applicable.
- ii. The severity of the violation and appropriate sanctions will be determined on a case-by-case basis, taking into consideration the nature and impact of the violation.

7. Implementation

7.1. Training and Awareness

- i. Osmania University is committed to providing regular training and awareness programs to educate the university community about IT policies, best practices, and emerging security threats.
- ii. Training programs will cover topics such as data protection, secure communication, safe internet browsing, and responsible use of IT resources.

7.2. Incident Reporting and Response

- i. All members of the university community have a responsibility to report any suspected security incidents, breaches, or policy violations to the appropriate university authorities.
- ii. The university shall establish a formal incident response process to promptly investigate and address reported incidents, minimizing potential damages and implementing necessary corrective actions.

7.3. Disaster Recovery and Business Continuity

- i. The university shall develop and maintain a comprehensive disaster recovery and business continuity plan for its IT infrastructure.
- ii. The plan shall include regular data backups, off-site storage, redundancy measures, and procedures for quickly restoring critical IT systems in the event of a disruption.

7.4. Compliance with Legal and Regulatory Requirements

- i. Osmania University is committed to complying with all applicable laws, regulations, and industry standards related to IT security, data protection, and privacy.
- ii. The university shall regularly review and update its IT policies to ensure compliance with changing legal and regulatory requirements.

7.5. Collaboration and Partnerships

- i. Osmania University shall collaborate with external partners, industry experts, and government agencies to stay informed about the latest IT security trends, best practices, and emerging technologies.
- ii. Collaborative initiatives may include information sharing, joint research projects, and participation in conferences, workshops, and forums related to IT security.

8. Review and Amendments

8.1. Policy Review

- i. This IT policy shall be reviewed at least once in every year or as deemed necessary by the university administration.
- ii. Reviews will consider feedback from stakeholders, technological advancements, government & reputed cyber security agencies and changes in the threat landscape.

8.2. Policy Amendments

- i. Amendments to this IT policy shall be approved by the appropriate university authorities and communicated to all members of the university community.
- ii. Updated versions of the policy shall be made readily available and accessible to ensure compliance.

9. Resource Allocation and Usage

9.1. IT Resource Allocation

- i. The university administration shall allocate appropriate resources to ensure the availability, reliability, confidentiality and performance of IT infrastructure, networks, and systems.
- ii. Adequate funding and manpower shall be allocated to support regular maintenance, upgrades, and expansion of IT resources as required.

9.2. Network and Internet Usage

- i. Users shall utilize the university's network and internet resources for academic, research, and administrative purposes in accordance with the university's policies and guidelines.
- ii. Network bandwidth and internet access will be monitored and managed to ensure fair and efficient utilization for all users through firewall.

9.3. Software and Application Usage

- i. Users shall utilize authorized and licensed software and applications provided by the university, for their respective roles and responsibilities.
- ii. Requests for new software or applications should be submitted through the appropriate channels and undergo a review process for compatibility, licensing, and security considerations.

10. Mobile Devices and BYOD (Bring Your Own Device)

10.1. Mobile Device Usage

- i. Users may connect their personal mobile devices to the university network, subject to compliance with the university's mobile device policy.
- ii. Mobile devices must be protected with strong passwords or biometric authentication, and users should install necessary security updates and antivirus software.

10.2. BYOD Policy

- i. Osmania University may adopt a Bring Your Own Device (BYOD) policy, allowing users to use their personal devices for work or educational purposes.
- ii. The BYOD policy shall establish guidelines for device compatibility, security requirements, data separation, and acceptable use of personal devices on the university network.

11. Data Management and Privacy

11.1. Data Classification

- i. The university shall establish a data classification framework (data centre) to categorize data based on its sensitivity, confidentiality, and regulatory requirements.
- ii. Data owners and custodians shall ensure appropriate security controls and access restrictions based on the data classification.

11.2. Data Privacy and Protection

- i. Osmania University is committed to protecting the privacy of personal information collected, stored, and processed in its IT systems.
- ii. Users shall handle personal data in compliance with relevant data protection laws, university policies, and privacy guidelines.

11.3. Data Backup and Retention

- i. Regular data backups shall be performed to ensure the availability and recoverability of critical data.
- ii. The university shall establish data retention policies to ensure compliance with legal, regulatory, and contractual obligations.

12. Policy Communication and Training

12.1. Policy Communication

- i. The IT policy shall be communicated to all members of the university community through appropriate channels, such as email, intranet, and orientation programs.
- ii. The policy shall be easily accessible and available in multiple formats to accommodate diverse users.

12.2. Training and Education

- i. The university shall provide regular training and educational programs to enhance users' understanding of IT policies, security best practices, and emerging threats.
- ii. Training programs may include workshops, seminars, online courses, and awareness campaigns to promote a culture of security and compliance.

By adhering to this IT policy, Osmania University aims to foster a secure, reliable, confidential and productive IT environment that supports its mission of academic excellence, research innovation, and administrative efficiency.

