Tel : 05942 - 235563
Fax No. : 05942 - 232262
email - registrar@kunainital.ac.in

कुमाऊँ विश्वविद्यालय, नैनीताल-263001 (उत्तराखण्ड)
KUMAUN UNIVERSITY, NAINITAL (UTTARAKHAND) INDIA
(Accredited "A" Grade by NAAC)

पत्रांक : IQAC/KU/2017/VICT

दिनांक 01.05.2017

INFORMATION TECHNOLOGY POLICY

(2016-17)

1. Introduction

1.1 Purpose of the Policy

The purpose of the Kumaun University Nainital IT Policy is to establish a framework that ensures the secure, efficient, and responsible use of information technology resources across the university. This policy aims to safeguard data, promote a secure computing environment, and support the university's mission of excellence in education, research, and administration.

1.2 Scope

This policy applies to all departments, faculty, staff, and students of Kumaun University Nainital. It covers all IT systems, networks, and technologies owned, operated, or contracted by the university.

2. Responsible Use of IT Resources

2.1 Acceptable Use

Users are expected to use university IT resources responsibly, respecting legal and ethical standards. Acceptable use includes academic and administrative activities, while unacceptable use encompasses activities that violate laws, compromise security, or disrupt operations.

2.2 User Responsibilities

Faculty, staff, and students share the responsibility of maintaining the security and integrity of IT resources. This includes safeguarding login credentials, reporting security incidents promptly, and adhering to the guidelines outlined in this policy.

2.3 Access Control

Procedures for granting and revoking access to university systems are defined in the Access Control Policy. Access permissions are based on roles and responsibilities, and regular reviews are conducted to ensure appropriateness.

3. Data Security and Privacy

3.1 Data Classification

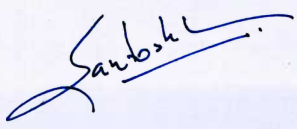
Data is classified based on sensitivity, ranging from public to highly confidential. Security measures, including access controls and encryption, are implemented according to the classification level.

3.2 Data Encryption

Data encryption is mandatory for sensitive information during transmission and storage. Encryption methods are in compliance with industry standards and best practices.

3.3 Privacy Policies

Kumaun University handles personal and sensitive information in accordance with applicable privacy laws. Privacy policies are designed to protect the rights and confidentiality of individuals.



4. Network Security

4.1 Network Access Control

Measures are in place to control unauthorized access to the university's network. Access is granted based on user roles, and monitoring systems are employed to detect and respond to suspicious activities.

4.2 Firewall and Intrusion Detection

Firewalls and intrusion detection systems are deployed to protect the network from external threats. Regular updates and monitoring ensure the effectiveness of these security measures.

5. Software and Hardware Management

5.1 Software Licensing

The university ensures compliance with software licensing agreements for all installed applications. Unlicensed software is prohibited.

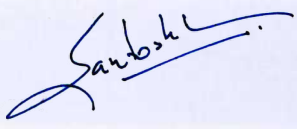
5.2 System Configuration Standards

Standards for configuring and maintaining hardware and software systems are established to ensure consistency, security, and optimal performance.

6. Incident Response and Reporting

6.1 Incident Reporting

Procedures for reporting IT security incidents promptly are outlined in the Incident Reporting Policy. Timely reporting is crucial for the effective management of security breaches.



6.2 Incident Response

In the event of a security incident, the university follows a structured incident response plan. This includes investigation, containment, eradication, recovery, and post-incident analysis.

7. Training and Awareness

7.1 IT Security Training

Ongoing IT security training programs are implemented to educate users about best practices, emerging threats, and the university's IT policies.

7.2 Awareness Campaigns

Regular awareness campaigns are conducted to keep the university community informed about the latest security threats and preventive measures.

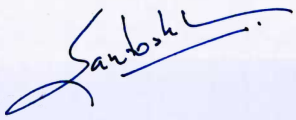
8. Compliance and Auditing

8.1 Regulatory Compliance

The university's IT practices are aligned with relevant laws and regulations governing information security and privacy.

8.2 Auditing

Regular IT security audits are conducted to identify vulnerabilities, assess compliance, and implement corrective actions.



9. Review and Revision

9.1 Policy Review

The IT Policy undergoes periodic reviews to ensure its relevance and effectiveness in addressing evolving technology and security threats.

10. Enforcement and Consequences

10.1 Violations

Violations of the IT Policy may result in disciplinary actions, including but not limited to account suspension, revocation of access privileges, and legal consequences as per university regulations.