

Gopal Narayan Singh University, Jamuhar, Sasaram, Rohtas (Bihar)

A State Private University established under the Bihar Private University Act-2013



INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

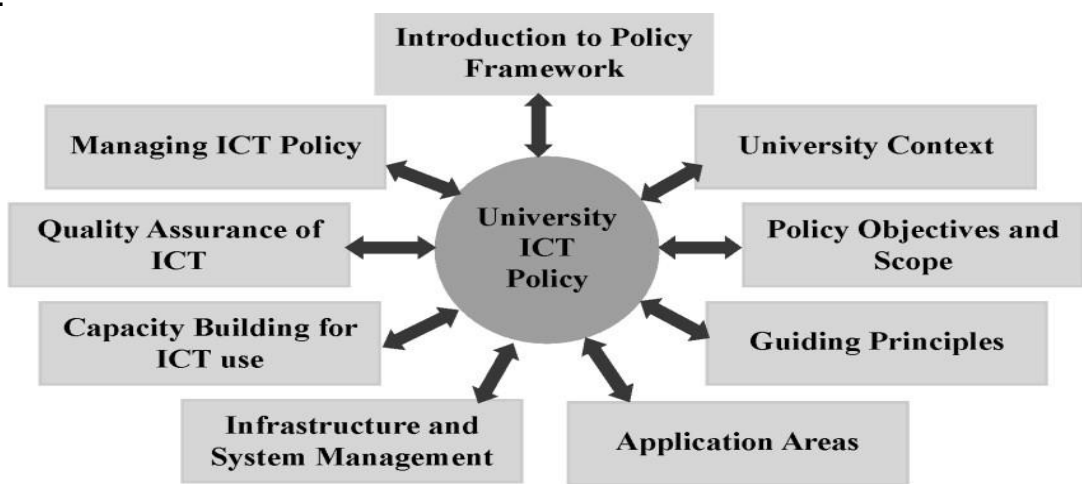
INDEX

S. NO.	CONTENT	PAGE NO.
1.	SHORT TITLE AND COMMENCEMENT	
2.	ADMINISTRATION	
3.	Preface	
4.	The University Context	
5.	Introduction	
6.	Objectives of ICT Policy	
7.	Scope of ICT Policy	
8.	The ICT Resources Covered by the Policy	
9.	Roles and Responsibilities	
10.	General Rules:	
11.	Acceptable Use	
12.	Privacy and Personal Rights	
13.	E-mail Policy	
14.	Social Media	
15.	User Compliance	
16.	Access to the Network	
17.	Monitoring and Privacy	
18.	Security Incident Management Process	
19.	Intellectual Property	
20.	Enforcement	
21.	Deactivation	
22.	Audit of GNSU Network Infrastructure	
23.	Review	
24.	IT Hardware Installation Policy	
25.	Software Installation and Licensing Policy	
26.	Network (Intranet & Internet) Use Policy	
27.	Video Surveillance Policy	
28.	Disposal of ICT equipment	
29.	Responsibilities of University Computer Maintenance Cell (CMC)	
30.	Breach of This Policy	
31.	Revisions to Policy	

ICT POLICY

1.	SHORT TITLE AND COMMENCEMENT	
	1.1	This policy may be called ICT POLICY of Gopal Narayan Singh University, Jamuhar, Sasaram, Rohtas (Bihar). The ICT Policy Document will serve as detailed guidelines and will be useful to all the concern related to the same.
	1.2	This Policy namely ICT POLICY , Gopal Narayan Singh University shall come into force on the date of their approval from the Board of the Management of the Gopal Narayan Singh University, Jamuhar.
	1.3	This policy is prepared to ensure the better support to deploy and maintain a world-class ICT infrastructure and information resources, and to facilitate the effective use of the technology in all academic and administrative processes.
	1.4	In the light of the objectives of the University as spelt out in the notification of ACT, steps have been taken to ensure the maximum utilization of the ICT resources in the University.
2.	ADMINISTRATION	
	2.1	The said policy shall function under overall supervision and administrative control of Registrar of the University.
	2.2	There will be one in charge for smooth functioning of the said Policy and the day to day's activities related to the same will monitored by the said in charge.
3.	PREFACE	
	We at Gopal Narayan Singh University, Bihar realizing the critical role of Information and Communication Technology (ICT) in higher education, are committed to the application of ICT for enhancing administrative efficiency and to optimize learning experiences. The University ICT Policy states that:	
	3.1	Access, economy, efficiency, effectiveness, relevance, transparency, privacy, accountability, sustainability, learner-centred, pedagogically driven and quality assurance shall be the guiding principles of the ICT Policy.
	3.2	The ICT applications cover the areas like system management, research, teaching and learning, student evaluation, support services, community engagement, student data management, human resource development networking and quality assurance.
	3.3	As an ongoing process, ICT applications shall take note of the rapid pace of technology changes.
	3.4	ICT policy management shall be integrated with the overall institutional development plan of the university.

	3.5	ICT system management must ensure integrity, security and legitimate applications of ICT.
	3.6	Use ICT effectively for building national and international networks to ensure innovative changes in providing quality education.
	3.7	The University shall take appropriate measures for the capacity building of academic, administrative and professional staff to effectively use ICT in all university operations.
4.	THE UNIVERSITY CONTEXT	
	4.1	Gopal Narayan Singh University (GNSU), established in 2018, is a leading private university in Bihar, India, recognized by the University Grants Commission (UGC). With a sprawling campus of over 60 acres, GNSU offers a diverse range of programs and aims to provide quality education across various disciplines. The university has several faculties dedicated to various fields, including Medicine, Management Studies, Commerce, Nursing, Information Technology, Law, Pharmacy, Paramedical Sciences, Agricultural Sciences, Mass Communication & Journalism, Library & Information Sciences, and Engineering. GNSU emphasizes Integrity, Innovation, entrepreneurship, Research, Empathy, and Social Outreach, along with quality education. The university provides state-of-the-art infrastructure, including modern classrooms, laboratories, libraries, sports facilities, and hostels, to support students' growth and well-being.
	4.2	Its mission being Social Transformation through Dynamic Education, the University is continuously reengineering its academic and administrative processes so as to make them student centred and student friendly–by deploying the latest ICT tools. The University's ICT infrastructure is huge which includes thousands of computers, best internet connectivity for individual constituent units, wi-fi connectivity in all institutions, latest general and discipline specific software and video-conferencing facilities.
	4.3	The University has its own ICT Centre to develop, deploy and maintain a world-class ICT infrastructure and information resources, and to facilitate the effective use of the technology in all academic and administrative processes. Accordingly, the ICT Centre established by the university aims at enhancing the Quality of the products and processes of the University by providing exhaustive and efficient ICT services to its stake holders. University's constituent units are interconnected, and together are connected to University's own Data Centre.

5.	INTRODUCTION	
5.1	Gopal Narayan Singh University (GNSU) provides IT resources to support the educational, instructional, research, and administrative activities of the University and to enhance the efficiency and productivity of the students, researchers and employees. Students, Teaching and Non - Teaching Staff, Management and visiting Guests and Research Fellowship Members of GNSU 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.	
5.2	 <p style="text-align: center;"><i>Policy Framework for ICT Applications</i></p>	
6.	OBJECTIVES OF ICT POLICY	
	The objective of this policy is to ensure proper access to and usage of GNSU's IT resources and prevent their misuse by the users. Use of resources provided by GNSU implies the user's agreement to be governed by this policy.	
6.1	University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the GNSU campus.	
6.2	This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.	
6.3	Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.	
7.	SCOPE OF ICT POLICY	

This policy applies to people, referred as 'users' using ICT resources provided by the University, including but not limited to;	
7.1	Students enrolled at various constitute units of the University
7.2	Staff (teaching and non-teaching) employed by the University
7.3	Temporary, casual or agency staff working for or on behalf of the University
7.4	Contractors, consultants and suppliers working for or on behalf of the University
7.5	Visitors to the University
8.	THE ICT RESOURCES COVERED BY THE POLICY
This policy applies to ICT resources and systems made available to the users by or on behalf of the University including but not limited to;	
8.1	Personal computers, laptops and terminals.
8.2	Peripherals such as printers, copiers, scanners and multimedia devices
8.3	Mobile devices such as smartphones and tablets
8.4	Networks with wired, wireless, dialup and/or internet connections
8.5	Internet services such as world-wide-web, blogs and wikis
8.6	E-mail and other messaging, social networking or collaboration services such as blogs, chats and forums
8.7	System and application software, services and databases
8.8	Removable media such as CDs, DVDs and USB drives
9.	ROLES AND RESPONSIBILITIES
The following roles and responsibilities are envisaged from each entity respectively.	
9.1	GNSU shall implement appropriate checks and balances to ensure compliance with this policy by their users.
9.2	GNSU Computer Maintenance Cell (CMC) shall be the primary Implementing Agency and shall provide necessary support in this regard. The Computer Maintenance Cell will be headed by any suitable technical person competent in the area as deemed fit by the University. Computer Maintenance Cell has been established to provide hardware and software support to the desktop users of the University. CMC is situated at the back side of guest house. Technical support is available between 09:30 am -04:30 pm from Monday to Saturday (except holidays).
9.3	Computer Maintenance Cell shall ensure resolution of all incidents related to the security aspects of this policy by their users. Implementing Agency shall provide the requisite support in this regard.

	9.4	Use GNSU IT resources for those activities that are consistent with the academic, research and public service mission of the University and are not “Prohibited Activities”.
	9.5	All users shall comply to existing national, state and other applicable laws.
	9.6	Follow copyright laws regarding protected commercial software or intellectual property.
	9.7	As a member of the University community, GNSU provides use of scholarly and/or work-related tools, including access to the library, certain computer systems, servers, software and databases and the Internet. It is expected from University Community to have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources. Authorized users can expect their right to access information and to express their opinion to be protected as it is for paper and other forms of non-electronic communication.
	9.8	Users of GNSU shall not install any network/security device on the network without consultation with the Implementing Agency (IA).
	9.9	It is responsibility of the University Community to know the regulations and policies of the University that apply to appropriate use of the University's technologies and resources. University Community is responsible for exercising good judgment in the use of the University's technological and information resources.
	9.10	As a representative of the GNSU community, each individual is expected to respect and uphold the name and reputation of the University in any activities related to use of ICT communications within and outside the university.
	9.11	Competent Authority of GNSU should ensure the dissemination of the policy among the stakeholders.
10.	GENERAL RULES	
	10.1	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.
	10.2	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

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

	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.
10.3	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.
10.4	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
10.5	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 Libre Office/ OpenOffice/ WPS Office and computing software's like GNU-Octave, respectively. In case of technical limitation in such adaptation, relaxation may be requested from competent authority on valid grounds.
10.6	The broader concept of data privacy must be honored by each user. 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. No user should attempt to gain unauthorized access to information and disclose the same to self or other unauthorized users.
10.7	Any interference, disruption or encroachment in the University IT resources shall be a clear violation of the University policy.
10.8	The University may be required to provide its IT information, resource and/ or records, in parts or full, to third parties if it is desired as part of any investigation.

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

		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
	10.9	Users are expected to take good care of IT resources of the University. In the event of any damage is observed the same has to be reported to the Computer Maintenance Cell (CMC). The CMC have the right to fix responsibility after proper investigation of the damage.
	10.10	The users should not move, repair, reconfigure, modify, or attach external devices to the systems. If such things happen then the user/s are liable for action.
	10.11	Violations of policy will be treated as academic misconduct, mis demeanour, or indiscipline as appropriate. Depending upon the nature of the violation, the University authorities may take an action.
	10.12	The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately as deemed fit by the authorities.
11.	ACCEPTABLE USE	
	11.1	An authorized user may use only the IT resources he/she has authorization, unauthorized access to other's account will result in penal action.
	11.2	As an authorized GNSU user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of GNSU or a personal computer that is connected to the GNSU campus wide Local Area Network (LAN).
	11.3	The university is bound by its End User License Agreement (EULA), respecting certain third-party resources; a user is expected to comply with all such agreements when using such resources.
	11.4	Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access.
	11.5	No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
	11.6	Users must comply with the policies and guidelines for any specific set of resources to which he/she have been granted access.

	11.7	When other policies are more restrictive than this policy, the more restrictive policy takes precedence.
12.	PRIVACY AND PERSONAL RIGHTS	
	12.1	All users of the university's IT resources are expected to respect the privacy and personal rights of others.
	12.2	Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).
	12.3	While the University does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of the competent authority.
13.	E-MAIL POLICY	
	13.1	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.
	13.2	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.
	13.3	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.
	13.4	Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:
	13.4.1	The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
	13.4.2	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.
	13.4.3	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.
	13.4.4	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.
	13.4.5	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.
	13.4.6	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.
	13.4.7	User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
	13.4.8	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.
	13.4.9	Impersonating email account of others will be taken as a serious offence under the university IT security policy.
	13.4.10	There may be instances when the University, based on approval from competent authority, reserves and retains the right to access and inspect stored information in email/social media with or without the consent of the user.
14	SOCIAL MEDIA POLICY	
	14.1	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.
14.2	PROCEDURES
14.2.1	The following principles apply to professional use of social media on behalf of GNSU as well as personal use of social media when referencing Gopal Narayan Singh University (GNSU).
14.2.2	Employees need to know and adhere when using social media in reference to Gopal Narayan Singh University (GNSU).
14.2.3	Employees should be aware of the effect their actions may have on their images, as well as Gopal Narayan Singh University (GNSU), image. The information that employees post or publish may be public information for a long time.
14.2.4	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 Gopal Narayan Singh University (GNSU), its employees, or would be students.
14.2.5	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.
14.2.6	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.
14.2.7	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.
14.2.8	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.
14.2.9	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.

	14.2.10	Social media use shouldn't interfere with employee's responsibilities at Gopal Narayan Singh University (GNSU). The University's computer systems are to be used for education 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, Gopal Narayan Singh University (GNSU)blogs and 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.
	14.2.11	Subject to applicable law, after---hours online activity that violates or any other University policy may subject an employee to disciplinary action or termination.
	14.2.12	It is highly recommended that employees keep Gopal Narayan Singh University (GNSU) related social media accounts separate from personal accounts, if possible.
	14.2.13	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/Staff (As they belong to a very respected GNSU community).
15	USER COMPLIANCE	
	15.1	When an individual uses GNSU's IT resources, and accepts any University issued computing accounts, it means that the individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep oneself up-to-date on changes in the IT policy of GNSU and adapt to those changes as necessary from time to time.
16	ACCESS TO THE NETWORK	
	Access to Internet and Intranet	
	16.1	A user shall register the client system and obtain one-time approval from the competent authority before connecting the client system to the University Campus wide LAN.
	16.2	GNSU shall maintain two independent networks, i.e. Internet and Intranet. Both the networks shall not have any physical connection/devices between them. End point compliance shall be implemented on both the networks to prevent unauthorized access to data.
	16.3	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.

16.1	ACCESS TO GNSU'S WIRELESS NETWORKS	
		For connecting to a GNSU's wireless network, user shall ensure the following:
	16.1.1	A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the GNSU's wireless network.
	16.1.2	Wireless client systems and wireless devices shall not be allowed to connect to the GNSU's wireless access points without due authentication.
	16.1.3	To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.
16.2	FILTERING AND BLOCKING OF SITES:	
	16.2.1	Computer Maintenance Cell (CMC) or any other Implementing Agency (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.
	16.2.2	Computer Maintenance Cell (CMC) or any other Implementing Agency (IA) may also block content which, in the opinion of the university, is inappropriate or may adversely affect the productivity of the users.
17	MONITORING AND PRIVACY	
	17.1	Computer Maintenance Cell (CMC) or any other Implementing Agency (IA) shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.
	17.2	IA/Nodal Agency, 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 University provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.
	17.3	IA may monitor user's online activities on University network, subject to such Standard Operating Procedures of GoI norms.
18	SECURITY INCIDENT MANAGEMENT PROCESS	
	18.1	A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of University's data.
	18.2	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 the university.

	18.3	Any security incident noticed must immediately be brought to the notice of the IA.
	18.4	Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the IA shall be done as per the IT Act 2000 and other applicable laws.
	18.5	IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny or release of logs.
19	INTELLECTUAL PROPERTY	
	19.1	Material accessible through the GNSU's network and resources 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, trade marks, trade secrets or other proprietary information. Users shall not use GNSU's network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.
20.	ENFORCEMENT	
	20.1	This policy is applicable to all the users of GNSU as specified in Section 1 of this document. It is mandatory for all users to adhere to the provisions of this policy.
	20.2	Each entity of GNSU shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the user entities in this regard.
21	DEACTIVATION	
	21.1	In case of any threat to security of GNSU's systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the IA.
	21.2	Subsequent to such deactivation, the concerned user and the competent authority of the university shall be informed.
22.	AUDIT OF GNSU NETWORK INFRASTRUCTURE	
	22.1	The security audit of network infrastructure shall be conducted periodically by an organization approved by the university.
23.	REVIEW	
		Future changes in this Policy, as deemed necessary, shall be made by the Technical Committee with the approval of the Competent Authority of the university.
24.	IT HARDWARE INSTALLATION POLICY	

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICY

	University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.
24.1.	Who is Primary User
	An individual in whose room the computer is installed and is primarily used by him/her, is considered to be "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.
24.2	What are End User Computer Systems
	Apart from the client PCs used by the users, the university will consider servers not directly administered by CMC, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the CMC, are still considered under this policy as "end- users" computers.
24.3	Warranty & Annual Maintenance Contract
	Computers purchased by any Section/ Department/ Project should preferably be with 3 years on site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include standard repair and maintenance procedures as may be defined by Computer Centre from time to time.
24.4	Power Connection to Computers and Peripherals
	All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging, till such instances wherein the UPS is to be left unattended. Further, these UPS systems should be connected to the electrical points that are provided with proper earthing and have properly laid electrical wiring.
24.5	Network Connection
	While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

	24.6	File and Print Sharing Facilities
		File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.
	24.7	Maintenance of Computer Systems provided by the University
		For all the computers that were purchased by the university centrally and distributed by the Estate Branch, University Computer Maintenance Cell (CMC) will attend to the complaints related to any maintenance related problems.
25.	SOFTWARE INSTALLATION AND LICENSING POLICY	
	25.1	Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.
	25.2	Respecting the anti-piracy laws of the country, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network. In case of any such instances, university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.
	25.1.1	Operating System and its Updating
		Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through internet. Checking for updates and updating of the OS should be performed at least once in a week or so. University as a policy encourages user community to go for open-source software such as Linux, Open office to be used on their systems wherever possible.
	25.2	Use of software on Desktop systems
	25.2.1	Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the competent authority.
	25.2.2	Any software installed should be for activities of the university only.
	25.3	Antivirus Software and its updating
		Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus

		protection policy. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.
	25.4	Backups of Data
		Individual users should perform regular backup so their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc.
26	NETWORK (INTRANET & INTERNET) USE POLICY	
		Network connectivity provided through the University, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the University IT Policy. The CMC is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to CMC.
	26.1	IP Address Allocation
	26.1.1	Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the Computer Centre. Following a systematic approach, the range of IP addresses that will be allocated will be based on Virtual LAN(VLAN) created against each entity or objective. Any device connected to the network will be allocated IP address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorized from any other location.
	26.1.2	As and when a new computer is installed in any location, it will be allocated as per the DHCP pool policies.
	26.1.3	An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.
	26.2	DHCP and Proxy Configuration by Individual Departments/Sections/Users
	26.2.1	Use of any computer at end user location as a DHCP server to connect to more computers through an individual switch/hub and distributing IP addresses (public or private) should strictly be avoided, as it is considered absolute violation of IP address allocation policy of the university. Similarly, configuration of proxy

	servers should also be avoided, as it may interfere with the services run by the CMC.
26.2.2	Even configuration of any computer with additional network interface card and connecting another computer to it is considered as proxy/DHCP configuration.
26.2.3	Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned department/user.
26.3	Running Network Services on the Servers
26.3.1	Individual departments/individuals connecting to the university network over the LAN may run server software, e.g., HTTP/ Web server, SMTP server, FTP server, only after bringing it to the knowledge of the CMC in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in termination of their connection to the Network.
26.3.2	CMC takes no responsibility for the content of machines connected to the Network, regardless of those machines being University or personal property.
26.3.3	CMC will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.
26.3.4	Access to remote networks using a University's network connection must be in compliance with all policies and rules of those networks. This applies to any and all networks to which the University Network connects. University network and computer resources are not to be used for personal commercial purposes.
26.3.5	Network traffic will be monitored for security and for performance reasons at CMC.
26.3.6	Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.
26.4	Internet Bandwidth obtained by Other Departments
26.4.1	Internet bandwidth acquired by any department of the university under any research programme/project should ideally be pooled with the university's Internet bandwidth, and be treated as university's common resource.
26.4.2	Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such network should be totally separated from the

		university's campus network. All the computer systems using that network should have separate VLANs based on grouping criterion.
	26.4.3	IP address scheme (private as well as public) and the university gateway should not be specified as alternative gateway. Such networks should be adequately equipped with necessary network security measures as laid down by the university IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes used may be submitted to CMC.
	26.4.4	Non-compliance to this policy will be direct violation of the university's IT security policy.
	26.5	Institutional Repository (IR)
		GNSU shall be providing services related to Institutional Repository (IR) through Central Library of the university as per the following policies.
	26.5.1	A University-based institutional repository (IR) is a set of services that a University Library offers to the members of its community for the management and dissemination of digital materials created by the University or institution and its community members.
	26.5.2	Most common items in the repository are the outputs of research journal articles (pre-print and post- print), conference papers, technical reports, computer programs, preservations, technical manuals, Video and audio recordings, e-Books, Seminar and Webinar lectures, Thesis and Dissertations and Rare books etc. Institutional Repository (IR) also contains other items such as convocation addresses, student handbooks, as well as teaching materials quotes sources which suggest that a repository should be integrated with the University's course management system and display e-learning features.
	26.5.3	Mainly the Bonafide members i.e. faculty members, research scholars, students and other staff members having institutional e-mail IDs (i.e. @gnsu. ac. in) are authorised members to access the IR of Gopal Narayan Singh University.
27.	VIDEO SURVEILLANCE POLICY	
	The System	
	27.1	The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.
	27.2	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.
	27.3	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 Camera installation is in use.
	27.4	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.
27.1	Purpose of the system	
	27.1.1	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 individual's privacy. These purposes will be achieved by monitoring the system to:
	27.1.2	Deter those having criminal intent.
	27.1.3	Assist in the prevention and detection of crime.
	27.1.4	Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order.
	27.1.5	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.
	27.1.6	In the case of security staff to provide management information relating to employee compliance with contracts of employment.
28.	DISPOSAL OF ICT EQUIPMENT	
	28.1	The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the university.
29.	RESPONSIBILITIES OF UNIVERSITY COMPUTER MAINTENANCE CELL (CMC)	
	29.1	MAINTENANCE OF COMPUTER HARDWARE & PERIPHERALS
		CMC 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.
	29.2	Receiving Complaints

	<p>CMC may receive complaints, if any of the particular computer systems are causing network related problems. CMC may receive complaints from the users if any of the computer systems or peripherals that are under maintenance through them are having any problems.</p> <p>The designated person in CMC receives complaints from the users 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.</p>
29.3	Scope of Service
	CMC 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.
29.4	Installation of Un-authorized Software
	CMC 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.
29.5	Reporting IT Policy Violation Incidents
	If CMC 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 university authorities.
29.6	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 CMC. After taking necessary corrective action CMC or service engineers should inform University authority about the same, so that it can be turned on by them.
29.7	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.
	29.8	Coordination with staff of respective Faculty:
		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 CMC/service engineer may coordinate with the staff to resolve the problem with joint effort. This task should not be left to the individual user.
30.	BREACH OF THIS POLICY	
	30.1	Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Helpdesk complaints.it@gnsu.ac.in . On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user's access to University's Data.
	30.2	If any breach of this Policy is observed, then (in addition to the above) disciplinary action upto and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.
31.	REVISIONS TO POLICY	
		The University reserves the right to revise the terms of this Policy at any time. Any such revisions will be noted in the revision history of the policy, which are available on the GNSU website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.