St. Albert's College

An initiative of the Archdiocese of Verapoly

Affiliated to Mahatma Gandhi University, Kottayam

(Accredited with "A" Grade by NAAC)

IT POLICY

Approved on: 02-02-2021

Approved by: Chairman

St. Albert's College

Prepared by:
Vice Chairman

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM, KOCHI-18

Approved by:
Chairman

Revised date: 02-02-2021

Revision number: 1

IT POLICY

St. Albert's College (Autonomous)

DIGITAL INFRASTRUCTURE MANAGEMENT CELL (DIMC) OPERATIONAL STATEMENT

The mission of the Digital Infrastructure Management Cell (DIMC) of St. Albert's College (Autonomous) is to work in partnership with the staff (teaching and non-teaching), students, and beneficiaries of St. Albert's College (Autonomous) to provide the most efficacious use of audio, video, digital and networking resources.

Prepared by: Vice Chairman	Approved by: Chairman
Revised date: 02-02-2021	Revision number: 1

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM

The DIMC aims to facilitate the faculty of St. Albert's College (Autonomous) to achieve the mission and strategic goals. It is the responsibility of the DIMC team to empower students, faculty, staff and beneficiaries to effectively utilize technology resources by striving to provide high standards of support services and infrastructure.

Table of Contents

INTRODUCTION

The use of Information Technology is one of the keys to effective and efficient productivity, enabling staff, faculty and students to achieve their goals through all methods that are made available. These ever-broadening capabilities allow St. Albert's College (Autonomous) go beyond the horizons of knowledge and extend Higher Education to those who would not otherwise have the opportunity to attend. DIMC at St. Albert's College (Autonomous) permeates every campus facility for the productivity and security of all who use it. The purpose of this policy is to establish an overall framework for guiding the growth and use of the digital resources of the college in accomplishing the broader goals of St. Albert's College (Autonomous) . The IT policy supplements the St. Albert's College (Autonomous) Personnel Policy and Procedures Manual.

A. PERMISSION

It is not the intent of these policies to unduly interfere with educational and research use of the network or to limit academic freedom in any way, but to provide an appropriate framework for the proper exercise of those freedoms with responsibility. Furthermore, it is not the intent of these policies to impinge on the intellectual property rights of authorized users.

St. Albert's College (Autonomous) employees and students who comply with this policy may:

1. Use St. Albert's College (Autonomous) owned computers, software, and data to which each individual has authorized access.

2. Use the St. Albert's College (Autonomous) network, including access to the Internet.

3. Use computing and networking facilities and resources in a manner that is consistent with the mission and educational purpose of St. Albert's College (Autonomous) .

B. DEFINITIONS

All definitions are included in Appendix A of this Policy.

C. POLICY MAINTENANCE

The DIMC at St. Albert's College (Autonomous) will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to review the effectiveness of these policies and, if necessary, to modify and amend some sections of the policies and procedures, or to add new procedures.

The primary responsibility for maintenance and administration of this policy rests with the DIMC Team Leader (DTL). DTL is responsible for drafting any updates and changes to the policies and procedures, which are to be reviewed and approved by the Chairman of St. Albert's College (Autonomous) . If the changes are approved by the Chairman/Manager, the changes will become effective and implemented. DTL will publish and announce the new or revised policy. Some policy revisions or additions may require the signatures of each employee acknowledging notice of the revised policy.

D. APPLICABILITY OF POLICY

This policy applies to all St. Albert's College (Autonomous) employees, students and/or non-employees (beneficiaries) who may be authorized to use St. Albert's College (Autonomous) Technology Resources as defined by this policy. They shall be required to agree and adhere to these policies before being granted permission to access these resources.

IT Policy

This policy applies to all campus facilities, equipment and services that are managed by the St. Albert's College (Autonomous) Digital Infrastructure Management Cell, including off-site data storage, computing and telecommunications equipment. This policy also applies to application-related services purchased from commercial cloud services, and Internet-related applications and connectivity.

St. Albert's College (Autonomous) users shall also apply this policy when using St. Albert's College (Autonomous) IT resources to navigate through networks or computing systems beyond the local systems.

Use of the St. Albert's College (Autonomous) technology resources shall be for the purpose of facilitating the exchange of information and furtherance of education, research, and administering missions of the college. The use of St. Albert's College (Autonomous) technology resources will be consistent with the purposes and objectives of St. Albert's College (Autonomous) .

All computer equipment may or may not be attached to the St. Albert's College (Autonomous) network. However, to protect these resources from misuse and/or accidental damage, these resources will still be set up by the DIMC team to require the use of login accounts. The same procedures for requesting network login accounts will be followed for this type of resource, despite their lack of actual network connectivity.

St. Albert's College (Autonomous) Information Technology Resources that are covered under this policy, but is not limited to, the following:

1. LAN and WAN network equipment and appliances

2. Servers, blade centers and virtual server appliances

3. Server operating systems and data base management software

4. Print servers and enterprise printers

5. Distance Learning Equipment

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM KOCHI-18

Approved by:
Chairman

Revision number: 1

6. Enterprise VoIP systems and phones

7. Enterprise Applications and educational learning systems

8. Wireless equipment

This Plan applies to all college-owned workstations, laptop computers, apple computers, desktops, tablets, peripherals (printers, scanners, projectors, and interactive whiteboards), network hardware (servers, switches, routers, bridges, and other key network devices), cable plant and physical infrastructure, and the institution-wide software, including operating systems, office productivity products and other site-licensed desktop applications running on those devices.

E. SANCTIONS

Violation of any of the provisions of this, or any St. Albert's College (Autonomous) IT policy or procedure will be dealt with immediately and may result in disciplinary action as stated in the Personnel Policy and Procedures Manual and Student Code of Conduct. The full range of disciplinary actions is available, including, but not limited to:

1. Permanent loss of computer use privileges.

2. Denial of future access to St. Albert's College (Autonomous) IT resources.

3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Governing Council of St. Albert's College (Autonomous) .

4. Dismissal from the college; and/or

5. Taking legal action

6. Reporting a local, state, or federal criminal offense to local authorities.

USE OF ST. ALBERT'S COLLEGE (AUTONOMOUS) INFORMATION TECHNOLOGY RESOURCES POLICY

St. Albert's College (Autonomous) owns all College computing systems and applications. This policy is intended to provide campus users with guidelines for responsible and appropriate utilization of these College computing and technology resources. This policy supplements the St. Albert's College (Autonomous) Personnel Policy and Procedures Manual. Rapid change in technology is perpetual and St. Albert's College (Autonomous) reserves the right to determine, at any time, what constitutes appropriate use of technology resources covered in this policy. St. Albert's College (Autonomous) is responsible for overseeing the appropriate use of College Technology Resources and ensuring compliance with tribal, state and federal law. This policy is intended to provide College employees, students, and other users of these resources with guidelines for responsible and appropriate use. Additional policies, procedures and standards may also apply to the use of computer assets. This policy assumes that all St. Albert's College (Autonomous) employees and students will act honestly, responsibly and with good judgment to protect these resources and to fulfill the responsibilities of proper ethics.

A. GOALS

The goals of the use of St. Albert's College (Autonomous) computers policy are to:

1. Help assure the integrity and reliability of the St. Albert's College (Autonomous) internal networks, hosts on those networks and any computing resource connected to them.

2. Ensure the security and privacy of the St. Albert's College (Autonomous) computer systems and networks.

3. Ensure the protection and retention of sensitive College data.

4. Establish appropriate guidelines for the use of St. Albert's College (Autonomous) - owned technology on and off- campus.

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM, KOCHI-18

5. Effectively combat the unauthorized distribution of copyrighted material by users of St. Albert's College (Autonomous) network, without unduly interfering with educational and research use of the network.

B. RESPONSIBILITIES

All users of the St. Albert's College (Autonomous) network have a responsibility to comply with this policy and to understand their responsibilities. This includes the requirement for confidentiality, retention and access to records detailed there.

1. Confidentiality, Retention and Access to Electronic Records

a. All St. Albert's College (Autonomous) employees should be aware that electronic mail, facsimile transmissions, and voice mail are technologies that may create an electronic record. An electronic record is reproducible and, therefore, could ultimately be disclosed to third parties. Such records are considered writings and all writings may be disclosed for audit or legitimate St. Albert's College (Autonomous) operational or management purposes. Whatever an employee sends or receives on a College e-mail account is the property of the College and can be accessed or viewed by the College without notice. All records and information generated and stored on electronic message systems is kept according to appropriate e-mail retention schedules.

b. Education records of students attending the College are confidential and can only be released in accordance with the Family Education Rights and Privacy Act of 1974 (FERPA) and the administrative rules of the College.

2. Logging and Monitoring

a. St. Albert's College (Autonomous) has the right to log and monitor employee use of the St. Albert's College (Autonomous) IT Resources and to ensure their appropriate use for business-related privileges. This may include, but is not limited to, review of employee computers, file server space, user accounts and all electronic documents. St. Albert's College

(Autonomous) employees should not expect privacy in their use of St. Albert's College (Autonomous) state resources.

C. GENERAL EXCEPTIONS

The use of St. Albert's College (Autonomous) resources shall be for the purpose of facilitating the exchange of information and furtherance of education, research, and administration of missions of the college. Employees may not use St. Albert's College (Autonomous)resources, including any person, money or property, for private benefit or for the personal gain of the employee or any other person. However, employees may make occasional, but limited, personal use of St. Albert's College (Autonomous) Information Technology resources only if all the following conditions are met:

1. Prior permission of the Chairman / DTL is acquired

2. There is little or no cost to the College

3. Any use is brief in duration and occurs infrequently.

4. The use does not interfere with the performance of the employee's official duties.

5. The use does not disrupt other employees and does not obligate them to make a personal use of resources.

6. The use does not compromise the security, privacy, or integrity of the College network, information, or software.

D. PROHIBITED USES

The use of St. Albert's College (Autonomous) Information Technology Resources is strictly intended for use by St. Albert's College (Autonomous) employees, students and authorized beneficaries. This prohibits others, such as family members and friends, from using St. Albert's College (Autonomous) Information Technology Resources for any purpose. Additionally, the College specifically prohibits certain use by anyone, including employees, including:

1. Any use for the purpose of supporting, promoting or soliciting for an outside organization, group, business, political candidate, or political party, unless provided for in this policy under general exceptions or authorized by the St. Albert's College (Autonomous) Chairman or designee.

2. Use that promotes personal business or financial interests.

3. Any use that constitutes political campaigning or lobbying, whether for an individual, a private business, a non-profit organization or a political party, except as noted below. This includes participating in or assisting in an effort to lobby the state legislature, a state agency head, or any governmental entity.

4. Solicitation of contributions using the St. Albert's College (Autonomous) Information Technology Resources for political purposes.

5. Use for advocacy of personal beliefs including, but not limited to, those related to political policies and religious organizations and religious ideologies.

6. Commercial uses, such as advertising or selling for personal business or personal financial interests.

7. Use of St. Albert's College (Autonomous) e-mail distribution lists for personal purposes.

8. Use for any illegal or unethical activity.

9. Use for infringement of copyrights or any intellectual property rights.

10. Any form of harassment, including sexual and racial harassment.

11. Discrimination on the basis of race, creed, color, marital status, religion, sex, national origin, age, veteran's status, sexual orientation or because of the presence of any disability.

12. Accessing, downloading or disseminating any information that a reasonable person would deem inappropriate for the workplace, such as pornography or racist materials. This

restriction does not prohibit such access or retention of such materials if they are being used solely for a specific academic purpose.

13. Downloading software or files via the Internet for personal use.

14. Any activity using excessive network band-width, such as downloading music, videos. Such activity is prohibited, even if the use is brief in duration or occurs infrequently, because it compromises St. Albert's College (Autonomous) 's network and legitimate business activities. However, this prohibition does not apply to students when being done as directed by a faculty member for specific educational purposes.

15. Private use of any St. Albert's College (Autonomous) Information Technology Resources removed from St. Albert's College (Autonomous) , even if there is no cost to the College.

16. Hacking, attempting to subvert or assisting others to breach the security of any St. Albert's College (Autonomous) network or Information Technology Resources, or to facilitate unauthorized access.

17. Use of any St. Albert's College (Autonomous) Information Technology Resources to create, disseminate or execute self-replicating or destructive programs (e.g., viruses, worms, malware).

18. Participating in activities involving disclosure or masquerading or defaming the college.

19. Viewing, copying, altering or destroying data, software, documentation or data communications belonging to St. Albert's College (Autonomous) or to another individual or entity without permission.

20. Allowing another individual (whether they might otherwise be authorized to use the St. Albert's College (Autonomous) Information Technology Resources or not) to use a login account credential.

USE OF THE ST. ALBERT'S COLLEGE (AUTONOMOUS) NETWORK AND DATA MANAGEMENT SYSTEMS POLICY

St. Albert's College (Autonomous) owns the St. Albert's College (Autonomous) Information Technology Resources including the network systems and applications. This policy is intended to provide St. Albert's College (Autonomous) network users with guidelines for responsible and appropriate utilization of these resources. Use of the St. Albert's College (Autonomous) network and St. Albert's College (Autonomous) data management systems shall be for the purpose of facilitating the exchange and storage of information, including information on students and/or employees, and compliance with and furtherance of, the education, research, and administrative missions of the college.

St. Albert's College (Autonomous) reserves the right to determine at any time what constitutes appropriate use of the St. Albert's College (Autonomous) network and any computing access and services provided by St. Albert's College (Autonomous) .

A. GOALS

The goals of this policy are to:

1. Assure the integrity and reliability of the College internal networks, systems on those networks, databases, legacy systems, web-accessible resources, and any computing resource connected to them.

2. Ensure the security and privacy of the College computer systems, networks and data.

3. Ensure the protection and retention of sensitive data.

4. Establish appropriate guidelines for the use of the College network and data, whether accessed from on or off-campus.

B. PROHIBITED USE

Specifically prohibited uses of the St. Albert's College (Autonomous) network and data management systems include:

1. Hacking, attempting to hack, or assisting others to hack or breach the security of any St. Albert's College (Autonomous) data, network, or technology resource, or to facilitate unauthorized access.

2. Use of any St. Albert's College (Autonomous) network or data management system to create, disseminate or execute self-replicating or destructive programs (e.g., viruses, worms, Trojan horses, malware).

3. Viewing, copying, altering or destroying data, software, documentation or data communications belonging to St. Albert's College (Autonomous) or to another individual without permission.

4. Individuals allowing another individual (regardless of whether they might otherwise be authorized to use the St. Albert's College (Autonomous) network and/or St. Albert's College (Autonomous) data management systems) to use their login account password.

5. Accessing data for any purpose other than to perform the official duties of a St. Albert's College (Autonomous) position.

6. Unauthorized disclosure of information to a third party.

7. Bypassing the St. Albert's College (Autonomous) data management systems "time-out" feature, unless specifically authorized by the DTL.

C. RESPONSIBILITIES

All users of the St. Albert's College (Autonomous) IT Resources, including its network and data management systems, have a responsibility to comply with this policy and to understand their responsibilities and all expectations as spelled out in their job duties. This includes the requirement for confidentiality, retention and access to records stored within the College systems. St. Albert's College (Autonomous) DTL and its representatives also have responsibilities under this policy. These include the responsibilities for logging and monitoring networks, data management systems and electronic messaging systems.

ST. ALBERT'S COLLEGE (AUTONOMOUS) ERNAKULAM KOCHI-18

COPYRIGHT INFRINGEMENT POLICY

It is the policy of St. Albert's College (Autonomous) to fully respect all rights that exist in any material protected by the copyright laws of the India while also encouraging usage of the material that furthers the educational mission of St. Albert's College (Autonomous). This Policy provides guidance to faculty, staff, and students, and beneficiaries on the usage of copyrighted material.

A. TECHNOLOGY-BASED DETERRENT

St. Albert's College (Autonomous) uses software and firewall to manage bandwidth utilization on campus.

B. COMMUNITY EDUCATION

All students are given the opportunity to attend a session at orientation on current technology issues. This session addresses copyright infringement and other common policy violations that result through technology. At the start of college year an email is sent to all currently enrolled students from DIMC. This email provides a number of notifications and guidelines in compliance with federal and state regulations.

C. PROCEDURES FOR HANDLING UNAUTHORIZED DISTRIBUTION OF COPYRIGHTED MATERIAL

Upon receiving notification of copyright infringement through a takedown notice, DTL has a set procedure of enforcement. The infringing user is identified. First time offenders are disconnected from the network and sent a notification of infringement as well as a request to agree not to share copyright material on the network without proper permission. The user is afforded the opportunity to meet in person to discuss the takedown notice. The user may be disconnected up to two weeks. During the disconnection period students still have access to the network using lab and checkout workstations. Further infringement violations will be referred to the disciplinary procedure. St. Albert's College (Autonomous) disallows the sharing of copyrighted material.

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM KOCHI-18

Approved by:
Chairman

Revision number: 1

EMAIL USAGE POLICY

Electronic mail tools are provided to St. Albert's College (Autonomous) employees and students in order for them to efficiently communicate. A number of St. Albert's College (Autonomous) IT security standards are in place to define the practices, processes and controls related to using St. Albert's College (Autonomous) provided e-mail resources. In order to ensure that the integrity and reliability of the St. Albert's College (Autonomous) internal networks are not compromised by inappropriate use, users will comply with all provisions of these standards. Email from any St. Albert's College (Autonomous) computer system shall not be used to create or distribute any content that is:

1. Disruptive

2. Offensive

3. Derogatory

4. Malicious

5. Discriminatory about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and/or practices, political beliefs or national origin.

6. Otherwise in violation of any binding law or St. Albert's College (Autonomous) policy.

A. PROHIBITED USE

1. Unauthorized distribution of copyrighted material.

2. Sending discriminatory, harassing or threatening messages or images.

3. Sending content that is deemed to be offensive, including the use of vulgar or harassing language/images.

4. Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages.

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTO
ERNAKULAM KOCHI-18

Approved by:
Chairman

Revision number: 1

5. Sending, receiving, or accessing pornographic materials.

6. Sending malicious emails, i.e. any information that could be used to sabotage institutional progress or as personal attacks.

7. Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate College purposes.

8. Sending unauthorized copies of College files or other College data.

9. Destroying, deleting, erasing, or concealing College emails intended for legitimate College business.

10. Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the College's networks or systems or those of any other individual or entity.

11. Becoming involved and promoting in partisan politics.

12. Causing congestion, disruption, disablement, alteration, or impairment of College email systems.

13. Using email to promote recreational games or Ponzi schemes.

14. Hacking into another user's email account.

15. Engaging in private or personal business activities.

16. Extensive personal use or for personal gain.

17. Use that is in violation of any binding law or St. Albert's College (Autonomous) policy. If there are questions about what is considered prohibited use, employees should check with DIMC.

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM, KOCHI-18

INTERNET USAGE AND SOCIAL MEDIA POLICY

A. PURPOSE

St. Albert's College (Autonomous) operates an internal private network as part of its educational infrastructure. It also extends and operates external connections to the Internet. The purpose of this policy is to clearly delineate the limitations of Internet use available through that network.

The internet access of St. Albert's College (Autonomous) is through a dedicated network provided exclusively for the benefit of St. Albert's College (Autonomous) students, employees, staff, and others directly involved in campus life and the academic community. The private St. Albert's College (Autonomous) network is available through both wired and wireless terminals, but access is not extended to the public at-large. Special requests for public access will be reviewed on the same basis as the Third-Party Access.

Public access to the St. Albert's College (Autonomous) wireless network is not allowed. To ensure the continued privacy of the St. Albert's College (Autonomous) network, security measures, policies and standards are implemented to only grant access to the network through campus facilities or through authorized user authentication and access codes, such as mac id authorization, login accounts and passwords. Devices using the College's wireless network will be configured by the St. Albert's College (Autonomous) DIMC support personnel to require the registration of such a wireless device to an authorized St. Albert's College (Autonomous) user.

B. INTERNET USAGE POLICY

Employees, students, and beneficiariesare responsible for reading and adhering to the St. Albert's College (Autonomous) Personnel, Policies, and Procedures when using the Internet. Violations of certain policies can occur through the use of the Internet. Investigations of violations of those policies can include evidence obtained through the use of the Internet.

If a user of St. Albert's College (Autonomous) Internet service is unsure about what constitutes acceptable Internet usage, the user should ask their supervisor or the concerned DIMC member for further guidance and clarification.

1. St. Albert's College (Autonomous) users are expected to use the Internet responsibly and productively.

2. Activities include research and educational tasks that may be found via the Internet that would help in a staff, faculty and student's role.

3. The student personal use is allowed to the extent that is does not interfere with business and education and to the extent there is no unauthorized distribution of copyrighted material. St. Albert's College (Autonomous) reserves the right to limit or discontinue personal use by blocking streaming and social media sites or other personal use activities if the use impedes educational network communication, violates the intellectual property rights of others, or otherwise constitutes unlawful or unauthorized access.

4. Employees accessing the Internet with College-owned equipment shall limit their personal use to a minimum and usage should not be performed during business hours.

5. All Internet data that is composed, transmitted and/or received by St. Albert's College (Autonomous) computer, network, and internet systems is considered to belong to St. Albert's College (Autonomous) and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties. Employees have no expectation of privacy of their internet searches, internet browser history, or other data composed, transmitted, and/or received through St. Albert's College (Autonomous) computer, network, and internet systems.

6. The equipment, services and technology used to access the Internet are the property of St. Albert's College (Autonomous). The College reserves the right to monitor Internet traffic and access data that is composed, sent or received through its online connections.

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM . KOCHI-18

Approved by:
Chairman

Revision number: 1

7. All sites and downloads may be monitored and/or blocked by St. Albert's College (Autonomous) DIMC if they are deemed to be harmful, unlawful, unauthorized, and/or not productive to business.

8. The installation of software on any St. Albert's College (Autonomous) equipment including, but not limited to, instant messaging software is strictly prohibited.

9. Prohibited use of the Internet by Staff, Faculty and Students includes all harmful, unlawful, or unauthorized use. This includes, but is not limited to:

a. Streaming radio or music services using College computers in College offices during business hours.

b. Unauthorized distribution of copyrighted material.

c. Using computers to perpetrate any form of fraud, and/or software, film or music piracy. d. Stealing, using, or disclosing someone else's password without authorization.

d. Downloading, copying or pirating software, media files and electronic files that are copyrighted or without authorization.

e. Sharing confidential material, trade secrets, or proprietary information outside of the organization.

f. Hacking into unauthorized websites.

g. Sending or posting information that is defamatory to the college, its products/services, colleagues and/or consumers.

h. Introducing malicious software onto or jeopardizing the security of the College network and/or systems.

i. Defeating or attempting to defeat security restrictions on college systems and applications

j. Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.

k. Passing off personal views as representing those of St. Albert's College (Autonomous).

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM, KOCHI-18

l. Academic cheating and plagiarism.

m. Accessing any St. Albert's College (Autonomous) course materials for which distribution and use has been specifically prohibited by the instructor. This includes, but is not limited to St. Albert's College (Autonomous) materials found on crowdsourcing course siteswhich contain materials such as graded quizzes and exams, homework answers, etc., along with any questions that are or might be intended for future quizzes and exams.

C. SOCIAL MEDIA POLICY

This policy provides guidance for staff, faculty and student use of social media, which should be broadly understood for purposes of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information and media with others in a contemporaneous manner.

Social media use should not interfere with employee's or student's responsibilities at St. Albert's College (Autonomous). The primary purpose for St. Albert's College (Autonomous) computer systems is to be for business and academic purposes.

The following principles apply to professional use of social media on behalf of St. Albert's College (Autonomous) as well as personal use of social media when referencing St. Albert's College (Autonomous).

1. Users should be aware of the effect their actions may have on their reputation and the reputation St. Albert's College (Autonomous). The information that users post or publish may be public information or otherwise accessible for a long time.
2. Users should be aware that St. Albert's College (Autonomous) may observe content and information made available by users through social media. Users should use their best judgment in posting material that is either inappropriate or harmful to St. Albert's College (Autonomous), its employees or consumers.

3. Although not an exclusive list, some specific examples of prohibited social media conduct include posting commentary, content, or images that are unlawful, unauthorized, defamatory, pornographic, proprietary, harassing, libelous, or that can create a hostile workplace or student community environment.
4. Employees are not to publish, post or release any information that is considered confidential. If there are questions about what is considered confidential or protected by FERPA, employees should check with the DIMC.
5. Social media networks, blogs and other types of online content sometimes generate press and media attention or legal questions. Employees should refer these inquiries to the authorized St. Albert's College (Autonomous) DIMC member.
6. If users encounter a situation while using social media that threatens to become antagonistic or threatens to harm others or themselves, this should be reported either to DIMC or the office. Supervisors and DIMC members must report every incident to the DTL and their chain of command.
7. When using St. Albert's College (Autonomous) computer systems, use of social media for business purposes is allowed (ex: Facebook, Twitter, St. Albert's College (Autonomous) blogs and LinkedIn), but personal use of social media networks or personal blogging of online content is prohibited and could result in disciplinary action.
8. If employees, students, or beneficiaries publish content after-hours that involves work or subjects associated with St. Albert's College (Autonomous), a disclaimer should be used, such as this: "The opinions on this site are my own and may not represent St. Albert's College (Autonomous) positions, strategies or opinions."
9. It is imperative that employees, students, and beneficiaries keep St. Albert's College (Autonomous) related social media accounts separate from personal accounts. Use of College email addresses to establish personal social media accounts is strictly prohibited.

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM KOCHI-15

INFORMATION TECHNOLOGY SECURITY POLICY

St. Albert's College (Autonomous) acknowledges the obligation to provide adequate security and protection of all Information Technology (IT) usage within its domain of ownership and control. This policy serves as an umbrella that governs all other St. Albert's College (Autonomous) policies pertaining to IT usage on campus, and complies with the appropriate IT policies. It is also the intent of St. Albert's College (Autonomous) to take precautions to prevent revealing specific security policies, standards and practices containing information that may be confidential or private regarding St. Albert's College (Autonomous) business. '

The St. Albert's College (Autonomous) IT security policy is acknowledged as a "dynamic" document that may require alteration periodically to address changes in technology, applications, procedures, legal and social imperatives, and unanticipated changes.

A. INFORMATION TECHNOLOGY SECURITY

It is the sole responsibility of the DTL to provide oversight management of all tasks and procedures that directly pertain to maintaining IT security on campus. It is the responsibility of all members of the college community to participate and share this obligation, as specified by all supportive policies and procedures pertaining to technology use on campus.

B. IT SECURITY

IT security is defined as:

1. Protecting the integrity, security, availability and confidentiality of information assets managed by St. Albert's College (Autonomous) .
2. Protecting information assets from unauthorized release or modification, and from accidental or intentional damage or destruction.
3. Protecting technology assets such as hardware, software, telecommunications, networks (infrastructure) from unauthorized use.

C. MAINTENANCE OF SECURITY

IT security will be maintained by upholding the following guidelines and standards:

1. St. Albert's College (Autonomous) will operate in a manner consistent with the goals of the Information Technology Department to maintain a shared, trusted environment within St. Albert's College (Autonomous) and within the College community system for the protection of all data relating to business and education.

2. St. Albert's College (Autonomous) will maintain an IT security audit portfolio that includes comprehensive documentation of all security processes and configuration of all firewalls and defensive mechanisms, such as virus and malware protection will be included in this audit portfolio. This portfolio and all documentation related to any security policies will be maintained by the St. Albert's College (Autonomous) DIMC. The templates are provided in the Appendix A.

3. St. Albert's College (Autonomous) will ensure that all college employees are appropriately familiar with all IT security policies and procedures, and are aware of their personal responsibilities to protect IT resources on campus. St. Albert's College (Autonomous) DIMC will provide training to each employee in the security procedures for which they are responsible.

4. St. Albert's College (Autonomous) will review its security processes, policies, procedures, and practices annually. In the event of any significant changes to its business, computing, or telecommunications environments, St. Albert's College (Autonomous) will make appropriate updates as necessary.

5. A compliance audit of this IT security policy will be conducted when deemed necessary. The nature and scope of the audit must be commensurate with the extent that St. Albert's College (Autonomous) is dependent on secure IT to accomplish its critical business functions. St. Albert's College (Autonomous) will maintain documentation showing the results of its review or audit and the plan for correcting material deficiencies revealed by the review or audit.

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM, KOCHI-18

Approved by:
Chairman

Revision number: 1

D. RESPONSIBILITIES OF DIMC

1. Providing the college with secure business applications, services, infrastructures, and procedures for addressing the business needs of the College.

2. Following and enforcing internal security standards established for creating and maintaining secure sessions for application access.

3. Notifying the appropriate administrator(s) when an individual or individuals have knowingly compromised IT security on campus. The DTL is not responsible for determining disciplinary action for individuals who violate IT security policies. This responsibility will be managed by the respective office, administrator, or local law enforcement, depending on the scope and nature of the violation.

E. SECURITY BREACH NOTIFICATION PROCEDURE

This procedure governs the actions of any St. Albert's College (Autonomous) employee who discovers or is notified of a breach or possible breach of the security of unencrypted personal information collected and retained by St. Albert's College (Autonomous) as computerized data. This breach can be the result of a compromise of a St. Albert's College (Autonomous) computing system or network, the loss or theft of any physical device in which personal information is stored, or the loss or theft of any storage medium upon which personal information is maintained. If the security of any St. Albert's College (Autonomous) system storing or processing computerized data that includes unencrypted personal information is compromised and a notification must be issued.

The DIMC will take any measures to determine the scope of the breach and restore the integrity of the affected data system.

The notification may be delayed if law enforcement needs to be contacted for a criminal investigation.

1. Physical Breach

ST. ALBERT'S COLLEGE (A
ERNAKULAM, KOCHI-18

i. If a report is made to the St. Albert's College (Autonomous) office of the bursar of the theft of a computing or storage device, the office will:

   1. Follow their normal procedures regarding theft of college property
   2. Report it to law enforcement, and act as liaison with any law enforcement agency involved in the situation.
   3. Notify the DIMC of the incident.

ii. If a report is made to the DIMC of the theft of a computing or storage device, ITD will:

   1. Notify the office of the bursar.
   2. Provide any inventory information to the person concerned of the theft.
   3. Participate in any investigatory actions as directed by the PRO.

2. Technical Breach

i. A technical breach is defined as the discovery by technical support staff of a breach of security of a computer or the St. Albert's College (Autonomous) network.

ii. If the presenting incident is discovery of a network breach, the DIMC technical support personnel will:

   1. Begin network and computer technical investigations addressing intrusion detection and incident response. This will continue until the security and technical aspects of the situation are resolved.
   2. Report to the DTL, all aspects of the breach and how it occurred.
   3. Determine if a person or group responsible can be named.
   4. Determine safeguards that need to be put in place to prevent a reoccurrence.
   5. In some circumstances, it may be appropriate to report a breach of the security of the network or St. Albert's College (Autonomous) computers to law enforcement, as well.
   6. The DTL, Chairman or designee and law enforcement will:

iii. Consult regarding the nature and scope of the security breach and determine whether law enforcement needs to be engaged.

iv. Decide whether and to what extent members of the St. Albert's College (Autonomous) campus community and victims of such breach need to be notified.

v. Research each incident and determine how it is to be handled.

vi. If it is determined that a breach may have compromised the security, confidentiality, or integrity of St. Albert's College (Autonomous) - managed personal information, the Director of Information Technology (or designee) will initiate a meeting as soon as possible with the executive council consisting of the following or their designees: a) Chairman b) Vice-Chairmen c) Bursar d) Principal e) Vice-principals f) Deans g) PRO and h)DIMC members.

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM KOCHI-18

INFORMATION TECHNOLOGY SECURITY PLAN

This document summarizes the St. Albert's College (Autonomous) 's comprehensive written Information Technology (IT) Security Plan. In particular, this document describes the IT Security Plan elements pursuant to which the Institution intends to ensure the security and confidentiality of covered records, protect against any anticipated threats or hazards to the security of such records, and protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to the College's IT consumers.

A. DESIGNATION OF REPRESENTATIVE

The Digital Infrastructure Management Cell Team Leader (DTL) is designated as the IT personnel who shall be responsible for coordinating and overseeing the IT Security Plan. The DTL may designate other representatives of the DIMC team to cover and coordinate a particular element of the IT Security Plan.

B. SCOPE

The IT Security Plan applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information:

1) A student or other third party provides in order to obtain a financial service from the Institution,

2) About a student or other third party resulting from any transaction with the Institution involving a financial service, or

3) Otherwise obtained about a student or other third party in connection with providing a financial service to the person.

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM, KOCHI-18

C. ELEMENTS OF THE IT SECURITY PLAN

1) Risk Identification and Assessment: The institution intends, as part of the IT Security Plan, to undertake to identify and assess external and internal risk to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. In implementing the IT Security Plan, the DTL will establish procedures for identifying and assessing such risk in each relevant area of the Institution's operation, including:

a. Employee training and management: The DTL will coordinate with representatives in the Institution's Human Resources and Financial Aid offices to evaluate the effectiveness of the Institution's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the Institution's current Personnel, Policies and Procedures Manual and the IT Policy.

b. Information System and Information Processing and Disposal: The DTL will coordinate with representatives of the Institution's Financial Aid and College Office to assess the risks to nonpublic financial information associated with the Institution's information system, including network and software design, information processing, and the storage, transmission, and disposal of nonpublic financial information.

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM KOCHI-18

USE OF THE COLLEGENETWORK AND DATA MANAGEMENT SYSTEMS POLICY

The DTL will also assess procedures for monitoring potential information security threats associated with software systems and for managing security updates for software and operating systems.

A. DETECTING, PREVENTING AND RESPONDING TO ATTACKS

The DTL will coordinate with other relevant units to evaluate procedures for and methods of detecting, preventing, and responding to attacks, other systems failures, and network access. The DTL will evaluate the IT security policies and procedures for coordinating responses to network attacks and developing incident response teams and policies. The DTL may elect to delegate to a representative of the DIMC the responsibility for monitoring and disseminating information about known security attacks and other threats to the integrity of networks utilized by the Institution.

B. DESIGNING AND IMPLEMENTING SAFEGUARDS

The risk assessment and analysis shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper, or other form. The DTL will implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

C. OVERSEEING SERVICE PROVIDERS

The DTL shall institute methods for selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they have access. In addition, the DTL will work with other designated institutional officials to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. D. Adjustment to IT Security Plan The DTL is responsible for evaluating and adjusting the IT Security Plan based on the risk identification and assessment activates undertaken pursuant to the IT Security Plan, as well as any material changes to the Institution’s operations or other circumstances that may have a material impact on the IT Security Plan.

COMPUTER LABS POLICY

St. Albert's College (Autonomous) provides students access to computing technology resources in numerous labs and computer classrooms across all campuses. Since the student population on campus is very dynamic and diverse, it is imperative that careful articulation of the policies, expectations, and standards for use of these resources be provided to them, and to the St. Albert's College (Autonomous) staff and faculty who support those students in their educational endeavors. This policy is intended to meet that imperative, and to provide all campus users with guidelines for responsible and appropriate use of these campus computing and technology resources. The primary purpose of the St. Albert's College (Autonomous) computer labs is to provide computing technology resources for students and to facilitate the exchange of information related to, and in furtherance of the education, research and academic missions of the College.

A. GOALS

The goals of the St. Albert's College (Autonomous) computer labs are to:

1) Provide a computer labs environment across centers that are supportive of learning.

2) Help assure the integrity and reliability of the St. Albert's College (Autonomous) internal networks, hosts on those networks, and any computing resource connected to them.

3) Ensure the security and privacy of the St. Albert's College (Autonomous) computer systems and networks.

4) Establish appropriate guidelines for the use of St. Albert's College (Autonomous) - owned technology.

B. PROHIBITED USE

Using St. Albert's College (Autonomous) Information Technology Resources for uses and/or communications that are specifically prohibited in the policy Use of St. Albert's College (Autonomous) Computer Resourceswhich violate any other St. Albert's College (Autonomous) policy, state and federal rule or law is strictly forbidden. Those specifically prohibited uses of any St. Albert's College (Autonomous) ITresource include:

1) Subverting, attempting to subvert, or assisting others to subvert or breach the security of any St. Albert's College (Autonomous) network or other Information Technology Resource, or to facilitate unauthorized access.

2) Use of any St. Albert's College (Autonomous) IT Resource to create, disseminate or execute self-replicating or destructive programs (e.g., viruses, worms, Trojan horses).

3) Viewing, copying, altering or destroying data, software, documentation, or data communications belonging to St. Albert's College (Autonomous), or to another individual without permission.

4) Individuals allowing another individual (authorized or not to use the St. Albert's College (Autonomous) IT Resource) to use their login account password.

5) Disclosing access credentials or masquerading using access granted to another user.

6) Using St. Albert's College (Autonomous) computing resources for personal or private financial gain without written authorization.

7) Unauthorized distribution of copyrighted material.

8) Tampering or theft of equipments or devices of St. Albert's College (Autonomous) from within the lab.

C. ACCESS TO COMPUTING LABS

St. Albert's College (Autonomous) computer labs are open for computer use only under the leadership of authorized faculty, staff, for currently enrolled St. Albert's College (Autonomous) students. Access to any St. Albert's College (Autonomous) computing lab is managed through the St. Albert's College (Autonomous) network.

1) All labs are to be monitored and proper registers are to be maintained

2) Non-student adult visitors may be allowed in monitored labs only with the prior permission of the Chairman or designee under the supervision of a DIMC member. In the event of a non-student visitor violating any provisions of this policy or the computer labs procedures,

the lab-in-charge for the specific lab may instruct the visitor to leave. Non-student visitors will not be allowed into any unmonitored lab.

3) Faculty and staff may only use St. Albert's College (Autonomous) computer labs in furtherance of their support of the learning objectives of St. Albert's College (Autonomous) students.

4) St. Albert's College (Autonomous) computer labs will not be used to perform duties or tasks normally performed in the employee's office environment.

D. LABS AND CLASSROOMS

St. Albert's College (Autonomous) provides different types of computing facilities for use in supporting student learning on campus. These policies apply equally in all these facilities, unless exceptions are otherwise specifically stated. These facilities are: electronic classrooms, computer classrooms, specialized computer labs.

1) Electronic Classrooms provide multimedia capabilities for instruction from a single, centralized instructor station. These rooms are scheduled for use in the same manner as any other classroom at St. Albert's College (Autonomous) following standard St. Albert's College (Autonomous) policies and procedures.

2) Computer Classrooms provide hands-on technical instruction in a classroom environment. These labs are only available for use during those times that have been specifically scheduled. Registered must be maintained and students must be designated to a specific seat in the lab.

3) Specialized Labs are equipped with specialized hardware and software devoted to supporting the program's unique educational mission. These labs support such varying disciplines as physics, math and language, and are often assigned to students as a part of their regular class work. These labs are staffed by faculty and/or lab assistants who provide additional tutorial assistance within the program's specialty. Use of these labs are restricted to users taking the specific classes supported by the facility monitored through registers.

E. SENSITIVE MATERIALS

All St. Albert's College (Autonomous) computer labs are considered shared public places. Users should be aware that some materials accessed on the Internet may be considered controversial, offensive, inappropriate or inaccurate. St. Albert's College (Autonomous) asks users, out of consideration for others, to take care not to display, or broadcast in any St. Albert's College (Autonomous) -shared public place, any images, sounds, or messages that could create an atmosphere of discomfort, harassment or intimidation for others, and to refrain from transmitting such images, sounds or messages to others using St. Albert's College (Autonomous) computing resources.

In some situations, the display or broadcast of such materials is necessary to further a legitimate educational purpose. In these cases, St. Albert's College (Autonomous) asks that users be sensitive to the public nature of shared facilities and make arrangements to access these materials in a private environment.

In some situations, the display or broadcast of such materials, if unlawful or otherwise prohibited by this Policy could be grounds for disciplinary action.

F. GENERAL LAB RULES

1) Computing labs will only be used for legitimate academic purposes. Bags, food, and drinks are not permitted.

2) All St. Albert's College (Autonomous) computer labs are intended to be quiet work and study environments, similar to a library. Users are encouraged to avoid excessive noise, keeping the level of conversational noise at a minimum.

3) Children under the age of 16 will not be allowed in any St. Albert's College (Autonomous) computer lab unless specific written authorization has been granted by the Chairman.

4) Operating hours Lab hours will be posted in each lab. All users shall complete their work, including obtaining any printouts, before closing time. Users are not permitted to stay in the computer lab areas after closing time. Refusal to comply may result in disciplinary actions.

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM, KOCHI-18

Approved by:
Chairman

Revision number: 1

5) Printers are provided in most St. Albert's College (Autonomous) computer labs wherever necessary as a privilege for student use only; faculty and staff should refrain from printing in a lab. Users should exercise discretion in the use of printers in computing labs. Most programs have print preview functions which should be used prior to printing any final document. Print usage on the student network may be actively monitored for abuse. Those users identified as printing excessively will be notified and asked to comply with this policy.

6) Users may not store any files on the hard drives of any lab computers without specific permission from computing services. Faculty may, for a class in which the ability to store files locally is a part of the classroom curriculum, negotiate blanket permission to do this for students enrolled in their class. Users are encouraged to save often and to make frequent backups of their storage media.

7)Any student using any lab computer for non-educational purposes may be denied further access to the lab resource by a lab-in-charge or responsible teaching faculty in charge of the student.

8)St. Albert's College (Autonomous) will not be responsible for personal lost or stolen items left in any lab. Items found in the lab will be sent to the College office. Users should label all media with their name for easy identification, if misplaced.

9) Aggressive behavior will not be tolerated in any St. Albert's College (Autonomous) computer lab. If necessary, lab-in-charges will report incidents that cannot be resolved in a quiet, orderly manner to the tutor,Heads of the Departments,Vice-principal or principal. Disciplinary actions will be taken if the issue is escalated.

10) For safety reasons, it is important that computer lab users make an effort to keep aisles clear. Materials such as books and pens brought into a computer lab should be taken out when the user leaves. After classes held in computer labs, the faculty in charge of the specific classshould, ensure that students have cleaned and properly arranged their workspaces.

11) No equipment in any classroom lab may be moved within the classroom or removed from a lab without permission of the Chairman, Vice-Chariman, Bursar, or DTL. This includes

all computer hardware, including monitors, mice and keyboards and peripheral devices, such as surge protectors, UPS or printers. No user should disconnect any technology resources from any computer or network connection, nor move any tables upon which computing equipment rests without prior approval. All damaged equipment discovered in any lab should be reported to the DIMC.

12) Users will be held responsible for the IT resources they use in any St. Albert's College (Autonomous) lab. Under no circumstances will users leave a computer unattended and unlocked for more than fifteen (15) minutes. Users should never leave their workstation unattended without first saving any data upon which they are working. If a computer in the open lab is left unattended for more than fifteen (15) minutes, labin-charges may log the user off the computer to make it available for other users. Any personal effects in the area of the computer will be moved.

13) Unauthorized access to accounts, files or data held on St. Albert's College (Autonomous) computing systems, or the use of St. Albert's College (Autonomous) computing systems and networks to access any other system without authorization is a violation of these policies and potentially a criminal offense. Such unauthorized access is strictly prohibited.

G. RESPONSIBILITIES

All users of the St. Albert's College (Autonomous) computer labs have a responsibility to know, understand, and comply with this policy, to understand their responsibilities, and to meet all the expectations of this and all other St. Albert's College (Autonomous) IT security policies and standards. These responsibilities include assumption of any civil and/or criminal liability which may arise from their individual use or misuse of St. Albert's College (Autonomous) technology resources.

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS) ★ ERNAKULAM, KOCHI-18 ★

Approved by:
Chairman

Revision number: 1

INFORMATION TECHNOLOGY RESOURCES BY THIRD PARTIES POLICY

St. Albert's College (Autonomous) frequently provides access to its Information Technology Resources, including computer facilities, to private company resources, tribal offices and community members to conduct College business when such resources are not in direct use for business or academic purposes, provided such use substantially relates to and does not interfere with the mission of the College. This access to St. Albert's College (Autonomous) facilities includes access to the wireless network, computer classrooms, computer labs, and electronic classrooms on campus.

A. AUTHORITY

The DIMC Team Leader or designee has primary responsibility for all aspects of third-party access to all St. Albert's College (Autonomous) IT resources. These entities must agree to comply with this Policy, the security policies, and standards of St. Albert's College (Autonomous). St. Albert's College (Autonomous), through DIMC members, reserves the right to determine, at any time, what constitutes appropriate use of the St. Albert's College (Autonomous) technology resources and the St. Albert's College (Autonomous) network resources, including any access and/or any computing services provided by St. Albert's College (Autonomous) .

B. PERMISSION FOR TEMPORARY USE

Any of these entities must provide documentation of the duration, the list of systems and access required and the location where access is required. This request must be approved by the DTL and forwarded to the Chairman or designee. The DIMC personnel will create a Help Desk Ticket to document the access and actions taken during the period of access.

C. LIMITATIONS ON USE

All third-party use will have a documented duration which will be reviewed at the end of the duration. Access will need to be renewed with a new approval for the level of access.

D. SECURITY RIGHTS

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS)
★ ERNAKULAM KOCHI-18 ★

Approved by:
Chairman

Revision number: 1

Third Parties are granted standard security privileges or access to the computing equipment in St. Albert's College (Autonomous) computer resources sufficient to accomplish their business or educational goals. Individual decisions to allow more access beyond the standard rights will be made by the DTL in consultation with the Chairman. The impact of the request will be evaluated and balanced against the potential risk and threat to the College network, using the IT security standard addressing security privileges as a guideline.

SOFTWARE LICENSING COMPLIANCE POLICY

St. Albert's College (Autonomous) acquires software licenses for the use and distribution to faculty, staff and students for productivity and efficiency of the operation of the college and its interaction with the students. St. Albert's College (Autonomous) expects all students, faculty, and staff members to comply with applicable local, state, and federal laws governing licensed software. This policy ensures that St. Albert's College (Autonomous) and all its employees and students follow the letter and spirit of both state and federal law regarding software licensing.

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM KOCHI-18

Approved by:
Chairman

Revision number: 1

TECHNOLOGY HARDWARE AND SOFTWARE ACQUISITION POLICY

A. PURPOSE

The purpose of this policy is to provide guidelines and the process for acquiring and maintaining institution-wide hardware, software and cloud services identified as mission critical. The intent of the policy is to ensure that computer technology and services comply with College defined support standards and security safeguards.

B. RESPONSIBILITIES

Enterprise network, server and storage appliances for institutional-wide applications will be acquired by the DIMC in consultation with the finance committee (Federal/State Fund) or finance council (Management Fund) as per the funding source. The DIMC Center, IMC server rooms and closets are specially designed with the environment conducive to equipment efficiency and with backup power. The DIMC is responsible for the system management, updates, upgrades and new releases. These systems will be managed and maintained regularly to assure all maintenance procedures are properly scheduled. Planning of such processes will be coordinated with all users impacted. DIMC is responsible for all back-up and restore procedures. All systems will be backed up regularly and with efficiency for restore times. Here are the requirements when acquiring this type of equipment.

1. All computer technology for business and academics must be purchased through ITD.
2. All computer technology assets purchased with College funds (Federal, State, or Management) are the property of the College and not a specific faculty or staff member's department property. College funds include, but are not limited to, grant funds, restricted, or unrestricted funds.

3. Funding for maintenance or support agreements must be coordinated with ITD prior to purchase.

4. DIMC must approve any server or specialized appliance requiring network connectivity prior to acquisition. In addition, the device must meet the required conditions for connectivity.

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM, KOCHI-18

Approved by:
Chairman

Revision number: 1

5. Network connected servers or appliance devices must reside in an environment managed by DIMC must approve any technology that incorporates any kind of wireless access to ensure standards prior to purchase.

6. DIMC must review and approve any software application system or cloud service prior to acquisition.

ST. ALBERT'S COLLEGE (AUTONOMOUS) * ERNAKULAM, KOCHI-18 *

TECHNOLOGY HARDWARE AND SOFTWARE REPLACEMENT AND UPGRADE POLICY

A. PURPOSE

This document defines the policy of St. Albert's College (Autonomous) regarding the replacements of all college-owned technology equipment at the end of its life cycle and also the upgrades of institution-wide software. Adequate computer and network hardware and software are essential for the delivery of instructions, student learning, research and creative activities; and for the efficient and effective management of the institution. Rapid changes in technology require that a well-managed institution have a systematic plan for upgrading and replacing technology to ensure that it offers access to the most basic services. The purpose for this plan is to:

1. Provide consistency of hardware and maintain a standard that will limit the variety of parts and supplies.

2. Regulate the purchasing of computers by establishing a useful life table.

3. Improve the level of support by limiting the number of operating systems, office productivity products and other standard software installed in these systems.

4. Reduce the downtime and outages because of outdated or incompatible equipment.

5. Provide a guideline for evaluation or assessment of IT infrastructure on a regular basis

   a. To assess bandwidth usage and the need to expand or enhance capabilities

   b. To reduce possible failures due to normal aging.

   c. To assure sustainability by replacing it with newer technology.

6. Provide sufficient backup solutions for power, network equipment and server systems for redundancy and high availability.

ST. ALBERT'S COLLEGE (AUTONOMOUS) ★ ERNAKULAM, KOCHI-18 ★

7. To preemptively implement necessary changes. This systematic plan is meant to align with the College's Strategic Plan and to provide a framework for meeting the technology needs of the stakeholders of St. Albert's College (Autonomous) . Input from the DIMC,Chairman, Vice-chairmen, Registrar, Bursar, Principal, and Deans could help encapsulate varying ideas for a more complete plan.

B. RESPONSIBILITIES

1. Administration/Department Heads - Each department head is responsible for identifying any exception (earlier or delayed replacements/upgrades) necessary to ensure that an employee can effectively perform his/her job duties. This information is then passed on to the DTL or designee for the replacement or upgrade process. The Bursar is responsible for reviewing and approving requested exceptions and divisional budgets.

2. DTL or designee is responsible for acquiring estimates for replacements and upgrades and also executing equipment replacements institution-wide including software upgrades according to established replacement cycle. The DTL also makes technical decisions on equipment and software standards and upgrades and replacements based on industry trends, software development life cycles, costs and risks to systems stability.

C. PLAN STATEMENT

St. Albert's College (Autonomous) will maintain modern computer and network hardware and software capable of supporting its educational and business activities. To accomplish this, technology hardware will have to be budgeted for replacement. If a hardware item is determined to be irreparable by DIMC or if the cost to repair exceeds the current market value of the item, the item may be replaced earlier than indicated in the table above with all costs for replacement covered by the College responsible department budget.

Prepared by:
Vice Chairman

Revised date: 02-02-2021

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM KOCHI-18

Approved by:
Chairman

Revision number: 1

PRINTER STANDARDIZATION POLICY

Purchasing will standardize on a network printer from a vendor using special government rate pricing for administrative and institutional use at the College. Each printer will come with built-in double-sided duplex printing capability and a 1-year warranty. Extended warranties can also be purchased with proper justification. Choices will include black and white, color, and multifunction printing. Standardization will provide for better College discounts and support. It will also enable us to keep our printing services sustainable. Approved printer model has undergone reviews and testing to confirm its usability, functionality and supportability on the DIMC network print queue system, and will be made easily accessible on managed computers. Purchase of the recommended printers will ensure a quick and smooth installation. In the event you feel you have printing needs not addressed by the recommended model, please contact the DIMC or submit a Help Desk Ticket. All printers already connected to the St. Albert's College (Autonomous) networks and print server will continue to be supported as per the fund policy.

ST. ALBERT'S COLLEGE (AUTONOMOUS) ★ ERNAKULAM KOCHI-18 ★

Prepared by:
Vice Chairman

Approved by:
Chairman

Revised date: 02-02-2021

Revision number: 1

APPENDIX A

DEFINITIONS

All terms defined in St. Albert's College (Autonomous) policies are applicable. St. Albert's College (Autonomous) Network This includes the administrative and student local area networks (LAN), the wide area networks (WAN) supporting sites separated from the main St. Albert's College (Autonomous) campus, Internet connectivity, networked infrastructure devices such as hubs, switches and servers, warrior web, and all other computers, networks and electronic messaging systems operated for the benefit of St. Albert's College (Autonomous) employees and students. St. Albert's College (Autonomous) Data Management Systems This includes the student information management system, human resources system, finance information management system, cashiering, degree audit and individual databases created by individual departments or the college. St. Albert's College (Autonomous) Information Technology Resources Includes, but is not limited to, St. Albert's College (Autonomous) -owned desktop, laptop or macs or servers, hardware or software; software licenses; workstations; data systems; personal digital assistants; electronic messaging systems; e-mail systems; telephones—both wired and cellular; SCAN services; voice mail systems; fax machines; St. Albert's College (Autonomous) network resources, whether wire-based or wireless; Internet connections, accounts or access; and documentation photocopiers authorized by St. Albert's College (Autonomous) to be used by employees, students and/or other beneficiaries.

AUDIT TEMPLATE

1. Do firewalls exist on all Internet or Extranet connections		
2. Are firewalls used internally to separate networks of different security levels?		
3. Is there a formal procedure for approving all external connections?		
4. Is the use of NAT or PAT implemented into your environment to		

ST. ALBERT'S COLLEGE (AUTONOMOUS) ★ ERNAKULAM, KOCHI-18 ★

hide internal network from the Internet?		
5. Is your firewall and router configured to conform with documented security standards?		
6. Is your firewall's CPU utilization monitored at least every 15 minutes?		
7. Are available security patches implemented within 30 days?		
8. Are security patches tested before they are deployed to production systems?		
9. Do all system changes go through a formal change control process?		
10. Does your cryptographic solution conform to applicable international and national standards, as well as all legal and regulatory controls?		
11. Are only crypto devices used that meet the approval standards and policies of your organization?		
12. Are there documented processes and procedures in place for encryption keys?		
13. Is access to keys restricted to the fewest number of custodians necessary?		
14. Is cardholder information retained when it is no longer needed for business reasons		
15. Is a quarterly inventory audit performed to verify if any stored cardholder information exceeds your retention requirements?		
16. Is CVV2 or magnetic stripe data stored in the database or log files?		

17. Are all passwords on network devices and systems encrypted?		
18. Is stored cardholder data encrypted by one of the following, one-way cipher (hash indexes) such as SHA-1 (not MD5), Truncation, Simple ciphers, index tokens and PADS, strong cryptography such as PGP or Triple-DES with associated key management processes and procedures?		
19. Is telnet or Rlogin used for remote system administration?		
20. Is externally accessible account data transmitted in unencrypted format?		
21. Is confidential account information transmitted via unencrypted email format?		
22. Is strong cryptography and appropriate key controls in place to safeguard data during transmission?		
23. Are modems connected to the internal systems or DMZ systems?		
24. Is anti-virus software installed on all servers and workstations?		
25. Have anti-virus signature files been updated to the latest signature file?		
26. Is account information access on a need to know basis only?		
27. Are access control policies in place for data access privileges to cardholder information?		
28. Is firewall administration limited to only the network security administration staff?		

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM KOCHI-18

29. Is a unique username and password required for each non-consumer user that logs into a system containing cardholder information?		
30. Is at least one of the following methods used to authenticate all non-consumer users when accessing cardholder information: unique user name and password? token devices (i.e., SecureID, certificates, or public key)? biometrics?		
31. Are non-consumer users required to change their password every 60 days?		
32. Are non-consumer user accounts locked within 6 invalid login attempts?		
33. Are password protected screen savers or terminal locks used on all critical systems?		
34. Are group passwords allowed on critical systems?		
35. Are passwords required to contain both numeric and alphabetic characters?		
36. Are individuals allowed to submit a new password that is the same as a previous password?		
37. Are all internal and external dormant accounts removed?		
38. Are applications run on default installations of operating systems?		
39. Is more than one application running as the primary function of a server at any given time?		
40. Are the minimum hardware components met on each network		

component for the software to function properly?		
41. Are all unnecessary services disabled on a server?		
42. Are security controls built into the application development process?		
43. Has the application code been tested for vulnerabilities prior to entering production?		
44. Do you perform penetration testing on your network and applications at least once a year and after any significant modifications?		
45. Is access to all audit trails logged on all critical systems?		
46. Do you log the following: success and failed logins by all users, access to audit trails, deletion of objects, identification of affected components, root/administrator access origination and destination?		
47. Are actions related to encryption key management logged on all servers that utilize the keys?		
48. Do logs include date and time stamp on all critical systems?		
49. Are audit trails on all critical systems secured in a way that they cannot be tampered with?		
50. Do you review audit logs at least once a week on critical systems?		
51. Are audit logs retained for at least six months on all critical systems?		
52. Are vulnerability assessments performed on the internal and external network on a monthly basis and after updates and/or upgrades		

to systems?		
53. Is there a file integrity monitoring system in place to alert personnel of unauthorized modifications to critical systems?		
54. Are security alerts from the intrusion detection sensor monitored 24 hours a day, 7 days a week?		
55. Do you have Network IDS on perimeter related systems?		
56. Are the latest intrusion detection system (IDS) signatures installed on all IDS sensors?		
57. Are file comparison checks being reviewed on critical systems at least once a day?		
58. Is staff provided with adequate training on operational business and recovery plan execution responsibilities?		
59. Are the disaster recovery plan (DRP) and the business contingency plan (BCP) tested annually?		
60. Are security roles and responsibilities formally defined?		
61. Are critical data backed up on a daily basis?		
62. Are backup tapes stored in a location that does not require authorized access?		
63. Are all associated third parties with access to cardholder data contractually required to adhere to CISP data security requirements?		
64. Are information security policies documented, kept current and disseminated to all employees, vendors, contractors and partners?		

65. Is there a security awareness and training program in place?		
66. Are pertinent security alerts monitored, analyzed and distributed to appropriate personnel?		
67. Is a security incident response plan formally documented?		
68. Are employees required to sign an agreement verifying they have read and understood the polices and procedures?		
69. Are employees with access to cardholder data permitted to begin work prior to completion of a background investigation (including credit and criminal record checks)?		
70. Is access to the data center restricted and closely monitored?		
71. Are all paper and electronic media — e.g. computer, networking, and communications hardware, telecommunications lines, etc. — containing cardholder information located in a physically secure environment?		
72. Have all discarded media been erased or destroyed using a formal procedure that ensures the complete deletion of all sensitive data?		
73. Do you maintain strict control over the internal and external distribution of any paper or electronic media containing cardholder data?		
74. Are visitors, including vendors, permitted to enter data centers or access sensitive systems without an escort?		
75. Are visitors asked to sign out and turn in their badge or tag before leaving the building?		

ST. ALBERT'S COLLEGE (AUTONOMOUS)
ERNAKULAM KOCHI-18

76. Is a visitor log retained for at least three months to retain a log of physical activity?		
77. Are all media devices properly inventoried and securely stored?		