# IT USAGE AND ACCESS CONTROL POLICY

Policy No. ITUAP 2024

KARE/IQAC/ITUAP/2024/01


**KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION**

(Deemed to be University)

**(**Under the section 3 of UGC act 1956)

Anand Nagar, Krishnankoil-626126, Srivilliputtur (Via), Tamil Nadu, India.

Phone: 04563-289042, Fax: 04563-289322

www.kalasalingam.ac.in **email:** info@kalasalingam.ac.in

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade
Anand Nagar, Krishnankoil, Srivilliputtur (Via), Virudhunagar (Dt) - 626126, Tamil Nadu | info@kalasalingam.ac.in | www.kalasalingam.ac.in

# IT USAGE AND ACCESS CONTROL POLICY

**Policy Preparation & Verification Team**

**Prepared: 2024**

| | | |
|---|---|---|
| **Prepared by** | Dr. R. Kottaimalai |  |
| **Reviewed by** | Dr. C. Sivapragasam |  |
| **Recommended by** | Dr. P. Deepalakshmi |  |
| **Approved by** | Vice-Chancellor |  |

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade
Anand Nagar, Krishnankoil, Srivilliputtur (Via), Virudhunagar (Dt) - 626126, Tamil Nadu | info@kalasalingam.ac.in | www.kalasalingam.ac.in

# IT USAGE AND ACCESS CONTROL POLICY

## 1. PURPOSE

The purpose of this IT Usage and Access Control Policy is to establish a robust framework governing the secure, ethical, and responsible use of information technology resources at Kalasalingam Academy of Research and Education (KARE). Information technology resources—including networks, systems, applications, devices, and data—are critical institutional assets that support academic delivery, research activities, administrative operations, and communication.

This policy aims to ensure that IT resources are used in a manner that protects the confidentiality, integrity, and availability (CIA) of institutional data while preventing unauthorized access, misuse, cyber threats, and data breaches. It also defines access control mechanisms to ensure that users are granted appropriate levels of access based on their roles and responsibilities.

## 2. SCOPE

This policy applies to all individuals and entities who access or use KARE's IT resources, including:

- Faculty, staff, and administrative personnel
- Students and research scholars
- Contractual employees, vendors, and third-party service providers
- Visitors or external collaborators granted temporary access

The policy covers all IT resources, including:

- Institutional networks (wired and wireless)
- Servers, databases, and cloud platforms
- End-user devices (desktops, laptops, mobile devices)
- Applications, software, and digital platforms
- Email systems and communication tools
- Data stored, processed, or transmitted through institutional systems

## 3. DEFINITIONS

Role-Based Access Control (RBAC): Access management approach whereby users are granted system privileges based on their official roles and responsibilities.

Multi-Factor Authentication (MFA): Authentication using two or more independent verification methods.

BYOD (Bring Your Own Device): Personally owned devices used to access institutional IT resources.

## 4. POLICY REQUIREMENTS

### 4.1 Acceptable Use of IT Resources

All users must utilize IT resources strictly for academic, research, administrative, and authorized institutional purposes. Usage must be responsible, lawful, and aligned with institutional values.

Users shall:

- Use IT systems in a professional and ethical manner
- Avoid activities that compromise system performance or security
- Respect intellectual property rights and licensing agreements
- Ensure that institutional resources are not used for illegal, offensive, or unethical purposes

Unauthorized activities such as hacking, spreading malware, accessing restricted systems, or misuse of institutional data are strictly prohibited.

### 4.2 User Access Control

Access to IT systems shall be governed by the principle of least privilege, ensuring that users are granted only the access necessary to perform their roles.

Key requirements include:

- Role-based access control (RBAC) implementation
- Unique user identification (User ID) for all users
- Secure authentication mechanisms (passwords, multi-factor authentication where applicable)
- Periodic review and validation of access rights
- All user accounts shall be created only upon approval by the authorized Department Head or designated authority and after verification of the user's institutional affiliation.

- User access privileges shall be assigned according to the principle of Role-Based Access Control (RBAC) and the principle of least privilege.
- User accounts shall be modified promptly whenever there is a change in role, department, responsibilities, or access requirements.
- Accounts of graduating students shall ordinarily be deactivated within thirty (30) days after completion of academic requirements unless continued access is specifically approved.
- Accounts of employees leaving the University shall be suspended immediately upon cessation of employment or as directed by the Human Resources Department.
- Dormant accounts remaining inactive for more than ninety (90) consecutive days may be disabled after review by the IT Department.

Access must be approved by authorized personnel and documented appropriately.

### 4.3 Authentication and Password Management

Strong authentication mechanisms must be implemented to prevent unauthorized access.

Users must:

- Use strong passwords with appropriate complexity
- Avoid sharing login credentials with others
- Change passwords periodically
- Report any suspected compromise of credentials immediately

The institution may enforce:

- Password expiration policies
- Multi-factor authentication (MFA)
- Account lockout mechanisms after repeated failed attempts
- Administrative or privileged accounts shall, wherever technically feasible, be protected using Multi-Factor Authentication (MFA).
- Default passwords supplied with hardware or software shall be changed before systems are placed into operational use.

### 4.4 Data Access and Confidentiality

Access to institutional data must be controlled and monitored to ensure confidentiality and compliance.

Users shall:

- Access only data required for their roles
- Protect sensitive and personal data from unauthorized disclosure
- Avoid copying, sharing, or transmitting data without proper authorization

Special care must be taken when handling:

- Student records
- Research data
- Financial information
- Sensitive institutional data, including student records, research data, financial records, examination materials, and confidential documents, shall not be stored on personal devices, personal cloud storage services, or personal email accounts unless specifically authorized by the IT Department and protected using approved security measures such as encryption.

**4.5 Network Security and Monitoring**

The University shall implement appropriate measures to ensure network security, including:

- Firewalls, intrusion detection/prevention systems
- Network monitoring and logging
- Secure Wi-Fi access controls
- Protection against malware, phishing, and cyber threats
- Monitoring of institutional networks, systems, and email services shall be carried out solely for legitimate purposes including cybersecurity, system administration, compliance verification, investigation of security incidents, and protection of institutional assets. Such monitoring shall be conducted in accordance with applicable laws, the University's Data Protection Policy, and privacy obligations. Personal communications shall not be routinely monitored except where required by law or during authorized investigations.

Users must not attempt to bypass security controls or connect unauthorized devices to institutional networks.

**4.6 Removable Storage Devices**

- The use of USB drives, external hard disks, memory cards, and other removable storage devices shall be restricted to legitimate institutional purposes.
- Only authorized removable storage devices may be connected to institutional systems where technically feasible.
- Sensitive or confidential institutional data shall not be copied to removable media unless specifically authorized and protected through encryption or other approved security controls.
- The IT Department may restrict, disable, or monitor the use of removable storage devices to minimize cybersecurity risks.

### 4.7 Use of Personal Devices (BYOD)

Use of personal devices to access institutional systems must comply with security requirements:

- Devices must have updated antivirus and security patches
- Access may be restricted based on security compliance
- Sensitive data should not be stored on personal devices without authorization
- Institutional confidential information shall not be synchronized or backed up to personal cloud storage services (e.g., personal Google Drive, OneDrive, Dropbox, iCloud) unless expressly approved by the University.

The institution reserves the right to restrict or monitor BYOD usage.

### 4.8 Email and Communication Systems

Institutional email systems must be used responsibly and professionally.

Users must:

- Institutional email services shall primarily be used for academic, research, administrative, and official communication. Limited personal use is permitted provided it does not interfere with official duties, consume excessive institutional resources, violate applicable laws, or contravene University policies.
- Verify authenticity before sharing sensitive information
- Use official communication channels for institutional matters

Emails may be monitored for security and compliance purposes.

Users shall not send, store, transmit, or distribute content including but not limited to:

- Malicious software or ransomware
- Spam or phishing messages
- Hate speech or discriminatory content
- Pornographic or sexually explicit material
- Copyright-infringing materials
- Content promoting violence, terrorism, or illegal activities
- Defamatory, abusive, or threatening communications

### 4.9 Software Usage and Licensing

All software used within the institution must be:

- Properly licensed and authorized
- Installed through approved channels
- Regularly updated and maintained

Unauthorized or pirated software installation is strictly prohibited.

### 4.10 Remote Access and Cloud Services

Remote access to institutional systems must be secure and controlled.

Requirements include:

- Use of VPN or secure access mechanisms
- Authentication controls for remote login
- Compliance with institutional policies when using cloud platforms

Cloud storage and services must be approved by the IT department.

### 4.11 Incident Reporting and Response

- All users shall report suspected cybersecurity incidents, unauthorized access, malware infections, phishing attacks, loss of institutional devices, or suspected data breaches to the IT Department immediately and, wherever practicable, not later than one (1) working day after discovery.
- The IT Department shall acknowledge receipt, initiate incident assessment, contain the incident where necessary, preserve evidence, implement corrective actions, and document lessons learned to prevent recurrence.

### 4.12 Data Backup and Recovery

- Critical institutional systems and databases shall be backed up regularly in accordance with the University's Backup and Disaster Recovery Procedures.
- Backups shall be periodically tested to verify successful restoration and integrity.
- Backup media shall be securely stored with appropriate physical and logical access controls.
- Backup retention periods shall be defined according to institutional and statutory requirements.

## 5. ROLES AND RESPONSIBILITIES

### 5.1 University Management

- Establish IT governance framework
- Ensure allocation of resources for IT security

### 5.2 IT Department

- Implement and maintain IT infrastructure and security controls
- Monitor systems and respond to incidents
- Manage user access and authentication mechanisms
- Review user access rights at least once every six (6) months.
- Maintain audit logs of privileged system activities.
- Ensure periodic backup and recovery testing.

### 5.3 Department Heads

- Ensure compliance within their departments
- Approve access requests where applicable

### 5.4 Users (Faculty, Staff, Students)

- Follow IT usage guidelines
- Protect login credentials and data
- Report security incidents

## 6. NON-COMPLIANCE WITH POLICY

Failure to comply with this policy may result in:

- Suspension or revocation of IT access
- Disciplinary action
- Legal consequences (in case of serious violations)
- Financial or reputational damage to the institution

Violations include unauthorized access, misuse of systems, data breaches, and security policy violations.

Examples of violations include:

- Sharing passwords or authentication credentials
- Installing unauthorized software
- Using unauthorized cloud storage
- Circumventing security controls
- Unauthorized copying of confidential information
- Connecting unauthorized devices to institutional networks

## 7. SUPPORTING POLICIES

This policy must be read along with:

- Data Protection Policy
- Cybersecurity Policy
- Records Management Policy
- Anti-Fraud Policy
- Disclosure (Whistleblower) Policy

## 8. FURTHER INFORMATION

For guidance or assistance, users may contact:

- IT Services Department
- System Administrator
- Institutional Helpdesk

Training and awareness programs will be conducted periodically.

## 9. DISCLAIMER

This policy is intended for institutional governance and IT security management. The institution reserves the right to update or modify the policy as required by technological advancements, regulatory requirements, or operational needs.

## 10. DEFINITIONS

- Access Control: Mechanisms that restrict access to systems and data
- Authentication: Process of verifying user identity
- Authorization: Granting permission to access resources
- Confidentiality: Protection of sensitive information from unauthorized access
- Data Breach: Unauthorized access or disclosure of data
- Network Security: Measures to protect network infrastructure
- User Account: Unique identity assigned to a system user

## CONCLUSION

This IT Usage and Access Control Policy ensures that Kalasalingam Academy of Research and Education maintains a secure, efficient, and reliable IT environment, enabling academic and administrative excellence while safeguarding institutional data and resources.