



भारतीय प्रबंध संस्थान बोधगया
**Indian Institute of Management
Bodh Gaya**

Indian Institute of Management Bodh Gaya

IT Policy Manual



Information Technology Systems Committee

Table of Contents

IT Policy Manual	5
1. Scope	5
2. Objective.....	5
3. Roles and Responsibilities.....	5
4. Acceptable Use	6
5. Privacy and Personal Rights	7
6. Privacy in Email	7
7. User Compliance	7
8. Access to the Network	7
8.1. Access to Internet and Intranet.....	7
8.2. Access to Institution Wireless Networks	8
8.3. Filtering and blocking of sites	9
9. Monitoring and Privacy	9
10. Access to Social Media Sites from Institution Network	10
11. Security Incident Management Process	10
12. Intellectual Property	11
13. Enforcement.....	12
14. Deactivation of Resources	12
15. Audit of Institution Network Infrastructure.....	12
16. IT Hardware Installation Policy.....	13
17. Software Installation and Licensing Policy	14
17.1. Purpose	14
17.2. Scope	14
17.3. Policy Guidelines.....	14
17.4. Roles and Responsibilities.....	15
18. Use of IT Devices on Institution Network.....	15
18.1. Scope	16
18.2. General Guidelines	16
18.3. Personally Owned Devices (BYOD).....	16
18.4. Device Misuse	16
18.5. Enforcement and Penalties	17
19. Network (Intranet & Internet) Use Policy	17
19.1. Purpose	17
19.2. Scope	17
19.3. General Guidelines	17

20.	Email Account Usage Policy	18
20.1.	Purpose	18
20.2.	Applicability	19
20.3.	Policy Guidelines.....	19
20.4.	Enforcement	20
21.	Institutional Repository (IR).....	20
21.1.	What is IR (Institutional Repository)?.....	20
21.2.	What Does IR contain?.....	20
21.3.	Who will be entitled to access Indian Institute of Management Bodh Gaya IR?	21
21.4.	How will you access the IR?	21
21.5.	Validity Period of Accessibility of IR	21
21.6.	Copyright Violation on IR Use.....	21
22.	Disposal of ICT equipment.....	21
23.	IT Hardware End-of-Life (EOL) Policy	21
23.1.	Purpose	21
23.2.	Scope	22
23.3.	Lifecycle of IT Assets.....	22
23.4.	EOL Management Guidelines	22
23.5.	Roles and Responsibilities.....	22
23.6.	Enforcement	22
24.	Budgetary provisions for ICT	23
24.1.	Purpose	23
24.2.	Scope	23
24.3.	Policy Guidelines.....	23
24.4.	Roles and Responsibilities.....	24
25.	Breach of This Policy	24
26.	Revisions to Policy	24
27.	Contact Us	25
	FORM FOR REQUISITION OF OFFICIAL EMAIL ID.....	26
	FORM FOR REQUISITION OF WI-FI ACCESS.....	27
	FORM FOR REQUISITION OF WI-FI ACCESS.....	28

Abbreviations

Sl. No.	Abbreviation	Description
1	IIMBG	Indian Institute of Management, Bodh Gaya.
2	CA	Competent Authority
3	LAN	Local Area Network
4	ITS COMMITTEE	Information Oasis Centre
5	ICT	Information and Communication Technology
6	IP	Internet Protocol
7	DHCP	Dynamic Host Configuration Protocol
8	IR	Institutional Repository
9	EULA	End User License Agreement
10	CAPEX	Capital Expenditure
11	OPEX	Operational Expenditure

IT Policy Manual

The Indian Institute of Management Bodh Gaya offers technological resources to support its administrative, academic, and academic activities as well as to increase employee effectiveness and productivity. These resources are designed to serve as tools for accessing and processing information relevant to their respective fields of expertise. Additionally, they assist users in staying informed and performing their tasks productively.

This document lays forward precise guidelines regarding how to utilize all of IIMBG's IT facilities. All users of IIMBG-owned or managed computer resources are subject to this policy. Faculty and visiting faculty, Non-faculty, students, alumni, visitors, external individuals, organizations, departments, offices, affiliated colleges, and any other entity under the management of the Indian Institute of Management Bodh Gaya that uses computing facilities to access network services are among the people covered by the policy.

In this policy, the term “IT Resources” refers to all hardware and software that is owned, licensed, or managed by the Institution, as well as the use of the Institution's network through either a physical or wireless connection, irrespective of the ownership of the machine or gadget that is connected to the network.

The improper use of these resources may lead to unnecessary risks and liabilities for the Institution. Consequently, it is anticipated that these resources will be utilized mainly for purposes related to the Institution and in a lawful and ethical way.

1. Scope

This policy outlines the guidelines for utilizing IT Resources from the viewpoint of an end user. This guideline applies to all individuals, users, and entities, as outlined in the second section who utilize the IT Resources.

2. Objective

This policy is designed at ensuring suitable accessibility as well as utilization of information technology assets at the Indian Institute of Management Bodh Gaya, while avoiding any misuse by users. The utilization of the assets supplied by the Institution signifies the user's consent to adhere to this policy.

1. Institution's IT policy exists to maintain, secure, and ensure legal and appropriate use of the Information technology infrastructure established by the Institution on the campus.
2. This policy establishes institution-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of information assets that are accessed, created, managed, and/or controlled by the Institution.
3. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

3. Roles and Responsibilities

The following roles and responsibilities are outlined by each entity, respectively.

1. Institutions shall implement appropriate controls to ensure compliance with this policy by their users. ITS COMMITTEE shall be the primary implementation point of contact and shall provide necessary support in this regard.

2. ITS COMMITTEE shall ensure resolution of all incidents related to the security aspects of this policy by its users. The Implementing Agency shall provide the requisite support in this regard.
3. Use Institution ITS COMMITTEE resources for those activities that are consistent with the academic, research and public service mission of the Institution and are not “Prohibited Activities”.
4. All users shall comply with existing national, state and other applicable laws.
5. Abide by existing telecommunications and networking laws and regulations.
6. Follow copyright laws regarding protected commercial software or intellectual property.
7. As members of the Indian Institute of Management Bodh Gaya, users are provided access to scholarly and work-related resources, including the library, computer systems, servers, software, databases, and the Internet. The ITS Committee is expected to ensure that these resources are available for unobstructed and legitimate use, while safeguarding users’ reasonable expectations of privacy and protection from misuse or intrusion by others. Authorized users have the right to access information and express their opinions through these electronic platforms, just as they would through traditional, non-electronic means of communication.
8. Users of Institution shall not install any network/security device on the network without consultation with the ITS COMMITTEE.
9. It is the responsibility of all members of the institutional community to be aware of and adhere to the regulations and policies governing the appropriate use of the Institute’s technologies and resources. Users are expected to exercise sound judgment in utilizing these technological and information resources. The mere fact that an action is technically feasible does not imply that it is appropriate or permissible to undertake that action.
10. All members of the institutional community, as representatives of the Institute, are expected to respect and uphold the Institute’s reputation and good name in all activities involving the use of ICT communications, both within and outside the institution.

4. Acceptable Use

1. An authorized user may use only the IT resources he/she has authorization. No user should use another individual's account or attempt to capture or guess other users' passwords.
2. Each user is responsible for the proper use of all resources given to them, such as their computer, network address or port, software, and hardware. They are accountable to the Institute for how these resources are used. Authorized users must not misuse IT resources or allow unauthorized people to access the Institute’s network, whether through Institute devices or their own personal computers connected to the campus LAN.
3. The institution 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.
4. Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access.
5. Users must not attempt to access restricted systems or applications without proper authorization.

6. Users must comply with the policies and guidelines for any specific set of resources to which he/she has been granted access.
7. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

5. Privacy and Personal Rights

1. All users of the institution's IT resources are expected to respect the privacy and personal rights of others.
2. Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA).
3. Although the institution generally does not keep an eye on or restrict the content of information sent over the campus-wide local area network (LAN), it does retain the right, under particular circumstances and with the proper authorization from the relevant authorities, to access and evaluate such information.

6. Privacy in Email

IIM Bodh Gaya makes every effort to protect the privacy of email users, but complete privacy cannot always be assured. Since faculty, Non faculty, and students are given access to the Institute's electronic systems and network services for official use, the Institute may, with approval from the competent authority, access and review stored information when needed, after taking the user's consent.

7. User Compliance

1. Accepting an Institute-issued account means agreeing to follow IT guidelines and to stay updated as rules change.
2. By using the Institute's IT resources or accepting an Institute-issued account, every user (faculty, Non faculty, student, or visitor) automatically agrees to abide by all current IT policies, regulations, and guidelines.
3. Users must ensure that IT resources are used only for authorized academic, research, and administrative purposes. Misuse, whether intentional or negligent, will be treated as a violation of policy.
4. Users must ensure that their use of IT resources does not harm the reputation of the Institute, compromise data security, or disrupt services for others.
5. Compliance with IT policies is mandatory, and failure to comply may lead to disciplinary action under the Institute's rules and regulations, including suspension of access, reporting to higher authorities, or legal action where applicable.

8. Access to the Network

8.1. Access to Internet and Intranet

1. Before connecting any client system (desktop, laptop, or other device) to the Institute's campus-wide Local Area Network (LAN), the user must register the system and obtain prior one-time approval from the competent authority (ITS Committee/IT Department). This ensures that only authorized and compliant devices are permitted on the network.
2. The Institute operates and maintains independent National Knowledge Network (NKN) connections for

Internet and Intranet access. Both networks are strictly segregated, with no physical connection or bridging devices permitted between them. End-point compliance mechanisms, such as firewalls, access control, and monitoring systems, shall be enforced on both networks to prevent unauthorized access, misuse, or data leakage.

3. Users shall not attempt to bypass network filtering systems, firewalls, or security controls through any website, proxy, tunneling software, or unauthorized application. Activities that compromise the performance, integrity, or security of the Institute's network are strictly prohibited and may result in disciplinary or legal action.
4. For security, auditing, and compliance purposes, all Internet and Intranet access through the Institute's network may be monitored and logged into by the IT Department. This includes, but is not limited to, websites visited, applications accessed, and data traffic patterns. Users are expected to respect these monitoring practices as part of institutional governance.
5. The Institute enforces a fair usage policy to ensure equitable distribution of bandwidth among all users. Excessive or unauthorized consumption of network resources (e.g., large personal downloads, streaming, or gaming) that negatively impacts academic and administrative usage may lead to suspension of network access.
6. Each user is responsible for all activities carried out through their assigned login credentials and registered devices. Sharing of credentials or unauthorized use of another user's system or account is strictly prohibited. Any violations will be traced to the registered user and dealt with under the Institute's disciplinary framework.
7. As a premier educational institution, IIM Bodh Gaya provides high-speed Internet access through the National Knowledge Network (NKN) to support academic, research, and administrative needs. The network infrastructure is a shared resource, and its proper use is critical for maintaining smooth academic operations, faculty research, online classes, digital libraries, and collaboration with other institutions. All members of the IIM Bodh Gaya community are expected to use these facilities responsibly and in alignment with the Institute's mission of academic excellence and integrity.

8.2. Access to Institution Wireless Networks

For connecting to an Institution wireless network, user shall ensure the following:

1. Access to the Institute's wireless networks (Wi-Fi) shall be granted only through proper authentication using Institute-issued credentials (such as username and password, or device MAC registration). Anonymous or guest access is not permitted unless explicitly approved by the competent authority.
2. Each user must register all personal and institutional devices (laptops, tablets, smartphones, etc.) with the IT Department before connecting to the wireless network. Unregistered devices may be blocked from accessing institutional resources.
3. Wireless connectivity is provided to support academic, research, and administrative purposes. Use of Wi-Fi for unauthorized activities such as peer-to-peer downloads, gaming, cryptocurrency mining, or any activity that disrupts the network or depletes bandwidth is prohibited.
4. Users are responsible for ensuring that devices connecting to the Wi-Fi network have up-to-date antivirus protection, operating system patches, and security configurations. The Institute may enforce endpoint compliance checks to block non-compliant devices.
5. Temporary Wi-Fi access for visitors, guest faculty, or event participants may be arranged through the IT Department with prior approval from the competent authority. Guest credentials will be time-bound and usage-monitored.
6. Wireless network activity is subject to monitoring and logging for security, auditing, and performance purposes. Fair usage limits may be applied to ensure equitable access for all users. Excessive or abusive

use may result in bandwidth restrictions or suspension of access.

7. The user whose credentials or registered device accesses the Wi-Fi network is fully accountable for all activities carried out as per institute. Sharing of Wi-Fi credentials or unauthorized hotspot creation is strictly prohibited.

8.3. Filtering and blocking of sites

1. The ITS Committee may block access to websites or online content that contravenes Government of India rules, regulations, directives, or other applicable legal provisions. This includes content restricted under the IT Act, UGC/MoE guidelines, or orders from statutory authorities.
2. Content or platforms that pose a potential security threat to the Institute's IT infrastructure, such as malware-hosting sites, phishing portals, or unauthorized VPN/proxy services, may be blocked without prior notice.
3. The ITS Committee may restrict access to websites or applications deemed inappropriate or non-academic in nature (e.g., gaming, streaming, social networking, or entertainment platforms) if they adversely impact user productivity or consume excessive bandwidth needed for academic and administrative functions.
4. In cases where blocked content is required for legitimate academic, research, or pedagogical purposes, users may request temporary access through a formal application to the IT Department, subject to approval by the competent authority.
5. Wherever possible, users will be notified when access to a website is blocked and may be provided with a reason (legal compliance, security, or productivity).
6. The list of blocked sites shall be periodically reviewed by the ITS Committee to ensure alignment with institutional needs, evolving technologies, and academic requirements.
7. Any attempt to bypass or tamper with the filtering mechanisms (e.g., through proxies, VPNs, or unauthorized software) will be considered a violation of the Institute's IT Policy as well as Government of India's IT and cyber regulations. Such actions may lead to suspension of network privileges, reporting to the competent authority, and disciplinary action as per IIM Bodh Gaya's rules, in addition to any legal consequences under applicable government laws.

9. Monitoring and Privacy

1. The Institute reserves the right to monitor, log, and review all activities conducted on its IT resources (including Internet, Intranet, Wi-Fi, email, and servers) to ensure compliance with institutional policies, security requirements, and applicable laws.
2. Monitoring may include, but is not limited to, tracking websites visited, bandwidth usage, applications accessed, login activities, emails (subject to approval), and data traffic across the Institute's network.
3. While IIM Bodh Gaya makes reasonable efforts to respect the privacy of its users, absolute privacy cannot be guaranteed when using Institute-provided IT resources. Users should have no expectation of complete confidentiality for information stored, transmitted, or accessed via institutional systems.
4. Access to a user's stored data, email, or files will only be undertaken with the approval of the competent

authority (e.g., Director or designated official), and where necessary, with the consent of the user, except in cases of suspected misconduct, legal obligations, or security threats.

5. Monitoring and access to user data will be carried out in accordance with the Information Technology Act, 2000, CERT-In directives, and other applicable Government of India rules and regulations.
6. Information gathered through monitoring will be used strictly for maintaining security, investigating policy violations, ensuring compliance, or meeting legal obligations. Such information will not be misused or disclosed to third parties without due authorization.
7. Wherever feasible, the Institute will notify users of monitoring practices through official communications or policy documents to maintain transparency and trust.
8. Any activity detected through monitoring that violates institutional policy, government laws, or compromises security will result in disciplinary action, which may include suspension of IT access, reporting to higher authorities, or legal action.

10. Access to Social Media Sites from Institution Network

1. Use of social networking sites by Institution users is governed by “Framework and Guidelines for use of Social Media for Government Organizations”.
2. Users shall comply with all the applicable provisions, while posting any information on social networking sites.
3. User shall adhere to the “Terms of Use” of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment, and other applicable laws.
4. User shall report any suspicious incident as soon as possible to the competent authority.
5. Users should always use high security settings on social networking sites.
6. User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.
7. Users shall not disclose or use any confidential information obtained in their capacity as an employee of the Institution.
8. User shall not make any comment or post any material that might otherwise cause damage to Institution reputation.

11. Security Incident Management Process

To ensure the confidentiality, integrity, and availability of IIM Bodh Gaya’s IT resources, the following process shall be followed for security incident management:

1. Incident Identification and Reporting
 - a. All users (faculty, non-faculty, students) must promptly report any suspected or actual IT security incidents (e.g., malware, phishing, unauthorized access, data breach, hardware theft) to the IT Department/ITS Committee Helpdesk.
 - b. Reports should include details such as the nature of the issue, affected system, time of detection, and any unusual activity observed.
2. Logging and Categorization
 - a. The IT Department will log on to every reported incident in the Security Incident Register.

- b. Incidents will be categorized based on severity:
 - i. Low: Localized issues (e.g., malware infection on one device).
 - ii. Medium: Service disruptions (e.g., email or Wi-Fi outage).
 - iii. High: Widespread/systemic issues (e.g., DDoS attack, major data breach).
3. Containment
 - a. Immediate action will be taken to limit the spread or impact of the incident (e.g., isolating infected devices, disabling compromised accounts, blocking malicious IPs/domains).
 - b. Users may be temporarily denied network access if their system is the source of the problem.
4. Investigation and Analysis
 - a. The IT Department, in consultation with the ITS Committee, will analyze system logs, network traffic, and security alerts to determine root cause and scope.
 - b. In case of major incidents, CERT-In (Computer Emergency Response Team – India) and law enforcement agencies will be notified as per Government of India requirements.
5. Eradication and Recovery
 - a. Removal of malware, unauthorized software, or compromised accounts.
 - b. Restoration of affected systems from backups or clean images.
 - c. Application of patches, updates, and security fixes to prevent recurrence.
6. Communication
 - a. Stakeholders (Director, faculty, non-faculty, students) will be informed of major incidents, service disruptions, and timelines for restoration.
 - b. Sensitive details will be shared only on a need-to-know basis to protect institutional security.
7. Post-Incident Review
 - a. A formal review will be conducted after resolution to document:
 - i. What happened
 - ii. How it was handled
 - iii. Lessons learned
 - iv. Preventive measures for the future
 - b. Recommendations will be incorporated into updated IT security policies and user awareness training.
8. Disciplinary Action
 - a. If the incident is caused by negligence, misuse, or violation of IT Policy, disciplinary measures will be taken against the responsible user(s), in addition to any legal action required under Government of India cyber laws.

12. Intellectual Property

All material accessible through the Institute's IT resources and network may be subject to intellectual property protections, including but not limited to copyrights, patents, trademarks, trade secrets, and other proprietary rights, as well as privacy and publicity rights. Users are prohibited from using the Institute's IT resources in any manner that infringes, misappropriates, dilutes, or otherwise violates such rights. It is the responsibility of every user to respect intellectual property laws and institutional policies while accessing, sharing, or distributing digital content.

13. Enforcement

1. This IT Policy applies to all users of the Institute's IT resources, including faculty, Non faculty, students, visiting scholars, and external collaborators. Compliance with these provisions is mandatory.
2. Each unit or entity of the Institute is responsible for ensuring adherence to this policy within their area of operation. The IT Department/ITS Committee will provide necessary technical assistance to support compliance.

14. Deactivation of Resources

1. **Immediate Deactivation:** In the event of any threat to the security, stability, or integrity of the Institute's IT systems or network arising from the activities of a user or their resources, the ITS Committee reserves the right to immediately deactivate the concerned resource (e.g., device, account, or network access) without prior notice. After such deactivation, the concerned user and the competent authority of the Institution shall be informed.
2. **Notification:** Following such deactivation, the concerned user and the competent authority of the Institute shall be formally notified of the action taken, along with the reason for deactivation and steps required for restoration of access.

15. Audit of Institution Network Infrastructure

1. **Purpose of Audit:** Regular audits of the Institute's network infrastructure shall be conducted to ensure security, reliability, efficiency, and compliance with institutional IT policies and Government of India regulations (including IT Act 2000, CERT-In directives, and data protection guidelines).
2. **Responsibility:** The IT Department/ITS Committee shall be responsible for planning, coordinating, and executing the audit of network infrastructure. External auditors or authorized agencies may be engaged for independent verification, wherever required.
3. **Scope of Audit:** The audit will include, but not be limited to:
 - a. LAN and Wi-Fi architecture, access points, and switches.
 - b. Firewalls, intrusion detection/prevention systems, and security appliances.
 - c. Server infrastructure and storage systems.
 - d. Access controls, user authentication, and endpoint compliance.
 - e. Logs, monitoring systems, and data backup processes.
 - f. Compliance with bandwidth allocation and fair usage policies.
4. **Frequency:** Comprehensive audits shall be conducted at least once a year. Critical security checks (e.g., vulnerability scans, penetration testing) may be conducted more frequently, based on risk assessment or emerging threats.
5. **Audit Reporting:** A formal Audit Report shall be prepared after each audit, highlighting vulnerabilities, risks, performance issues, and non-compliance with institutional or government standards. The report shall include recommendations and corrective measures to be implemented within a defined timeline.
6. **Follow-up and Compliance:** The IT Department shall ensure that corrective actions identified during audits are implemented promptly. Progress will be reviewed by the ITS Committee and reported to the competent authority of the Institute.

7. **Confidentiality:** Audit findings shall be treated as confidential information and shared only with authorized stakeholders (ITS Committee, competent authority, and relevant administrative units).
8. **Consequences of Non-Compliance:** Any deliberate attempt to obstruct, manipulate, or avoid the audit process will be treated as a serious violation of the Institute's IT Policy and may lead to disciplinary or legal action.

16. IT Hardware Installation Policy

Institution 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.

1. **Approval Requirement:** All IT hardware installations (desktops, laptops, printers, projectors, servers, networking equipment, etc.) must be approved by the ITS Committee/IT Department before deployment within the Institute.
2. **Procurement and Standards:** Only hardware procured through the Institute's approved procurement process, and meeting prescribed technical specifications, may be installed on the Institute's network or premises. Unauthorized personal hardware is not permitted for institutional use.
3. **Installation Responsibility:** Installation of all IT hardware shall be carried out exclusively by authorized IT Department personnel or by approved vendors under supervision of the IT Department. Users are not permitted to self-install institutional hardware.
4. **Configuration and Compliance:** All newly installed hardware must be configured according to the Institute's IT security and compliance standards (e.g., endpoint protection, antivirus, licensed operating system, and latest patches). Devices not meeting compliance requirements will not be allowed on the Institute's network.
5. **Network Integration:** Hardware intended for connection to the campus LAN, Wi-Fi, or servers must be registered with the IT Department and granted prior approval. Devices found connected without authorization may be disconnected.
6. **Power Connections and Safety:** All computers and peripheral devices (monitors, printers, projectors, UPS, etc.) must be connected only through approved electrical outlets, surge protectors, or UPS systems provided/authorized by the Institute. Direct or unsafe connections to power sources are prohibited. Users must not tamper with electrical fittings or overload circuits.
7. **Inventory and Asset Management:** Every piece of installed IT hardware must be recorded in the Institute's IT Asset Register with details of make, model, serial number, assigned user/department, and installation date.
8. **Maintenance and Warranty:** Installed hardware must remain under warranty, AMC (Annual Maintenance Contract), or Institute-approved maintenance schemes. Any service or repair must be coordinated through the IT Department to ensure standardization and accountability.
9. **User Responsibility:** Users to whom IT hardware is assigned are responsible for its safe custody, appropriate usage, and timely reporting of any malfunction to the IT Department.
10. **Decommissioning or Replacement:** When IT hardware is outdated, damaged beyond repair, or due for replacement, it must be returned to the IT Department. Proper decommissioning and disposal shall be carried out as per Government of India E-Waste Management Rules.
11. **Consequences of Non-Compliance:** Unauthorized installation, unsafe electrical connections,

tampering, or misuse of IT hardware will be treated as a violation of the Institute's IT Policy and may attract disciplinary or administrative action.

17. Software Installation and Licensing Policy

This policy ensures that all software used within the Indian Institute of Management Bodh Gaya (IIMBG) complies with legal, licensing, and security requirements as per Government of India regulations, including the Information Technology Act, 2000, copyright laws, and software licensing agreements.

Institution IT policy does not allow any pirated/unauthorized software installation on the Institution owned computers and the computers connected to the Institution campus network. In case of any such instances, Institution will hold the department/individuals personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

17.1. Purpose

This policy ensures that all software used within the Indian Institute of Management Bodh Gaya (IIMBG) complies with legal, licensing, and security requirements as per Government of India regulations, including the Information Technology Act, 2000, copyright laws, and software licensing agreements.

17.2. Scope

Applies to all faculty, non-faculty, students, visiting scholars, vendors, and contractors using IIMBG's IT resources. Covers all software installed on desktops, laptops, servers, mobile devices, and other IT infrastructure owned or managed by the Institute.

17.3. Policy Guidelines

1. Approval and Authorization
 - a. All software installations must be approved by the IT Department/ITS Committee.
 - b. Users are prohibited from installing software on Institute-owned systems without prior authorization.
2. Licensing Compliance
 - a. Only properly licensed, open-source, or institutionally procured software may be installed.
 - b. Unauthorized, pirated, or unlicensed software is strictly prohibited.
 - c. The Institute shall maintain a Software License Register recording all purchased and licensed software, including version, license type, validity period, and assigned users.
3. Procurement
 - a. All software must be procured through the Institute's approved procurement process, ensuring compliance with Government of India financial and IT procurement rules.
 - b. Preference should be given to open-source software where feasible, in alignment with Government of India's Open-Source Software Policy.
4. Installation and Configuration

- a. Software will be installed only by the IT Department or authorized personnel/vendors.
 - b. All installations must comply with Institute security standards, including updates, patches, and endpoint protection.
5. Usage Restrictions
 - a. Licensed software must only be used for the purpose specified in the license agreement (e.g., academic, administrative, or research use).
 - b. Users should not copy, share, or distribute software without proper authorization.
 - c. Software licenses assigned to individual users or systems must not be transferred without approval.
6. Auditing and Monitoring
 - a. The IT Department will conduct periodic audits to ensure software license compliance.
 - b. Any unauthorized or unlicensed software detected will be removed immediately, and the user may face disciplinary action.
7. Disciplinary Action
 - a. A penalty system will be implemented; in case someone is found violating the above-mentioned guidelines. The following penalty procedure shall be followed:
 - i. First Time- Warning shall be issued.
 - ii. Second Time- Network will be disconnected for a week.
 - iii. Third Time- Network will be disconnected for a Semester.
 - iv. Fourth Time- Network will be disconnected for the entire stay.
8. Security and Updates
 - a. All software must be regularly updated with security patches.
 - b. Outdated or unsupported software that poses a risk will be decommissioned.
9. Compliance with Government Regulations
 - a. The policy will adhere to the following Government of India directives:
 - b. IT Act, 2000 and Amendments – governing IT usage and cyber laws.
 - c. Copyright Act, 1957 (as amended) – protecting intellectual property rights.
 - d. CERT-In Guidelines – for security compliance.
 - e. Government of India Open-Source Software Policy (2015) – encouraging adoption of OSS where applicable.

17.4. Roles and Responsibilities

1. **Users:** Ensure they use only authorized software and report any licensing issues to IT.
2. **IT Department:** Approve, install, maintain, and audit software licenses.
3. **ITS Committee:** Oversee policy compliance, approve procurement, and recommend corrective actions.

18. Use of IT Devices on Institution Network

This section provides the best practices related to use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners on Institution network.

18.1. Scope

This policy applies to all devices (desktops, laptops, servers, printers, mobile phones, tablets, and IoT devices) that connect to the IIM Bodh Gaya campus network (LAN, Wi-Fi, or VPN). It covers both Institute-owned devices and personally-owned devices (BYOD – Bring Your Own Device).

18.2. General Guidelines

1. Registration and Approval
 - a. All devices must be registered with the IT Department before connecting to the Institute's network.
 - b. Unauthorized or unregistered devices may be blocked.
2. Security Compliance
 - a. Devices must have updated antivirus, licensed operating systems, and the latest security patches.
 - b. Users are responsible for keeping their devices compliant with Institute security standards.
3. Authorized Use Only
 - a. Devices connected to the Institute network may only be used for academic, research, and administrative purposes.
 - b. Activities such as gaming, cryptocurrency mining, or unauthorized streaming that consume excessive bandwidth are prohibited.
4. Network Access Controls
 - a. The Institute may implement access control mechanisms (firewalls, VLANs, endpoint compliance checks) to restrict non-compliant or unsafe devices.
5. Sharing and Hotspot Restrictions
 - a. Users must not create unauthorized Wi-Fi hotspots, share credentials, or provide access to outsiders through their registered devices.
6. Monitoring
 - a. All device activity on the network is subject to monitoring and logging by the IT Department to ensure compliance and security.

18.3. Personally Owned Devices (BYOD)

1. Personal devices may be permitted with approval but must follow the same security compliance requirements as Institute devices.
2. The Institute is not responsible for damage, data loss, or malfunction of personal devices connected to the network.
3. Personal devices may be denied access if found to pose a security threat.

18.4. Device Misuse

Users are prohibited from:

1. Running unauthorized servers or services on the network.
2. Attempting to bypass filters, proxies, or firewall restrictions.
3. Using devices to hack, probe, or disrupt the network.

4. Installing unauthorized networking equipment (routers, switches, repeaters).

18.5. Enforcement and Penalties

1. Any device found in violation of this policy may be disconnected immediately.
2. The user will be notified, and disciplinary action may follow depending on the severity of the violation.
3. In case of unlawful activity, the matter may be escalated to law enforcement agencies under the IT Act, 2000 and other applicable Government of India cyber laws.

19. Network (Intranet & Internet) Use Policy

This policy defines acceptable and responsible use of the Institute's Intranet (internal network) and Internet access to ensure academic, research, and administrative continuity while maintaining compliance with institutional policies and Government of India regulations (IT Act 2000, CERT-In directives, UGC/MoE guidelines).

19.1. Purpose

This policy governs the proper use of the Institute's network resources, including Intranet and Internet access, to facilitate secure and uninterrupted academic, research, and administrative operations, in compliance with institutional standards and national IT regulations.

19.2. Scope

Applies to all faculty, non-faculty, students, visiting scholars, contractors, and external collaborators using the Institute's LAN, Wi-Fi, or VPN services. Covers both wired (LAN) and wireless (Wi-Fi) access on campus.

19.3. General Guidelines

1. Authorized Use Only
 - a. Access to the Institute's Intranet and Internet is provided strictly for academic, research, and administrative purposes.
 - b. Personal use should be minimal and must not interfere with institutional work.
2. Registration of Devices
 - a. All devices must be registered and approved by the IT Department before accessing the network. Unauthorized devices may be blocked.
3. Compliance with Laws and Policies
 - a. Users must comply with the IT Act, 2000, cybersecurity directives from CERT-In, and institutional IT policies.
 - b. Any illegal activity (e.g., hacking, phishing, spreading malware, copyright infringement) will invite disciplinary and legal action.
4. Prohibited Activities
 - a. Users shall not:

- i. Host unauthorized websites or servers on the network.
 - ii. Use VPNs, proxies, or tunnelling to bypass network filters.
 - iii. Share offensive, obscene, or unlawful material.
 - iv. Run bandwidth-heavy personal activities (gaming, torrents, unauthorized streaming).
5. Fair Usage
 - a. Bandwidth is a shared resource. Users must avoid excessive usage that affects others' access. The Institute reserves the right to enforce bandwidth limits or block high-consumption activities.
6. Security Compliance
 - a. Users must keep their systems updated with licensed OS, antivirus, and patches.
 - b. Compromised or non-compliant devices may be quarantined or denied access.
7. Monitoring and Logging
 - a. Network activity (sites visited, applications used, bandwidth consumed) may be monitored and logged by the IT Department for security and compliance.
 - b. While efforts are made to safeguard user privacy, absolute confidentiality cannot be guaranteed.
8. Access to Intranet Resources
 - a. The Intranet hosts internal applications such as ERP, library systems, academic databases, and administrative portals. Access is restricted to authorized users only.
9. Guest Access
 - a. Temporary Internet/Intranet access for guests, external faculty, or event participants shall be provided only through formal approval and monitored credentials.
10. Consequences of Misuse
 - a. Violations of this policy may result in:
 - i. Immediate suspension of network access.
 - ii. Disciplinary action under IIM Bodh Gaya rules.
 - iii. Reporting to law enforcement under Government cyber laws.

20. Email Account Usage Policy

Institution provides official email access privileges to its users. To handle the efficient information dissemination among the administration, faculty members, non-faculty and students, it is recommended to avail official email with institution's domain.

20.1. Purpose

This policy defines the acceptable and secure use of institutional email accounts at IIM Bodh Gaya to ensure professional communication, safeguard data, and comply with institutional and Government of India IT regulations.

20.2. Applicability

Applies to all faculty, non-faculty, students, visiting scholars, and authorized users who have been assigned an official Institute email account (provided through the Gmail for Education/Google Workspace platform). Covers both individual accounts (e.g., user@iimb主.ac.in) and group/functional accounts (e.g., admissions@iimb主.ac.in, accounts@iimb主.ac.in).

20.3. Policy Guidelines

1. Authorized Use Only
 - a. Email accounts are provided strictly for official, academic, research, and administrative communication.
 - b. Personal or commercial use of institutional email is discouraged and must not interfere with official activities.
2. Group Email Restrictions
 - a. No individual user shall send, reply, or forward messages from group/functional email accounts without prior permission of the competent authority (e.g., HOD, Registrar, Director, or authorized delegate).
 - b. Access to such group mailboxes will be role-based and controlled by the IT Department.
3. Accountability
 - a. Each user is accountable for all activities carried out through their assigned account.
 - b. Sharing email credentials is strictly prohibited.
4. Gmail Security Practices (IIMBG-Specific)
 - a. Users must enable 2-Step Verification (2FA) for their Institute Gmail accounts.
 - b. Strong passwords, aligned with the Institute's password policy, must be used and changed periodically.
 - c. Users must not click on suspicious links or attachments; phishing attempts must be reported immediately to the IT Department.
 - d. Sensitive information (student records, financial data, research data) must not be shared over email without encryption or approval.
 - e. Auto-forwarding of official emails to personal email accounts is prohibited without written permission.
 - f. Users must log out of email accounts when using shared/public computers.
5. Retention and Backup
 - a. Email records related to academics, administration, or finance shall be retained as per institutional data retention policy.
 - b. Deleted or archived emails may still be retrievable by the IT Department under competent authority approval for compliance or investigation.
6. Monitoring and Privacy

- a. While the Institute respects user privacy, email accounts remain the property of the Institute.
 - b. Under approval from competent authority, the IT Department may access or monitor email accounts in cases of misconduct, investigation, or legal compliance.
7. Compliance with Laws
 - a. All email usage must comply with the IT Act 2000, Government of India's cyber security directives, and intellectual property laws.
 - b. Misuse of institutional email for spreading offensive content, spam, or unlawful activities will lead to disciplinary and/or legal action.

20.4. Enforcement

Violation of this policy may result in:

1. Suspension of email access.
2. Disciplinary action as per IIM Bodh Gaya rules.
3. Legal action under applicable Government of India IT and cyber laws.

21. Institutional Repository (IR)

Indian Institute of Management Bodh Gaya shall be providing services related to Institutional Repository (IR) through Central Library of the Institution as per the following policies.

21.1. What is IR (Institutional Repository)?

An Institution-based institutional repository (IR) is a set of services that an Institution Library offers to the members of its community for the Management and dissemination of digital materials created by the institution and its community members. It is most essentially an organizational commitment to the stewardship of these digital materials including long-term preservation, access, and dissemination of e-resources of an organization to its users.

21.2. What Does IR contain?

IR of the institution contains a wide variety of documents depending on the policy of the institution. Most common are the outputs of research journal articles (pre-print and post-print), conference papers, technical reports, computer programs, preservation, technical manuals, Video and audio recordings, e-Books, Seminar and Webinar lectures, Theses and Dissertations and Rare books etc. Grey literature is as important as published outputs in IR.

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 Institution's course Management system and display e-learning features. In practice, however, Institution's repository (IR) will provide a basic repository of such resources available through online which focus on research and academic publications.

21.3. Who will be entitled to access Indian Institute of Management Bodh Gaya IR?

Mainly the Bonafide members i.e. faculty members, research scholars, students and other non-faculty members having institutional e-mail IDs are authorized members to access the IR of Indian Institute of Management Bodh Gaya

21.4. How will you access the IR?

The registered members through their institutional e-mail address can log-in to IR link and browse the Institution IR and can download digital materials in pdf format purely for their academic purpose subject to provision of giving general information of the member provided in the Institution IR portal.

21.5. Validity Period of Accessibility of IR

Teachers, researchers, and students are authorized to access Institution's IR as long as they are in the Institution. The moment the tenure in the Institution or the course is completed and the no dues certificates are issued from the Institution's Library authority, the validity of access to Institution IR will be withdrawn.

21.6. Copyright Violation on IR Use

Indian Institute of Management Bodh Gaya IR digital materials are mainly grey literature. Any downloaded digital materials from the IR comes under the purview of copyright. The downloaded permissible materials cannot be reprinted and sold in the market for commercial purpose further. The created user-id and password are person specific and cannot be transferred to any other person and subject to the violation of SOPs of Indian Institute of Management Bodh Gaya IR.

22. Disposal of ICT equipment

The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the Institution.

23. IT Hardware End-of-Life (EOL) Policy

All IT hardware assets of the Institute will be considered to have reached End of Life (EOL) after completing five years of operational lifespan. The depreciated value of each asset will be calculated on a yearly basis. Upon reaching EOL, the hardware will be decommissioned and disposed of through resale or auction as part of the new IT system procurement cycle, in accordance with Institute policies and compliance requirements.

23.1. Purpose

This policy defines the guidelines for managing the end-of-life (EOL) and end-of-support (EOS) stages of IT hardware assets at IIM Bodh Gaya to ensure efficiency, security, and compliance with Government of India standards, including e-Waste (Management) Rules.

23.2. Scope

Applies to all IT hardware assets owned by the Institute, including desktops, laptops, servers, printers, projectors, networking equipment, and peripheral devices. Covers the complete asset lifecycle from procurement to decommissioning.

23.3. Lifecycle of IT Assets

1. **Standard Lifecycle:** The useful life of IT hardware assets at IIM Bodh Gaya shall be considered 5 years from the date of procurement, unless extended under exceptional approval by the competent authority.
2. **End-of-Life (EOL):** After 5 years of service, IT hardware will be classified as EOL and may no longer be used for primary academic, administrative, or research purposes.
3. **End-of-Support (EOS):** Once OEM (Original Equipment Manufacturer) warranty/support and updates are unavailable, the device will be marked as EOS, and continued usage may pose security or operational risks.

23.4. EOL Management Guidelines

1. **Assessment and Review:** The IT Department will conduct an annual review of IT assets to identify equipment reaching EOL/EOS status.
2. **Decommissioning:** EOL devices will be formally decommissioned and removed from active service. Users must return such devices to the IT Department for safe handling.
3. **Replacement:** Where required, EOL devices will be replaced with new assets as per institutional procurement policy.
4. **Secondary Use:** Devices beyond 5 years may be reassigned for limited secondary use (e.g., low-performance administrative tasks, student labs, or training), subject to IT Department approval and safety/security checks.
5. **Data Security:** Before disposal or reassignment, all Institute data will be securely wiped using standard data erasure tools, in compliance with data protection laws.
6. **Disposal:** Disposal of obsolete IT hardware will follow Government of India E-Waste (Management) Rules, 2016 (and amendments) through authorized e-waste vendors.

23.5. Roles and Responsibilities

1. IT Department: Maintain IT Asset Register, conduct annual reviews, and oversee decommissioning.
2. Users: Return assets at the end of their lifecycle and ensure no unauthorized use of obsolete hardware.
3. Administration: Approve procurement of replacements and disposal of obsolete assets.

23.6. Enforcement

Use of unapproved, obsolete, or EOL hardware on the Institute network is prohibited. Non-compliance may lead to disconnection of such devices and disciplinary action.

24. Budgetary provisions for ICT

24.1. Purpose

To ensure sustainable development, maintenance, and upgradation of ICT infrastructure at IIM Bodh Gaya, a structured approach to budgetary planning and allocation is essential. This policy defines how budget provisions for ICT shall be managed in alignment with the Institute's academic, research, and administrative needs.

24.2. Scope

Covers all ICT-related requirements, including:

1. Hardware procurement and replacement (desktops, laptops, servers, networking equipment, etc.)
2. Software licensing, renewals, and subscriptions
3. Cloud services and data storage
4. Annual Maintenance Contracts (AMC) and warranties
5. Network upgrades (LAN, Wi-Fi, firewalls, security appliances)
6. Audio-Visual (AV) and Smart Classroom infrastructure
7. IT manpower, training, and capacity building
8. Cybersecurity and compliance measures
9. e-Waste management and safe disposal

24.3. Policy Guidelines

1. Annual ICT Budget
 - a. A separate line item for ICT shall be included in the annual institutional budget.
 - b. The budget will cover both capital expenditure (CAPEX) for infrastructure expansion and operational expenditure (OPEX) for ongoing services, licenses, and maintenance.
2. Lifecycle-based Planning
 - a. ICT budget planning will incorporate the 5-year lifecycle of IT assets (as per the Institute's IT Hardware End-of-Life Policy).
 - b. Provision for replacement and upgradation shall be made well in advance to avoid disruption.
3. Centralized Procurement
 - a. All ICT-related procurement shall be carried out centrally through the IT Department/ITS Committee in consultation with user departments to ensure standardization, cost-effectiveness, and compliance with Government of India procurement norms (e.g., GFR, GeM Portal).
4. Contingency Provisions
 - a. A portion of the ICT budget shall be earmarked for contingency needs, such as emergency replacements, cybersecurity threats, or sudden technology requirements.
5. Capacity Building
 - a. Budget will also provide training of IT Non faculty, faculty, and students in emerging technologies, cybersecurity, and digital tools, ensuring optimal utilization of ICT infrastructure.
6. Review and Monitoring

- a. The ITS Committee shall annually review ICT expenditure and prepare a Budget Utilization Report for submission to the competent authority.
 - b. Periodic audits will ensure transparency and accountability.
7. Alignment with Institutional Goals
 - a. ICT budget provisions will be aligned with the Institute's strategic plan, digital transformation roadmap, and Government of India's Digital India initiatives.

24.4. Roles and Responsibilities

1. **ITS Committee:** Prepare budget estimates, prioritize ICT needs, and recommend allocations.
2. **IT Department:** Execute budgeted ICT activities, maintain financial records, and ensure cost-effective use of resources.
3. **Administration & Finance Office:** Approve and release funds as per institutional norms.

25. Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Help desk mail id. On receipt of notice (or where the Institution otherwise becomes aware) of any suspected breach of this Policy, the Institution reserves the right to suspend a user's access to Institution's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Non faculty, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the Institution's disciplinary procedures.

1. Users are required to remain vigilant and report any suspected violations of this policy immediately to the **IT Helpdesk (it.support@iimbmg.ac.in)**.
2. Upon receiving notice, or if the Institute otherwise becomes aware of a suspected breach, the Institute reserves the right to suspend a user's access to institutional IT resources and data to prevent further harm.
3. In addition to suspension, disciplinary measures may be taken as per institutional procedures, which may include:
 - a. **Employee:** Disciplinary action up to and including dismissal.
 - b. **Students:** Disciplinary action up to and including expulsion.
 - c. **Third Parties/Contractors:** Termination of contract or engagement.
4. Serious breaches may also be reported to relevant **Government of India authorities** under the IT Act, 2000 and other applicable cyber laws.

26. Revisions to Policy

The Institution 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 Institution website and by continuing to use the Institution's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

1. The Institute reserves the right to revise or update the terms of this policy at any time to reflect technological, legal, or institutional changes.
2. All revisions will be documented in the **Policy Revision History** and made available on the




भारतीय प्रबंध संस्थान बोधगया Indian Institute of Management Bodh Gaya

Institute's official website.

3. Continued use of institutional IT resources after such revisions will be deemed as **acceptance of the updated terms** by all users.

27. Contact Us

For queries, clarifications, or reports regarding this policy, users may contact the IT Department via email at:  IT.support@iimbg.ac.in

Appendix – I: Email Requisition Form

FORM FOR REQUISITION OF OFFICIAL EMAIL ID

(For Employee only)

First Name	:	
Middle Name	:	
Last Name	:	
Department/ Branch	:	
Current Email address*	:	
Mobile Number	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department
4. An official Email address would be created within 48 hrs. - 72 hrs.
5. Information regarding the official Email address created would be sent to your current Email address.

(Signature of the Head of the Department)

Appendix – II: Wi-Fi Access Requisition Form

FORM FOR REQUISITION OF WI-FI ACCESS

(For Students only)

Name	:	
Father's Name	:	
Gender	:	
DoB	:	
Department	:	
Course	:	
Semester	:	
StudentRegID	:	
Email address*	:	
Mobile Number	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective program office.

(Signature of the program office)

Appendix – III: Wi-Fi Access Requisition Form
FORM FOR REQUISITION OF WI-FI ACCESS

(For Employee)

Name	:	
Gender	:	
DoB	:	
Department/ Branch	:	
Email address*	:	
Mobile Number	:	

Note:

1. Please spell the names and all other information sought above correctly.
2. *This Email address should be currently used by you.
3. The filled in form should be submitted after getting duly signed from respective Head of the Department.

(Signature of the Head of the Department)