ANANT
NATIONAL
UNIVERSITY
॥ प्रज्वालितो ज्ञानमयः प्रदीपः ॥

India's First
DesignX
University

IT POLICY & GUIDELINES

October 2024, Version 1.0

1. Introduction

Anant offers IT resources to support the University's educational, instructional, research, and administrative activities, aiming to enhance students' and employees' efficiency and productivity.

This document establishes the policy and guidelines governing the usage of all IT resources Anant provides. The policy applies to all individuals utilising IT resources owned or managed by Anant.

For this document, "IT Resources" encompass all hardware and software owned, licensed, or managed by the university, as well as the use of the university network through physical or wireless connections, regardless of the ownership of the connected computer or device.

Misuse of these resources can expose the university to risks and liabilities. Therefore, these resources are expected to be primarily used for university-related purposes and in a manner that adheres to legal and ethical standards.

2. Scope

This document specifies the usage of IT Resources from an end user’s perspective. It applies to all individuals, users, and entities utilising Anant's IT resources.

3. Objective

This document aims to ensure the appropriate access and usage of Anant's IT resources while preventing misuse.

- The University IT policy is established to uphold the maintenance, security, and lawful and appropriate utilisation of the IT infrastructure implemented by the University within the campus.
- This policy defines University-wide strategies and responsibilities to safeguard the Confidentiality, Integrity, and availability of information accessed, created, managed, and/or controlled by the University.
- Information encompasses various elements, including data, information systems, computers, network devices, intellectual property, documents, and verbally communicated information.

4. Roles and responsibilities

The following are the roles and responsibilities expected from each user involved.

a. Anant expects its users to comply with this policy.
b. The IT department at Anant will take the lead in implementing this policy and assume primary responsibility for providing support and resolving any IT system and security-related incidents that may arise.
c. It is the responsibility of the IT department to ensure that all university IT operations are running efficiently and to conduct periodic audits to verify that all IT resources are functioning smoothly.
d. Anant's IT resources should be utilised for activities that align with the University's academic, research, and public service mission.
e. Users must adhere to all relevant national and state laws and regulations concerning telecommunications and networking.
f. As a part of the University community, Anant grants access to specific work-related tools, such as the Library, computer systems, servers, software, databases, and the Internet. It is expected that the University community will utilise these tools without obstruction, respect certain levels of privacy, and take measures to safeguard them against abuse and intrusion by others who also have access to these resources within the University community.
g. Users of Anant IT resources are strictly prohibited from installing any network or security devices, VPNs, or similar tools and software on the network or devices without obtaining prior approval from the IT Department.
h. It is the responsibility of the University Community to acquaint themselves with the regulations and policies set forth by the University regarding the proper use of its technologies and IT resources.

5. Acceptable Use

- An authorised user can access only the IT resources they have explicit authorisation. The use of another individual's account, as well as any attempt to guess or capture another user's password, is strictly prohibited.
- Each individual is responsible for appropriately using all assigned resources, including computers, network addresses or ports, software, and hardware. This involves ensuring that these resources are used ethically, securely, and in compliance with all relevant policies and guidelines.
- Each user is responsible for taking reasonable measures to protect their passwords and ensure the security of their resources, guarding them against unauthorised access.
- Users are strictly prohibited from attempting to access restricted areas of the network, operating systems, security software, or other administrative applications without obtaining the necessary authorisation.
- Laptops are issued to faculty and staff members of the University as a portable alternative to desktop computers. Their purpose is to facilitate work

in various locations on campus as dictated by job requirements. It is essential to note that laptops are intended exclusively for the individual employee's use and should not be shared with family, friends, or other employees.
- Users must adhere to the policies and guidelines established for any resources to which they have been granted access.

6. Privacy and Personal Rights

Users of the university's IT resources are expected to uphold the privacy and rights of others. Unauthorised access or copying of another user's email, data, or any other information is strictly prohibited without proper authorisation and approval from the Competent Authority.

7. Email Privacy

Although we make every effort to ensure the privacy of your official email, this may only sometimes be possible. Since every email user is granted access to electronic information systems for conducting University business, there may be instances when, with the approval of the competent authority, the University reserves the right to access and inspect stored information in your email, provided that the user consents to such access.

8. Use of IT Devices Issued by Anant

IT devices, such as desktops, laptops, external storage, and peripherals provided by Anant to faculty and staff, are designated for academic, research, and university-related purposes. Their use must adhere to legal and ethical standards, following the best practices outlined in the "Use of IT Devices on Anant Network" section.

The IT devices allocated to faculty and staff are recognised as university assets, issued based on their job roles and approved by respective department heads. Employees are responsible for preserving and securing these assigned devices. Any physical alterations or modifications to the devices are strictly prohibited. Upon the conclusion of employment, employees must return the devices to the Anant IT department on or before their final day. This process is an integral component of the no-dues sign-off procedure.

The employee is expected to promptly report any issues related to IT devices issued by Anant to the IT department. All repairs must be carried out exclusively by the Anant IT department; seeking service or repair from any other source is strictly prohibited.

Written approval from the employee's Head of Department (HoD) is necessary for any requests for additional IT devices and accessories, such as a mouse, keyboards, cables etc.

The IT department is responsible for installing standard licensed software on all Anant-issued devices. Additionally, they provide system support, assist with device use and operation, and offer guidance on software usage.

All software installed on university-owned devices must be licensed and compliant with university policies. Users are prohibited from installing unauthorised or unlicensed software. The IT Department reserves the right to audit university devices periodically to ensure software compliance and may remove any software found to violate these policies.

9. Access to the Network

a. Access to the Internet and Intranet

i. Anant operates two separate networks, namely the Internet and Intranet. Endpoint compliance measures are implemented on both networks to safeguard against unauthorised access to data.
ii. Before connecting to the University's Campus-wide LAN, every user must obtain one-time approval from Anant's IT department.
iii. Users are strictly prohibited from engaging in any activity through websites or applications (such as VPNs, etc.) to bypass network filtering or engage in unlawful acts that could compromise the performance or security of the network.

b. Access to Anant’s Wireless Networks

i. Each user may connect up to two devices to the university network. If users need to connect more devices, they must obtain prior approval from the department heads or IT department.
ii. Before connecting an access device to Anant's wireless network, users must register the device and obtain one-time approval from the competent authority.
iii. Wireless client systems and devices must authenticate appropriately before connecting to Anant's wireless access points.
iv. Users are strongly advised only to connect their devices to secured wireless networks.

c. Filtering and blocking of sites

i. The IT Department reserves the right to block internet content that violates provisions outlined in the IT Act 2000 or other relevant laws and any content that poses a security risk to the network.
ii. According to the university's judgement, the IT Department may also block inappropriate content likely to impact user productivity negatively.

10. Monitoring and Privacy

i. The IT Department is authorised to conduct regular network and system audits to ensure compliance with this policy.

ii. In the interest of security or compliance with applicable laws, the University reserves the right to access, review, copy, or delete electronic communications or files stored on University-provided devices. Users will be notified of such actions. This includes files, emails, posts on electronic media, internet history, and similar items.
iii. The IT Department may monitor users' online activities on the University network to ensure compliance with network security protocols, prevent unauthorised access, and maintain the integrity of university IT resources. This monitoring is carried out in compliance with privacy laws and ethical standards and only with prior approval from the relevant department head.

11. Email Usage Policy

Anant provides official email to its users, promoting efficient information dissemination among the university community. It is highly recommended that the official email with Anant's domain be utilised to effectively distribute critical information to faculty, staff, students, and administrators.

The university's email services and cloud storage (Drive) for file storage and collaboration are dedicated to formal university communication, official academic matters, and administrative purposes. Email service provides limited storage, and the allotments based on user categories are as follows:

User Category	**Storage (per email id)**
Faculty, Staff and Department	30 GB
Student	20 GB
Alumni	5 GB

Users needing additional storage must obtain prior approval from their department head. These services ensure the efficient delivery of messages, documents, and official notices to faculty, staff, students, and alums, encompassing administrative content, policy updates, general announcements, and related information.

University community members, including students, faculty, and staff, can access their official email by logging onto either https://gmail.com or "https://mail.anu.edu.in" using their email ID and password. When you join Anant, the IT department creates your official email ID in coordination with the relevant department. If you have yet to receive your email ID upon joining Anant, please contact the appropriate department for assistance (Faculty and staff can contact the HR department, while students can contact the department where they are admitted for further support).

Users should abide by the following policies when using the email and cloud storage facility:

1. The email facility should primarily be used for academic and official purposes, with limited personal use.
2. Engaging in illegal or commercial activities through the facility violates the university's IT policy and may result in the withdrawal of access. Prohibited use includes, but is not limited to, unauthorised copying or distribution of software, sending unsolicited bulk emails, and generating threatening, harassing, abusive, obscene, or fraudulent messages/images.
3. Users should ensure the recipient's email facility can receive such attachments when sending large attachments to others.
4. The university provides limited cloud storage; users are responsible for efficiently managing their email and Drive storage. This includes periodically cleaning up duplicate and unnecessary files and folders to optimise their allocated storage space.
5. Users should exercise caution when opening emails or attachments from unknown or suspicious sources. Even if the source is known, if an attachment appears suspicious or dubious, users should confirm its authenticity with the sender before opening it. This is crucial for the security of the user's computer, as such messages may contain viruses that can damage valuable information.
6. Users must not share their email account credentials with others, as individual account holders are responsible for any misuse of their email accounts.
7. Intercepting or attempting to gain unauthorised access to others' email accounts infringes upon users' privacy and is strictly prohibited.
8. When using shared computers, if another user's email account was accidentally left open, the current user should promptly close it without viewing its contents.
9. Spam emails are automatically filtered and placed in users' mail accounts in the "SPAM MAIL" folder. Users are advised to regularly check this folder for important emails that may have been mistakenly labelled as spam. Emptying the SPAM folder is often recommended.
10. Everyone ensures their email account adheres to the university's email usage policy.

The policies outlined above also apply to email services provided by other service providers such as Gmail, Hotmail, Yahoo, RediffMail, etc., as long as they are accessed from the university's campus network or by using resources provided by the university for official purposes, even when accessed from outside the campus.

12. Access to Social Media and OTT Platforms

The OTT platforms are accessible to all individuals only in the designated common areas between 6:00 PM and 8:00 AM, excluding weekends and holidays. On the other hand, social media sites are available to everyone within Anant's network. Users must adhere to the following guidelines:

- Any suspicious incidents should be promptly reported to the appropriate authorities.
- Users should always use high-security settings on social networking sites.
- Posting offensive, threatening, obscene, copyrighted, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or otherwise unlawful material is prohibited.
- Users must not disclose or use any confidential information obtained as an employee of the university.
- Comments or posts that could damage Anant's reputation should be avoided.

These guidelines ensure Anant users' responsible and respectful use of social media and OTT platforms.

13. Data Management Policy

This data management policy applies to all enterprise software applications that generate, modify, and archive Anant enterprise data.

a. Data Security

i. All data produced during Anant ongoing operations and academic activities must be securely stored to ensure business continuity. This data should be stored on an enterprise cloud or a secure shared server.
ii. Data stored on local machines is at risk of being inaccessible or deleted, hindering operations.
iii. All staff members are responsible for adopting appropriate practices to ensure the secure management of Anant data in their respective roles.

b. Data Privacy

i. Data privacy must be ensured by robustly regulating access to enterprise data through the User Access Policy.
ii. Data generated during Anant's ongoing operations must remain confidential and not be shared with external vendors or service providers unless there is a compelling business reason to do so. In such cases, prior written permission must be obtained from the Dean of Student and Administrative Affairs.

c. Data Retention

i. Data generated during Anant's ongoing operations will be retained within enterprise applications until necessary.
ii. The data stored in Anant enterprise systems will undergo periodic archiving to maintain optimal system performance.
iii. The data stored in Anant enterprise systems will only be deleted in compliance with legal or government mandates.

14. Hacking Prevention and Guidelines

The security of the university's IT resources is a shared responsibility between the IT department and all users, including faculty, staff, and students. The following guidelines aim to prevent hacking and ensure the safety and integrity of our digital infrastructure.

IT Department Responsibilities:

- **Maintain Software Updates:** Ensure all university-owned systems and software are regularly updated with the latest security patches.
- **Secure Network Infrastructure:** Manage and maintain network devices and firewalls and ensure secure configurations.
- **Provide Security Software:** Install and maintain antivirus and anti-malware software on university-owned devices.
- **Conduct Regular Backups:** Regularly back up critical university data and ensure data encryption.
- **Limit Access and Permissions:** Implement role-based access controls to restrict access to sensitive information.

End User Responsibilities:

- **Update Personal Devices:** Keep devices updated with the latest software patches and security updates.
- **Ethical Use of IT Devices:** Ensure that IT devices are used for academic, research, and university-related purposes in compliance with ethical and legal standards.
- **Use Strong Passwords:** Create and maintain strong and unique passwords for all university accounts.
- **Install Security Software**: Maintain up-to-date antivirus and anti-malware software on personal devices.
- **Enable MFA:** Utilize multi-factor authentication where available.
- **Be Vigilant with Emails:** Avoid clicking suspicious links or downloading attachments from unknown sources.
- **Backup Important Data:** Regularly backup important data to prevent loss in case of device failure or other unforeseen circumstances.
- **Report Suspicious Activity:** Immediately report any suspicious activity or security incidents to the IT department.
- **Perform Regular Maintenance:** Regularly perform maintenance tasks to ensure optimal device performance.
- **Use Licensed Software:** Use only licensed and authorised software on personally and university-owned devices.
- **Secure Connections:** Connect devices only to secure and authorised networks. Avoid using public Wi-Fi for sensitive activities.
- **Respect Privacy Regulations:** Follow privacy regulations and guidelines, especially when handling sensitive information.
- **Prompt Reporting:** Promptly report any security concerns, suspicious activities, or potential threats to the university's IT security team.

15. IT Support and Services

The IT Support services are available to assist staff and students in accessing University-owned IT resources securely.

If you have any queries about the university's IT services, email our IT Support team or visit them in person from Monday to Friday between 9:00 AM and 5:00 PM. To ensure quick resolution, we adhere to the following escalation matrix:

Level	Contact	Response Time	Resolution Time	Responsibilities
Level 1	**IT Helpdesk & Technical Support:** systems@anu.edu.in (Digital) ithelpdesk@anu.edu.in (Infrastructure)	Within 2 hours	Within 8 hours	Initial ticket analysis, basic troubleshooting , resolution or escalation
Level 2	**Sr. Executive & Subject Matter Experts:** janki.vaja@anu.edu.in (Digital) pragnesh.soni@anu.edu.in (Infrastructure)	Within 4 hours	Within 24 hours	Advanced troubleshooting , investigation, resolution of complex or critical issues, Expert-level support or escalation
Level 3	**Director IT** tauseef.hussain@anu.edu.in	Within 4 hours	Within 48 hours	Resolution of complex or critical issues, Management involvement in decision-making , resource allocation

16. User Compliance

By utilising Anant University's IT resources, including all hardware and software owned, licensed, or managed by the university, individuals agree to comply with the university's IT policies. This applies to using the university network through physical or wireless connections, regardless of device ownership.

Failure to comply may result in penalties, including those imposed by third-party service providers, for which the signatory will be responsible.