IT security and policies at Manav Rachna University

There are different categories of users are inManav Rachna Universities and their requirements are different, their portfolios are different. Therefore different policies are being implied based on the category of the users.

The categories are

1. Faculty
2. Staff general
3. Staff management
4. Staff support and security
5. Students

All the category users uses computers and internet through local area network. Therefore the network, the devices, the databases, the files created by the users are vulnerable to then risk of losing the data, damage of the devices, stealing of important informationetc.

The above threats do arrives from different sources viz. infected device and files bringing by the users, virus infection through unlicensed and untested applications, through emails, through browsing non- secured web sites, phishing internet web sites and finally hackers.

It is impossible to maintain different segregated IT infrastructure for different type of users. The only option to secure the data and devices through strong policy driven user accesses and segregating the infrastructure in virtual and logical way. The segregation also need to have provision of users communicating to each other, exchanging files, exchanging emails etc.

Threat management methodology

Therefore the threat management of the complete IT infrastructure is managed by logical partitioning, applications, devices and policies.

A. For logical portioning complete Local area network is segregated in three virtual network. Except for required port for communication all the ports of the network is closed to stop the unwanted traffic and data movement.
this also stops the direct accessibility of the files between the logical network.

B. Applications like Antivirus are deployed with in the network for scanning each data of the communication and traffic for presence of any virus, and malicious programs and files.

C. Some of the applications are also used to sniff and monitor the harmful activities of the users by installing un-licensed software or downloading the applications harmful to network and the data.

D. Devices like UTM (Unified Threat Management) has been deployed at the network gateway to internet having fire wall, threat management, malicious content filters and lockdown facilities in case of Denial of services.

E. Finally policies have been formulated and strongly implemented to all users of computers, printers, server and local area network. The users are briefed through email or training every time a new threat is discovered.

Data Safety

Most of the university data generated through ERP are stored and maintained by the third party vendor at their cloud storages governed by Service Level Agreements.

The other data like accounts and daily usages are being stored at the users local machines. It is the responsibility of the users to take necessary timely backups. However the office data generated from accounts are being backed up every day with a cumulative weekly and

monthly backups. These back up files are being kept at physically two different places. To restore during any catastrophe.

Manav Rachna strongly believes in antipiracy, therefore all software and applications are sourced from legitimate and vendors nominated by OEM. The renewal of licenses done regularly.

Physical security of the devices

Physical security of the computers and computing devices including network devices are being watched through enough number of CCTV cameras. All CCTV generated data is being stored for 30 days for any techno-legal requirements.

Budgetary Provisions

Adequate provisions of funds are kept in the Budget of the University to meet the expenses on IT Infra which includes Computers and software, cost of bandwidth etc.