GOA UNIVERSITY
IT POLICY

(Release: APRIL, 2016)

Contents

Office Order 2

A. Introduction 4

B. Aim 4

C. Purpose 4

D. Implementation 5

E. Coverage 5

F. Applicability 5

Rules and Regulations for IT services at GU 6

1. Computers, Digital Devices & Software: 6

1.1 Purchase and Installation 6

1.2 Maintenance 7

1.2.1 Maintenance Procedure 7

2. Uninterrupted Power Supply (UPS) 8

3. Shifting of Computers 8

4. Disaster Preparedness & Data Back-up 8

5. Usage of GUNET 8

6. Website Content Management 10

7. GUNET Management (Intranet & Internet) 11

8. E-Repositories 14

~~11.1~~ 8.1 Creation and Maintenance: 14

~~11.2~~ 8.2 Content: 14

9. Recommended fees for Internet Access 14

गोंय विद्यापीठ
ताळगांव पठार
गोंय - ४०३ २०६
फोन : ०८३२ - ६५१९०४८ / ६५१९३०२
फॅक्स : +०९१-८३२-२४५११८४ / २४५२८८९

Goa University
Taleigao Plateau, Goa - 403 206
Tel : 0832-6519048/6519302
Fax : + 091- 832-2451184/2452889
E.mail : registrar@unigoa.ac.in
Website : www.unigoa.ac.in

(Accredited by NAAC with Grade 'A')

Ref. No. 7/106/15-CC/3737 Date: 09.12.2015

ORDER

The Vice Chancellor is pleased to constitute a committee consisting of following members for preparing the IT Policy for Goa University.

1.	Prof. P. Mukhopadhyay Department of Economics	Chairman
2.	Prof. Kausthubh Priolkar Department of Physics	Member
3.	Dr. Gopakumar V University Librarian	Member
4.	Shri Ramrao Wagh Department of Computer Science & Technology	Member
5.	Shri Donald Rodrigues Deputy Registrar (Academic)	Member
6.	Shri Anselmo A.T.H. Rosa System Analyst	Member
7.	Shri M Chakraborty Head, Computer Centre	Member Secretary

Terms of Reference:

1. The committee shall consider various aspects of IT related activities in an Academic Institution while framing the policy.
2. The Committee shall submit the draft policy within two months from the date of issue of this order to the Registrar for approval.
3. The committee may co-opt any member/s who, the committee feels, shall be useful in preparing the policy.
4. Once the IT Policy is approved, all kinds of complaints/queries/violations etc on the policies shall be addressed by the same committee.
5. The committee is empowered to refer regulations/guidelines etc notified by any other Institute/Authority in dealing with the matter under reference.
6. The term of the committee is initially for a period of two years from the date of issue of the order.

N S Bhat 8.12.15
(Prof. N. S. Bhat)
Offg. Registrar

Copy to: 1. Chairman & Members of the Committee
2. All HODs & Divisional Heads
3. PA to Registrar
4. PS to Vice Chancellor

A. Introduction

Information Technology (IT) services at Goa University (GU) began in 1995 and currently more than 2500 user including students, faculty and staff are connected to the Goa University Network (GUNET). With increased use of computers and digital devices the demand for IT services has increased rapidly. The IT services include campus networking, intranet & internet facilities, email services, software & hardware solutions, etc. It also includes managing the University website (https://www.unigoa.ac.in), e-depositories, campus e-surveillance, biometric records and the University digital signage.The University currently has a 1GB Internet leased line from BSNL as part of the National Mission on Education through Information and Communication Technology (NMEICT) scheme of the National Knowledge Network (NKN). In addition, another20 MB internet leased line is from Tata Communications is in use. The entire campus is covered by the WI-FI facility.

Just as the benefits of information flows have increased social benefits, so have the threats to the infrastructure and its users. IT management in GU has emerged as a challenge. In consonance with the long term vision of the University, a systematic policy for providing state of the art services and to avoid arbitrary decisions that may be detrimental to the long term growth users, an IT policy is necessary. This would be in keeping with similar initiatives of other educational institutions and government bodies.

B. Aim

The aim of the IT Policy (hereafter, the Policy) is to provide a governance mechanism for delivery of state-of-the-art IT services without compromising the safety and sanctity of the user and the University.

C. Purpose

The IT services including the GUNET facility is created and maintained primarily to be used for official purposes –academic and administrative. While there is no restriction on use for personal purposes, any unauthorized, illegal or commercial usage of the GUNET facility would lead to the debarring of the user from using the GUNET facility and necessary disciplinary action will be initiated as per University rules or any other legal provisions as applicable. The Internet/Intranet should be used for Official/Education purpose only and should not be used for Hacking, Spamming, Phishing, etc. and not be used to send unsolicited email or improper network usage.

D. Implementation

The IT Committee (hereafter, the Committee) shallbe authorized to:

- implement the Policy by framing appropriate Rules and Regulations.
- take suitable action on all IT-related complaints/ queries/violations addressed to this Committee.
- continuously review and update the Rules and regulationsin view of the rapid changes in technology and institutional factors.
- record any violation of the policy and initiate/recommend disciplinary action by the competent authority, Third party administrator or the government as per existing rules from time to time.

E. Coverage

The Policy isdefined broadly to cover:

- IT Hardware
- IT Software
- Communication – including Intranet & Internet, E-mail (unigoa and as well as other Third Party domains) and Website (unigoa as well as other Third Party Domains).

F. Applicability

This IT policy shall be applicable to all the users – both on and off campus using any component of the hardware, software or communication assets of GU. The following come under the purview of this IT policy:

1. any user with his/her personal computer or smart device on the University network on or off campus, and
2. University associate (including faculty, students and staff), with University hardware on the University network on or off campus (including any remote location).

Rules and Regulations for IT services at GU

1. Computers, Digital Devices & Software:
Purchase, Installation & Maintenance

1.1 Purchase and Installation

Users on the GUNET should observe certain procedures at the time of purchase and installation of computers/devices or peripherals in order to avoid any inconvenience.

Hardware: It is advised that all the IT non-consumables Computers/LCD/Smart or Display Boards (including desktops, Laptops, Servers) and their peripherals should preferably be purchased with three years on-site comprehensive warranty.

Software: Any computer/ device being used on the GUNET or on the GU campus (whether it is owned by GU or is a personal device) must have Operating Software as well as other applications which are authorized and legally procured. Pirated/unauthorized software is not permitted for installation/use/distribution on the university owned or personal computers/devices connected to GUNET or on GU campus.

The legal liability in such matters will lie with the concerned user (in case of individual user machines) and/or the Head of the Department or Divisional/Sectional heads (hereafter, Head) for shared machines/devices.

It is recommended that open source and legally "Free" software be used where the user/department/section is unable to purchase authorized licenses for commercial software.

Anti-Virus: All the University owned Computers/devices and the computers/devices connected to the GUNET should have proper Antivirus software installed which is active and updated from time to time. Normally, the Computer Centre (CC) will procure campus wide licenses & install suitable antivirus software on all the GU computers/devices, however the user or the Head shall ensure that the Computers under their control are suitably secured with antivirus software. Assistance from CC may be requested if necessary.Computers without updated antivirus software shall be disconnected without any notice from GUNET as this imposes a security risk for all other users on the Network.

1.2 Maintenance

- Single User Desktop/laptop/device installed in an office and used primarily by a single user – The responsibilities for its maintenance shall lie with the user.
- Multiple user desktop/laptop/device installed in any Department/Section/Centre office which has multiple users – the HOD or Sectional Head would be responsible for maintenance of that Computer/laptop/device.
- In a computer laboratory where a group of students/faculty/staff are using multiple computers – the HOD, Sectional Head, or designated authority (as the case may be), shall be responsible for the above.

Maintenance Procedure

1.2.1 During the period of warranty:

Any complaint should be lodged directly with the manufacturer/vendor. This should preferably be done by the concerned user who is responsible (as defined above) for that computer/device.In case any manufacturer/vendor fails to rectify the compliant and resolve the issue suitably, the recommendations should be sent to Purchase Committee to initiate suitable action including blacklisting of the manufacturer/vendor.

1.2.2 After expiry of warranty period:

The University at present does not have any dedicated staff or unit to maintain IT equipments. Therefore, the following method is recommended for maintenance of Servers/Laptops/desktop Computers and other peripherals.

- Servers: The University should enter into Annual Maintenance Contract (AMC) with the supplier or the OEM for regular maintenance of the Servers before the expiry of warranty period so that there is no gap in maintenance.

  Desktops: The University Service Engineers hired specifically for this purpose and placed under the control of University Computer Centre, will attend to the complaint and rectify the issue only for those computers and devices which are not under warranty or AMC. If there are any replacement or repair of equipment required as reported by the Service Engineer, the concerned user/Head will follow University Purchase procedure to arrange the spares.

- Laptops and Peripherals: The user/Head should contact the supplier or the OEM for fault repair on case to case basis. In case there is funding available from sponsored research projects, funds from such projects may be suitably utilized.

2. Uninterrupted Power Supply (UPS)

All servers, desktops and peripherals (excluding laptops, Ipads) should be connected through an Uninterrupted power supply (UPS) unit for smooth functioning during brief power cuts and also protection of equipment during power surges. Power supply to the UPS should maintained adequately to ensure regular battery charging. In this regard the user/Head may coordinate with the University Estate Division to ensure the same.

3. Shifting of Computers

In case any Computer (other than a laptopor similar) is required to be shifted from one location to another location within the campus or off-campus, for whatever reasons, it should be done with prior written intimation to the Computer Centre. The justification for such shifting should be clearly stated, as every Computer is identified by its IP/MAC address configured by the Computer Centre depending on its location. Hence shifting a Computer from one location to another may disturb the configuration of IP address and disturb the availability of network connectivity at that hub. Unauthorised shifting would lead to the disabling of network access without any intimation to the user.

4. Disaster Preparedness &Data Back-up

Individual users are advised to perform regular backups of their vital data on external storage devices as in the event of a hard disk failure, recovery of data can be difficult.

GU should make efforts at making contingency plans for disaster- preparedness. While this involves initial costs, a portion of the budget should be devoted to this on a stated priority ranking of needs. In addition to on campus back-up, cloud storage options may also be explored.

5. Usage of GUNET

Goa University has its own dedicated domain.Students, faculty and staffare advised to use email as a preferred mode of communication for administrative as well as academic purposes.

Any important documents / notices /orders / circulars, required for circulation, should be sent through email as an attachment or placed on the web-page. This will significantly reduce the usage of paper and make retrieval of documents simpler.

The useraccounts of the GUNET domain users will be created and maintained by the CC. The user id will be in the format of 'username@unigoa.ac.in' which can be accessed by logging into "https://mail.unigoa.ac.in". Every University employee must ensure that he/she has been allotted an official University User-id. The use of the official User-id or the GUNET network (both on campus and from remote location) by any user will automatically bind him/her to the Terms and Conditions of ethical use as defined in the University Statutes and IT Policy from time to time. Inflammatory, divisive, abusive and defamatory messages should be avoided and would attract necessary suitable disciplinary action.

It is advised to use the following guidelines:

(1) Account: Ids of all users will be created and maintained by the CC.All faculty, staff (on campus), Deans of faculties and Principals of colleges will be eligible for use of GUNET account. On campus students will be eligible for email account on request for the period of their registration. New users are requested to contact the CC for the same.

(2) Official communications: Only the e-mail services provided by GU carrying its domain name should be used for all official communications.E-mail services provided by third party/other service providers shall not be used for any official communication.

(3) Dormant Account: Users should regularly use the email facility. If any user is found to beinactive for more than 90 days, the facility may be withdrawn without further notice by the CC.

(4) Closure of account: If any faculty or staff is superannuated or leaves GU for whatever reason, his/her user-id will be closed after90 days from the date of retiring/leaving.On special request, GU may permit him/her use of the 'unigoa' account as a forwarding account (to the individual's personal account) without using the server storage for a period to be determined on a case to case basis.

(5) Individual Password:

   (i) The user should immediately change the password, received from the CC, when he/she logs in for the first time.

   (ii) The user should never share his/her password with anyone else since there is a chance of misusing the account for which the owner of the user-id will be held responsible.

(iii) Auto-saving of password in the unigoa e-mail service shall not be permitted on any Computer due to security reasons.

(iv) The password shall be changed immediately if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

(v) If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session.

(vi) Users shall be required to change their passwords periodically and not be able to reuse previous passwords.

(vii) The "Remember Password" feature of applications should notbe used.

(viii) It is advised that the password should be a combination of upper and lower case characters (e.g. a-z, A-Z), digits (e.g. 0-9) and other characters (e.g., !@# $%^&*) in order to reduce chances of hacking and identity theft.

(6) Attachment File Size: The size of the file attachments in an outgoing e-mail is restricted to 25 MB. Larger file size attachments can be sent through other devices.

(7) Safety precaution to be undertaken by users:

a. Users shouldavoid opening any mail or attachment that is from unknown orsuspicious source. Even if it is from a known source, and if it contains any attachment that is of suspicious nature, user should ascertain itsauthenticity before opening it. This is to ensure the security of the user's computer, as well as GUNET as such messages may contain viruses.

b. The user should avoid keeping their account open whenever he/she leaves the Computer or device for whatever reason. This could allow misuse of the account for which the authorized user would then be liable.

(8) The emails, detected as spam, goes to SPAM folder. Users should visit the SPAM folder regularly to check if any trusted/known mail has been wrongly identified as spam. In that case the user should forward the mail to theInbox.

6. Website Content Management

The information on the official GU website https://www.unigoa.ac.in will be created and maintained by CC in consultation with HODs, faculty members, administrative divisions and other bodies of the University. Updates should be sent by the concerned HOD, faculty and the divisional/sectional heads to the Computer Centre to upload & update the website. Any information available on the website is always considered to be authentic and therefore, the concerned HOD (for the department's web-pages), individual faculty (for individual pages) and

the divisional/sectional heads are responsible for the authenticity of the information which is available on the website pertaining to their department, individual websites or division/ section. It is advisable to review the content periodically by the concerned HODs, faculty members and divisional heads.

It will be the endeavour of GU to make the web-content accessible to all sections of the society. In order to achieve this, it is recommended that the website content shall be hosted in the official languages of the state of Goa in addition to English as far as possible. It should also be made accessible to differently-abled by following the government guidelines in this matter.

7. GUNETManagement (Intranet & Internet)

(1) The CC will be responsible for the Design, implementation and maintenance of the GUNET.

(2) CC will allocate static IP address to all device on the GU network, and will reserve the right to change this allocated addresses any time with due intimation to the user.

(3) A formal request for an IP address is to be made to the Computer Centre and on allocation of the same by CC, it is to be displayed prominently on the CPU through a sticker. A log book of all the IP addresses allocated is to be maintained by the respective department/section.

(4) An address allocated to a device should not be changed by the individual user nor the same address be used on any other device even if the other device belongs to the same user/Department.

(5) IP addresses may also be dynamically obtained from the centrally run DHCP server. CC will decide to allot Static / Dynamic IP addresses based on the need.

(6) No services such as HTTP/HTTPS/FTP/DHCP should be run at the department level without the prior consent of the CC.

(7) Three Zones will be created on the Network. LAN, WAN and DMZ (De-militarized Zone). All the servers which require outside access will be placed on the DMZ zone. Servers which run internet services at the department level will not be provided access from WAN, DMZ and the internet traffic will be restricted to the respective VLAN (Virtual LAN) only.

(8) Wireless LAN will be provided wherever possible. IP for the Wireless LAN will be provided by a centrally run DHCP server.

(9) No Devices such as Router, Switch, Access Point, Software Hotspots which has bearing on Network Security are allowed to be connected to the GUNET without the prior

consent from the CC.

(10) All the traffic on the network shall be logged and monitored centrally on the firewall, switches and servers.

(11) All logs will be kept on the device as per availability of space on servers.

(12) Reports of the sites visited by an individual will be noted, recorded and provided to the university authority on specific request by the Competent Authority.

(13) Effort will be made to provide WLAN everywhere on campus but there may be variations in signal strength and WLAN coverage shall not be claimed as matter of right by any user.

(14) WLAN will normally be provided for registered GU users. However, WLAN may also be extended to guests visiting GU on authorization by respective authority.

(15) CC will generate Guest Access keys on prior requests and hand over the same to the respective departments. Departments are responsible to maintain the users credentials on a logbook before allotting the keys.

(16) WLAN may also be temporarily provided at locations where wireless access points exists,forgroup access to participants attending official Conferences and Seminars, etc.on formal request to the CC at least 3 working days in advance of the event by respective authority.

(17) WLAN access to users will be provided on registering their device with the CC.

(18) Departments shall send a list of students enrolled in their respective departments at the beginning of the academic year to CC. At the time of registering the student should carry a photo identity card issued by GU or a card issued by any other competent authority which clearly identifies the individual. Students who are not able to identify themselves may be denied WLAN registration.

(19) Wireless devices without Antivirus will be denied WLAN facility. If any virus activity is noticed from a wireless active device, the device will be disconnected from the WLAN till it is virus free. The individual owner of the device will be solely responsible to clean the device from Viruses.

(20) The CC will register the Device on WLAN and is not responsible to rectify networking or software faults arising within the Device during the time of registration.

(21) The Device information will be noted and the user will be provided WLAN access for not more than two years continuously. After the expiry of the period, the device is needed to be re-registered. The individual user should approach the CC again for re-registration.

(22) Hostels will be provided with WLAN facility only at a common place identified by the Hostel Committee.

(23) Students from affiliated colleges residing in the hostel will not be provided with GU internet access.

(24) Students will be allowed WLAN on Laptops / Desktops (in case of Hostel residents) and notebook only. No students will be provided with WLAN on their mobile devices.

(25) Faculty members and officers of the University may normally be provided with connections on approved university devices (desktops and laptops) by the respective authority. In addition, they may normally be permitted to register one personal mobile device only. Request for additional connections may be placed formally to the CC for consideration.

(26) Laptops purchased under department or project BH will be registered in the Department's name.

(27) Internet Traffic will be monitored and filtered centrally.

(28) The Filtration of sites shall be carried out based on website category. A website category will be decided by the UTM (Unified Threat Management / Firewall) vendor based on the recommendation of the advisory committee.

(29) The following category of sites will be permanently blocked.

a) Pornography
b) Malicious sites
c) Proxy Avoidance
d) Spam URLS
e) Hate and crimes
f) Dating
g) Gambling
h) Games
i) Unrated
j) Any other site deemed undesirable by the GU administration from time to time.

(30) Students' request for white listing of a particular site should be forwarded through the Head of the Department. The Committee will examine the request. Teachers and officers may send their request for listing of any site directly to the IT Committee/CC for consideration.

(31) Wrongly rated/Unrated sites should be brought to the notice of the CC through a note or an email. The same will be attempted to be resolved at the earliest.

(32) Some of the sites such as Online Shopping, Entertainment, News and Media will be disabled for all users during University working hours.

(33) During office hours access over internet will be restricted toeducationalsites, Government Sites and e-mail. All other permissible websites will be open only during non working hours. However, a Head wanting to provide access to any of the Computer/ Staff may do so through a special written request to the CC.

(34) Any deliberate attempt by an individual to bypass the firewall/web-filter through any

process / software or to breach firewall or wireless security by any means will be liable for disciplinary action, including debarring from further use of GUNET and a monetary fine double the amount of perceived damage determined by the Committee.

(35) Third party mail originating from outside the GUNET will not be allowed to access the GU user group mailing facility for mass mailing unless specifically authorized to do so.

8. E-Repositories

GU will aim to place all feasible academic and administrative information on its official website. These will include e-repositories of publications/ presentations of faculty members, dissertation and theses, as part of its open access for public information.

8.1 Creation and Maintenance:

The e-repositories may be created by the Library, IQAC or CC as feasible. These repositories will be hosted by CC on GU servers.

8.2 Content:

All publications of faculty members and students will be placed in the GU e-repository if the author's affiliation in the publication mentions GU. Any retired faculty member who continues to use the GU affiliation in their publication would also be included in the e-repository. However, a paper/document published by a faculty or student with any other affiliation will not enter the e-repository of GU. This information may however be placed under "Other Information" or on a personal website on a Third Party host by the user.

9. Recommended fees for Internet Access

An annual fee, as recommended by the Committee, for wireless/internet access shall be charged from all the students, faculty and staff.

Students: This fee shall be collected at the time of students' enrollment to any programme of the University. It is recommended that an amount of Rs 500 should be charged annually for one device. For transfer of access to another device a fee of Rs 250 will be chargeable.

Faculty and staff: All faculty and staff will be allowed use of one mobile device – smart phone. Any additional personal device will be charged at Rs 500 per year.