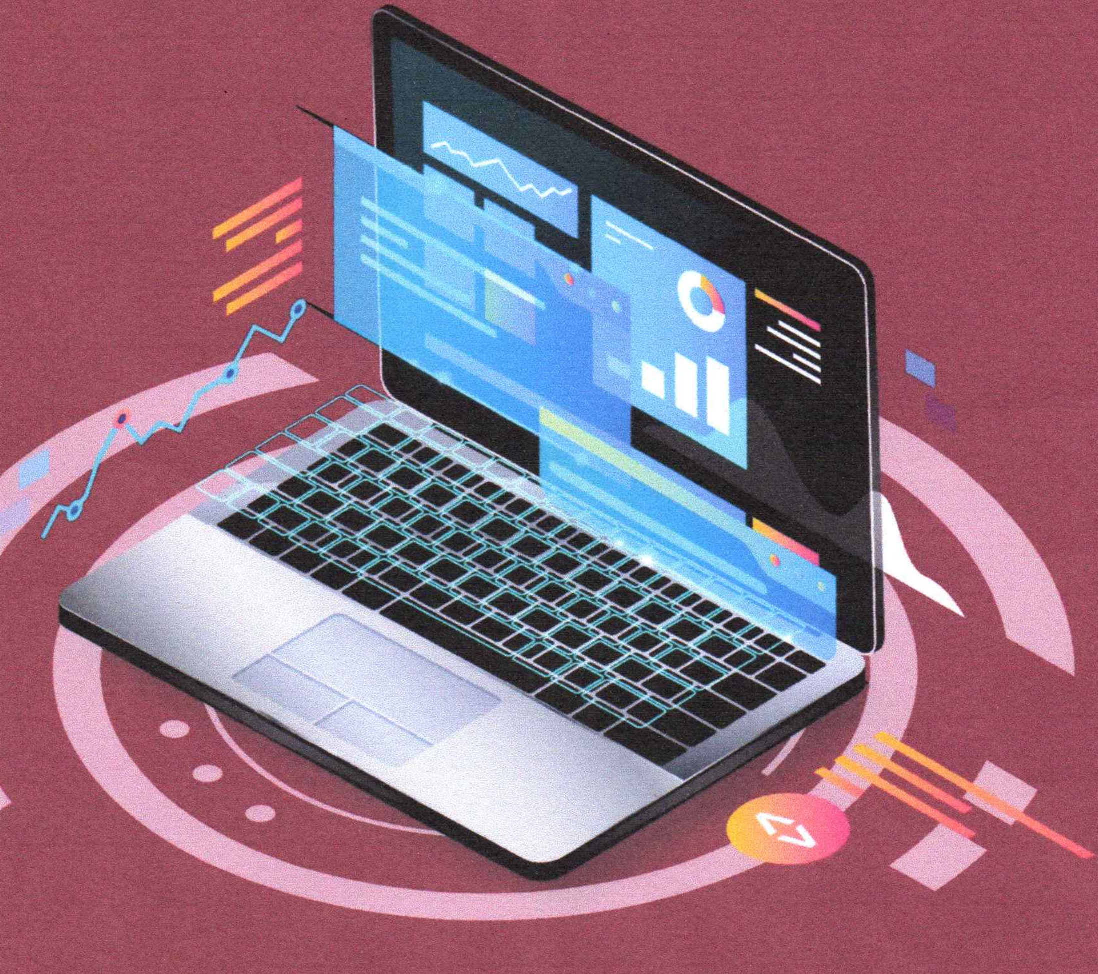
KAZIRANGA UNIVERSITY

KNOWLEDGE & BEYOND



IT POLICY

The Assam Kaziranga University IT Policy

Contents

Scope:

This policy applies to all employees and students of The Assam Kaziranga University who utilize company-owned, personally owned but operated for official use, or publicly-accessible PDA-based technology to access the organization's data and networks via wired and wireless means. Such access to enterprise IT resources is a privilege, not a right. Consequently, employment at The Assam Kaziranga University, does not automatically guarantee the granting of these privileges; and all access to IT resources is only need based. Addition of new hardware, software, and/or related components to provide access to resources /services operated by The Assam Kaziranga University will be managed at the sole discretion of The University Management. Non-sanctioned installations of computing Devices, related hardware, software, and/or related components, or use of same within the University premises, or to gain access to university computing resources, are strictly forbidden. This policy overrides any previously implemented policies dealing specifically with network access, wireless access, and remote access to the enterprise network, resources and services operated by The University.

Introduction:

Computer information systems and networks are an integral part of the university. The University has made a substantial investment in human and financial resources to create these systems. The enclosed policies and directives have been established in order to protect this investment, safeguard the information contained within these systems and reduce business and legal risk. Violations of this policy may result in disciplinary action.

Administration:

*The **IT Department** is responsible for the administration of this policy. Responsibilities include the development and maintenance of written standards and procedures necessary to ensure implementation of and compliance with these policy directives. Also to provide support and guidance to employees to fulfill their responsibilities under this directive.*

*Each **employee** shall be responsible for all computer transactions that are made with his/her User ID and password, not disclose passwords to others and adhere to procedures developed by the IT Department. Each Employee at the time of joining the organization is liable to accept the terms and conditions laid in this policy without which access to IT services is prohibited.*

Debdeep

ASSAM KAZIRANGA UNIVERSITY * JORHAT * KU

The Human Resource Department shall create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy. The HR shall notify IT promptly whenever an employee leaves the university so that his/her access can be revoked.

Device /Hardware Policy:

1.1 Whenever any employee requests hardware with the necessary supporting software they should apply to IT manager through the Dean and HOD of the respective schools/Department.

1.2 On exit it is mandatory for employees to obtain NOC from the IT department after returning the assets ingood condition. University does not allow transfer of assets on exit or otherwise in employeesname. Market value of the asset shall be deducted from the full and final in case an employee on exit fails to submit the assets to IT in good condition. In case of damage, Charges forrepairs beyond normal wear and tear to be recovered from the employee in full.

1.3 Computers and printers procured by the University are to be used for official purposes only. Under no circumstances may employees use their official computer for personal purpose.

1.4 The off-premises use of computers to access the university services, Data and networksare governed by the same policies as on premise use.

1.5 Certain devices, such as laptops, USB drives, mobile, tablets, portable projectors andcameras are by their nature portable. Employees to whom such devices are issued assume a special responsibility to guard them against theft, loss or damage. Loss or damage charges due to negligence shall be deducted from the employee.

1.6 In case of damage or loss, it is the employee's responsibility to inform the IT and concerned finance team immediately after the incident occurs. University does not permit the employee to arrange repair in part or full of any IT equipment without IT authorization. No
reimbursement will be allowed or entertained in case employees arranges repair on his own without prior authorization from the IT department.

Physical Security:

It is imperative to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

2.1 Employees shall exercise care to safeguard the equipment assigned to them. Charges for Breakage/physical damages/theft due to negligence to be recovered from the employee.

2.2 All Desktop Computers and printers to be protected by an uninterruptible power supply (UPS). Employee to ensure his/her desktop is always on a UPS and ensure the desktop is switched off before UPS runs out of backup to avoid damage due to abnormal shutdown.

ASSAM KAZIRANGA UNIVERSITY * JORHAT *

2.3 Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.

2.4 Employees shall not perform equipment installations, disconnections, modifications, and relocations on their own and not force the IT staff to perform these without approvals.

2.5 Employees shall not take shared portable equipment out of theoffice without the informed consent of the IT manager. Employees must sign out theequipment and note the purpose for which it will be used. In case allowed; such equipmentshall be solely used for official purpose after the office hours or otherwise.

2.6 To safeguard IT equipment and prevent data loss by means of theft, The University has deployed human security guards to man the gates; employees at all times shall cooperate with all security measures employed from time to time.

Copyrights and License Agreements:

3.1 It is the responsibility of the employee to comply with all laws regarding intellectual property. The university and employee are legally bound to comply with the Copyright Act and all proprietary software license agreements.

3.2 This policy applies to all software that is owned by university, licensed to university, or developed using university resources by employees or vendors. All persons who make use of any or all of university software or hardware are subject to the policies defined herein.

3.3 Employees shall not install software unless authorized by the IT department. Only software that islicensed to or owned by the university is to be installed on university computers. Staff shall notcopy or download software without proper authorization.

3.4 Software available on the internet or acquired through other sources in no way means that license compliance is not a must. Freeware / shareware / unlicensed software or tools without prior consent from authorized personnel shall not be used or installed on university systems.

E-mail and Internet Policy:

Acceptable Uses of the Internet and University E-mail:

Note: Internet is a paid resource and therefore shall be used only for business work.

4.1 E-mail access is controlled through individual accounts and passwords.
It is the responsibility of the employee to protect the confidentiality of their account and password information.

4.2 University encourages the use of the Internet and e-mail because it makes communication more efficient and effective. Occasional and reasonable personal use of university's Internet and email services is permitted, provided that this does not interfere with work performance. However, Internet service and e-mail are the University property.

*Use of any tools/enhancements like **torrents** and bandwidth accelerators that affect the performance of internet/bandwidth is not allowed.*

4.4 Though university has taken due care to safeguard its computers from viruses and attacks like hacking; still ignorance or visiting certain sites that contain malicious code may lead to a major security breach. Thus it is the employee responsibility to comply with safe guard measures.

4.5 Every employee has a responsibility to maintain and enhance the University's public image and to use university e-mail and Internet access in a productive manner.
Note: University has established the following guidelines for using e-mail and the Internet. Any unauthorized or improper use of e-mail or the Internet is not acceptable and will not be permitted.

4.6 The university e-mail and Internet access may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or materials that are obscene or X-rated. Harassment of any kind is prohibited.

4.7 No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual orientation to be transmitted or forwarded using the university email system.

4.8 No abusive, profane or offensive language may be transmitted through university's e-mail or Internet system. Company's harassment policy applies in full to e-mail and Internet use.
Employees do not have a personal privacy right regarding any matter created, received, stored or sent from or on the university's e-mail or Internet system or computers.

4.9 University's e-mail and Internet system also may not be used for any other purpose that is illegal, against university policy or contrary to university's best interest. Solicitation of non- university business or any use of university e-mail or Internet system for personal gain is prohibited.

4.10 Users shall not carry out any objectionable, frivolous or illegal activity on the internet that shall damage the university 's business or its image.

4.11 Users shall not post to public discussion groups, chat rooms or other public forums representing the university on the Internet unless pre authorizedby the university.

4.12 Users shall not send on the internet, any information other than job description as agreed between the employee and employer, thedisclosure of which may in any case cause harm or loss to either the university's or its customers' reputation.

4.13 The use of following is prohibited,
oDownload executable files.
oDownload through torrents/accelerators.

ASSAM KAZIRANGA UNIVERSITY
KU
* JORHAT *

oUnreasonable use of sites related to Social media, sports, finance, news, gaming and HR (jobs).
oUnreasonable use of webmail services like yahoo, Gmail, rediff, Hotmail etc. (All those who need to exchange mails over internet)
oUse of anonymizers to bypass University security policy.

Note: Work related access to some of the sites will only be provided subject to IT and functional head approval.

4.14 Users shall not attempt to circumvent or subvert security measures on either the university's network resources or any other system connected to or accessible through the internet.

4.15 Data Card for Internet access after office hours shall be provided on a "need to use" basis.
Anyone who requires it shall be given access after appropriate authorization. Such access shall be reviewed periodically by the IT Department.

Rules for Electronic and Voice Communications:
4.16 Each employee is responsible for the content of all text, audio, or images that he or she places on or sends over the university's e-mail or Internet system.

4.17 Employees may not hide their identities or represent that any e-mail or other electronic communications were sent from someone else or someone from another university.
4.18 Employees must include their name in all messages communicated on university's e-mail or Internet system.
4.19 Any messages or information sent by an employee to another individual outside university via university e-mail or Internet system (including bulletin boards, online services or Internet sites) are statements that reflect on university. Despite personal "disclaimers" in electronic messages, any statements may be tied to university.
4.20 All communications sent by employees via university's e-mail or Internet system must comply with all university policies and may not disclose any confidential or proprietary university information.

4.21 If employees receive an unsolicited e-mail from an outside university that appears to violate this policy, the employee should notify his or her superior immediately. Similarly, if any
employee accidentally accesses an inappropriate website in the normal course of business, the employee should notify his or her superior immediately.

4.22 The mobile phones and IP phones are solely provided to be available employees where the department(s) (Finance, HR, IT etc.) is serving internal customers
(employees) to enhance the business outcome. Each employee is responsible for the content audio, text messages, mms or images that he sends over university 's voice communication system.

Downloading/Uploading Software:

4.23 To prevent the downloading of computer viruses that could contaminate the e-mail or Internet system, no employee may download software from the Internet without prior authorization.

4.24 Any and all software that is downloaded from the Internet must be registered to university.
For authorization, please contact the system administrator.

*4.25 **Following is prohibited for download,***
□ Entertainment software or games, or playing games over the internet.
□ Images or videos unless there is an explicit business-related use for the material.
□ Display any kind of sexually explicit image or document on any University system.
□ Sexually explicit material shall not be accessed, attempted to be accessed, archived, stored, distributed, edited, or recorded using university network or computing resources.

4.26 Following is prohibited from upload without authorization,
□ Any software licensed to university
□ Data owned or licensed by university
□ Documents classified as university Proprietary, Confidential or Internal Use, without explicit authorization.

Computer Virus Security:

4.27 The IT shall install and maintain appropriate antivirus software on all computers, respond to all virus attacks, destroy any virus detected, and document each incident.

4.28 Employees shall not knowingly introduce a computer virus into university computers nor loadusb or executable files unless approved by the IT Coordinator. Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY notify the IT administrator.

Endpoint Data Security:

University has identified critical users whose data loss due to Drive Crashes, theft or accidental deletion may lead to business loss. Such employees have been provided with an automated cloud backup solution (Google Drive) to backup all critical data to the cloud. Employees need to ensure that they save critical data to G-drive.

4.28 Ensure only official data is getting backed up. Any personal data like movies/audio files are not allowed and can be deleted by IT staff without notice.
4.31 The data belongs to the university and an exit employee has to ensure the data is handed over to the respective HOD. Any deletion of such data may lead to legal action against the
employee.

Access Codes and Passwords:

4.36 The confidentiality and integrity of data stored on university computer systems must be

ASSAM KAZIRANGA UNIVERSITY
KU
* JORHAT *

protected by Controls to ensure that only authorized employees have access.

4.37 Access shall be restricted to those capabilities that are appropriate to each employee's job duties. Passwords shall not be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved.

4.38 Passwords should not identify an employee's name, address, date of birth, username, nickname, or any term that could easily be guessed by someone.

4.39 Passwords are not to be displayed or concealed on your workspace.

4.40 Password should be changed if an employee suspects foul play.
The computing devices used contain vital university information/data; employee shall ensure a strong password to avoid sabotage.
University 's password policy will address the passwords for the following IT systems,
□ Network and client operating system
□ Gmail.
□ Servers, Switches, Firewall and Routers
□ Websites
□ SBL ERP/ CRM.

4.41 Administrative Passwords:
□ Administrative passwords are only to be used by the IT administrator responsible for the service.
□ These passwords are subject to stringent composition, frequent change, and limited access. This includes passwords for routers, switches, Wider Area Network links, firewalls, servers, Internet connections, administrative-level network operating system accounts, and any other IT resource.

4.42 SOP for posting on KU's Social Media:
1. Email request: Share a formal email request with the subject line "Required social Media Posting"
2. Required Format: In the email request please give out the following details:
-Name of the Event:
-Description of th event:
-Details/Link (If available)
-Level of Event: Internal-University, Outside university, City level, National Level, International Level
3. Photos/Videos: Please attach the photos/videos/poster for the event in the same email.
4. Voice of language- The voice of KU's social media is from student's perspective. All the posters, captions and other communication that goes out from KU's digital handles will be from first person perspective of student's of KU.
5. Special Request: If a special poster design is required, please share a special request in the email for a poster design along with the information required in the poster.

ASSAM KAZIRANGA UNIVERSITY
KU
* JORHAT *

Dos and Don'ts for Social Media design KU

Dos:

1. Margin size - Using the grids, we leave about 1-2 pixels for safe space to place the logo.

2. Logo placement - should be ideally placed on the top (left & right), keeping in mind the grid and text.

3. Logo size - should be within the grids provided (ranging from 5-6 pixels)

4. Always write sources if mentioning any facts and stats.

Don'ts:

1. Not candid, Staged Looking, straight in the camera.

2. Can't use only emblem with "KU" written on it.

3. Don't post offensive and political stuffs.

ASSAM KAZIRANGA UNIVERSITY * JORHAT *

KU