**GOKUL
GLOBAL
UNIVERSITY**
Approved By Govt. of Gujarat
(Recognized by UGC under Section 22 & 2(f) of 1956)
(Gujarat Private State University Act 4 of 2018)

IT POLICY

GOKUL
GLOBAL
UNIVERSITY
Approved By Govt. of Gujarat
(Recognized by UGC under Section 22 & 2(f) of 1956)
(Gujarat Private State University Act 4 of 2018)

INFORMATION TECHNOLOGY INFRASTRUCTURE USAGE POLICY

Introduction

Students, Teaching and Non - Teaching Staff, Management and visiting Guests and Research Fellowship Members of Gokul Global University availing computing, networking, and IT facilities are expected to abide by the following rules, which are intended to preserve the utility and flexibility of the system and protect the privacy and work of students and faculty.

General Rules

1. Students, Teaching and Non - Teaching Staff, Management and visiting Guests and Research Fellowship Members are authorized to use the computing, networking, and other IT facilities for academic purposes, official university business, and for personal purposes as long as such use does not violate any law or any university policy.

2. The University prohibits its users from gaining or enabling unauthorized access to forbidden IT resource on the University network. Any such attempt will not only be the violation of University Policy but may also violate national and international cyber laws, provisions under The Information Technology Act of India and infringe the principals of National Cyber Security Policy, and subject the user to both civil and criminal liability. However, the University reserves all the rights to access and analyze the IT resource and Information for any legal and/ or institutionally provisioned operation, on its own or through its affiliates.

3. The University prohibits its users from sending, viewing or downloading fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or University policy. Therefore, user's inhibitive discretion is solicited where category of certain content could be doubtful e.g. when such content is received through e-Mail etc. As a generalized policy, any contribution towards the destruction or distortion of congenial academic or work environment is prohibited.

4. Users must not violate various IPR and copyright law(s), and licensing policies as associated with copyrighted materials and software. Any unlawful file- sharing, use of any form of illegal or pirated or un-licensed software, on the University's IT resources (including individually owned IT resource being used under Institutional IT privileges) is strictly prohibited and any such act shall constitute a violation of the University policy.

5. University also recommends its students, faculty and office staff, to use Open Source Operating Systems (OS) and Processing Software (PS) such as Ubuntu/ CentOS or other and Libra Office/ OpenOffice/ WPS Office, respectively. Further, users of the computers sponsored directly or indirectly by Gokul Global University should migrate on the recommended OS & PS as their primary software and should generate expertise on it. In case of technical limitation in such adaptation, relaxation may be requested from competent authority on valid grounds.

GOKUL
GLOBAL
UNIVERSITY
Approved By Govt. of Gujarat
(Recognized by UGC under Section 22 & 2(f) of 1956)
(Gujarat Private State University Act 4 of 2018)

6. By agreeing to abide by the terms of use of various online media forums, the users are expected to adhere with the norms as prescribed by respective social networking websites, mailing lists, chat rooms, blogs, Unless a user has proper authorization, no user should attempt to gain access to information and disclose the same to self or other unauthorized users. The broader concept of data privacy must be honored by each user.

7. No user should attempt to vandalize, damage or change any data inappropriately, whether by accident or deliberately. The basic notion of trustworthiness of information resources must be preserved by all of its users. Any interference, disruption or encroachment in the University IT resources shall be a clear violation of the University policy.

8. No user should attempt to affect the availability of IT resource, whether accidently or deliberately.

9. As long as individual departments, Hostel, individual units etc. can retain consistency in compliance of the IT (Usage) Policy, Gokul Global University, they may further define and implement additional "conditions of use" for IT resources under their control. It will be the responsibility of the Units to publicize and enforce such conditions of use. In cases where use of external networks is involved, suitable policies can be practiced in compliance with the broad prerogatives of (Usage) Policy of the University.

10. As a part of certain investigation procedures, the University may be required to provide its IT information, resource and/ or records, in parts or full, to third parties. Also, for proper monitoring and optimal utilization of University IT resources, the University may review, analyze and audit its information records, without any prior notice to its Users. Further, the University may also seek services from third-party service providers. Accordingly, the users can only have reasonable expectation of privacy on the University's IT resources.

11. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, reconfigure, modify, or attach external devices to the systems.

12. No food or drink is permitted in the laboratories. Also making noise either through games/music/movies or talking and/ or singing loudly (the list is not exhaustive) is prohibited.

13. Violations of policy will be treated as academic misconduct, misdemeanor, or indiscipline as appropriate. Depending upon the nature of the violation, the University authorities may take an action.

14. The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through the news groups.

**GOKUL
GLOBAL
UNIVERSITY**
Approved By Govt. of Gujarat
(Recognized by UGC under Section 22 & 2(f) of 1956)
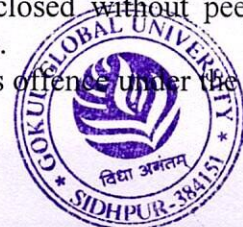(Gujarat Private State University Act 4 of 2018)

Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal University communications are official notices from the University to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general University messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the email facility by logging with their User **ID** and **password**. For obtaining the university's email account, user may contact HR for email account and default password by submitting an application in a prescribed proforma.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

1. The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
2. Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
3. While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
4. User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
5. User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have potential to damage the valuable information on your computer.
6. Users should configure messaging software on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.
7. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
8. User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
9. While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
10. Impersonating email account of others will be taken as a serious offence under the university IT

GOKUL
GLOBAL
UNIVERSITY
Approved By Govt. of Gujarat
(Recognized by UGC under Section 22 & 2(f) of 1956)
(Gujarat Private State University Act 4 of 2018)

security policy.

11. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.
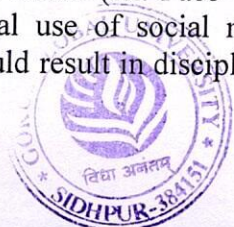
Social Media Policy

POLICY

- This policy provides guidance for employee use of social media, which should be broadly understood for purposes of this policy to include What's App, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others.

PROCEDURES

- The following principles apply to professional use of social media on behalf of Gokul Global University as well as personal use of social media when referencing Gokul Global University.
- Employees need to know and adhere when using social media in reference to Gokul Global University.
- Employees should be aware of the effect their actions may have on their images, as well as Gokul Global University's Image. The information that employees post or publish may be public information for a long time.
- Employees should be aware that The University may observe content and information made available by employees through social media. Employees should use their best judgment in posting material that is neither inappropriate nor harmful to Gokul Global University, its employees, or customers.
- Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile work environment or which may hurt religious & Sentiments of any one or any Community.
- Employees are not to publish post or release any information that is considered confidential or not public. If there are questions about what is considered confidential, employees should check with the Human Resources Department.
- Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to the authorized University spokespersons.
- If employees encounter a situation while using social media that threaten to become antagonistic, employees should disengage from the dialogue in a polite manner and seek the advice of Human Resources Department.
- Employees should get appropriate permission before they refer to or post images of current or former employees, members, vendors or suppliers. Additionally, employees should get appropriate permission to use a third party's copyrights, copyrighted material, trademarks, service marks or other intellectual property.
- Social media use shouldn't interfere with employee's responsibilities at Gokul Global University. The University's computer systems are to be used for business purposes only. When using University's computer systems, use of social media for business purposes is allowed only to those staff whose work profile requires use of social media (ex: Face book, Twitter, LinkedIn, What's app, Instagram, any other) , but personal use of social media networks or personal blogging of online content is discouraged and could result in disciplinary action.

GOKUL
GLOBAL
UNIVERSITY
Approved By Govt. of Gujarat
(Recognized by UGC under Section 22 & 2(f) of 1956)
(Gujarat Private State University Act 4 of 2019)

- Subject to applicable law, after---hours online activity that violates or any other company policy may subject an employee to disciplinary action or termination.
- It is highly recommended that employees keep Gokul Global University related social media accounts separate from personal accounts, if Possible.
- Employees should not use any type of offensive /abusive language or make any comment/post any photo which is not in line with their image as a faculty/Teacher (As they belong to a very respected community).

Responsibilities of University IT Center

A. Maintenance of Computer Hardware & Peripherals

IT CENTER is responsible for maintenance of the university owned computer systems and peripherals that are either under warranty or annual maintenance contract, and whose responsibility has officially been entrusted to this Cell.

B. Receiving Complaints

IT CENTER may receive complaints from INTERNET UNIT, if any of the particular computer systems are causing network related problems.

IT CENTER may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.

The designated person in IT CENTER receives complaints from the users/INTERNET UNIT of these computer systems and coordinates with the service engineers of the respective brands of the computer systems to resolve the problem within a reasonable time limit.

C. Scope of Service

IT CENTER will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the university and was loaded by the company.

D. Installation of Un-authorised Software

IT CENTER or its service engineers should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests.

E. Reporting IT Policy Violation Incidents

If IT CENTER or its service engineers come across any applications that are interfering with the network operations or with the IT policies of the university, such incidents should be brought to the notice of the INTERNET UNIT and university authorities.

F. Reporting incidents related to Network Operations

When the network port of any particular computer system is turned off due to virus or related activity that is affecting the network performance, the same will be informed to the IT CENTER by INTERNET UNIT. After taking necessary corrective action IT CENTER or service engineers should inform INTERNET UNIT about the same, so that the port can be turned on by them.

G. Rebuilding the Computer System

When the service engineers reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers should make sure that its latest engine and pattern files are also downloaded from the net.

Further, before reformatting the hard disk, dump of only the data files should be taken for restoring

it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.

H. Coordination with INTERNET UNIT

Where there is an element of doubt as to a particular problem on the computer connected to the network is related to the network or the software installed or hardware malfunctioning IT CENTER/service engineer may coordinate with INTERNET UNIT staff to resolve the problem with joint effort. This task should not be left to the individual user.

Guidelines for Desktop Users

These guidelines are meant for all members of the University Network User Community and users of the University network.

Due to the increase in hacker activity on campus, University IT Policy has put together recommendations to strengthen desktop security.

The following recommendations include:

1. All desktop computers & Laptops should have the latest version of antivirus such as Symantec Anti- Virus (PC) and should retain the setting that schedules regular updates of virus definitions from the central server.
2. When a desktop computer & Laptop is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend once in a week cycle for each machine. Whenever possible, security policies should be set at the server level and applied to the desktop machines.
3. All Windows desktops & Laptops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default.
4. The password should be difficult to break. Password, defined as:
i. must be minimum of 6-8 characters in length
ii. must include punctuation such as ! $ % & * , . ? + - =
iii. must start and end with letters
iv. must not include the characters # @ ' " `
v. must be new, not used before
vi. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No.etc.
5. passwords should be changed periodically and also when suspected that it is known to others.
i. Never use 'NOPASS' as your password
ii. Do not leave password blank and
Make it a point to change default passwords given by the software at the time of installation
6. The password for the user login should follow the same parameters outlined above.
7. The guest account should be disabled.
8. New machines should activate the built-in firewall.
9. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.
10. All the software on the compromised computer systems should be re-installed from scratch
11. In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.
12. In addition to the above suggestions, INTERNET UNIT recommends a regular backup strategy. It

should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise.

Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

13. If a machine is compromised, INTERNET UNIT will shut the port off. This will isolate the computer, until it is repaired as per the guidelines. At that time, the port will be turned back on.

14. For departments with their own subnets and administrators, standard filters can be applied at the subnet level. If a department has its own servers, INTERNET UNIT technical personnel can scan the servers for vulnerabilities upon request.

Video Surveillance Policy

The system

1.1   The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.

1.2   Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

1.3   Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Cemera installation is in use.

1.4   Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

2.0   Purpose of the system

2.1   The system has been installed by university with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment
The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking

2.2   Covert recording

2.2.1   Covert cameras may be used under the following circumstances on the written authorisation or request of the Senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

2.2.2   Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.

2.2.3   The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

3.0   The Security Control Room

3.1   Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

3.2   No unauthorised access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorised members of senior management, police officers and any other person with statutory powers of entry.

3.3   Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorisation from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Control Room.

3.4   Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorisation.

**GOKUL
GLOBAL
UNIVERSITY**
Approved By Govt. of Gujarat
(Recognized by UGC under Section 22 & 2(f) of 1956)
(Gujarat Private State University Act 4 of 2018)

4.0   Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Cemera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Cemera.

5.0   Recording

5.1   Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

5.2   Images will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

5.3   All hard drives and recorders shall remain the property of university until disposal and destruction.

6.0   Access to images

6.1   All access to images will be recorded in the Access Log as specified in the Procedures Manual

6.2   Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

6.3 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

CCTV/IP Cemera digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by C.C.T.V. /IP Cemera is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. Subject Access Request Forms are obtainable from

GOKUL
GLOBAL
UNIVERSITY
Approved By Govt. of Gujarat
(Recognized by UGC under Section 22 & 2(f) of 1956)
(Gujarat Private State University Act 4 of 2013)

the Security Office, between the hours of 1020 and 1400 and 1430 to 1800 Monday to Saturday (except Second and fourth Saturday), except when university is

7.0 Request to prevent processing

7.1 An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

7.2 All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Data Protection Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

8.0 Complaints

8.1 It is recognised that members of University and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralised Complaints Procedure by obtaining and completing a University Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer, These rights do not alter the existing rights of members of University or others under any relevant grievance or disciplinary procedures.

DECELARATION:

I,_____, Employee ID/Enrollment No:_____, do hereby declare that as a Employee / student in Gokul Global University will abide by the above-mentioned rules. I accept that any act of mine that can be considered to be the violation of the policy will be dealt with as mentioned in rule.

Date:_____   Signature: _____

Registrar
Gokul Global University, Sidhpur