ANANT
NATIONAL
UNIVERSITY
॥ प्रज्वालितो ज्ञानमयः प्रदीपः ॥

IT POLICY & GUIDELINES

October 2025, Version 1.1

1. Introduction **4**

2. Definition **4**

3. Scope **5**

4. Objective **5**

5. Roles and responsibilities **6**

6. Acceptable Use **6**

- a. General Responsibilities 6
- b. Explicitly Prohibited Activities 7
- c. Enforcement 7

7. Privacy and Personal Rights **7**

8. Email Privacy **8**

9. Use of IT Devices Issued by Anant **8**

- a. Ownership and Responsibility 8
- b. Device Configuration and Support 8
- c. Connection of External Devices 9
- d. Monitoring and Control 9
- e. Loss, Theft, or Misuse 9

10. Network Access and Security **9**

- a. General Access 9
- b. Official VPN for Secure Remote Access 9
- c. Guest Network Access 10
- d. Filtering and Blocking of Sites 10
- e. Monitoring and Security Compliance 10

11. Password Policy **10**

- a. Password Complexity 10
- b. Password Expiration & Change 10
- c. Password Reuse Restrictions 10
- d. Multi-Factor Authentication (MFA) 11
- e. Single Sign-On (SSO) 11
- f. Password Storage & Sharing 11
- g. Administrative Accounts 11

12. Monitoring and Privacy **11**

- a. Scope of Monitoring 11
- b. User Notification 11
- c. Data Retention 12
- d. Consent & Acknowledgment 12
- e. Safeguards 12

13. Bring Your Own Device (BYOD) Policy **12**

- a. Responsibilities of Users 12
- b. University Responsibilities and Rights 13
- c. Compliance and Enforcement 13

d. Acknowledgment 13

14. Email Usage Policy 14

15. Access to Social Media and OTT Platforms 15

16. Data Management Policy 16

a. Data Security 16

b. Data Privacy 16

c. Data Retention 16

17. Hacking Prevention and Guidelines 16

a. IT Department Responsibilities 16

b. End User Responsibilities 17

18. IT Support and Services 17

19. Policy Review and Updates 18

a. Review Frequency 18

b. Responsible Authority 18

c. Approval 19

d. Communication of Updates 19

20. User Compliance and Declaration 19

21. Annexures 19

Annexure A 20

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. Definition

For the purpose of this IT Policy, the following terms shall have the meanings as defined below.

1. Anant - Anant National University
2. IT Resources - All hardware, software, systems, networks, cloud services, and data owned, licensed, or managed by Anant University, including devices connected to the university network, whether university-owned or personal.
3. User - Any faculty, staff, student, contractor, vendor, consultant or visitor, including visiting guest faculty, who is authorised to access or use Anant’s IT resources.
4. University Network - All wired, wireless, and virtual private networks (VPNs) managed or approved by the university, including internal intranet and internet connections.
5. Sensitive Data - Any data classified as confidential, restricted, or personally identifiable (PI), including student records, employee information, financial data, and research outputs.
6. Confidential Information - Information accessible only to authorised personnel due to its sensitive nature; unauthorised disclosure may adversely affect the university and/or individuals.
7. Data Owner - A university official responsible for classifying, approving access, and setting retention rules for a specific set of data.
8. Data Custodian - The individual or team responsible for implementing security measures, backups, and operational controls for data, under the direction of the Data Owner.
9. End User - An individual who uses IT resources but is not responsible for system administration or policy enforcement.

10. BYOD (Bring Your Own Device) - The use of personal devices (e.g., laptops, smartphones, tablets) to connect to the university network or access university resources.
11. Encryption - The process of converting information into a secure format that can only be accessed or decrypted by authorised parties.
12. Incident - Any event that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of IT resources (e.g., data breach, malware infection, system outage).
13. Disaster Recovery (DR) - The set of procedures and tools used to restore IT systems and data following an outage, breach, or disaster.
14. Business Continuity Plan (BCP) - A documented strategy to ensure essential operations continue during and after disruptive incidents.
15. Third-Party Vendor - Any external contractor, supplier, or service provider who is granted access to, or handles, university IT resources, systems, or data.
16. Acceptable Use - The set of rules and responsibilities governing proper and authorised usage of IT resources in compliance with laws, policies, and ethical standards.

3. 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.

4. 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.

5. 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.

6. Acceptable Use

An authorised user may access only the IT resources for which they have been granted explicit permission. Each individual is responsible for using assigned resources (computers, accounts, software, devices, and network access) in an ethical, secure, and policy-compliant manner.

a. General Responsibilities

i. Protect passwords and accounts from unauthorised use.
ii. Safeguard IT resources against misuse or compromise.
iii. Adhere to all relevant university policies and applicable laws.

b. Explicitly Prohibited Activities

The following activities are strictly prohibited when using Anant University’s IT resources:

i. Misuse of Accounts and Access

1. Using another individual’s account or attempting to capture/guess another user’s password.

    2. Attempting to access restricted areas of the network, operating systems, or administrative applications without authorisation.

ii. **Commercial and Unethical Use**

    1. Using IT resources for personal financial gain, private business, or unauthorised commercial purposes.
    2. Engaging in fraudulent, harassing, threatening, defamatory, or obscene communication.

iii. **Piracy and Intellectual Property Violations**

    1. Downloading, distributing, or using pirated software, media, or copyrighted material without proper licensing or approval.

iv. **Security Violations**

    1. Intentionally introducing malware, viruses, worms, trojans, or any malicious code.
    2. Attempting to bypass security mechanisms, firewalls, or network filtering systems (e.g., via unauthorised VPNs or proxies).

v. **Improper Use of University Platforms**

    1. Unauthorised use of social media and OTT platforms during official working hours, unless work-related.
    2. Using IT resources in a manner that disrupts university operations, reduces productivity, or negatively impacts the institution’s reputation.

vi. **Device and Resource Misuse**

    1. Sharing university-issued laptops or devices with non-authorised individuals (e.g., family, friends, outsiders).
    2. Installing unlicensed or unauthorised software on university-owned devices.

c. Enforcement

Any violation of this Acceptable Use Policy will result in disciplinary action, which may include suspension of IT privileges, academic/administrative penalties, or legal action under applicable laws.

7. 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 without proper authorisation and approval from the Competent Authority is strictly prohibited.

8. 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.

9. Use of IT Devices Issued by Anant

IT devices such as desktops, laptops, external storage media, and peripherals provided by Anant University are designated strictly for academic, research, and official university use. Their use must adhere to legal, ethical, and security standards, following the best practices outlined in this policy.

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.

a. Ownership and Responsibility

i. All IT devices allocated to faculty and staff are university property and are issued based on job requirements approved by the respective Head of Department (HoD).

ii. Employees are responsible for safeguarding assigned devices and must return them to the IT Department upon separation from the university as part of the no-dues clearance process.

b. Device Configuration and Support

i. Only the IT Department is authorised to install or modify system configurations, software, or hardware.

ii. All software must be licensed and pre-approved by the IT Department.

iii. Repairs, replacements, or upgrades must be handled exclusively through the IT Department; external servicing is prohibited.

c. Connection of External Devices

i. The connection of external storage devices (e.g., USB drives, portable hard disks) to any university-owned system is restricted and requires approval from the respective Head of Department (HoD).
ii. Users are prohibited from transferring confidential, sensitive, or personally identifiable data to non-approved external devices.

d. Monitoring and Control

i. The IT Department reserves the right to audit connected devices and maintain logs of external device usage.
ii. Systems are equipped with endpoint protection to detect, block, or restrict unauthorised device connections.
iii. Any unauthorised connection attempt will be reported as a security incident and may result in disciplinary action.

e. Loss, Theft, or Misuse

i. In case of loss, theft, or suspected misuse of a university device or any connected external media, users must report the incident immediately to the IT Department.

10. Network Access and Security

Anant provides secure network access to support academic, research, and administrative activities. To maintain security and compliance, the following guidelines apply:

a. General Access

i. Access to the University’s campus-wide LAN and wireless networks requires prior one-time approval from the IT Department.
ii. Users must register their devices before connecting. Each user may connect up to two devices unless additional access is approved by the IT Department or Head of Department.

b. Official VPN for Secure Remote Access

i. Use of unauthorised VPNs or tunnelling applications to bypass security controls is strictly prohibited.
ii. The University provides an official, secure VPN service for approved faculty, staff, and students who require remote access to internal resources.
iii. Access to the official VPN is granted only upon request, subject to IT Department approval, and requires multi-factor authentication (MFA).

c. Guest Network Access

i. Guests and visitors may be granted access to a segregated Guest Wi-Fi network for internet browsing only.

ii. The Guest Wi-Fi does not provide access to internal university systems, servers, or data.
iii. Access is time-limited (e.g., 24 hours or duration of visit) and requires sponsorship by a faculty or staff member.

d. Filtering and Blocking of Sites

i. The IT Department may block content that violates the IT Act 2000, relevant laws, or university policies.
ii. Content deemed inappropriate, illegal, or harmful to productivity or network security may also be blocked.

e. Monitoring and Security Compliance

i. The IT Department conducts periodic network audits and monitoring to ensure compliance.
ii. Any suspicious or unauthorised activity will result in immediate revocation of access and may lead to disciplinary action.

11. Password Policy

To safeguard university systems and data, all users must adhere to the following password standards:

a. Password Complexity

i. Minimum length of 10 characters.
ii. Must include at least:
   1. One uppercase letter (A–Z)
   2. One lowercase letter (a–z)
   3. One number (0–9)
   4. One special character (!, @, #, $, %, etc.)

iii. Passwords must not contain personal information (e.g., name, date of birth, student ID).

b. Password Expiration & Change

i. Passwords must be changed at least once every 21 days.
ii. Users will receive automated reminders prior to expiration.
iii. Passwords must be changed immediately if compromise is suspected.

c. Password Reuse Restrictions

i. The last five passwords cannot be reused.
ii. Similar or sequential passwords (e.g., “Password1”, “Password2”) are prohibited.

d. Multi-Factor Authentication (MFA)

i. MFA is mandatory for all sensitive systems, remote access (VPN), and administrative accounts.

e. Single Sign-On (SSO)

i. Anant uses Single Sign-On (SSO) for select enterprise and departmental applications to enhance security and simplify user access.
ii. Users authenticated through SSO are subject to the same password complexity and MFA requirements as outlined in this policy.
iii. Password changes made under SSO automatically apply across all linked University systems.
iv. Users must not share SSO credentials under any circumstances; any compromise must be reported immediately to the IT Department.

f. Password Storage & Sharing

i. Passwords must never be shared with others.
ii. Passwords must not be written down or stored in unencrypted files.
iii. Use of university-approved password managers is recommended.

g. Administrative Accounts

i. Default passwords on new systems must be changed immediately.
ii. Shared or generic administrative accounts are prohibited; each administrator must have a unique ID.

12. Monitoring and Privacy

Anant recognises the importance of balancing institutional security with individual privacy rights. Accordingly, monitoring of IT resources is carried out in a transparent and lawful manner, with the following clarifications:

a. Scope of Monitoring

i. The IT Department may monitor:
    - Network traffic (metadata such as source, destination, time, bandwidth usage).
    - Device and system logs (login/logout times, access attempts, system errors).
    - Email and file content only when required for compliance, investigation of misconduct, or security incident response, and with prior approval from the competent authority.

ii. Routine monitoring does not include continuous inspection of personal communications unless explicitly warranted.

b. User Notification

i. Users are notified of this monitoring through:
    - This IT Policy and its regular updates.
    - Mandatory acknowledgement at the time of receiving IT account access.
    - Periodic reminders during annual compliance or awareness training.

c. Data Retention

i. Monitoring logs and audit records are retained for a period of 180 days by default.
ii. In case of a security incident, investigation, or legal requirement, records may be retained longer until the matter is resolved.
iii. Retained data is stored securely and access is limited to authorised IT Security personnel.

d. Consent & Acknowledgment

i. All users must formally acknowledge this policy by signing the IT Policy Acknowledgement Form before being granted access to university systems.
ii. Use of university IT resources constitutes consent to monitoring under the terms defined in this policy.

e. Safeguards

i. Monitoring is conducted in compliance with applicable privacy and data protection laws.

Any access to user data beyond metadata requires documented approval from the competent authority.

13. Bring Your Own Device (BYOD) Policy

This policy establishes the rules for using personally-owned devices to access Anant National University’s network, systems, and data. Its goal is to support flexible academic and administrative work while maintaining the Confidentiality, Integrity, and Availability (CIA) of University information. This policy applies to all faculty, staff, students, contractors, and visitors who use personal laptops, tablets, or mobile phones to connect to University systems or services.

a. Responsibilities of Users

Users connecting personal devices to the University network must:

Secure the Device

i. Use strong authentication methods, such as a password, PIN, or biometric lock, in accordance with the University’s Password Policy.
ii. Keep the operating system and all applications up to date with the latest security patches.
iii. Install and maintain updated antivirus or anti-malware software.

Access Controls

i. Connect only through University-approved wireless networks (e.g., Anant-Staff, Anant-Student).

ii. Use of unauthorised hotspots, routers, or network-sharing tools is prohibited.
iii. Remote access to internal systems must occur only through the official University VPN with multi-factor authentication (MFA).

Data Handling

i. University Data, particularly confidential or sensitive information, must not be permanently stored on personal devices.
ii. All institutional files must be stored on University-approved cloud or network drives.
iii. Upon separation from the University or a change in role, users must permanently remove all University data and licensed applications from their personal devices.

Incident Reporting

i. Any loss, theft, or suspected compromise of a personal device that has accessed University systems must be reported immediately to the IT Department.

b. University Responsibilities and Rights

i. The IT Department will assist only with network connectivity and access to licensed University applications; it will not service, configure, or repair personal hardware or software.
ii. The University reserves the right to monitor and log traffic from any device connected to its network, as outlined in the Monitoring and Privacy section of this policy.
iii. Devices found to pose security risks may be disconnected or blocked from the University network without notice.

c. Compliance and Enforcement

Non-compliance with this BYOD Policy or the broader IT Policy & Guidelines may result in immediate suspension or revocation of network access, as well as disciplinary action in accordance with University regulations.

d. Acknowledgment

Use of a personal device to access University IT resources constitutes acknowledgement of, and agreement to, these terms and all relevant sections of the Anant University IT Policy & Guidelines.

14. 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 are 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.

15. 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.

16. Data Management Policy

This data management policy applies to all enterprise software applications that generate, modify, and archive Anant enterprise data (Refer to the Data Management Policy for detailed information).

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.

17. 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.

a. IT Department Responsibilities

i. Maintain Software Updates: Ensure all university-owned systems and software are regularly updated with the latest security patches.

ii. Secure Network Infrastructure: Manage and maintain network devices and firewalls and ensure secure configurations.

iii. Provide Security Software: Install and maintain antivirus and anti-malware software on university-owned devices.

iv. Conduct Regular Backups: Regularly back up critical university data and ensure data encryption.

v. Limit Access and Permissions: Implement role-based access controls to restrict access to sensitive information.

vi. Cybersecurity Awareness and Training: Conduct regular user awareness and cybersecurity training programs to help faculty, staff, and students identify and prevent social engineering, phishing, and other cyber threats. Participation in these sessions is mandatory for all network users.

b. End User Responsibilities

i. Update Personal Devices: Keep devices updated with the latest software patches and security updates.

ii. 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.

iii. Use Strong Passwords: Create and maintain strong and unique passwords for all university accounts.

iv. Install Security Software: Maintain up-to-date antivirus and anti-malware software on personal devices.

v. Enable MFA: Utilize multi-factor authentication where available.

vi. Be Vigilant with Emails: Avoid clicking suspicious links or downloading attachments from unknown sources.

vii. Backup Important Data: Regularly backup important data to prevent loss in case of device failure or other unforeseen circumstances.

viii. Report Suspicious Activity: Immediately report any suspicious activity or security incidents to the IT department.

ix. Perform Regular Maintenance: Regularly perform maintenance tasks to ensure optimal device performance.

x. Use Licensed Software: Use only licensed and authorised software on personally and university-owned devices.

xi. Secure Connections: Connect devices only to secure and authorised networks. Avoid using public Wi-Fi for sensitive activities.

xii. Respect Privacy Regulations: Follow privacy regulations and guidelines, especially when handling sensitive information.

xiii. Prompt Reporting: Promptly report any security concerns, suspicious activities, or potential threats to the university's IT security team.

18. 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

19. Policy Review and Updates

a. Review Frequency

i. This IT Policy shall be reviewed annually, or sooner if required due to changes in technology, legislation, regulatory requirements, or significant security incidents.

b. Responsible Authority

i. The IT Governance Committee, chaired by the Director of IT, is responsible for reviewing and recommending updates to this policy.

ii. Proposed changes shall be reviewed in consultation with relevant stakeholders, including academic departments, administration, and legal counsel (if required).

c. Approval

i. Final approval of updates rests with the University Academic Council.

d. Communication of Updates

i. All changes to this policy will be communicated to users within 30 days of approval.

ii. Updated versions will be published on the University's official website/portal, and users will be notified via official email.

20. User Compliance and Declaration

By accessing or using Anant University's IT resources - including systems, software, email, network, internet, cloud services, and devices - users agree to:

- Comply with all rules, procedures, and standards outlined in the Anant University IT Policy & Guidelines.
- Use IT resources solely for authorised academic, research, administrative, and institutional purposes.
- Abide by applicable laws and regulations, including those governing data protection, intellectual property, and cybersecurity.
- Acknowledge that the university may monitor and log IT activities to ensure security and policy compliance, in accordance with legal requirements and institutional oversight.
- Promptly report any suspicious, unethical, or unauthorised IT activities to the IT Department.

Failure to comply with this policy may result in disciplinary action, including suspension of access, termination of privileges.

21. Annexures

Annexure A: IT Policy Acceptance Form

Annexure B: Data Management Policy (Detailed guidelines for handling, classifying, retaining, and protecting university data.)

Annexure A

(IT Policy Acceptance Form)

All users must complete this form before being granted access to university IT resources.

Name	
Employee/ Student ID	
Designation/ Department	
Email Address	
Mobile Number	

Declaration:

1. I hereby acknowledge that I have read, understood, and agree to comply with the Anant University IT Policy & Guidelines.
2. I understand that all IT activities on university resources are subject to authorised monitoring for security and compliance purposes.
3. I agree to use these resources responsibly, ethically, and lawfully, and I acknowledge that violating this policy may result in disciplinary or legal action.

Signature : ____________________________________

Date : ____/_____/______