

Guru Nanak Dev University, Amritsar

IT Policy

Introduction

Guru Nanak Dev University provides the excellent IT resources as well as IT enabled services for its research, academic and administrative activities to enhance the research activities and efficiency of its employees, research scholars as well as students. These resources are opened for all the students, research scholars, faculty members as well as other employees of the university like as 24 hours access of internet in the campus, access of journals, use of IT resources in the digital language of the library, access of university portal etc. University is upgrading these resources time to time in an efficient and effective manner. This Policy establishes specific requirements for the use of all IT resources at GNDU Amritsar. This policy applies to all users who are accessing the numerous computing resources owned or managed by GNDU. For the purpose of this policy, the term 'IT Resources' includes all university owned, licensed, or hardware and software, and use of the university network through wired, wireless or hot spots, regardless of the ownership of the computers or device connected to the network. It is, therefore, expected that these resources are used primarily for university related purposes and in a lawful and ethical way.

Scope and Objective

This policy is applicable to all individuals/ users/ entities that use the IT resources of GNDU. This policy governs the usage of IT Resources from an end user's perspective.

The objective of this policy is to ensure proper access to and usage of GNDU's IT resources, infrastructure, devices and prevent their misuse by the users. Use of resources provided by GNDU implies the user's agreement to be governed by this policy. University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.

Standard Approval Process

GNDU IT Policy Committee members are responsible for the development and review of standards needed to implement approved policies. The Chairman will consult with relevant constituent groups such as the IT Officials, Heads, legal Cell and GNDU Competent authority team prior to approval of standards.

Website Policies

University website is divided into different sub domains. These sub domains are created to facilitate users to access different type of software applications related to students, employees and general public. Different web pages on the website relate to the University's mission and are being maintained and updated periodically by the website in charges. The personal data about the employees and students is password protected and hence cannot be accessed by the general public.

User Policy

- An authorized user (employee/student) should access only those IT resources for which he/she has authorization. No user should access another user's account, or attempt to capture or guess other users' passwords.
- Users should also make an effort to protect his/her passwords and to secure resources against unauthorized use or access.
- When an individual uses any resources it automatically means that the individual agrees to comply with all IT related policies. It is the

responsibility of the individual to keep oneself up-to-date on changes in the IT policy of GNDU.

Privacy Policy

- The user can visit the university website without identifying himself/herself or revealing any personal information. However, the use of certain e-services requires submission of personal information. University however does not disclose, sell, swap or rent to any third party any such personal information for commercial purposes.
- The information filled by user will be utilized only for the purpose stated in the application. To accomplish such a purpose, University may disclose the information to its employees and consultants who have a legitimate need to know the information.
- We may collect certain information about the User, such as Internet protocol (IP) addresses, date and time of the visit and the pages visited etc.

Copyright Policy

- The public content featured on the University website may be reproduced free of charge with the approval of competent authority. However, the content is required to be reproduced accurately and not in a misleading context. Whenever the content is being published, the source must be prominently acknowledged.
- User may not copy, download or export data obtained from the Website and store it outside of the system, e.g., in a database or other external repository without the permission of University.

Network Policies

Purpose

The Network Policy is implemented in order to facilitate a glitch-free network access in the present day heterogeneous environment and threat-free environment (free of spamware, ransomware and malware) at gateway level. The implementation of this is to reduce the likelihood of external intrusions in the network, with minimum chance of transmission of risk in different segments of the network. The policy helps users to follow network ethics and maximize the efficient use of network resources.

The Terminology

- The term VLANs (Virtual Local Area Networks) describes segments of the main campus network e.g., network comprising of Wireless / Wired PCs at various Hostels / Departments within the University premises.
- The UTM refers to the Unified Threat Management Appliance installed in the core of the network, to prevent external intrusions into the network and to implement user-based and group-based network access policies.
- The term Switches refers to the Cisco Network switches installed in the department(s) to ensure high-speed network access with access policies for each department.

The Policy

The University requires that all users exercise care in connecting devices to the University network and that connected devices do not interfere with the operation of the network or the operations of others using it.

Applicable in all areas

- Every computer on the network should have authenticated access to the internet using the University resources.
- Due to the known multiple vulnerabilities on the older versions of operating systems (Windows 7 or older), users have higher probability of being exploited when online. Therefore, use of machines having OS

Older than Windows 7 on the University network for Internet and Intranet access is not advised to the University network users (Upgrade to newer versions before connection).

- Every network user is advised to have all (applicable) currently published security fixes\patches applied as soon as possible, including OS updates.
- Every user must get registered through their department in order to obtain Login Credentials for the University's Captive Portal for Internet Access through UTM installed at the core of the network.
- All computers connected to the University network through labs or personal devices are advised to use anti-virus software package and Anti-virus software pattern files (list of detectable viruses) should be updated at least weekly.
- No computer system shall be used to hamper network access, and disrupt network traffic. However, the remote access to peers offering a specific service is permissible.
- No computer system shall be used to interfere with the operation of the campus wide network by acting as a network device (router, switch, hub, DNS server, DHCP server, etc.). Connection of switches, routers, hubs or broadcast of any wireless signal, disrupting the University wi-fi network access or wired access, from any such device is forbidden.
- No computer shall act as a gateway to the network by virtue of offering dial in, Wireless Hotspot or direct access to third parties.
- Any computing device or users that are found to be disrupting or degrading the operation of the network service intentionally or otherwise is subject to disconnection. In extreme cases this may be done without warning.
- The downloading/ uploading/ sharing of illegal/streaming, pirated or unlicensed content (Images, software, music etc.) is forbidden.
- The official group mail accounts like head@gndu.ac.in, faculty@gndu.ac.in etc. should be judiciously used. These accounts have been created to facilitate the distribution of official e-communications and should not be used to circulate personal messages.
- Any creation of a personal World Wide Web page or a personal collection of electronic material that is accessible to others must include a disclaimer that reads as follows: "The material hosted at this site is not

endorsed, sponsored or provided by or on behalf of Guru Nanak Dev University, Amritsar."

- Personal Web pages that are maintained by University's computer account holders must not contain paid advertising. This guideline is consistent with the University's policy against use of resources for private gain or commercial purposes.
- Internet access accounts and Email accounts are for the exclusive use of the individual to whom they were assigned. Users must not allow or facilitate access to these accounts to others. Users may not set up a proxy or anonymous re-mailer for purposes of allowing access to others.
- Any traffic on the University's network, stripped of information content, maybe monitored for operational or research purposes by the Network Management Team.
- Recreational use is prohibited: Do not play games, Minimize the use of chat programs such as IRC, ICQ, Discord except to access technical services, do not log into a remote access server and then log into other machines.
- Use of services like VPN or TOR to circumvent university's web policy enforced through UTM is prohibited.
- Hosting of FTP/HTTP serverlocally without prior permission from Network Management Team for any purpose is not allowed.
- No Wi-Fi Router or AP using WEP or WPA Security protocols will not be allowed to use university's network.
- No computing device should use any spoofing techniques to gain unauthorized access.
- For users own protection, Users should not use alternate methods to access any sort of network traffic deemed harmful and blocked by the UTM.

Applicable to VLANs

Apart from terms and conditions laid above following clause are applicable to VLANs.

- The University does not guarantee the privacy or security and accepts noresponsibility for loss caused by use or failure of these networks.

These networks should be regarded as insecure and users are advised not to transmit any vital information over these networks unless that communication is encrypted.

- The University's Internet Cell will not engage in the repair or configuration of any device that is not University's property.
- Authorized users may access University's computing equipment, systems and networks for personal uses if the following conditions are met:
- The use does not overload the University's computing equipment or systems, or otherwise negatively impact the system's performance.
- The use does not result in commercial gain or private profit. In no case may University's computing resources be used for solicitation of external activity for monetization.
- The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security or in any way attempts to gain unauthorized access.
- The use does not involve sending or soliciting chain letters, nor does it involve sending unsolicited bulk mail messages (e.g., "junk mail," or "spam")
- The use does not involve using university's network and computing resource to attack other system.
- Individuals/ Owners in breach of this policy are subject to disciplinary procedures. If an individual/ computer perform an activity that violates any clause of the policy, the University reserves the right to impose a financial penalty or terminate the access to the network for such individuals/ computers. The amount of the financial penalty and the period of deactivation will depend upon the severity of the damage done by the activity.

Important Note:

Every user on the network should read the network policy and abide by the same as an individual and as an owner of computer(s) in their respective domain(s); it is mandatory to accept the terms and conditions in the policy in order to gain access to the network. Any act done by any user against the law will be dealt strictly as per law of land.

Internet Cell Team, with the explicit agreement of the network management team, may be exempted from some clauses. Any amendments to these policies will be circulated among all the users as and when applicable.