Cyber Security Policy

MANGALORE UNIVERSITY

Category	Information and Communication Technology
Type of Document	**Policy**
Approved By	**Mangalore University**
Date on which the Policy Proposed	**08, November 2022**
Date on which the Policy Approved	**31, January 2023**
Compiled by	**Prof. H L Shashirekha** **The Director** **Computer Centre** **Mangalore University**
Drafted by	**Mr. Vijay G** **Mrs. Asha Hegde** **Computer Centre** **Mangalore University**

MANGALORE UNIVERSITY
POLICY MANUAL

Subject: **CYBER SECURITY POLICY**

1 DEFINITION

The use of the term "MU" is in reverence to the following organization: Mangalore University.

2 INTRODUCTION

This Cyber Security Policy is a formal set of rules to be abided by the people who are given access to MU information assets.

The Cyber Security Policy serves several purposes. The main purpose is to inform MU users: employees, students, research scholars and other authorized users of their obligatory requirements for protecting the technology and information assets of the MU. The Cyber Security Policy describes the information and technology assets that one must protect and identifies many of the threats to those assets.

The Cyber Security Policy also describes the users' responsibilities and privileges in terms of the acceptable use and the rules regarding Internet access. The policy describes the users' limitations and informs the users about the penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the information and technology assets of MU.

3 PROTECTION OF INFORMATION AND TECHNOLOGY ASSESTS

It is the obligation of all the users of MU information and technology assets to protect them from unauthorized access, theft and destruction. The information and technology assets of MU are made up of the following components:

- Computer Hardware, Web Portal, Application Servers, Email, Application Software, System software etc.
- System Software includes operating systems, database management systems, backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments within the MU that includes custom written software applications and commercial off-the-shelf software packages.
- Communications Network hardware and software including routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, leased lines, surveillance system, and associated network management software and tools.
- OFC and structured cabling.

3.1 Classification of Information

User information found in computer system files and databases shall be classified as either confidential or non-confidential and MU shall classify the information accordingly. The MU designee is required to review and approve the classification of the information and determine the appropriate level of security to protect it.

3.1 Classification of Computer Systems

Security Level	Description	Example
RED	This system contains confidential information – information that cannot be revealed to personnel outside MU. Even within the MU, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life threatening consequences and/or an adverse financial impact on the activities of the MU.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information. Data pertaining to Examination section and financial transactions.
GREEN	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	Department PCs used to access Server and application(s) and Management workstations used by systems and network administrators.
WHITE	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
BLACK	This system is externally accessible. It is isolated from RED or GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public Static Web server with non-sensitive information.

3.2 Local Area Network (LAN) Classifications

A LAN will be classified based on the systems directly connected to it. For example, if a LAN contains even one RED system, all network users will be subject to the same restrictions as RED systems users. Further, a LAN will assume the Security Classification of the highest level systems attached to it.

4 DEFINITIONS

Externally accessible to public: The system accessible outside MU via dial-up connection through Internet without providing a logon id or password. It is possible to "ping" the system from the Internet and the system may or may not be behind a firewall. A public Web Server is an example of this type of system.

Externally accessible to Non-Public: The system accessible via the Internet or the private Intranet with a valid logon id and password. These systems will have at least one level of firewall protection between its network and the Internet. A MU mail server and a private FTP server used to exchange files are examples of this type of systems.

Internally accessible: Users having a valid logon id and password can access the systems that have at least two levels of firewall protection between its network and the Internet. It may have a private Internet (non-translated) address and it does not respond to a "ping" from the Internet as it is not visible to Internet users. A wireless authentication server is an example of this type of system.

Chief Information Officer. The Director of the Computer Centre shall serve as the Chief Information Officer of MU.

Security Administrator. An employee of Computer Centre shall be designated as the Security Administrator of MU.

5 Threats to Security

5.1 Employees

One of the biggest security threats is by the users. They may cause damage to the systems either through incompetence or on purpose. The following security aspects have to be mitigated to compensate for such threats:

- Giving appropriate rights to systems and limiting the access to only office hours.
- Users are not allowed to share the login information to others to access the systems.
- Keeping detailed system logs of all the activities in a system.
- Securing the computer assets physically so that only the concerned staff can access the system.

5.2 Amateur Hackers and Vandals

These people are the most common type of attackers on the Internet and the probability of these attacks is extremely high. These amateur hackers keep scanning the Internet looking for well-known security holes to plant virus, Trojan horses, or to use the resources of the system for their own means. Web servers and electronic mail are the favorite targets of these attackers.

5.3 Criminal Hackers and Saboteurs

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

6 User Responsibilities

This section establishes usage policy for the computer systems, networks and information resources of the office. It pertains to all employees, students, research scholars and other officials who use the computer systems, networks, and information resources:

6.1 Acceptable Use

Users are responsible for protecting all information including their logon IDs and passwords used and/or stored in their accounts. Further, they are prohibited from making unauthorized copies of confidential information and/or distributing it to unauthorized persons outside MU.
Users shall not purposely engage in any of the activities with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to MU systems for which they do not have authorization.
Users shall not use unauthorized devices on their PCs or workstations, unless they have received specific authorization from the MU IT designee.
Users shall not download unauthorized software from the Internet onto their PCs or workstations. Users are required to report any weaknesses in the MU computer security, any incidents of misuse or violation of this policy to MU IT designee.
Unauthorized use of the system in violation of the law may constitute grounds for either civil or criminal prosecution.

6.2 Use of the Internet

MU will provide Internet access to its internal users that includes: employees, students, research scholars and other officials, who are connected to the internal network and has an academic/official need for this access. These internal users shall obtain the access to **MU information and systems in writing from the Director, Computer Centre, Mangalore University.**
The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for “chain letters” or any other purpose which is illegal or for personal gain.

6.3 User Classification

All users are expected to have the knowledge of the Cyber Security Policy and must conform to the Acceptable Use Policy defined in this document. and are required to report any violations to the Security Administrator. MU has established the following user groups and defined the access privileges and responsibilities accordingly:

User Category	Privileges & Responsibilities
Department Users (Employees)	Access to application and databases as required for job function. (RED and/or GREEN cleared)
System Administrators	Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only.
Security Administrator	Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
Systems Analyst/Programmer	Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices.
Service Providers/Consultants	Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function.
Other Agencies and Business/ IT Partners	Access allowed only when contract or inter-agency access agreement is in place or required by applicable laws.
Employees, students, research scholars and other officials	Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information.

6.4 Monitoring the Use of Computers

MU has the right and capability to monitor electronic information created and/or communicated by the persons using MU computer systems and networks, including e-mail messages and usage of the Internet. It is not the MU policy or intent to continuously monitor all computer usage by the employees or other users of the MU computer systems and network. However, users of the systems should be aware that the MU may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with MU policy.

7 Access Control

The fundamental objective of the Cyber Security Policy is to have controlled access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are given to individuals who are authorized to access specific resources. Access controls exist at various layers of the system, including the network and is implemented by logon ID and password. At the application and database level, other access control methods are implemented to restrict the access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

7.1 User System and Network Access – Normal User Identification

All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with any one. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Passwords must not be found in any English or foreign dictionary as they can be easily cracked using standard “hacker tools”.
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- User accounts will be frozen after 3 failed logon attempts.
- Logon IDs and passwords will be suspended after 90 days without use.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users will not be allowed to logon as a System Administrator.

Employee Logon IDs and passwords will be deactivated as soon as the employee is retired, terminated, fired, suspended, placed on leave, or otherwise leaves the employment of MU.

Supervisors / Managers shall immediately and directly contact the Director, Computer Centre to report change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must give a request to the Director, Computer Centre, Mangalore University, to get a new password assigned to their account.

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee’s password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

7.2 System Administrator Access

System Administrators, network administrators, and security administrators will have access to host systems, routers, hubs, and firewalls as applicable to fulfill the duties of their job.

All system administrator passwords will be DELETED immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the MU.

7.3 Special Access

Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the Computer Centre and require the permission of the user’s Director, Computer Centre. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to University. The reports will show who currently has a special access account, for what reason, and when it will expire. Special accounts will expire in 3 days and will not be automatically renewed without written permission.

7.4 Connecting to Third-Party Networks

This policy is established to ensure a secure method of connectivity provided between MU and all third-part companies and other entities required to electronically exchange information with MU.

"Third-party" refers to the vendors, consultants and business partners doing business with MU, and other partners who have a need to exchange information with MU. Third-party network connections are to be used only by the employees of the third-party only for the academic/official purposes of MU. The third-party MU will ensure that only authorized users will be allowed to access information on the MU network. The third-party will not allow Internet traffic or other private network traffic to flow into the network. A third-party network connection is defined as one of the following connectivity options:

- A network connection will terminate on a central network core switch and the third-party will be subject to standard MU authentication rules. This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

- All requests for third-party connections must be made by submitting a written request and be approved by MU.

7.5 Connecting Devices to the Network

Only authorized devices may be connected to the MU network(s). Authorized devices include PCs and workstations owned by MU that comply with the configuration guidelines of the MU. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: Non-MU computers that are not authorized, owned and/or controlled by MU. Users are specifically prohibited from attaching other external devices to the MU network.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD's.

7.6 Remote Access

Only authorized persons may remotely access the MU network. Remote access is provided to those employees and academic/business partners of the MU that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to MU network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

7.7 Unauthorized Remote Access

The attachment of switches/routers/hubs/networking devices to a user's PC or workstation that is connected to the MU LAN is not allowed without the written permission of the MU. Additionally, users may not install personal software designed to provide remote control of

the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

8 Penalty for Security Violation

The MU takes the issue of ICT security seriously. Those people who use the technology and information resources of MU must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, employees, students, research scholars and other officials of MU may be subject to discipline up to and including discharge. The specific discipline imposed will be determined on a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee, student, research scholar and other officials shall be administrated in accordance with any appropriate rules or policies and the MU Policy Manual.

If the accused person is not an employee of MU the matter shall be submitted to the (MU designee). The (MU designee) may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

9 Security Incident Handling Procedures

This section provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the MU network. Some examples of security incidents are:

- Illegal access of a MU computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to a MU computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a MU web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computer outside of the MU network. For example, the system administrator notices a connection to an unknown network and a strange process of accumulating a lot of server time.

Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their (MU designee) immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

10 Internet Access Policy (Wired)

This section provides the policy guidelines to distribute the Internet facilities over the MU campus.

- Separate VLAN to each department/office: The separate VLAN must be provided to each department/office in the MU campus. This will help in reducing the incidence of collisions in network traffic and decreases the number of network resources wasted by acting as LAN segments.
- Bandwidth allocation to each VLAN: Bandwidth allocation to each VLAN is provided based on the requirement and internet usage of each department/office. The allocation of bandwidth for each VLAN may be arrived at after considering the requirement of the department/office. On demand, extra bandwidth may be allotted to the existing VLAN and it will be restored after the accomplishment of that demand.
- Policy for Guest login and access: The network resource of MU is restricted to only authorized users. However, on special occasion the provision to use the network resources temporarily may be permitted. The access to the services in such situations must be defined clearly and documented. A detailed guideline should be in place to handle such situations.
- Policy to bypass firewall: All network communication will pass through a firewall system which is embedded with strong security policies. At times it is necessary to access information by bypassing this firewall. A formal written permission should be taken by the user before approving bypassing the firewall service. Such requests should be reviewed time to time to maintain the integrity of security policies.
- Monitoring and Reporting: All network services are continuously monitored and recorded in the network analyzer. Every network activity is reported frequently and analysis of such report should be carried out to prevent unauthorized, illegal, and unwanted access of the network resources.
- Access Control Policy to each VLAN: Every department/office should submit the following details to access network resources.

Sl.No.	Department/Office	Number of Computers available	Bandwidth allocation	Allow to access Social Media Site (Y/N)	If Yes, Time Schedule
1.					
2.					
3.					
4.					

11. Wireless Network Access Policy

This section provides the guidelines to access and control the wireless network.

- Maximum devices enabled for each person: Depending on the type of the user, wireless access can be provided to a maximum of two devices per registered user. Staff/officials of university are entitled to get access for two devices. Research scholars and students can register for only one device to access the wireless network. The registration of the user will get ceased automatically once association of the user is terminated with the university.
- Authentication levels: By design two levels of authentication are provided for wireless access. MAC address of the device and login credentials are used for this purpose.

- Access Control Policy: There is no bandwidth restriction to access the network resources, but social media resources, chatting services, and online shopping websites are blocked.
- Policy to Guest Login and access: The wireless network resource of MU is restricted to only authorized users. However, on special occasions the provision to use the wireless network resources may be permitted temporarily. The access to the services in such situations must be defined clearly and documented. A detailed guideline should be in place to handle such situations.
- Monitoring and Reporting: All wireless network services are continuously monitored and recorded in the network analyzer. Every wireless network activity is reported frequently and analysis of such report should be carried out to prevent unauthorized, illegal, and unwanted access of the network resources.

12. Policy regarding Surveillance System

Guidelines to access and control the surveillance system are provided in this section

- Authorized person/s who can access the System: Designated person by the university should look after the entire surveillance system. The responsibility covers the maintenance of the equipment, up gradation, and redesign of the system.
- Footage viewing/copy request policy: Footage viewing /copy services can be provided based on the request received. The formal approval may be obtained by the head of the institution by submitting predesigned form.
- Backup policy: As per the government guidelines, 30 days of video footage of the camera is stored in Network Video Recorder (NVR).
- Biometric usage and reporting policy: It is compulsory to record biometric staff attendance of the university. Monthly attendance report will be sent to the head of the institution for verification.

13. Email account policy

MU has hosted in-house email server for official communication. This section provides the guidelines to access email server.

- User account policy: Institutional email id is provided only to the staff and research scholars of the university. Email account will be created only for the registered users. No personal communication will be allowed through this email account. The email account of the user will get ceased automatically once association of the user is terminated with the university.
- Storage space restriction: Maximum of 2GB storage space for research scholars and 10GB storage space for staff members is allotted.
- Password management: A predefined password is allotted during the creation of email account. The user has to change the password during first login. It is encouraged to change the password of user account frequently.
- Spam/Virus handling: An in-built spam assassin and antivirus protection is enabled as security measure. Apart from this, a Firewall is deployed behind the Gateway to scan any threat and block those.

14. Software Policy

All the systems in the university comes with OEM software license and operating system. Only legal / licensed software is allowed for installation in user department/office. Illegal copy / unauthorized copy of software installation is prohibited and department head/office head held responsible for any miss-deed. It is advisable to use open source software wherever it is feasible/available. Installation of any new/customized software should be informed to the Chief Information Officer and get his/her consent in writing.