Adi Shankara
INSTITUTE OF ENGINEERING AND TECHNOLOGY

Approved by AICTE & Affiliated to APJ Abdul Kalam Technological University
(Owned by Adi Sankara Trust)

IT Policy

Adi Shankara
INSTITUTE OF ENGINEERING AND TECHNOLOGY

IT POLICY

Adi Shankara Institute of Engineering & Technology, Kalady, Kerala established in 2001 and affiliated to A P J Abdul Kalam Technological University, accredited by NBA and approved by AICTE. The various UG branches are Civil Engineering, Computer Science and Engineering (AI), Computer Science and Engineering, Computer Science and Engineering (DS), Electronics & Communication Engineering, Electronics & Biomedical Engineering, Electrical & Electronics Engineering, Mechanical Engineering, Robotics and Automation and PG Branches are Computer Science & Engineering, Communication Engineering, VLSI & Embedded Systems, Power Electronics & Power Systems, MBA and MCA.

This document provides IT policies of Adi Shankara Institute of Engineering & Technology (ASIET). All the selection and deployment of computing, networking, IT Infrastructure are based on IT policy. All employees and students must follow the IT policies. The Policy consists of the following.

1. Firewall Policy
2. Software Licensing
3. Email Policy
4. Wi-Fi Access Policy
5. Website Policy
6. Library Software Access Policy
7. Anti-Virus Policy
8. Backup Policy (Firewall, Wi-Fi, Library Software's, HRMS)
9. HRMS Software Policy (ETLAB)
10. E-waste Policy

Primary Responsibility: IT Team

Secondary responsibility: IT Manager

The policy is managed by the IT Manager and IT Team. Periodical review and audit are conducted.

FIREWALL POLICY

Purpose

Firewall is an essential component of college security infrastructure. Firewalls are defined as security systems that control and restrict network connectivity and network services. Firewalls establish a control point where access controls may be enforced. Connectivity defines which computer systems are permitted to exchange information. A service is sometimes called an application, and it refers to the way for information to flow through a firewall. Examples of services include file transfer protocol (FTP) and web browsing (HTTP). This policy defines the essential rules regarding the management and maintenance of firewall at college.

Scope and Procedures

This policy applies to the firewall in college and is managed by the Department of CSE. Departures from this policy will be permitted only if approved in advance and in writing by the IT Manger/ HOD-CSE or IT Team. In some instances, systems such as routers, Access Point Controllers, telecommunications front ends, or gateways may be functioning as though they are firewalls when they are not formally known as firewall. In some instances, this will require that these systems be upgraded so that they support the minimum functionality defined in this policy.

Required Documentation

Prior to the deployment of college firewall, a diagram of permissible paths with a justification for each, and a description of permissible services accompanied by a justification for each, must be submitted to the IT Teams. Permission to enable such paths and services will be granted by the IT Team only when these paths or services are necessary for important reasons, and sufficient security measures will be consistently employed. The conformance of actual firewall deployments to the documentation provided will be periodically checked by his/her designee. Any changes to paths or services must go through this same process as described below.

Default To Denial

Every connectivity path and service that is not specifically permitted by this policy and supporting documents issued by the Central IT Administration must be blocked by College firewall. The list of currently approved paths and services must be documented and distributed to IT Team with need to know by the Central IT Administration. An inventory of all access paths into and out of college internal networks must be maintained by the IT team.

Regular Testing

Because firewalls provide such an important control measure for college networks, their strength and proper configuration must be tested on a regular basis. Where vendor software supports it, this testing must include the use of software agents that automatically check to determine whether firewalls remain configured and running in a manner that is consistent with college security policies.

This testing process must include consideration of defined configuration parameters, enabled services, permitted connectivity paths, current administrative practices, and adequacy of the deployed security measures. These tests must include the regular execution of vulnerability identification software and the regular performance of penetration tests those responsible for either the administration or management of the firewall must perform these tests.

Logs & Reports

All changes to firewall configuration parameters, enabled services, and permitted connectivity paths must be logged. All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures also must be logged. The integrity of these logs must be protected with checksums, digital signatures, encryption, or similar measures. These logs must be promptly removed from the recording systems and stored in a physically protected container for at least One year after the time they were recorded. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

Intrusion & Prevention Detection

All ASIET firewalls must include intrusion and Prevention detection systems approved by the Information Technology department. Each of these intrusion detection systems must be configured according to the specifications defined by the Information Technology department. Among other potential problems, these intrusion detection systems must detect unauthorized modifications to firewall system files, and detect denial of service attacks in

progress. Such intrusion detection systems must also immediately notify by pager the technical staff that is in a position to take corrective action. All technical staff working on firewalls must be provided with remote access systems and privileges so that they can immediately respond to these incidents even when they are physically removed from the firewall.

Contingency Planning

Technical staff working on firewalls must prepare and obtain IT Manager approval for contingency plans that address the actions to be taken in the event of various problems including system compromise, system malfunction, system crash, system overload, and Internet service provider unavailability. These contingency plans must be kept current to reflect changes in the ASIET information systems environment. These plans must be periodically tested to ensure that they will be effective in restoring a secure and reliable networking environment.

External Connections

All in-bound real-time Internet connections to college internal networks or multi-user computer systems must pass through a firewall before users can use it. Aside from personal computers that access the Internet on an outbound single user session-by- session dial-up basis, no college computer system may be attached to the Internet unless it is protected by a firewall. The computer systems requiring firewall protection include web servers. Unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution, and system usage will be monitored and logged.

Firewall Access Mechanisms

College Firewall must have unique passwords or other access control mechanisms. The same password or access control code must not be used on any internal Credentials. Whenever supported by the involved firewall vendor, those who give technical assistance, must have their identity must be validated.

Firewall Access Privileges

Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a few technically trained individuals. Unless. Firewall must have at least two trained members who are adequately trained to make changes, as circumstances require. Such training includes periodic refresher training course or conference attendance to permit these staff members to stay current with the latest developments in firewall technology and firewall operations. Care must be taken to schedule out-of-town vacations so that at least one person capable of effectively administering the firewall is always readily available.

Disclosure Of Internal Network Information

The internal system addresses, configurations, products deployed, and related system design information for college networked computer systems must be restricted such that both systems and users outside the college internal network cannot access this information.

Routing Policies

Connection from the ISPs are directly connected to the Firewall ports. Inside the firewall use NAT (Network Address Translation), Internet is Distributed to college network. Firewall Policies are writes as USER Based Authentication Policy.

LAN Access

Internet access through Combination of Static IP, Username and password. IT Team will Provide IP Address to Computers in the College LAN. Users must authenticate themselves with their user ID and password to use the Internet.

Wi-Fi Access

Students/Staff in the College can access Wi-Fi after he/she fill up the Wi-Fi Registration form by Simply5. The MAC address of the Device & Mobile Number is registered in the firewall. Staff can access the internet in Laptop/Mobile. Student access is restricted to laptops only.

Staff Policy

Staff must use their Username and password to use Internet Staffroom PCs, Laptop and Mobiles of Staff are controlled through SIMply5 (Wi-Fi access management) in the policy.

Students Policy

Student must use their Username and password to use Internet in Computer Lab PCs, Laptop of Students are running through SIMply5 (Wi-Fi access management) in the policy. In- order to meet peak time during the working hours, this policy runs through a filtered policy. As per the requests given from concern departments, Changes can be applied.

SOFTWARE LICENSING POLICY

Purpose

This policy provides guidelines for software use for our employees within the campus to ensure that all software we use are appropriate and authorized.

Scope and Procedures

- All the employees of the campus follow the software rights as per the software license.
- Each department should check the software and audit for ensuring copy rights of **licensing agreement** and it should be documented. This is audited periodically.
- All the software installation should be carried out by lab instructor in coordination with IT Team.
- All the computer purchases should be verified, and the concerned licensed software is installed in the computer.
- Employees and students are prohibited from bringing software from home and loading it to the campus computer hardware.
- In case any employee uses unauthorized software this will be referred to the Principal for necessary corrective action.

EMAIL POLICY

Purpose

Email accounts and email services are provided to the ASIET community in support of the mission of the College, including teaching, learning, research, and the administrative functions to carry out that mission. ASIET subscribed Google Apps for Education and use Google Apps for Email Service. Users of ASIET email services are expected to act in accordance with the College's Technology Ethics and Privacy Agreement and its Acceptable Use Policy, as well as with professional and personal courtesy and conduct. All users have the responsibility to use these resources in an efficient, effective, ethical, and lawful manner.

Scope and Procedures

This policy and related policies sets forth the framework in which all email services are provided and are to be used at ASIET. Use of the ASIET email system evidences the user's agreement to be bound by this policy. Violations of this policy may result in restriction of access to the ASIET email system and/or other appropriate disciplinary action.

Account Creation

Email accounts are created based on the official name of the staff or faculty as reflected in Human Resource and Registrar records. Faculty and staff members are issued an official ASIET email account when new employees are Joined into the college. Faculty and staff will be notified of their username and Default password from IT Administration team. User can change the password once they logged in. Student can create their own Email ID in College domain on demand basis.

Accessing E-Mail

User can access ASIET Mail Service from Gmail Login.

Group Mail ID

Group mails are created to increase the communication efficiency in teaching, learning, research, and the administrative functions to carry out that mission. Group Mail IDs of Staffs Contains Official Mail Ids of Individuals. Student group mail IDs contains their Personal Email IDs.

E-Mail Quota

Google Apps Provide 30 GB for Email, G-Drive and all the Applications provided by Google.

WI-FI ACCESS POLICY

Purpose

System Configuration:
Simply5 Edge solution comes with a preconfigured Edge gateway to be deployed on- site, it connects the location to Edge user management platform & deliver the service though the locations Wired or Wireless passive network to end clients. Edge device act like a relay between the location & Simply5 cloud service.

Scope and Procedures

Data management:
All the locations data like configuration, policy data & user authentication logs are stored & accessible fromSimply5 Edge dashboard. No user traffic is stored on the Edge.

User Access Levels:

Primary admin account is setup at the time of deployment. Multiple Admin accounts can be created per location basis from Cloud portal. Contact Simply5 support for additional user's onboarding.

Dashboard:

On successful login, you will land on Dashboard which gives you various chats of Demographic data of the users connecting at the location. Though the menu you will be able to access various sections of the product.

Internet Access houses all the Access methods which are used for managing the user access controls. We will explore the modules in details & use cases where it is useful.

- Free Wi-Fi
- Whitelisting
- Vouchers
- Paid WiFi
- Staff
- IoT

All the modules can be individually control by Adding, Rearranging or Removing Access.

Free Wi-Fi

This method is used to provide basic internet access to anyone connecting to guest networking at the location. Admin can enforce Mobile/Email Authentication or Skip Registration based on location requirement. Different policies can be set for Registered & Un-Registered users.

Whitelisting

Module is useful to onboard know users visiting a location. Users are identified by their mobile no. & after the OTP authentication, this policy is applied to their account automatically.

Vouchers

Voucher modules is useful to onboard large numbers of users without prior registration. Unique voucher codeshare generated which can be handed over by Helpdesk / Reception staff when required.
You will be able to select validity period and usable from date to pre-generate the vouchers before the event date & avoid misuse.

Paid WiFi

For user who do not have free access to internet at the location, Paid WiFi module will allow purchasing &use the internet. The module comes pre-integrated with necessary payment gateways to allow this facility. Any amount collected will be added to the wallet balance.

Staff

Usable for providing access to staff at a location with monthly FUP data limits.

IoT

Onboard devices which do not have a display or devices too old to go through portal authentication process using their mac ID. Once added these devices are authorized to access the internet based on speed limits but will not have any data cap.

Deployment Options

Edge gateway can be deployed into your passive network in multiple way.

WEBSITE POLICY

Purpose:

The purpose of the college website is to serve as a central hub for information and resources for both current and prospective students, faculty, staff, and the broader community. It aims to provide up-to-date information on academic programs, admissions, campus events, and research opportunities. Additionally, the website facilitates communication between the college and its stakeholders by offering access to essential services, such as online learning platforms, library databases, and administrative portals. By maintaining a comprehensive and accessible website, the college enhances its educational mission and supports the academic and personal growth of its students. Furthermore, the website reflects the college's commitment to transparency, inclusivity, and engagement with the global educational community

Scope and Procedure

The college's official website is hosted and meticulously maintained by M/s. Intersmart Solutions. The responsibility for the routine upkeep and content management of the site falls under the purview of the college's IT department, led by the IT Manager. To ensure the website remains current and functional, the college has established a Website Monitoring Committee, chaired by the Principal and includes Heads of Departments (HODs) as key members. This committee plays a crucial advisory role, recommending updates and enhancements to keep the website aligned with the college's mission and educational objectives.

Furthermore, to facilitate specialized content management and ensure the accuracy and relevance of information, individual departments are granted separate administrative logins. This enables departments to independently update their sections of the website, allowing for the timely publication of department-specific news, events, and academic materials. In alignment with best practices in IT governance, the college commits to regular reviews of its website management protocols. This includes updating security measures to protect against unauthorized access and ensuring compliance with applicable data protection regulations. The college also emphasizes the importance of accessibility, striving to make the website usable and inclusive for all visitors, including those with disabilities. Through these policies, the college aims to maintain a dynamic,

secure, and user-friendly online presence that effectively serves the needs of its students, faculty, and the broader academic community.

LIBRARY SOFTWARE ACCESS POLICY

Koha

Koha is a fully featured Open-Source Integrated Library System (ILS). The Software is installed in the Central library and Managed by Librarian.

DSpace

DSpace is a web application, allowing researchers and scholars to publish documents and data. While DSpace shares some feature overlap with content management systems and document management systems, the DSpace repository software serves a specific need as a digital archives system, focused on the long-term storage, access and preservation of digital content thus making DSpace the software of choice for academic open digital repositories. DSpace preserves and enables easy and open access to all types of digital content including text, images, moving images, mpegs and data sets.

E -Journal Policy –

Staff and Students can access College purchased E journals from anywhere in the college. Access tothe E Journals is through this policy.

ANTI-VIRUS POLICY

Purpose : This policy is designed to help prevent infection of computer viruses and other malicious code in computers, networks, and Servers of Adi Shankara Institute of Engineering & Technology. This policy is intended to help prevent damage to user applications, data, files, and hardware.

Scope

All faculties, staff, students and research within the University that involves access to college computers, networks and/or Servers, will be subject to the provisions of this policy. Any other parties, who use, work on, or provide services involving College computers, networks, and Servers will also be subject to the provisions of this policy.

Policy Statements

- All computer devices connected to the College network or networked resources shall have anti-virus software installed and configured so that the virus definition files are current, routinely and automatically updated. The anti-virus software must be actively running on these devices.
- All computers owned by the College and used by faculty and staff must have the most recent version of anti-virus provided by the college installed.
- All PC's are to be configured such that they schedule regular operating system updates as provided by the vendor (Windows updates).
- All files on computer devices will be scanned periodically for viruses.
- If found necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the College network until the infection has been removed.
- Exceptions to this policy may be allowed if a computer device cannot have anti-virus software installed. Possible examples of this would be vendor-controlled systems, or devices where anti-virus software has not yet been developed. In these cases, a plan must develop to protect the device from infection.
- An exception may be granted if an infected computer device is discovered that performs a critical function and may not be immediately taken off-line without seriously impairing some critical business function. Under those circumstances, a plan will be developed to

allow the computer device to be taken off-line and the infection purged while protecting the function of the device.

Anti-Virus Software

IT Team provides Windows Defender anti-virus/anti-malware software to College owned Computers.

BACK UP POLICY

Responsibility

Primary Responsibility: IT Team.

Secondary Responsibility: HOD Computer Department.

Procedures

- The Main objective of the Backup process is to prevent loss of valuable data of our institution. If it happens, immediate data recovery from respective backup files.
- Data should be backed up periodically from the server side. Also provide facilities to back up their data for Departments/staff.
- The frequency and extent of backups must be in accordance with the importance of the information
- The Data Custodian will determine the importance of the data via risk assessment and notify IT Services of the required backup frequency.
- The backup and recovery process for each system must be documented and reviewed at least 6Months.
- Backup files should be stored onsite as well as offsite. Offsite backup storage locations must meet or exceed the physical access controls of the source location.
- Backup operations must include verification processes to ensure the integrity of the operation. Backups must be periodically tested, at least annually, to ensure that they are recoverable.

BACKUP PROCESS

Koha and DSpace Backup

Koha and DSpace is hosted inside the college on a dedicated server.

Total code backup will be done every 6 months. If a change / modification happens in Koha and DSpace, Total code backup will be done before and after the job.

Database is critical so that the backup will be done manually in every week. Backup file is a zip file. Name of the backup file is “Koha_Backup_date” Backup file is a zip file. Name of the backup file is “Dspace_Backup_date”.

ERP SOFTWARE POLICY (ETLAB)

Etlab - Campus ERP is an innovative software to take education beyond the walls and is now used by 50+ esteemed institutions to manage their day-to-day administration helping them save human resources through automation and assure reliability through error-free computation. The list of our happy clients includes prominent governmental and non-governmental institutions across the state. With our commitment, hard work and a zero-tolerance policy in product quality, data security and data privacy, during our 10 years of service there was no incident of data hazards or violations occurring to our clients.

The technology we use for the Etlab web application is the PHP Yii framework and the database technology is MySQL. Etlab android mobile application is developed in Kotlin and Java and the iOS mobile application is developed using Swift language. Other technologies we use are React, HTML, JavaScript and Bootstrap. We are using a secure Linux-based server with encrypted storage.

As provided for all our other clients, in ASIET also each user has a unique username and password to log in and they get restricted access to the software as per their user type (admin, teaching staff, non-teaching staff, parents and students). Vertical privilege escalation and horizontal privilege

escalation mitigation protocols are strictly followed. Once the software is handed over to the college, all the privileges for access control and other management are completely vested with the super admin in the college.

Also, the database is regularly backed up to the college server as well as to Etlab server. Etlab is developed using the Yii framework, one of the most secure PHP frameworks widely used and regular internal security audit is performed using OWASP guidelines.

All the user credentials are encrypted, and the user can update their credentials whenever they require. All data transfers through Etlab are encrypted using HTTPS and SSL protocols. Database access permission is currently restricted using user access. Etlab server is protected using multiple-level security protocols.

We are committed towards ensuring data protection and privacy of our clients and we will never compromise the trust of our users.

E-WASTE POLICY

Purpose

E-waste management

Scope

E-waste storage and disposal. It covers all academic departments, Office and Hostels

Responsibilities

Primary Responsibility: Facility Manager

Secondary Responsibility: HODs of various departments, Office superintendent & hostel wardens

Procedures

At the beginning of the academic year the facility manager initiates action to identify e- waste material in each department (refer e-waste management rules-2011 published by Ministry of environment and forest, central government). The items are checked and verified by concerned experts and a report is prepared identifying that the material is not repairable and declared as e-waste. The report to be approved by persons defined as secondary responsibility & Principal. The approved report is sent to Facility Manager and will make following updates:

- Such items are removed from existing stock register
- Such items are stored in one place and updated in the E-waste register

- Get quotations from vendors who are approved by the Pollution Control Board. Based on the recommendation and approval of Principal the items are disposed.
- The details to be recorded and filed in Form 2 as per following reference.

Reference

E-waste management rules-2011 published by Ministry of environment and forest, central government.

MURALI M S

Digitally signed by MURALI M S
Date: 2024.08.08 17:41:46 +05'30'