IT POLICY



BISHOP JEROME INSTITUTE

Fatima College Road, Kollam 691001

Policy Ref: BJI/06-2025_V01
Revision: V02
Issue Date: 30-10-2026
Version 1
Responsible Executive: *Manager, BJI*
Responsible Office: *Dean, CSE / System Administrator*



Index

1) Introduction

2) IT Policy of the College

3) IT infrastructure of the College

4) Wi-Fi

5) Software Installation and Licensing Policy/Open Source

6) Network (Intranet and Internet) Use Policy

7) Use of E-mail Account

8) Web Site Hosting Policy

9) Use of College Database

10) Maintenance in Action

11) Budget Allocation for IT Infrastructure

12) Password Policy

13) Data Backup Recovery Policy

14) Social Media Usage Guidelines

15) Data Privacy & Confidentiality Policy

16) E-Waste Policy

17) Conclusion

BISHOP JEROME INSTITUTE KOLLAM 1

IT POLICY

1) Introduction

The computing resources at **BISHOP JEROME INSTITUTE** is intended to support the educational, instructional, research, and administrative requirements of the college and the use of these resources is a privilege that is extended to all members of the College community.

The IT policy of the college is formulated to maintain, secure, and ensure legal and appropriate use of Information Technology infrastructure established in the campus and provide guidelines on acceptable and unacceptable use of IT resources.

This policy establishes strategies and responsibilities for protecting the confidentiality, integrity, and availability of the information assets that are accessed, created, managed, and/or controlled by the College. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

In addition, this policy supports effective organizational security and protects users and IT resources from, but not limited to cyber criminals, bullying, misuse of accounts and assets as well as the spread of malicious software.

The IT Infrastructure of the College is under the charge of the following personnel:

1. Manager, in general
2. Dean, Computer Science and Engineering Department
3. Website Admin and System Administrator
4. Faculty entrusted with responsibilities in the respective Departments.

Software Management team led by the System Administrator runs the Firewall security, DHCP, DNS, email, web and application servers and manage the network of the college. Software Management Unit has been taking appropriate steps by installing firewalls, access controls and content filtering software at the gateway.

BISHOP JEROME INSTITUTE KOLLAM 1

This document contains the policy of the College for the effective utilization and maintenance of its IT infrastructure. While formulating this policy, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users.

Further, due to the dynamic nature of Information Technology, information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

The purpose of the IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines are created and provided to help the institution, the departments and individuals who are part of the institutional community to understand how the college policy applies to some of the significant areas and to bring conformity with the stated policies.

2) IT Policy of the College

It is the policy of the College to provide and maintain the latest IT facilities (Computers, Laptops, Internet connectivity through LAN and Wi-Fi etc.) to all staff and students working or studying at the College.

The institution spends a remarkable percentage of its annual budget for up-keeping its IT infrastructure in terms of hardware as well as software. BJI has a dedicated team of staff members to maintain its IT infrastructure. We have formulated an IT Policy statement, which reads as follows:

"BISHOP JEROME INSTITUTE is committed to provide state of the art IT infrastructure and facilities to the campus community to work or study with maximum efficiency, ensuring fool proof information security and trust".

BJI takes keen interest in doing everything possible to realize this policy for the benefit of its staff and students.

BISHOP JEROME INSTITUTE KOLLAM 1

3) IT infrastructure of the College

Bishop Jerome Institute provides cutting-edge IT facilities to its staff and students for the various course of domains through various department labs and a 48 node Central Computing Facility (CCF). All the academic buildings and departments are connected directly to the server room through Optical fibre cable. The Network Core Switch TP Link JetStream 24-Port Gigabit L2+ Managed Switch with 4 10GE SFP+ Slots and 24 PORT POE + TP LINK TLSG3428XMP/ 10G SFP+ L2 MANAGED SWITCH 384Wacts as the core networking switch.

The firewall security system which is being used is FG-120GTK25046374 acting as a UTM (Unified Threat Management) for the entire network. The college network is linked to the Internet via three dedicated leased lines of 50Mbps/100 Mbps/1 Gbps each from BSNL/Railtel/Asianet enabling round-the-clock Internet connectivity on the campus.

The Network architecture follows a hierarchical model: perimeter security at the firewall, separate core switching for data and surveillance, and access switching at selected floors or operational areas. The MDF/server room is the central equipment location for core network services and server infrastructure. The data core aggregates all designated data access switches. The surveillance core aggregates all designated CCTV access switches using a physically separate fibre path.

3.1) Main Equipments & Roles:

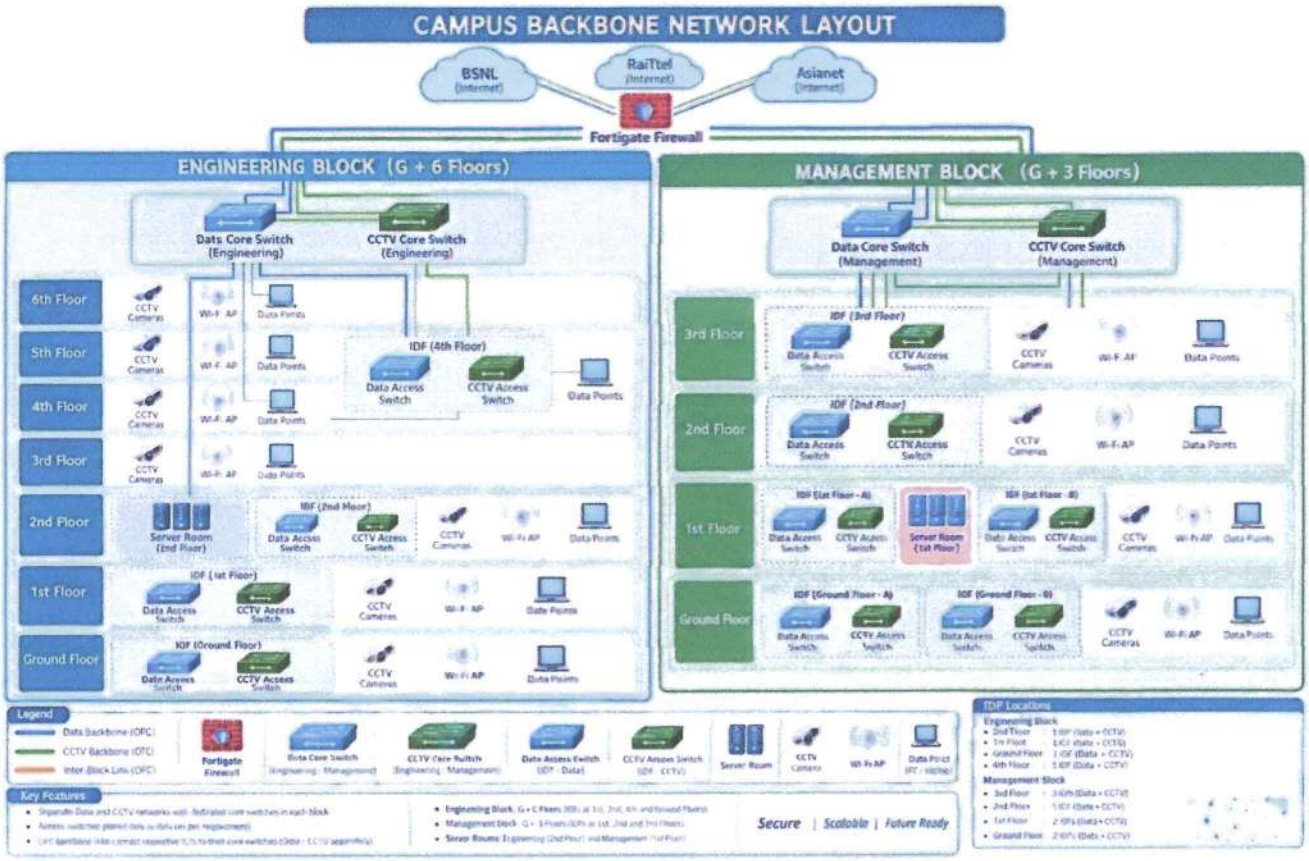
- FortiGate firewall: provides the perimeter security gateway and, subject to the deployed configuration, policy enforcement, internet access control, logging and secure routing.
- Data Core Switch: aggregates the data access switches supporting data, voice, Wi-Fi and approved server connectivity.
- Surveillance Core Switch: aggregates CCTV surveillance access switches. It is intended to connect directly to the firewall as specified in the latest design instruction.
- Data Access Switches: provide wired connectivity at Main block (GF, FL1, FL2/server room, FL3 Lab 1, FL3 Lab 2 and FL4) and Management block (GF, FL1 , FL2 , FL3)
- Fibre backbone: provides inter-block and floor uplinks. Data and surveillance links are kept separate and clearly labelled at both ends.

BISHOP JEROME INSTITUTE KOLLAM 1

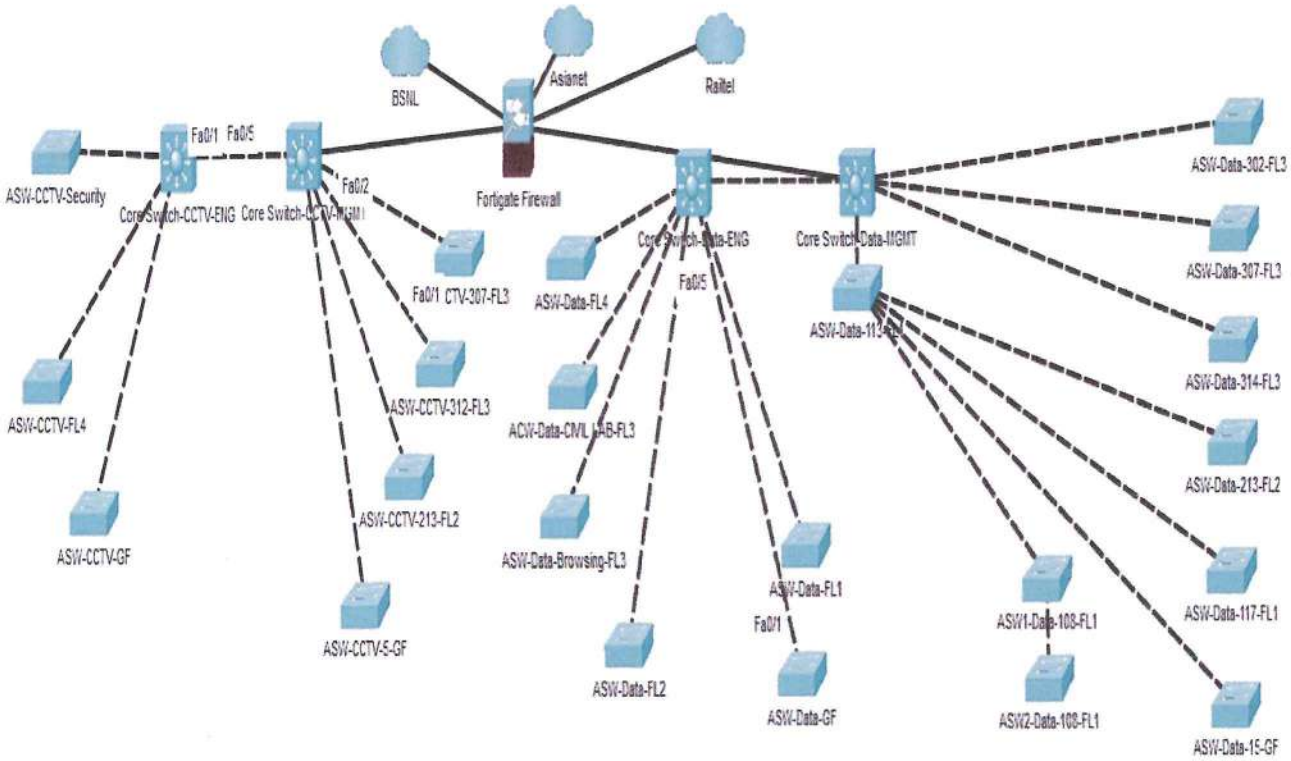
- Wireless access points, PCs and servers: connected to the data network in accordance with approved port, VLAN and addressing plans.

- CCTV cameras and monitoring workstation: connected to the surveillance network; the monitoring workstation connected to the surveillance switching path and authorized for surveillance operations.

The entire campus is Wi-Fi enabled, providing seamless mobility and uninterrupted access to the Internet and related digital services. The campus-wide Wi-Fi network allows faculty, staff, and students to connect to the Internet anytime and from anywhere within the campus. To ensure comprehensive wireless coverage, the institution has deployed more than 21 Wi-Fi access points across the campus. In addition, the campus network supports a robust security infrastructure with over 70 surveillance cameras connected to the network, ensuring continuous monitoring and enhanced safety for students, staff, and visitors.



BISHOP JEROME INSTITUTE
KOLLAM 1



3.2) Physical and logical separation

The data and surveillance networks are designed with separate core switches and separate fibre links. No direct link should be configured between the Data Core Switch and Surveillance Core Switch. The surveillance core should have its own direct connection to the FortiGate firewall where required for controlled access, remote viewing or other approved services. Any inter-network access must be implemented through documented firewall policies rather than an unfiltered switch-to-switch connection. If surveillance is intended to be completely isolated from the internet and other networks, the firewall policy explicitly deny unnecessary outbound and cross-network traffic.

BISHOP JEROME INSTITUTE KOLLAM 1

3.3) VLAN and IP Addressing

The following VLAN and subnet used for the institute network.

Sl. No.	VLAN / Network Name	IP Subnet	VLAN ID
1	Data-Office	192.168.10.0/24	10
2	Data-Staff Room	192.168.11.0/24	11
3	Data-Class Rooms-ENG	192.168.12.0/24	12
4	Data-Class Rooms-MGM	192.168.13.0/24	13
5	Data-Seminar Hall	192.168.14.0/24	14
6	Data-Library	192.168.15.0/24	15
7	WI FI-Office	192.168.16.0/24	16
8	WI FI-FACULTY	192.168.17.0/24	17
9	WI FI-STUDENTS-ENG	10.0.0.0/22	18
10	WI FI-Students-MGM	10.0.5.0/22	19
11	WI FI-Seminar/Auditorium	192.168.20.0/24	20
12	WI FI-Guest	192.168.21.0/24	21
13	Data-LAB 311 Civil Software	192.168.22.0/24	22
14	Data-LAB2 312 Browsing	192.168.23.0/24	23
15	Data-LAB3	192.168.24.0/24	24
16	Data-LAB4	192.168.25.0/24	25
17	Data-LAB5	192.168.26.0/24	26
18	CCTV-BJI	192.168.30.0/24	30
19	Device MGMNT	192.168.5.0/24	50

3.4) Network Security and Access Control

Firewall and perimeter controls

- Maintained a documented firewall policy approved by the institution's authorised IT representative.
- Permitted only required traffic between the data network, surveillance network, servers and external networks.
- Applied a default-deny approach to unsolicited inbound traffic and restrict administrative interfaces to authorised management hosts.
- Enabled logging for security-relevant firewall events and review alerts periodically.
- Backing up firewall configuration after approved changes and store backups securely.

Data and surveillance segregation

- Data Core Switch and Surveillance Core Switch unconnected to each other.
- Connected all designated data access switches to the Data Core Switch through the assigned data fibre links.
- Connected all designated surveillance access switches to the Surveillance Core Switch through the assigned surveillance fibre links.
- Connected the Surveillance Core Switch directly to the FortiGate firewall as specified; enforce required access using firewall policies.
- Restricted CCTV switch, camera, recorder and monitoring workstation management to authorised personnel.

BISHOP JEROME INSTITUTE KOLLAM 1

3.5) Network Inventory

Sl	Item	Specification	Qnty
1	Network Core switch-Data	TP-Link SG3428X 28-port JetStream Layer 2+ managed switch featuring 24 Gigabit RJ45 ports,4 10Gbps SFP+ fiber slots, a 128 Gbps switching capacity	2
2	Network Core switch-CCTV	TP-Link SG3428XMP 28-port JetStream Layer 2+ managed switch featuring 24 Gigabit RJ45 ports,4 10Gbps SFP+ fiber slots, a 128 Gbps switching capacity Total PoE Budget: 384 Watts	2
3	Network Access Switch-Data	TP-Link JetStream TL-SG2428P is a 28-port Gigabit Smart Managed Switch featuring 24 Gigabit PoE+ ports backed by a 250 W total PoE budget, along with 4 dedicated Gigabit SFP slots for fiber uplinks	3
4	Network Access Switch-CCTV	TP-Link JetStream TL-SG2428P is a 28-port Gigabit Smart Managed Switch featuring 24 Gigabit PoE+ ports backed by a 250 W total PoE budget, along with 4 dedicated Gigabit SFP slots for fiber uplinks	3
5	Network Access Switch- Data&CCTV	TP-Link Omada ES228GP is a 28-port Gigabit Easy Managed Switch o 24 Gigabit PoE+ ports with a 250 W power budget, 2 dedicated non-PoE Gigabit RJ45 ports, and 2 Gigabit SFP slots for fiber link aggregation	13
6	Network Access Switch-CCTV	TP-Link Omada ES210GP is a compact 10-port Gigabit PoE Easy Managed Switch	1
7	Firewall	FortiGate 120G Fixed RJ45 Copper Ports: 16 × Gigabit Dedicated Management Ports: 1 × GE RJ45 Management, 1 × GE RJ45 Fiber Slots: 8 × Gigabit SFP Slots High-Speed Uplinks: 4 × 10 Gigabit SFP+ Firewall Throughput: 39 Gbps IPS Throughput: 5.3 Gbps NGFW Throughput: 3.1 Gbps Threat Protection Throughput: 2.8 Gbps SSL Inspection Throughput: 3 Gbps IPsec VPN Throughput: 35 Gbps Concurrent Sessions: 3,000,000	1

BISHOP JEROME INSTITUTE KOLLAM 1

8	Wireless Controller	TP-Link Omada OC300 Hardware Controller. Total Managed Devices: Supports up to 700 total devices. Access Points (APs): Up to 500 Omada access points. Switches: Up to 100 JetStream managed switches. Gateways/Routers: Up to 100 SafeStream/Omada routers. Maximum Connected Clients: Handles up to 15,000 active clients	1
9	Wireless Access point	TP-Link Omada EAP620 HD is a high-performance AX1800 Wi-Fi 6 Ceiling/Wall Wi-Fi Rating: AX1800 Dual-Band 5 GHz Band Speeds: Up to 1201 Mbps 2.4 GHz Band Speeds: Up to 574 Mbps	24

3.6) Campus Wi-Fi with Restricted Student Access

Campus Wi-Fi support wireless connectivity across designated institutional areas. Access is differentiated by user category, with restricted access for students to help protect institutional resources and maintain appropriate use of the campus network.

- Campus wireless coverage is provided in designated areas for institutional users, subject to the installed access-point layout.
- Student Wi-Fi access is restricted through the applicable wireless authentication and/or network access policy.
- Student wireless users should be limited to approved internet and learning resources; access to staff, administrative, server and device-management networks are accessible to specifically authorised personnel.
- Separate wireless network names and VLANs are recorded in the institute's network plan, including WIFI-Office (VLAN 16), WIFI-FACULTY (VLAN 17), WIFI-STUDENTS-ENG (VLAN 18), WIFI-Students-MGM (VLAN 19), WIFI-Seminar/Auditorium (VLAN 20) and WIFI-Guest (VLAN 21).
- The firewall and switching configuration enforces the approved restrictions between student Wi-Fi, institutional internal networks and guest access.

BISHOP JEROME INSTITUTE KOLLAM 1

3.7) CCTV Surveillance Inventory

Sl	Item	Specification	Qnty
1	Network Video Recorder	Network Video Recorder 32 CH 4K 4 SATA 256 Mbps CP PLUS CPUNR 4K4324-FI	4
2	Network Camera	Bullet Camera CP-UNC-TA41L3B-D-LQ-0360 4 MP 3.6mm 30 Meter Full Color IR 2 Way Audio IP67	101
3	Storage	HDD WD 6TB Surveillance	8

3.8) Desktops Installed

The College is **equipped with 11 (eleven) computer labs** to meet the requirement of the computer practical sessions for all courses. Apart from the department computer labs, the college has ensured a **central computing facility with more than 48 systems for the general use** of staff and students.

The details of computer labs are as follows:

Sl. No.	LAB NAME	NO OF COMPUTERS	CUMULATIVE
1	CCF	48	370
2	Civil CAD Lab	40	
3	ME CAD Lab	48	
4	CSE Lab	60	
5	AI Lab	40	
6	ECE Workshop	30	
7	ECE Digital Processing Lab	11	
8	Language Lab	20	
9	EEE Power System Lab	13	
10	EEE Microprocessor Lab	30	
11	B.Arch. NATA Lab	30	

BISHOP JEROME INSTITUTE KOLLAM 1

Computers available for Faculty and staff use

Administration			
12	Principal Room	1	13
13	Vice Principal Room	1	
14	KTU Exam Cell	1	
15	Series Exam Cell	1	
16	Valuation Camp	1	
17	Office	4	
18	Bursar Room	1	
19	Accountant Room	1	
20	Admission Cell (B- Tech, B- Arch)	1	
21	Admission Cell (MBA)	1	
HoD Rooms			
22	CSE HoD Room	1	6
23	Civil HoD Room	1	
24	ME HoD Room	1	
25	EEE HoD Room	1	
26	MBA HoD Room	1	
27	B Arch HoD Room	1	
Faculty Rooms			
28	Civil Staff Room-01	1	11
29	ME Staff Room-01	1	
30	EEE Staff Room -2	2	
31	ECE Staff Room-1	1	
32	MBA Staff Room-04	4	
33	B Arch Staff Room-01	1	
34	Basic Science	1	
Other Locations			
35	Store	1	7
36	NAAC Accreditation	1	
37	MBA Dean Room	1	
38	B. Tech Dean	1	
39	Dean of Studies – CSE	1	
40	Placement Cell	1	
41	Library Front Cabin	1	
Laptops			
42	Laptops	22	22
TOTAL - 429			**429**

BISHOP JEROME INSTITUTE KOLLAM 1

4) Wi-Fi

The major portions of campus including hostels are Wi-Fi enabled with high-speed internet connection that allows students to access the internet, no-matter where they are on campus. Staff and Students are provided with Internet authentication credentials during their joining time for secure access to the internet. About 21 access points are deployed across the campus for efficient Wi-Fi coverage. The newly installed APs are Wi-Fi 6 compatible. All the access points are centrally managed by the TP-Link OC 200/300 Wi-Fi Controller.

Wi-Fi Access Points installed

Wi-Fi Controller: TP-Link OC 200/300

No.	Access Point Model	Nos.
1)	TP LINK EAP620HD AX1800	24

Internet Access - Bandwidth

The College provides high speed internet facility to students and faculty members. A state-of-the-art campus network with a 50 Mbps/100 Mbps/ 1Gbps Leased line Internet connection offers unlimited access to the Internet for students and staff round the clock, for their educational and research needs.

The 50 Mbps/100 Mbps/1 Gbps Mbps internet leased lines from BSNL, RAILTEL and ASIANET runs through optical fiber cable that is directly terminated at the server room. All these lines act as load balancing internet gateway for the college.

UTM Support for Internet

FG-120GTK25046374 firewall was implemented across the entire network to secure the internet traffic in the LAN. Functions such as in-line application inspection and control, website filtering, HTTPS inspection, Intrusion Prevention System, VPN, and granular bandwidth controls are controlled by FortiGate firewall. The FortiGate G-120GTK25046374 firewall can handle the internet activities of 700 users simultaneously.

CCTV Cameras installed

As a part of safety measures and monitoring purposes the college has installed more than 70 CCTV surveillance cameras inside and outside the campus blocks like verandas, auditorium, main gate, canteen, hostel etc. It helps in monitoring and keeping track of complete activities taking place in the college premises.



Authorized staff maintain the functioning of CCTV under the guidance of the Manager. The CCTV infrastructure acts as a supportive mechanism to make sure that the campus is safe and secure without any crime or theft.

Projectors in Classrooms / Seminar Rooms / Conference Rooms

All the classrooms, seminar rooms and conference rooms are equipped with LCD projectors. There are 44 such projectors installed across the campus facility.

5) Software Installation and Licensing Policy/Open Source

Any computers purchased by any individual Department should ensure that such systems have all open-source software (operating system, antivirus software and necessary application software) installed in it. Respecting the anti-piracy laws of the country, the College IT policy does not allow any unauthorized software installation on the college owned computers and any computers connected to the campus network. In case of any such instance, the department/individual shall personally be responsible for any software installed on the computers, and any consequential damages caused thereby.

The College promotes the use of Free and Open-Source Software (FOSS) as far as possible; however, depending on the requirement, individual users have the freedom to choose the software we want.

6) Network (Intranet and Internet) Use Policy

Network connectivity provided through the College, either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the College IT Policy.

The System Administrator is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the network should be reported to Network Administrator.

IP Address allocation: Any computer (PC/Server) that is connected to the network, should have an IP address assigned by the Network Administrator. The range of IP addresses that will be allocated to each group is decided under a systematic approach. Accordingly, any computer connected to the network from that group will be allocated an IP address only from that Address pool.

BISHOP JEROME INSTITUTE KOLLAM 1

As and when a new computer is installed in any location, the concerned user can contact the Network Administrator for IP address allocation. An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and is connected to the same port.

IP addresses are given to the computers but not to the ports. IP address for each computer should be obtained separately.

7) Use of E-mail Account

In an effort to increase the efficient distribution of critical information to all faculty, staff, and other essential personnel, the college provides dedicated e-mail services for all formal communication, either academic and other official purposes (e.g., user@bji.ac.in; principal@bji.ac.in; hodmba@bji.ac.in etc…)

Email for formal communications will facilitate the delivery of messages and documents to all members. Formal communications and official notices from the college to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general messages, official announcements, etc. To receive these notices, it is essential that the email address be kept active by using it regularly.

For obtaining the college's email account, the user may contact the System Administrator for allocation of an email account and default password. Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

a) The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.

b) Using the facility for illegal/commercial purposes is a direct violation of the IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages, and generation of threatening, harassing, abusive, obscene or fraudulent messages and/or images.

BISHOP JEROME INSTITUTE KOLLAM 1

c) While transmitting emails with large attachments, user should make sure that the recipient has sufficient email facility that allows him to receive such large attachments.

d) User should keep the mail box used space within about 80% usage threshold, as *'mail box full'* or *'mailbox almost full'* situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.

e) User should not open any email or attachment that is from unknown and suspicious sources. Even if it is from a known source, and if it contains any attachment that is of a suspicious nature or looks dubious, user should obtain confirmation from the sender about its authenticity prior to opening it. This is very much essential from the point of security, as such messages may contain viruses that has the potential to damage valuable information.

f) User should not share his/her email account credentials with others, as the individual account holder shall be personally accountable, in case of any misuse and/or manipulations.

g) User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.

8) Web Site Hosting Policy

The college Network Administrator is responsible for maintaining the official website of the college viz., *https://bji.ac.in/*

The College may, at its discretion, provide space for the creation of individual profile for faculty members under their respective department. In such cases, it is recognized that each individual faculty will have their own requirements for his/her pages. Hence, faculty may be permitted to have their personal pages linked to the official website of the college that he/she wants to be added in the official website of the college.

However, illegal or improper usage of this facility will result in termination of the hyperlink without notice. The contents of personal pages must not violate any applicable laws and regulations, must not constitute a copyright or trademark infringement, must not be used for commercial! Purposes, must not be used for political lobbying, and must not otherwise violate any local, state, or central government laws.

BISHOP JEROME INSTITUTE KOLLAM 1

9)Use of College Database

This relates to the databases maintained by the college administration. Data is vital and an important resource for providing useful information. Its use must be protected even when the data may not be confidential. Bishop Jerome Institute has its own policies regarding the creation of databases and access to information. These policies outline the college's approach to both the access and use of the college resource.

Bishop Jerome Institute is the data owner of all the institutional data generated at the campus. Individual sections or departments generate portions of data that constitute the college's database. They may have custodianship responsibilities for portions of that data. Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

General policy guidelines and parameters for users of data from Departments and Administrative unit are given below.

a) The college's data policies do not allow the distribution of data that is identifiable to a person outside the college.

b) Data from the College's Database including data collected by departments or individual faculty and staff, is for internal college purposes only.

c) One's role and function, as defined, will be needed to carry out one's official responsibilities/rights. Through its data access policies, the college makes information and data available based on those responsibilities/rights.

d) Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including government agencies and surveys and other requests for data. All such requests are to be forwarded to the authorities.

e) Requests for information from any courts, attorneys, etc., are handled by the College Office. Departments should not, and are not authorized, to respond to such requests, even with a subpoena. All requests from law enforcement agencies are to be forwarded to the Office for adequate official response.

BISHOP JEROME INSTITUTE KOLLAM 1

f) At no time may information, including that identified as 'Directory Information', be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and/or companies which may be acting as agents for the college or its departments.

g) All reports for UGC, MHRD, University and other government agencies will be prepared/compiled and submitted by the College office, with the help of other wings.

10)Maintenance in Action

The System Administration team is responsible for the up keeping and maintenance of all the computers, Wi-Fi, projectors and surveillance cameras and is also responsible for maintaining the network and internet inside the campus.

Periodic maintenance of all equipment's are done on regular intervals. The users have to log in their requirement or complaint in the log-book available in the college office or in the google sheet established for this purpose, and the System Administrator or any authorized personnel will attend the maintenance of computer and/or internet systems.

11)Budget Allocation for IT Infrastructure

Every year the College sets aside necessary funds in its budget to procure new IT equipment and software, and maintain the facilities for the use of the stakeholders.

12) Password Policy

- Passwords should contain at least six characters with uppercase, lowercase, numbers, and special characters.
- Passwords should not be shared with others.
- Users should avoid easily guessable passwords.
- Users are advised to change passwords periodically.
- Any suspected compromise of passwords must be reported immediately.

13) Data Backup and Recovery Policy

- Critical institutional data shall be backed up periodically.
- Backup copies shall be securely maintained.
- Recovery procedures shall be tested regularly.
- Departments shall coordinate with the System Administrator for secure backup practices.

BISHOP JEROME INSTITUTE KOLLAM 1

14) Social Media Usage Guidelines

- Staff and students shall use social media responsibly.
- Confidential or objectionable institutional content shall not be posted online.
- Official announcements shall only be made through authorized accounts.
- Misuse of social media may invite disciplinary action.

15) Data Privacy and Confidentiality Policy

- Access to institutional data shall be limited to authorized users.
- Personally identifiable information shall not be disclosed without approval.
- Sensitive institutional information shall be treated as confidential.
- Any data breach must be reported immediately.

16) E-Waste Disposal Policy

- Electronic waste shall be disposed responsibly.
- E-waste disposal shall comply with government regulations.
- Data stored in storage devices shall be erased before disposal.
- Disposal shall be carried out through authorized recycling agencies.

17) Conclusion

Bishop Jerome Institute is committed to fostering a secure, reliable, ethical, and technology-enabled academic and administrative environment through the effective implementation of this IT Policy.

All stakeholders, including management, faculty, staff, students, and other authorised users, are expected to adhere to the provisions of this policy and contribute to the responsible use, protection, and optimal utilisation of the Institute's IT infrastructure and digital resources.

The Institute shall periodically review and update this policy in accordance with technological advancements, emerging cybersecurity threats, applicable legal and regulatory requirements, and institutional development priorities.

Through collective responsibility, continuous improvement, and the strategic integration of information technology, Bishop Jerome Institute aims to strengthen academic excellence, administrative efficiency, innovation, and the overall quality of institutional governance.

Anil. A.R

PRINCIPAL
BISHOP JEROME INSTITUTE
FATIMA COLLEGE ROAD
KOLLAM - 691 001

Principal
Dr. Anil A.R.
Bishop Jerome Institute
Tel: +91 62386 77683
Email: principalbji@gmail.com; principal@bji.ac.in

BISHOP JEROME INSTITUTE
KOLLAM 1