Uncompromising Organization safety….

INSTITUTE INFORMATION TECHNOLOGY SECURITY CENTRE POLICY OF KITSW - 2022

(*w.e.f August 2022*)

(Institutional security mechanism to eliminate scope of Intrusion

Estd.1980
KITSW

Prepared By:
Password encryption and reset policy committee
On
8th August, 2022 (Monday)

***

INSTITUTE INFORMATION TECHNOLOGY SECURITY CENTRE POLICY

This document brings out the conditions under which access to the network and computing resources at Kakatiya Institute of Technology and Science, herein after mentioned as KITSW, are granted to users. This covers all services and resources provided through KITSW, either through the institute information technology security centre (IITSC) or through any individual department. This document is subject to revision from time to time without advance notice.

Anyone who needs to use computing or network resources / equipment through the KITSW must agree to the conditions of this policy. If anyone does not agree with any provisions of this document, the access to the facilities shall be withdrawn by the IITSC.

The salient features of this document are summarized as follows:

1. These policy statements are framed in line with the guidelines of the Government of India and are subject to interpretation in the light of the existing laws of this country.
2. The primary usage of IT resources is for academic and research purposes. In case of any conflict of interest, academic usage shall be given priority over non-academic requirements.
3. To maintain privacy and to reduce the threat of crime protecting KITSW premises and safety of all the staff members, students and visitors, the video surveillance system shall be utilized.
4. The policy for replacement of provision of IT accessories such as computer/laptop/ printer/router/server and other network components shall be provided by the Institute for all the emergency purposes.

PREFACE

KITSW recognizes the role of information technology in the academic environment teaching learning, research and related administrative activities. As more information is used and shared in a digital format by students, faculty and staff, both within and outside the Institute, suitable efforts are made to protect the information and the information technology resources that support the diverse functions of KITS.

In line with the vision, mission and strategies of the KITSW, the IITSC envisions and provides IT services, computing and information resources including all relevant systems, data and requisite access. Facilities and services are to be provided to cater to the needs of Institute's community of employees, students, visitors, partners and suppliers as relevant.

Increased protection of information and information technology resources to assure the utility and availability of those resources is the primary purpose of this Policy. The Policy also addresses privacy and security issues.

PURPOSE AND SCOPE

The purpose of this policy is to outline the acceptable use of IT services at KITSW. These rules are in place to protect the students, faculty and other employees. Inappropriate use exposes stakeholders to risks including virus attacks, compromise of network systems and services, and legal issues.

Thus, this policy applies to students, employees, contractors, consultants, temporary and other workers at KITSW including faculty, staff, project associates, and all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by KITSW and also to any privately owned equipment that may be connected to the network services provided.

The policies are described in the following sections.

1.0. GENERAL FEATURES OF POLICY

1.1. Institute provides access to IT services only to authorized users amongst existing employees and students as well as identified visitors, partners and suppliers.

1.2. Acceptable usage of IT assets, facilities and services includes and is strictly limited to conducting specific and related business activities of KITSW, other organizations, visitors, suppliers and partners as well as participation in discussion groups on subjects of professional interest and exchange of knowledge.

1.3. Access to IT assets, facilities and services is a privilege and not a right, and requires the individual, authorized users/organizations to act responsibly and limiting their usage for which they have been explicitly authorized by the KITSW and must safeguard the implicit and explicit interests of the Institute at all times.

1.4. Users shall respect the rights of other users, respect the integrity of the KITSW IT assets, facilities and services, and observe all relevant laws, licensing policy, rights to use, copyrights, intellectual property rights, regulations, and contractual obligations as applicable and implied.

1.5. Users, who have been provisioned in Active Directory Services, may have the access rights to use selected Institute IT assets, facilities and services as per authorization provided by KITSW as well as the respective Department they belong to.

1.6. All information about an authorized user as well as other information/data within or in the IT Assets of KITSW, facilities and/or services and/or held in any other device or form is the sole property of the KITSW and may not be copied, removed or tampered with.

1.7. In addition, identified, authorized personnel of the KITSW may access IT assets, facilities, services and information, data, files and/or any other as required of another user(s) requirements on written approval of the competent authority, unless they have been explicitly given these rights by virtue of their roles and responsibilities.

1.8. All users shall act to protect the KITS's IT assets, facilities and services and the integrity of information/data contained in them. These shall be governed by KITSW IT policies, processes, procedures and in conjunction with the Institute's HR policies, processes, procedures and code of conduct as applicable

in general as well as specific to each category of users.

1.9. The Acceptable use of Policy for KITSW Information Technology and Digital Resources governs all uses of the Institute's information technology resources. All members of the Institute are expected to be familiar with and adhere to this policy.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

2.0. INFRASTRUCTURE USAGE POLICY

In its endeavor to provide all faculty, students and staff with a modern, fully networked computing and IT environment for academic use, KITSW has framed IT infrastructure Policy.

Users of computing, networking and other IT facilities are expected to abide by the following rules, which are intended to preserve the utility and flexibility of the system, protect the privacy and work of students and faculty, and preserve the right to access the international networks to which the system is connected. In case of complaints, appropriate action shall be decided by the person in-charge of the facility in consultation with the Principal or Head of the IT facilities/ Dean of Students Affairs.

Faculty, staff, and students with authorized accounts may use the computing and IT facilities for academic purposes, official Institute business and for personal purposes so long as the use:

2.1. Does not violate any law of Institute policy or IT Act of the Government of India.

2.2. Does not interfere with the performance of Institute duties or work of an academic nature (as judged by the Executive Committee).

2.3. Does not result in commercial gain or private profit other than that allowed by the Institute.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

3.0. PRIVACY POLICY

3.1. Users are expected to respect the privacy of fellow users and must not allow any other person to use their password or share their account. It is the responsibility of the user to protect their account from unauthorized use by changing passwords periodically. Sharing of passwords for any purpose, whatsoever, is strictly prohibited.

3.2. Users may share the required files through own cloud or other sharing software with proper access control.

3.3. Users shall exercise care while entering their passwords at other non-trusted sites and should not be misled by purported emails from admin or other IDs. Every user has to verify the sender DKIM signature before trusting such emails.

3.4. Any attempt to circumvent system security, guess others' passwords or in any way gain unauthorized access to local or network resources is forbidden. Users shall not use another computing account, attempt to forge an account identity or use a false account or e- mail address.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

4.0. POLICY ON SECURITY

4.1. Every user has to keep passwords secure and should not share accounts. Authorized users are responsible for the security of their passwords and accounts. It is recommended that system level passwords should be changed quarterly and user level passwords should be changed every six months. All PCs, laptops and workstations should be secured with a password or by logging- off when the host shall be unattended.

4.2. All equipment placed in public locations, are for general use and IITSC cannot guarantee that such machines are free of viruses or other malicious software. Users are expected to take adequate precaution and to delete all personal information before logging out of these machines.

4.3. Any derogatory/inflammatory postings by students or employees is prohibited

4.4. All hosts used by the user that are connected to the Institute Internet/Intranet, whether owned by the user or not, shall be continually executing approved virus- scanning software with a current virus database.

4.5. Users must use caution when opening e-mail attachments received from unknown senders, which may contain viruses.

4.6. Users should not use the Institute IT infrastructure in any way so to compromise the security of any other user, system or network anywhere, inside or outside the institute.

4.7. Users aware of any breach of security in any part of the IT infrastructure must report such situations to the system administrator or the department representative responsible for security in that Unit.

4.8. Users should use a strong password to protect any accounts owned by them on the Institute IT infrastructure including but not limited to email accounts. A password must be immediately changed if it is suspected of being disclosed or known to have been disclosed to anyone besides the authorized user.

4.9. Users are not allowed to extend or otherwise tamper with the Institute network.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

5.0. POLICY ON UNACCEPTABLE USE

The following activities are, in general, prohibited. Under no circumstances is a user of the Institute network resources authorized to engage in any activity that is illegal under local, State, Central or International law while utilizing KITSW owned resources. The activities given below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use:

5.1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations, including, but not limited to, the installation or distribution of

"pirated" or other software products that are not appropriately licensed for use by the Institute.

5.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the end user does not have an active license.

5.3. Possessing or distributing material that may be considered a violation of the privacy or other rights of any individual; decisions on objectionable nature of material shall be made by a suitably constituted and empowered committee appointed by the Principal

5.4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal; the management of the Institute should be consulted prior to export of any material that is in question.

5.5. Introduction of malicious programs or viruses into the network or server is strictly prohibited

5.6. Revealing account password to others or allowing use of one's own account by others is strictly prohibited including that of family members when work is being done at home.

5.7. Using KITS computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the local jurisdiction of the user is prohibited

5.8. Making fraudulent offers of products, items or services originating from any Kakatiya account is a punishable offence.

5.9. Making statements about warranty, expressly or implied, unless it is a part of routine duty through IT resources is strictly prohibited.

5.10. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet is strictly prohibited.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

6.0. INTERNET USAGE POLICY

6.1. Controlled internet access may be provided to employees, students, visitors, partners and suppliers based on "need to access" and shall be monitored.

6.2. Access to internet shall be only through the firewall when operating in KITS domain.

6.3. The access to Internet shall always be used for Business requirements only.

6.4. All official communications shall be routed through the KITSW email ID only. Any deviations will be considered as violation of this policy.

6.5. All information downloaded through Internet shall always be screened through Anti- Virus Scanner before being used.

6.6. Instant messaging creates a written business record that can be subpoenaed and used as evidence in litigation or regulatory investigations. The IIT SC's IT assets, facilities and services under explicit permission from the Executive Committee reserve the right to monitor all transmissions.

6.7. Any employee found sending confidential or sensitive information is liable for strict disciplinary procedure.

6.8. Any employee found sending sensitive and inflammatory messages in all

social media platform are liable to be punished.

6.9. Users must inform IITSC of any potentially vulnerable website encountered so that IT Security group can take action in blocking the website.

6.10. Users should be aware that the IITSC accepts no liability for their exposure to offensive material that they may access via the Internet.

6.11. The ability to connect with a specific web site does not in itself imply that users permitted to visit that site.

6.12. The IITSC has the right to monitor and log any and all aspects of Internet usage including, but not limited to, monitoring Internet sites visited by users, Chat and newsgroups, file downloads, and all communications sent and received by users with explicit permission from the competent authority.

6.13. The IITSC reserves the right for punitive action against any erring user in accessing or using internet that is against the interest of the Institute or any individual associated with the Institute.

6.14. Users aware of any breach of security in any part of the IT infrastructure must report such situations to the system administrator or the departmental representative responsible for security in that area.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

7.0. SYSTEMS USAGE POLICY

7.1. Users are prohibited from downloading and installing any software in their systems without the consent of Head, IITSC.

7.2. Only legally valid and business related Applications Software must be installed based on approval from IITSC/Dean/Head of the Department

7.3. Applications shall be installed in desktops and laptops only with the coordination of IITSC.

7.4. Administrative rights will not be provided to users of desktops and laptops.

7.5. Mobile devices should not be converted to hotspots. The use of public hotspots should be limited and instead use protected Wi-Fi from a trusted network operator or mobile wireless connection.

7.6. All systems including desktops, laptops and smart phones/devices provided by KITS shall be used only for academic, research and administrative purposes.

7.7. All employee and student owned desktops, laptops and smart phones/devices used to access IT Assets, Facilities and Services shall adhere to this Policy.

7.8. IITSC reserves the right to seize any employee and student owned desktops, laptops and smart phones/devices which are used to access KITS or related organization business, to perform forensic investigations if considered to be violation of this policy.

7.9. All important and critical data in the desktops like mark sheets, question papers, reports, proposals and configuration documents shall be secured and appropriately stored and access restricted to authorized personnel.

7.10. All new users shall sign the Confidentiality Agreement at the time of joining

7.11. All users shall login to the domain with the domain user account and not the local user accounts wherever applicable.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from their service and dismissal, depending on the severity of the case.

8.0. CYBERSECURITY POLICY

8.1. As the first step towards cyber security, the Institute shall allow and use only licensedsoftware.

8.2. Local area network (Wired and Wi-Fi network) shall be protected by Firewall with Intrusion Detection and Prevention system to block harmful traffic from and to the Internet and at the local intranet level.

8.3. The access to the Wi-Fi network and Internet for all users shall be based on either user or device authentication. The users can login to the system or network using a central authentication mechanism.

8.4. All the computers must be installed with a licensed Antivirus system which should be regularly updated.

8.5. Each computer shall be 'Administrator password' protected, which will not be known to the user. The user shall have only usage privileges and cannot install any software. The installation of the licensed software shall be carried out only by the staff of the IITSC.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from their service and dismissal, depending on the severity of the case.

9.0. DATA BACKUP, STORAGE AND RECOVERY POLICY

9.1. Electronic backups are a business requirement to enable the recovery of data and application in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors. The purpose of this Data Backup and Storage Policy is to establish the rules for the backup and storage of KITSW electronic information.

9.2. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk.

9.3. The Information Resources backup and recovery process for each system must be documented as a standard operating procedure and periodically reviewed.

9.4. All data and software essential to the continued operation of the Institute, as well as all data that must be maintained for legal purposes, must be backed up. All supporting material required to process the information must be backed up as well. Critical data, as defined by the Institute must be backed up on a daily basis.

9.5. Backup data must be stored at a backup location/Cloud storage that is physically different from its original usage location (i.e. The Disaster Recovery Site)

9.6. Full back-up and Incremental backup schedule shall be fixed based on consultation with the IITSC.

9.7. Data shall be retained in line with current legal requirements.

9.8. Data backed-up shall at-least be tested half-yearly.

9.9. Recovery procedures must be tested at least half-yearly and Disaster Recovery procedures must be tested at least yearly. Recovery tests must be documented.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from their service and dismissal, depending on the severity of the case.

10.0. ONLINE EXAMINATIONS POLICY

10.1. Online examinations provide students with the flexibility to undertake the examination in an environment of their choice. To ensure the credibility of the examination and to provide a just and fair mechanism, the online examinations are proctored using video recording software or AI based proctoring or remote proctors.

10.2. Each student shall undergo an initial verification of identity and subsequently scan the environment and also enable intermittent scanning during the examination if necessitated.

10.3. It is the responsibility of each student to maintain an appropriate examination ecosystem, and periodically follow the instructions from the Controller of Examinations.

10.4. Failure to follow the policy and the instructions shall result in referral to the Malpractice Enquiry Committee. The committee shall review the behaviour of the student during the conduct of the examination for adherence to this policy based on the recorded video; the enquiry committee shall provide its recommendation to the Controller for necessary action.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including dismissal, depending on the severity of the case.

11.0. POLICY ON REPLACEMENT OF IT EQUIPMENT AND ACCESSORIES

11.1. The Institute shall provide, on call, technical support through its personnel employed in the helpdesk to address hardware and software related issues faced by all stakeholders. This service shall be provided only to emergency related requirements. However, if IT accessories require replacement especially in the computer related devices, such as laptop, printer, router, dongle and other server and network components the Institute shall provide service as early as possible.

11.2. In case of negligence by the user, the Head, IITSC may submit a report to the Principal giving the details of his observation. The Principal in turn shall appoint a committee of three experts to enquire and submit a report. This report shall be taken to the Disciplinary committee to fix responsibility and any disciplinary action.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

12.0. VIDEO SURVEILLANCE POLICY

12.1. The video surveillance system is installed with the primary purpose of reducing the threat of crime, protecting the premises and ensuring the safety of all staff members, students, and visitors while respecting the individual's privacy.

12.2. The data storage of the video surveillance system shall be centralized and stored at the Data Centre of KITS. Images/Videos captured by the system shall be monitored in the Security Control Rooms.

12.3. Unauthorized access to the Control Rooms shall not be permitted at any time. Access shall be strictly limited to the duty officers, authorized

members of senior management, police officers and any other person with statutory powers of entry.

12.4. Staff members, students and visitors may be granted access to the Control Rooms on a case-by-case basis and only with the written authorization from the Principal.

12.5. The identity of any visitor and authorization shall be verified before allowing access to the Control Rooms. All visitors shall be required to complete and sign the visitors' log, which shall include details of their name, their department or organization, the person who granted authorization and the time of entry and exit from the Centre.

12.6. All staff working in the Security Control Rooms shall be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisors will ensure that all staff are fully briefed and trained with respect to the functions, operational and administrative, arising from the use of CCTV/IP Cameras.

12.7. Recordings will normally be retained for twenty days from the date of recording, and then automatically overwritten. Once a hard drive has reached the end of its use it shall be erased prior to disposal and the log shall be updated accordingly.

12.8. All access to the recording shall be recorded in the access log as specified by the standard operating procedures.

12.9. Disclosure of recorded material will only be made to law enforcement agencies in strict accordance with the purpose of the request and should be approved by the Principal.

12.10 A person whose image has been entered and retained and who wishes access to the data must apply in writing to the Principal. The Principal has the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

12.10. All documented procedures shall be kept under review and a report periodically made to the Executive Committee.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

13.0. POLICY ON TRANSFERRING AND DOWNLOADING

13.1. Transferring copyrighted materials to or from the Institute systems without express consent of the owner is a violation of international law. In addition, use of the Internet for commercial gain or profit is not allowed from an educational site. If done so, it shall be the sole responsibility of the user. Downloading of copyrighted movies/books/games is punishable and receipt of any such complaints will initiate appropriate disciplinary action.

13.2. Downloading and installing of new software has to be done with the explicit consent of the Dean/Head of the Department. Installation of unlicensed software on KITSW systems, or on individual machines connected to the network, is strictly prohibited.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

14.0. POLICY ON BLOGGING AND WEBSITE CREATION

14.1. Students, faculty and other employees shall not engage in any form of blogging that may affect the prestige and image of the Institute.
14.2. Privacy policy mentioned earlier is applied in the case of blogging
14.3. Any blogging activity is to be done in a professional manner and the concerned person shall be held responsible if such activity affects his/her routine work.
14.4. Students, faculty and other employees shall not attribute personal statements and opinions or beliefs while blogging using KITSW facilities.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.

15.0. INFORMATION RETENTION AND DISPOSAL

It is essential to address the retention and disposal of information/data across KITSW in astandard manner, fulfilling statutory requirements.

Since no one person or unit is responsible for retention of information across the Institute, users across the community share the responsibility in adhering to this policy. Eachdepartment is responsible to establish appropriate retention period and practices to manage the same effectively in consultation with IITSC.

15.1. Each department must implement its information management practices:
15.2. To ensure the management practices are consistent with the policy;
15.3. To educate the staff and students within the department in understanding sound information management practices;
15.4. To ensure that information is retained in a readable format regardless of changes in technology or equipment obsolescence by
- printing out the documents and saving to a file system,
- maintaining the old equipment and software applications
- migrating the records to a new technology;

15.5. To preserve inactive records of historic value and if necessary transfer such recordsto the Institute archives;
15.6. To destroy inactive records that have no archival value upon expiry of the retention period;
15.7. To ensure restricted access to confidential files;
15.8. To ensure that outside suppliers/vendors used for record storage follow the Institute Retention policy.
15.9. Information/ Data needs to be disposed in accordance with the policy of retention.

Violation of any one of the above mentioned clauses shall lead to penal/legal action including termination from service and dismissal, depending on the severity of the case.