Information Technology Resource Usage પોલીસીના અમલીકરણ બાબત.

જૂનાગઢ કૃષિ યુનિવર્સિટી
જૂનાગઢ

જાહેરનામુ

આથી સબંધ કર્તા સર્વેને જણાવવામાં આવે છે કે, તા.૦૮.૦૪.૨૦૧૬ના રોજ જૂનાગઢ ખાતે મળેલ જૂનાગઢ કૃષિ યુનિવર્સિટીના વિદ્યાપરિષદની ૩૬મી બેઠકની કાર્યનોંધના મુદ્દા નં. ૩૬.૧૦ તથા તા.૨૨.૦૪.૨૦૧૬ના રોજ જૂનાગઢ ખાતે મળેલ જૂનાગઢ કૃષિ યુનિવર્સિટીના નિયામક મંડળની ૪૧મી બેઠકની કાર્યનોંધના **મુદ્દા નં. ૪૧.૧૦ થી Information Technology Resource Usage પોલીસીના અમલીકરણ બાબતે** નીચે મુજબ ઠરાવેલ છે.

"આથી ઠરાવવામાં આવે છે કે, જૂનાગઢ કૃષિ યુનિવર્સિટી દ્વારા Information Technology Resource નો યોગ્ય હેતુ અનુસાર ઉપયોગ થાય તેમજ અયોગ્ય અને બિન અધિકૃત ઉપયોગ અટકાવવા Government of India દ્વારા બહાર પાડવામાં આવેલ Gazette Notification of Policy on Use of IT Resources of Government of India, F.No.2(22)/ 2013-EG-II (Vol.II-B), Dt.19.02.2015 મુજબની માર્ગદર્શીકાની યુનિવર્સિટીના અધિકારી/ કર્મચારીશ્રીઓ તેમજ વિદ્યાર્થીઓ માટે અમલવારી કરવાની મંજુરી આપવામાં આવે છે."

(એન.કે. ધમસાણીયા)
કુલસચિવ

જા.નં.જૂકૃયુ/૨જી/આઇ.ટી./આઈ.ટી.પોલીસી/ ૨૦૨-૨૬૬/૨૦૧૬ તા.૦૭.૦૫.૨૦૧૬

નકલ સવિનય રવાનાઃ-
1. નિયામક મંડળના તમામ સભ્યશ્રીઓ તરફ.
2. માન. કુલપતિશ્રીના રહસ્ય સચિવશ્રી, જૂનાગઢ કૃષિ યુનિવર્સિટી, જૂનાગઢ
3. આ યુનિવર્સિટીના તમામ યુનિટ / સબ યુનિટ અધિકારીશ્રીઓને ઉકત વિગતે E-Mail દ્વારા જાણ કરવા સારૂ.

નકલ રવાનાઃ-
1. કુલસચિવશ્રીના રહસ્ય સચિવશ્રી, જૂનાગઢ કૃષિ યુનિવર્સિટી, જૂનાગઢ
2. આ કચેરીની તમામ શાખાઓ તરફ.
3. જાહેરનામાં ફાઇલ.

Read: F. No. 2(22)/2013-EG-II, Ministry of Communication & Information Technology, Department of Electronics & Information Technology, Government of India.

POLICY ON USE OF INFORMATION TECHNOLOGY (IT) RESOURCES AND SERVICES

JUNAGADH AGRICULTURAL UNIVERSITY, JUNAGADH

GUJARAT – 362001

Contents

1. Introduction

1.1 Organization [1]Junagadh Agricultural University (JAU), provides IT resources and services to its employees and students to enhance their efficiency and productivity. These resources and services are meant as tools to access and process information related to their areas of work and help Organization's community to remain well informed and carry out their functions in an efficient and effective manner.

1.2 For the purpose of this policy, the term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices, peripherals like printers and scanners, and the software associated therewith etc. and the term 'IT Services' includes internet, web mail etc.

1.3 Misuse of these resources and services can result in unwanted risk and liabilities for the Organization. It is, therefore, expected that these resources and services are used primarily for Organization related purposes and in a lawful and ethical way.

2. Scope

This policy governs the usage of IT Resources and Services from an end user's [2] perspective**.** This policy is applicable to all users that use the IT Resources and Services of Organization.

3. Objective

The objective of this policy is to ensure proper access to and usage of Organization's IT resources and services and prevent their misuse. Use of IT resources and services provided by Organization implies the user's agreement to be governed by this policy.

4. Roles and Responsibilities

The following roles are required in Organization using its IT resources and services. The official identified for the task shall be responsible for the management of the IT resources and services deployed for the use of entire user base under their respective domain.

4.1 Competent Authority [3] as identified by Organization.

4.2 Designated Nodal Officer [4] as identified by Organization.

4.3 Implementing Agency [5] as identified by Organization.

5. Access to the Network

5.1 Access to Internet and Intranet

a) A user shall obtain one time approval from concerned Head of Unit/Sub Unit of the Organization and shall register the client system to IA before connecting the client system to the Organization's network.

b) It is strongly recommended that sensitive offices shall maintain two independent networks, i.e. Internet [6] and Intranet [7]. Both the networks shall not have any physical connection/devices between them. Users in such deployments shall have two access devices, i.e. desktops. One shall be connected to the internet and the other to the intranet. End point compliance [8] shall be implemented on both the networks to prevent unauthorized access to data.

c) Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security

5.2 Access to Organization Wireless Networks

For connecting to an Organization's wireless [9] network, user shall ensure the following:

a) A user shall register the access device and obtain one time approval from the competent authority before connecting the access device to the Organization's wireless network.

b) Wireless client systems and wireless devices shall not be allowed to connect to the Organization's wireless access points without due authentication.

c) To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

5.3 Filtering and blocking of sites:

a) IA may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.

b) IA may also block content which, in the opinion of the Organization concerned, is inappropriate or may adversely affect the productivity of the users.

6. Monitoring and Privacy

6.1 IA shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

6.2 IA, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on Organization provided devices under intimation to the user. This includes items such as files, e-mails, and Internet history etc.

6.3 IA may monitor user's online activities on Organization's network, subject to such Standard Operating Procedures as the Organization may lay down in this regard.

7. E-mail Access from the Organization's Network

7.1 Users shall refrain from using private e-mail servers from Organization's network.

7.2 E-mail service authorized by the Organization and implemented by the IA shall only be used for all official correspondence. For personal correspondence, users may use the name-based e-mail id assigned to them on the Organization authorized e-mail Service.

7.3 More details in this regard are provided in the **Annexure - I "Guidelines for Email Usage"**.

8. Access to Social Media Sites from Organization's Network

8.1 Use of social networking sites by Organization is governed by "Framework and Guidelines for use of Social Media [10] for Government Organizations" available at http://deity.gov.in.

8.2 User shall comply with all the applicable provisions under the IT Act 2000, while posting any data pertaining to the Organization on social networking sites.

8.3 User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.

8.4 User shall report any suspicious incident as soon as possible to the competent authority.

8.5 User shall always use high security settings on social networking sites.

8.6 User shall not post any material that is offensive, threatening, and obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or

is otherwise unlawful.

8.7 User shall not disclose or use any confidential information obtained in their capacity as an employee/contractor [11] of the Organization.

8.8 User shall not make any comment or post any material that might otherwise cause damage to the Organization's reputation.

9. Use of IT Devices Issued by Organization and/or privately owned in Organization

IT devices issued by the Organization to a user shall be primarily used for Organization related purposes and in a lawful and ethical way and shall be governed by the guidelines mentioned in **Annexure - II "Guidelines for Use of IT Devices on Network".**

9.1 Users are not allowed to use privately owned IT devices in Organization except prior permission is taken from the concerned Head of Unit/Sub Unit of the Organization and follows the appropriate guidelines mentioned in Annexure II.

10. Responsibility of User Organization

10.1 Policy Compliance

a) Organization shall implement appropriate controls to ensure compliance with this policy by their users.
IA shall provide necessary support in this regard.

b) A periodic reporting mechanism to ensure the compliance of this policy shall be established by the competent authority of the Organization.

c) Nodal Officer of the user Organization shall ensure resolution of all incidents related to the security aspects of this policy by users. IA shall provide the requisite support in this regard.

d) User shall not install any IT resources on the network without consultation with the IA.

10.2 Policy Dissemination

a) Competent Authority of the user Organization should ensure proper dissemination of this policy.

b) Orientation programs for new recruits shall include a session on this policy.

11. Security Incident Management Process

11.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Organization data.

11.2 IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of that Organization.

11.3 Any security incident [12] noticed must immediately be brought to the notice of the IA.

12. Scrutiny/Release of logs

12.1 Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any Network Security Resource maintained by IA, to Law Enforcement agencies and other Organizations by the IA shall be done as per the IT Act 2000 and other applicable laws.

12.2 IA shall neither accept nor act on the request from any other Organization without prior permission from competent authority for scrutiny or release of logs.

13. Intellectual Property

Material accessible through the IA's network, resources and services may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the Organization network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

14. Enforcement

14.1 This policy is applicable to all users of Organization. It is mandatory for all users to adhere to the provisions of this policy.

14.2 Organization shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the Organizations in this regard.

15. Deactivation

15.1 In case of any threat to security of the Organization's systems or network from the resources and services being used by a user, the resources and services being used may be deactivated immediately by the IA.

15.2 Subsequent to such deactivation, the concerned user and the competent authority of Organization shall be informed.

16. Review

Future changes in this Policy, as deemed necessary, shall be made by Implementing Agency with approval of the Competent Authority.

ANNEXURE-I

GUIDELINES FOR EMAIL USAGE

1. Introduction

The Organization uses e-mail as a major mode of communication. Organization has formulated the **"Policy on Use of IT Resources and Services"**. This document supports the implementation of this policy by providing the best practices related to use of e-mail services.

2. Basic requirements of Organization e-mail Service

2.1 Security

a) Considering the security concerns with regard to a sensitive deployment like e-mail, it is recommended to use e-mail services provide by the IA.

b) Organization should migrate their e-mail services to the centralized deployment of the IA for security reasons and uniform policy enforcement. For the purpose of continuity, the e-mail address of the Organization migrating their service to the IA deployment shall be retained as part of the migration process. Wherever it is technically feasible, data migration shall also be done.

c) Secure access to the Organization email service

I. It is recommended for users working in sensitive offices to use VPN[13]/OTP[14] for secure authentication as deemed appropriate by the competent authority

II. It is recommended that Organization's officials on long deputation/stationed abroad and handling sensitive information should use (VPN) / (OTP) for accessing Organization e-mail services as deemed appropriate by the competent authority.

d) From the perspective of security, the following shall be adhered to by all users of Organization e-mail service:

I. Relevant Policies framed by Ministry of Home Affairs, relating to classification, handling and security of information shall be followed.

II. Use of Digital Signature Certificate (DSC) [15] and encryption shall , be mandatory for sending e-mails deemed as classified and sensitive, in accordance with the relevant policies of Ministry of Home Affairs. Updation of current mobile numbers under the personal profile of users is mandatory for security reasons. The number would be used only for alerts and information regarding security sent by the IA. Updation of personal e-mail id (preferably from a service provider within India), in addition to the mobile number, shall also be mandatory in order to reach the user through an alternate means for sending alerts.

III. Users are recommended not to download e-mails from their official e-mail account, configured on the Organization's mail server, by configuring POP [16] or IMAP [17] on any other e-mail service provider. This implies that users should not provide their Organization e-mail account details (id and password) to their accounts on private e-mail service providers.

IV. Any e-mail addressed to a user, whose account has been deactivated /deleted, shall not be redirected to another e-mail address. Such e-mails

may contain contents that belong to the Organization and hence no e-mails shall be redirected.

V. The concerned nodal officer of the Organization shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User.

VI. In case a compromise of an e-mail id is detected, the IA reserves the right to reset the password of that particular e-mail id under intimation to the nodal officer.

VII. In case of a situation when a compromise of an email id impacts a large user base or the data security of the deployment, the IA shall reset the password of that email id. This action shall be taken on an immediate basis, and the information shall be provided to the user and the nodal officer subsequently.

VIII. Forwarding of classified/sensitive e-mail from the e-mail id provided by Organization to the Organization official's personal id outside the Organization e-mail service is not allowed due to security reasons. Official e-mail id provided by the IA can be used to communicate with any other user, whether private or public. However, the user must exercise due discretion on the contents that are being sent as part of the e-mail.

IX. Auto-save of password in the Organization e-mail service shall not be permitted due to security reasons.

2.2 E-mail Account Management

a) Based on the request of the user, IA may create two ids, one based on the designation and the other based on the name. Designation based id's are recommended for officers dealing with the public. Use of alphanumeric characters as part of the e-mail id is recommended for sensitive users as deemed appropriate by the competent authority.

b) Organization's officers who resign or superannuate after rendering at least 20 years of service shall be allowed to retain the name based e-mail address i.e. username@jau.in for one year post resignation or superannuation. Subsequently, a new e-mail address with the same user name but with a different domain address (for instance, username@pension.jau.in), may be provided by the IA for their entire life.

2.3 Delegated Admin Console

Organization can avail the "Delegated Admin Console" service from IA. Using the console, the authorized person of an Organization can create/delete/change the password of user ids under that respective domain as and when required without routing the request through IA.

2.4 E-mail Domain & Virtual Hosting

a) Organization provides virtual domain hosting for e-mail. If an Organization so desires, the IA can offer a domain of e-mail addresses as required by them. This implies that if an Organization requires an address resembling the website that they are operating, IA can provide the same.

b) By default, the address "username@jau.in" shall be assigned to the users.

c) Organization desirous of an e-mail address belonging to other sub domains (e.g. xxxx@pension.jau.in, yyyy@alumni.jau.in) need to forward their requests to the IA

2.5 Use of Secure Passwords

All users accessing the e-mail services must use strong passwords for security of their e-mail accounts.

2.6 Privacy

Users should ensure that e-mails are kept confidential. IA shall take all possible precautions on maintaining privacy. Users must ensure that information regarding their password or any other personal information is not shared with anyone.

3. Responsibilities of Users

3.1 Appropriate Use of E-mail Service

a) E-mail is provided as a professional resource to assist users in fulfilling their official duties. Designation based ids should be used for official communication and name based ids can be used for both official and personal communication.

b) Examples of inappropriate use of the e-mail service

I. Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.
II. Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.
III. Unauthorized access of the services. This includes the distribution of e-mails anonymously, use of other officers' user ids or using a false identity.
IV. Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.
V. Creation and exchange of information in violation of any laws, including copyright laws.
VI. Willful transmission of an e-mail containing a computer virus.
VII. Misrepresentation of the identity of the sender of an e-mail.
VIII. Use or attempt to use the accounts of others without their permission.
IX. Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing anti-national messages, sending e-mails with obscene material, etc.
X. Use of distribution lists for the purpose of sending e-mails that are personal in nature, such as personal functions, etc.

Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation [18] of the account. Further, such instances may also invite scrutiny by the investigating agencies depending on the nature of violation.

3.2 User's Role

a) The User is responsible for any data/e-mail that is transmitted using the Organization e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.

b) Sharing of passwords is prohibited.

c) The user's responsibility shall extend to the following:

I. Users shall be responsible for the activities carried out on their client systems, using the accounts assigned to them.
II. The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.
III. Back up of important files shall be taken by the user at regular intervals. The IA shall not restore the data lost due to user's actions.

4. Security Incident Management Process

4.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Organization data. Security incidents can be due to factors like malware, phishing [19], loss of a device, compromise of an e-mail id etc.

4.2 It shall be within the right of the IA to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service.

4.3 Any security incident, noticed or identified by a user must immediately be brought to the IA.

5. Deactivation

5.1 In case of threat to the security of the Organization service, the e-mail id being used to impact the service may be suspended or deactivated immediately by the IA.

5.2 Subsequent to deactivation, the concerned user and the competent authority of Organization shall be informed.

ANNEXURE-II

GUIDELINES FOR USE OF IT DEVICES ON NETWORK

1. Introduction:

Organization has formulated the **"Policy on Use of IT Resources and Services"**. This document supports the implementation of this policy by providing the best practices related to use of IT devices issued by the Organization or privately owned. These IT resources include desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners etc.

2. General Guidelines for IT resources

2.1 Software installed on IT resources must be licensed software.

2.2 Annual Maintenance Contract shall be made annually for IT resources which are not cover under warranty.

2.3 Cleanness at laboratory must be maintained.

3. Desktop Devices

3.1 Use and Ownership

Desktops shall normally be used only for transacting Organization work. Users shall exercise their own good judgment and discretion towards use of desktop devices for personal use to the minimum extent possible.

3.2 Security and Proprietary Information

a) User shall take prior approval from the competent authority to connect any access device to the Organization network.

b) User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords.

c) All active desktop computers shall be secured with a password-protected screensaver which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.

d) Users shall ensure that updated licensed virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.

e) User shall report any loss of data or accessories to the concerned Head of Unit/Sub Unit of the Organization.

f) User shall obtain authorization from the concerned Head of Unit/Sub Unit before taking any Organization issued desktop outside the premises of the Organization.

g) Users shall properly shut down the systems before leaving the office/laboratory.

h) In case an Organization does not have two networks, as recommended in the Policy on "Use of IT Resources and Services" Classified/ sensitive data shall not be stored on the desktop connected to the internet.

i) Users shall encrypt all sensitive information while storing it on the desktop.

j) The IA reserves the right to limit the user's client system as and when required.

k) Booting from removable media shall be disabled.

l) Users shall abide by instructions or procedures as directed by the IA from time to time.

m) If users suspect that their computer has been infected with a virus (e.g. it might

have become erratic or slow in response), it should be reported to the IA for corrective action.

n) The Annual Maintenance Contract with service providers should include a clause that Hard Disk should be retained by the Organization, even if it is faulty. While disposing the Hard disk it should be destroyed so that data cannot be retrieved.

3.3 Use of software on Desktop systems

a) Users shall not copy or install any software on desktop devices including privately owned shareware and freeware without the approval of the concerned head of Unit/Sub Unit of the Organization.

b) A list of allowed software shall be made available by the IA. Apart from the Software mentioned in the list, no other software will be installed on the client systems. Any addition to the list by the Organization should be done under intimation to IA.

3.4 Sharing of data

Users shall not share their account(s), passwords, security tokens (i.e. smartcard), Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

3.5 Use of network printers and scanners

a) User shall use a strong administrator password on the device to help defend against attacks and to prevent re-configuration by an unauthorized user.

b) Where the device supports Access Control Lists (ACLs), the devices shall be configured to block all traffic from outside the Organization's IP range.

c) IA may enable or disable FTP and telnet server on the printer as and when required.

d) User shall disable any protocol or service not required.

4. Use of Portable devices

Devices covered under this section include laptops, mobiles, iPads, tablets, PDAs etc. Appropriate rules for the desktop devices in clause 3 are also applicable on portable devices. Moreover, Use of such devices shall be governed by the following:

a) User shall be held responsible for any unauthorized usage of Organization issued access device by a third party.

b) Users shall keep the Organization issued devices with them at all times or store them in a secured location when not in use. User should not leave the devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).

c) User shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong.

d) User shall ensure that remote wipe feature is enabled on the Organization issued device, wherever technically feasible. Users shall not circumvent security features on their devices.

e) The concerned nodal officer of the Organization shall ensure that the latest licensed software, operating system, anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls shall be enabled, if possible.

f) Lost, stolen, or misplaced devices shall be immediately reported to the concerned Head of Unit/Sub Unit of the Organization.

g) Data transmissions from devices to the services on the Organization network shall be over an encrypted channel.

h) When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

5. External Storage Media:

Devices covered under this section include Organization issued CD/DVD's, USB storage devices etc. Use of these devices shall be governed by the following:

a) Use of external storage [20] media, by default shall not be allowed in the Organization network. If the use of external storage is necessary, due approval from the concerned Head of Unit/Sub Unit of the Organization shall be taken.

b) To use the external storage will be allowed as per the policies configured by the IA.

c) Users shall use only the media issued by the Organization for all official work. The user shall be responsible for the safe custody of devices and contents stored in the devices which are in their possession.

d) Classified data shall be encrypted before transferring to the designated USB device. The decrypting key shall not exist on the same device where encryption data exists.

e) Classified/ sensitive information shall be stored on separate portable media. User shall exercise extreme caution while handling such media.

f) Unused data on USB devices shall be cleaned through multiple pass process (like wipe/eraser software)

g) Users shall not allow USB device belonging to outsiders to be mounted on Organization systems.

5.1 Use of External storage media by a visitor

a) Competent authority shall ensure that process is in place that visitors to an Organization shall not be allowed to carry any portable media without permission.

b) If it is necessary to allow the visitor to use a USB memory device for any reason, it shall be used only on designated systems meant for presentation purpose. Under no circumstances the USB device belonging to visitors shall be mounted on systems that are connected and belong to the Organization network without prior permission of the concerned Head of Unit/Sub Unit of the Organization.

5.2 Authority issuing External storage devices of Organization shall adhere to the following:

a) The concerned Head of Unit/Sub Unit of an Organization shall ensure that process is in place to maintain records for procurement, issue, return, movement and destruction of the storage devices.

b) All obsolete USB devices shall be physically destroyed to avoid misuse.

c) Self-certification for verification of USB devices by individuals at regular intervals of 6 months shall be carried out by issuing authority to ensure that devices issued to them are under their safe custody.

GLOSSARY

S. No.	Term	Definition
1.	**Organization**	Junagadh Agricultural University (JAU), Junagadh
2.	**Users**	Refers to employees/contractual employees, guests/visitors and students of JAU who are accessing the JAU's IT resources and services
3.	**Competent Authority**	Hon. Vice Chancellor, JAU, Junagadh
4.	**Nodal Officer**	Director, Information Technology Cell, JAU, Junagadh responsible for all matters relating to this policy who will coordinate on behalf of the Organization
5.	**Implementing Agency (IA)**	Information Technology Cell, JAU, Junagadh A Body which will be responsible for ensuring compliance with this policy with reference to network services and managing all Organization's IT resources and services on behalf of Organization.
6.	**Internet**	Internet is a network of the interlinked computer networking worldwide, which is accessible to the general public. These interconnected computers work by transmitting data through a special type of packet switching which is known as the IP or the internet protocol
7.	**Intranet**	An intranet is a private network that is contained within an Organization. For the purpose of this policy, IT resources connected to an intranet and dealing with classified or sensitive data are not allowed to connect to internet.
8.	**End point compliance**	End point compliance is an approach to network protection that requires each computing device on a network to comply with certain standards before network access is granted. Endpoints can include desktops, laptops, smart phones, tablets etc.
9.	**Wireless**	Any type of computer network that uses wireless data connections for connecting network nodes. For the purpose of this policy, all the Organization's wireless networks will be deployed in a secure manner.
10.	**Social Media**	Applies to social networking sites, blogs, electronic newsletters, online forums, social networking sites, and other services that permit users to share information with others in a contemporaneous manner.
11.	**Contractor/contractual employees**	An employee who works under contract for Organization. A contract employee is hired for a specific job or assignment. A contract employee does not become a regular addition to the Organization staff and is not considered a permanent employee of Organization.

12.	**Security Incident**	Any adverse event which occurs on any part of the Organization data and results in security threat/breach of the data.
13.	**VPN**	A virtual private network extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network.
14.	**OTP**	A **one-time password** (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords.
15.	**DSC**	A digital **signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives the recipient reason to believe that the e-mail was created by a known sender, such that the sender cannot deny having sent the e-mail (authentication and non-repudiation) and that the e-mail was not altered in transit (integrity).
16.	**POP**	**POP i**s short for **P**ost **O**ffice **P**rotocol, a protocol used to retrieve e-mail from a mail server.
17.	**IMAP**	**IMAP** is short for "**The Internet Message Access Protocol",** a protocol used to retrieve e-mail from a remote mail server. Unlike POP, in IMAP, Messages are displayed on your local computer but are kept and stored on the mail server. IMAP allows you to sync your folders with the e-mail server which is not possible using POP.
18.	**Deactivation**	**Deactivation** of an account means that the account can no longer be accessed. All e-mails sent to a deactivated account shall bounce to the sender.
19.	**Phishing**	**Phishing** is a fraudulent attempt, usually made through e-mail, to steal a user's personal information. Phishing e-mails almost always tell a user to click a link that takes the user to a site from where the personal information is requested. Legitimate Organizations would never request this information via e-mail. Users should never click on a link. A user should always type a URL in the browser even if the link appears genuine**.**
20.	**External Storage**	In computing, external storage comprises devices that temporarily store information for transporting from computer to computer. Such devices are not permanently fixed inside a computer.