Information Technology, Cyber Security and E-Waste Management Policy

The University has a policy of upgrading the desktops/laptops every five years. The network upgrade cycle is 7 to 10 years. The servers, peripherals and software upgrades are needed, and a provision for such upgrades is made in the annual budget based on estimated needs. The institute plans to increase the internet speed by increasing the ILL capacity periodically (every six months to 1 year). The University frequently reviews the IT infrastructure as per the time requirement. The IT infrastructure strategies are developed as per the guidelines of the state government as well as UGC from time to time. Software and hardware are upgraded regularly and as and when a demand for the same arrives. Students, teachers, and research scholars are allowed to use the 24-hour, 360-day broadband Internet through Wi-Fi connectivity and access online resources from NPTEL and all other freely available sources.

The central government offered the university connectivity through the National Knowledge Network (NKN). The university is connected to the NKN network, which provides access to a large number of libraries, online lectures, archived lectures of various IITs, virtual classrooms, and many other facilities available under NKN. The internet bandwidth obtained is used to provide internet access to the computers placed in Laboratories. From block to block, optical fiber connectivity is provided.

With the growth of users, IT services, and increasing demand for internet bandwidth, the university has scaled up its switching capabilities and implemented the latest managed wired and Wi-Fi access. The university has very high-end core switches and servers. The university has implemented a private Cloud to provide high-quality services to end users and for ease of management. The university is committed to providing state-of-the-art IT infrastructure and services.

Features of the IT Policy

The university has a comprehensive IT policy with regard to

IT Service Management: NICHE is a campus-specific entity responsible for planning and forecasting specific needs for improving the campus's IT infrastructure, specific maintenance of the IT infrastructure, and uninterrupted delivery of IT services to the user community. To take care of

day-to-day user issues, a complaint management portal/helpdesk is maintained where the individual user can register the complaint and track the resolution status.

Information Security: The policy aims to minimize the risk associated with Internet and email services and define controls against the threats of unauthorized access, theft of information and malicious disruption of services. Periphery network security is implemented using Firewalls and UTM devices to mitigate such risk. These devices are configured in high availability mode and can handle intrusion detection, intrusion prevention, content filtering, application filtering, spam filtering, antivirus and malware detection and filtering. These devices are also used for identity-based network access control.

Network Security: The university campus has completely switched to an available voice-enabled network. The network has a layered architecture consisting of Security, Core, Distribution and Access layers. The users are segregated into different categories, and each category can have different access. This is achieved by dividing the entire network into different logical networks, and access to these logical networks is controlled by implementing the desired access policy.

Risk Management: The core components of the infrastructure providing critical services are implemented in a high-availability Mode. The entire student, faculty, staff, and administrative records are stored in the servers placed in the computing Centre. In addition to this, provisions have been made for power backup, fire alarms, etc.

Software Asset Management: We categorize software assets as open-source and proprietary. The open-source software assets are maintained for accounting purposes. The computing centre maintains the proprietary software assets used for the institution. The concerned departments maintain the software purchased for individual departments' research and teaching. The computing centre signs campus agreements with major software vendors, such as Microsoft, Oracle, MATLAB, etc., to provide licensed copies of software and productivity tools to faculty and staff members of the university.

Open-Source Resources: To reduce the dependence on propriety software and tools, we strongly promote Open-source software, tools, and applications. Currently, the institute supports various versions of the Linux operating system for training and production servers. University extensively uses open-source software tools to support computer-assisted learning, teaching, and design. Some of the open-source software tools used are JDK, Star UML, Visual Paradigm, Eclipse, G++, GCC, SSH, My-SQL server & client, Virtual Box, GNU plot, gcj-jdketc.

***Green Computing:** NICHE strives hard to reduce its carbon footprint. Most of the administrative activities pertaining to faculty, staff, and students are handled through the ERP servers in the data

centre. All the notices are electronically circulated through e-mails. E-mail confirmation is allowed and is preferred over printed letters. NICHE strictly discourages the use of printers and printed materials. The power reduction is managed by replacing the older and power-hungry technology /devices with newer devices requiring less power, e.g., replacing CRT monitors with LCD monitors.

Cyber Security Measures

User Accounts and Administration

NICHE Campus/Hotspot Network usually utilizes a captive portal to allow WIFI-users (authorized) access to the internet. Guests must log in using a local user/ RADIUS/AAA, which they can buy or obtain for free at the Net-lab (Computing Centre). Ours a captive portal with voucher support and can easily create them on the fly.

Intrusion Detection & Prevention

The aim of an inline IPS system is to enhance performance and minimise CPU utilisation. This deep packet inspection system is very powerful and can be used to mitigate security threats at wire speed. Ruleset is an excellent anti-malware IDS/IPS ruleset that significantly enables users with cost constraints to enhance their network-based malware detection. The deep packet inspection system is very powerful and can be used to mitigate security threats at wire speed. IDS/IPS can help you stop torrent seeding, proxy connector VPN tunnelling, etc. IPS is capable of SSL communication, which can be blocked at the initial connection attempt by dropping the SSL key.

Data Security

NICHE stateful firewall keeps track of and monitors the state of active network connections while analyzing incoming traffic and looking for potential traffic and data risks. Basic firewall features include blocking traffic designated as dangerous from either coming into a network or leaving it. It is important to monitor the state and context of network communications because this information can be used to identify threats based on where they are coming from, where they are going, or the content of their data packets. The three-way handshake involves synchronizing both sides of the data transmission process to initiate a connection and then acknowledging each other. In this process, each side transmits information to the other side, and these are examined to see if anything is missing or not in the proper order. As the handshake occurs, a stateful firewall can examine the data being sent and use it to glean information regarding the source, destination, how the packets are sequenced, and the data within the packet itself. If threats are detected, the firewall can reject the data packets.

Network and Communication Security

Virtual Private Network: Utilize the integrated site-to-site VPN (IPsec or SSL VPN / OpenVPN) to create a secure network connection to and from your remote offices. Enjoy the easy configuration and get you started quickly. Enjoy unlimited VPN users and no need to pay any commercial VPN clients. Traffic shaping is very flexible and organized as pipes, queues and corresponding rules. FX defines the allowed bandwidth and streamlines them as weightage within the bandwidth, and the rules are used to apply the shaping to a certain package flow. The shaping rules are handled independently from the firewall rules and other settings. Multi-WAN scenarios are commonly used for failover or load balancing, but combinations are also possible with the FX Firewall. Features such as WAN Failover, WAN Load Balancing, and Combining Balancing & Failover allow you to deal with Multi-WAN to provide continuity. Report & Monitoring System Health graphs with the option to zoom in and export data. Net-flow and analyzer to see the most active users, interfaces, ports & applications.

E-Waste Management Policy

1. Purpose

This policy aims to ensure that NICHE Deemed to be University adopts sustainable practices in managing electronic waste (e-waste) by minimizing its environmental impact and promoting responsible disposal and recycling methods.

2. Importance

This policy applies to all departments, faculty, students, staff, contractors, and anyone associated with NICHE who uses or disposes of electronic equipment owned by the university.

3. Definitions

- E-waste refers to discarded electronic and electrical devices and equipment, such as computers, phones, printers, cables, batteries, etc.

- Recycling: The process of converting waste materials into reusable materials, reducing the need for extracting raw materials.

4. Policy Statements

NICHE is committed to minimizing its e-waste footprint through the following principles:

1. Reduce: Avoid unnecessary purchases of electronic equipment and extend the life of existing devices wherever possible.

2. Reuse: Reuse or donate electronics that are still functional but are no longer needed by the university.

3. Recycle Partner with certified e-waste recycling vendors to ensure the environmentally friendly disposal of obsolete or non-functional electronics.

5. Responsibilities

5.1 University Administration

- Establish and monitor compliance with this policy.
- Engage with certified e-waste management partners for environmentally safe disposal.
- Maintain records of e-waste disposal and recycling efforts.

5.2 Departments

- Promote awareness of e-waste policies and procedures among students and staff.
- Participate in the collection and proper disposal of departmental e-waste.

5.3 Faculty, Staff, and Students

- Comply with the university's e-waste policy when disposing of campus personal and institutional electronic equipment.
- Report any instances of improper e-waste disposal to the administration.

6. Procedures for E-Waste Management

1. Inventory Assessment

Each department shall maintain an up-to-date inventory of electronic devices and conduct annual assessments to determine items eligible for disposal.

2. Collection and Storage

Designate collection points for e-waste within each department. E-waste must be stored in these locations until collected by the authorized recycler.

3. Disposal

All e-waste will be handed over to authorized and certified recycling vendors. NICHE will ensure the recyclers comply with the guidelines outlined by the Ministry of Environment, Forest, and Climate Change (MoEF&CC) and adhere to industry best practices.

4. Data Security

All electronic devices should be wiped clean of any sensitive or confidential data before disposal. The IT Department will

Registrar

Dr. P. THIRUMALVALAVAN,
Registrar,
Noorul Islam Centre for Higher Education,
Kumaracoil - 629 180, Thuckalay,
Kanyakumari District.