



muportal

Intranet Portal for MAHE



Home Leadership Institutes & Centres Administrators Messages IT services Feedback Downloads Contact Us

MAHE Website
 Manipal O365 Email/Portal
 IT Service Desk
 MSPM
 EPF Trust - Portal
 RMS Portal
 Grants Mgmt. Portal
 Student Information System(SIS)
 Purchase and Inventory
 Elearning
 Library portal
 UIS Reports
 MAHE Telephone Directory
 Khinfo Hospital Intranet
 Statistical Consultancy Service
 (Dept. of Data Science)
 Event Management System
 Staff Grievance
 WO Tracker

Overview of MAHE IT Policies


Manipal Academy of Higher Education (MAHE) has IT policies in place that govern the use and security of its IT / computing systems, networks, information and digital assets. All MAHE users who access MAHE's information assets and resources, including faculty, staff, students, and third parties working across all MAHE institutions, are expected to understand these policies and the consequences of violating them. Information security policies ensure that everyone's use of the institute's computing and information technology resources best supports its educational, research, and administrative needs and expectations.


All IT policies are owned by the Digital & IT department of MAHE, supporting policy approvals, implementation, maintenance, and updating. It does so with the help and support of various MAHE functional departments / institutions of MAHE. Any policy exceptions will be handled through MAHE's exception management procedure.

All users must comply and adhere to all applicable policies, and if they have any questions, they can contact the MAHE Information security at infosec.admin@manipal.edu.

Mission, Vision and Manipal
 Values
 Quality Policy and Environment,
 Energy Policy
 Integrated Management System
 Waste Management
 NAAC Self study report
 Fire Safety Basics
 EMS Documents-MIS
 Feedback on EMS & EnMS
 HR policies and forms
 MAHE IT Policies
 MAHE Research Policy
 Academic Council Circulars
 IBSC and RCGM documents
 International
 Partnerships/Agreements
 Gender Sensitization
 Resource Consumption Data

Social Media Posts

**Manipal A...**
Follow Page

**Manipal
Academy of
Higher
Education**
on Thursday

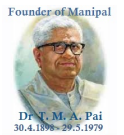
The Federation of Indian Chambers of Commerce and Industry (FICCI), in collaboration with Manipal Academy of Higher Education (MAHE), initiated the third batch of the Leadership Development Program (LDP) today. This exclusive three-day residential program is hosted at the MAHE

Developed and Maintained by Department of Digital & Information Technology, MAHE, Manipal
No of online users:3
muportalweb2



muportal

Intranet Portal for MAHE



Home Leadership Institutes & Centres Administrators Messages IT services Feedback Downloads Contact Us

MAHE Website

Manipal O365 Email/Portal

IT Service Desk

MSPM

EPF Trust - Portal

RMS Portal

Grants Mgmt. Portal

Student Information System(SIS)

Purchase and Inventory

Elearning

Library portal

UIS Reports

MAHE Telephone Directory

Khinfo Hospital Intranet

Statistical Consultancy Service

(Dept. of Data Science)

Event Management System

Staff Grievance

WO Tracker

Acceptable Usage Policy

Policy Statement

All the IT assets and services provided by MAHE are for carrying out institution related operations. Users must ensure that information resources are used safely and its usage does not disrupt operations and bring disrepute to the institution(s).

Acceptable usage applies to proper care and maintenance of assets and following the security requirement as laid down in this policy. Users must ensure that appropriate controls that are enforced by MAHE for preventing infections through malicious codes are followed diligently.

Access to removable media such as flash drives, storage cards etc., are provided to support educational and operational activities. Users are responsible for ensuring that removable media are used responsibly.

User account and passwords for systems or services must not be shared with anyone under any condition. All systems must be kept secure by installing the latest security patches.

Clear Desk and Clear Screen Policy

- Users must "log off" or "lock" their computers when their workspace is unattended;
- Users must "shut down" their computers at the end of the workday;
- All "Highly Restricted", and/or "Confidential" information in printed form/ hard copy must be removed from the desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday;
- File cabinets containing "Highly Restricted", and/ or "Confidential" information must be locked when not in use or when not attended;
- Keys used to access "Highly Restricted", and/ or "Confidential" information must not be left unattended;
- Laptops must be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday;
- All Users should ensure that unattended equipment is appropriately protected.
- Passwords must not be posted on or under a computer or in any other accessible location;
- Keep passwords confidential and refrain from sharing them with others
- Change passwords on a periodic basis or as per system settings or if there is an indication of a possible compromise of the systems or passwords. Passwords for privileged accounts such as system administrator shall be changed every 90 days, whereas normal user passwords shall also be changed every 90 days;

Mission, Vision and Manipal

Values

Quality Policy and Environment,

Energy Policy

Integrated Management System

Waste Management

NAAC Self study report

Fire Safety Basics

EMS Documents-MIS

Feedback on EMS & EnMS

HR policies and forms

MAHE IT Policies

MAHE Research Policy

Academic Council Circulars

IBSC and RCGM documents

International

Partnerships/Agreements

Gender Sensitization

Resource Consumption Data

Social Media Posts

BACK TO TOP

- Notify MAHE IT team in case any security breach is observed
- Documents containing confidential information must be immediately removed from printers, photocopiers or facsimile machines;
- Users must take adequate precaution to ensure that sensitive information is not displayed when sharing the screen or when the screen is visible to others. In addition, users must ensure that the screen is not visible to others when working in public areas or from home.

Guidelines for Workstation Usage

The guidelines are applicable to desktops, laptops, net books given by the institute to Users.


- Any changes in hardware or software must be done by the MAHE IT Team. The end user must request for changes to the MAHE IT Team through the Helpdesk.
- Users must terminate active sessions when they have finished their purpose of connectivity e.g. Logging out from the account after operations. Users must adopt formal log-off procedures instead of just switching off the PC screen or terminal. The importance of these good user practices must be spread through systematic awareness programs.
- Users must keep their equipment clean and free from dust.
- Users of laptop must prevent damages to the laptop due to inappropriate handling of laptop.
- During travel, care must be taken that laptops are not to be packed in checked in baggage. The user must ensure that the laptop is always under his supervision and never left unattended.
- Laptops that are not regularly connected to the network must be checked for any changes and to keep the OS, applications, anti-virus up to date.
- If user believes that some data has been modified or deleted from his system then it means that his system has been compromised. The end user must immediately inform the MAHE IT Team about the same.
- If any user finds that his desktop has changed and any files are missing in his system, he must immediately contact IT and report it as an incident.
- All workstations must have the latest patches applied to software and application as and when released from the vendors.


Printer Usage

- Printers are recommended to be used for printing documents for institutional requirements only.
- Users printing documents must ensure that they collect it personally from the printers and not designate others to collect it from the printers.
- Printed documents must not be left to accumulate in the machine. Stringent care must be taken to ensure that any document that was printed by mistake, or has an error is destroyed. It must not be used for any other purpose.
- Paper shredders must be used for shredding restricted and confidential documents.

Usage of Internet

Internet access is provided to Users to assist them in carrying out functions that are required as part of the operations. Non-institutional related activities must not be carried out over the internet. Occasionally, internet can be used for personal reasons. However, the usage must not


Manipal A...
[Follow Page](#)


Manipal Academy of Higher Education
 on Thursday

The Federation of Indian Chambers of Commerce and Industry (FICCI), in collaboration with Manipal Academy of Higher Education (MAHE), initiated the third batch of the Leadership Development Program (LDP) today. This exclusive three-day residential program is hosted at the MAHE

BACK TO TOP

interfere with work performance.

Users' access to internet must be through the internet service provided by MAHE.

Access to the Internet is restricted through a gateway proxy. Depending on the content of the website and the risks associated the institute has the right to filter and prohibit access to websites deemed inappropriate.

The MAHE IT team has the right to monitor the internet usage of the end users and collect logs which may represent the website visited etc., for the purpose of monitoring and not for any other activity.

Following guidelines must be followed by the users accessing internet.

- Users must not use the internet facility to carry out malicious activity such as hacking, eavesdropping, cracking, unauthorized scanning, Denial of Service (DOS), Distributed Denial of Service (DDOS) etc., against internal and/or external network or users connected to such networks.
- Users must not violate copyrights by downloading and distributing copyrighted material.
- Uploading institutional data to any internet site, file sharing site etc., is subject to/limited to official purpose.
- Usage of internet for carrying illegal activities such as gambling, accessing obscene material, identity theft etc is strictly prohibited and may lead to disciplinary action leading to termination and / or legal action.
- Users must not involve in executing any form of network monitoring which will intercept data not intended for the Users', unless this activity is a part of the Users' normal job/duty.
- Users must not involve in interfering with or denying service to any user other than the Users host (for example, denial of service attack).
- Opinion about the institution posted on any websites needs proper authorisation from the appropriate authorities.
- Users must not use the internet facility to download entertainment software, music, videos and games or play games over the internet. Apart from unnecessary wastage of bandwidth, these files may contain malicious codes.
- All devices connected to the Internet must be equipped with the latest version of anti-virus software. The MAHE IT Team must prohibit internet access to systems that do not meet any security requirements.
- All forms of data transmitted from the institute over the Internet must be checked for virus in advance. Any suspicious activity must be reported to the infosec.admin@manipal.edu for further action.
- Users must not download any virus creating tools or software nor must otherwise create malware codes. Users must not distribute or infect any internal systems or external network interfaces with any malware.
- If the users come across any abnormal situation while using the internet, they are requested to contact the infosec.admin@manipal.edu immediately and not take any action on their own.

Usage of E-mail

Users must use their institute e-mail account to communicate with external parties / MAHE team members and not through their personal e-mail accounts. Similarly, where possible e-mails must be sent to the receiver's official e-mail and not to their personal e-mail.

BACK TO TOP

Once a User resigns or if his/her services are terminated, it is important to revoke their e-mail account immediately after confirmation from HR, the responsibility lies with the MAHE IT team.

E-Mail access is available only for MAHE team members and outside party must not have access to the institutional e-mail account. Partner team/service providers have to take approval from MAHE IT team to get email access to work as per service agreement and should not be used for any other purpose. Users are responsible for the data that is originated, replied, forwarded from their account to others (third parties as well as to other users within the institution) as in line with the institutional data privacy policy.

Following guidelines must be followed by Users having access to MAHE's E-mail.

- Users sending any e-mail must ensure that the address in the 'to', 'cc' is the intended recipient.
- Users must not send any email containing any defamatory, offensive, racist or obscene remarks. E-Mail messages sent must not be used to harass or intimidate people.
- All e-mail sent by Users within the institution will be scanned for virus and malicious code. When sending e-mails using internet connectivity other than the institutional internet, it is the User responsibility to ensure that there is adequate protection and the e-mails or attachments does not contain any malicious code.
- Institutional e-mail account must not be used to send chain mails, for political reasons, personal amusement and entertainment.
- Institutional e-mail account must not be used as a medium to transmit any document, software, or any other information protected by copyright or any other law.
- Email accounts or devices logged into email accounts must not be shared and maintained securely.
- Users may report spam or objectionable messages to MAHE - IT as an incident.
- All e-mails sent must have a disclaimer. The disclaimer is approved by the Director – Digital & IT/Registrar, MAHE and the sender must not modify the content of the disclaimer.

Use of mobile devices

- Users must not allow others/ family to use MAHE devices
- Users must not access MAHE network with unauthorized devices
- Users must log out of all MAHE n/w and apps if non-official devices are used for access
- Users must ensure anti-virus or equivalent software is updated in mobile devices used to access MAHE network.

Physical document protection

- Users must sign off – asset movement in register or equivalent
- Highly restricted and/ or confidential documents should not be moved/shared out of MAHE premises or systems without appropriate approval/ exemption.
- Internal physical documents can only be taken out temporarily and should be returned with the allotted time.

BACK TO TOP

Office 365

- MAHE users should use O365 tools and its respective apps only for official purpose
- Users are responsible for the documents while using one-drive, SharePoint and information should be disclosed only on a need-to-know basis
- Users must not send any messages containing any defamatory, offensive, racist or obscene remarks. Messages must not be used to harass or intimidate people.
- Usage of Microsoft teams should be internal by the MAHE team members and for official purpose only.
- Please go through "MAHE Information Classification and Handling Policy" for data classification before using O365 tools and its respective apps
- Access to teams folder with any non-public classification must be restricted on a need to know basis. The folder owner shall be responsible for controlling and monitoring access to the information.

Developed and Maintained by Department of Digital & Information Technology, MAHE, Manipal
No of online users:3
muportalweb2

BACK TO TOP

MAHE Website

Manipal O365 Email/Portal

IT Service Desk

MSPM

EPF Trust - Portal

RMS Portal

Grants Mgmt. Portal

Student Information System(SIS)

Purchase and Inventory

Elearning

Library portal

UIS Reports

MAHE Telephone Directory

Khinfo Hospital Intranet

Statistical Consultancy Service

(Dept. of Data Science)

Event Management System

Staff Grievance

WO Tracker

Information Security Policy

Security of information assets of MAHE is of paramount importance. We are committed to maintaining the confidentiality, integrity and availability of these assets at all times through controls commensurate with the nature of information assets and its value.

The MISP provides management directive for information security and recommends appropriate security controls that need to be implemented to maintain and manage the information security in MAHE by:

- Establishing and maintaining an Information Security Program consisting of an Information Security Policy document, supporting Procedures and a Risk Management Framework;
- Ensuring that the designed policies and related procedures align themselves to the Risk Management Framework;
- Ensuring that Risk Assessment is performed on a periodic basis to identify & minimize the impact of the risks, posed by various threats and vulnerabilities, to an acceptable level across the universities associated with MAHE;
- Deploying appropriate technology, resources and infrastructure at MAHE for reasonable, practical and affordable level of protection required for MAHE's information and information technology;
- Establishing a documentation framework that details all the information and information assets to support effective implementation of this policy;
- Educating Users on MISP, its supporting normative standards, and guidelines;
- Ensuring that Users handle, distribute and dispose information as mandated in the Information Classification and Handling Policy;
- Identifying, classifying and protecting the confidentiality, integrity and availability of the information during all stages of the information life cycle;
- Ensuring that access to information and information technology assets are controlled, monitored, and authorized based upon the user's identified job function, 'need-to-know' and 'need-to-perform' criteria;
- Improving the effectiveness of the Information Security program by performing constant monitoring, review, exception-reporting and taking appropriate corrective & preventive actions;
- Ensuring that compliance violations are documented, reported and investigated by authorized personnel or team at MAHE;
- Creating and maintaining a security conscious culture across MAHE and its associated universities;
- Ensuring conformance to all information security requirements specified by University/ internal functional owners in adherence to regulatory requirements; and
- Ensuring that information security management system requirements are integrated into academic processes. Ensuring that the information security policies must be reviewed and revised annually based on academic and (or) technological requirements. The revised and approved

Mission, Vision and Manipal

Values

Quality Policy and Environment,

Energy Policy

Integrated Management System

Waste Management

NAAC Self study report

Fire Safety Basics

EMS Documents-MIS

Feedback on EMS & EnMS

HR policies and forms

MAHE IT Policies

MAHE Research Policy

Academic Council Circulars

IBSC and RCGM documents

International

Partnerships/Agreements

Gender Sensitization

Resource Consumption Data

Social Media Posts

documents must be published on the internal/ intranet portal.

Review and Evaluation

The MISP document must be reviewed at the time of any major change(s) in the existing environment affecting policies and procedures or once every year, whichever is earlier. The MISP document must be reviewed by the Assistant/Deputy Director, IT and approved by the Information Security Steering Committee (hereafter referred to as 'ISSC'). The reviews must be carried out for assessing the following:


- Impact on the risk profile due to, but not limited to, the changes in information assets, deployed technology/ architecture, regulatory and/ or legal requirements; and
- The effectiveness of the policies.


As a result of the reviews, additional policies could be issued and/ or existing policies could be updated, as required. These additions and modifications would be incorporated into the MISP document. Policies that are identified to be redundant must be withdrawn.

Developed and Maintained by Department of Digital & Information Technology, MAHE, Manipal

No of online users:4

muportalweb2

**Manipal A...**
Follow Page

**Manipal Academy of Higher Education**
on Thursday

The Federation of Indian Chambers of Commerce and Industry (FICCI), in collaboration with Manipal Academy of Higher Education (MAHE), initiated the third batch of the Leadership Development Program (LDP) today. This exclusive three-day residential program is hosted at the MAHE

MAHE Website

Manipal O365 Email/Portal

IT Service Desk

MSPM

EPF Trust - Portal

RMS Portal

Grants Mgmt. Portal

Student Information System(SIS)

Purchase and Inventory

Elearning

Library portal

UIS Reports

MAHE Telephone Directory

Khinfo Hospital Intranet

Statistical Consultancy Service

(Dept. of Data Science)

Event Management System

Staff Grievance

WO Tracker

Communications Security Policy

Appropriate security controls to ensure the protection of information in networks and its supporting information processing facilities to ensure confidentiality, integrity and availability of information residing on MAHE information systems.

General Guidelines

- External connections to MAHE networks, i.e., connections between a MAHE network and a non-MAHE network shall be protected by a firewall;
- Necessary network and security components shall be implemented, managed, and maintained in a secure manner;
- All network and security components shall be configured to provide audit logs for necessary and continual security monitoring;
- Confidentiality and integrity during transmission of critical data shall be ensured using appropriate encryption as required (refer to Cryptography Policy);
- Access to the network components and security devices shall require strict access control and authentication as per the Access Control Policy;
- Remote management of critical servers and network components shall only be done through proper encrypted channels; RDP as an option will be enabled as necessary with proper approval.
- All internet connection shall be passed through a content filtering solution to block undesirable web sites;
- Appropriate network redundancy shall be built in the environment as per business requirements;
- Network components and the cabling of MAHE network shall be protected;
- Detailed network architecture diagram shall be maintained up to date by the Assistant/Deputy Director, IT/the designated assignee; and access to authorised users will be given on a need-to-know basis.
- Required documentation in support of all activities, related to network and security components, shall be created and maintained.

Remote Access Policy

- The Assistant/Deputy Director, IT/the designated assignee shall be responsible for the management and administration of remote access services; (access over SSL VPN)
- All MAHE users with remote access privileges to MAHE information assets are responsible to ensure that their remote access connection shall have the same controls as their on-site connection;
- Remote access security shall be controlled and enforced using strong password as per MAHE 'Password Management' section within the Access Control Policy;

Mission, Vision and Manipal

Values

Quality Policy and Environment,

Energy Policy

Integrated Management System

Waste Management

NAAC Self study report

Fire Safety Basics

EMS Documents-MIS

Feedback on EMS & EnMS

HR policies and forms

MAHE IT Policies

MAHE Research Policy

Academic Council Circulars

IBSC and RCGM documents

International

Partnerships/Agreements

Gender Sensitization

Resource Consumption Data

Social Media Posts


- MAHE will incorporate different methods/types of access to its network assets from remote hosts, such as Teams & other collaboration services, Remote Access Tools etc.;
- TELNET service shall not be used to access MAHE's information assets;
- All sensitive data sent through Remote Access shall be over an encrypted tunnel;
- MAHE user with remote access privileges must ensure that their MAHE owned or personal computer or workstation, which is remotely connected to MAHE University network, is not connected to any other network at the same time;
- Devices that connect to the MAHE network must have its personal firewall enabled, operating system patches updated and should have active and updated Anti-virus software installed. Non-compliance device/system will be quarantined by the IT Department, without notice;
- For Non-MAHE users, access to production system will not be permitted;
- Access to production system for Non-MAHE users may be permitted against written approvals from the respective HOI/HOD/Functional Head and Director IT & Digital;
- Components providing remote services must be configured to terminate inactive connections based on timeout. For details, please refer to the Network Security Guideline; and
- The Assistant/Deputy Director, IT must ensure that the reconciliation of remote access rights to MAHE network is conducted once in every six months with the business owners' approved authorization list, and any discrepancies identified are communicated to the respective functions for further appropriate action.


Wireless Guideline

- Necessary controls shall be established to protect the confidentiality, integrity, availability and authenticity of data passing over wireless networks;
- All wireless Access Points/Base Stations connected to the University network must be registered, and approved by Assistant/Deputy Director, IT;
- These Access Points/Base Stations shall be subject to periodic penetration tests and audits;
- Necessary assessment shall be performed to assess the threats and risks involved with wireless communication on a periodic basis; and
- Wireless network shall be segregated from other networks based on necessary risk assessment.

Firewall Policy

- Firewalls shall deny all Inbound & Outbound traffic that do not support MAHE's business objectives;
- Current Firewall Access rule set shall be maintained by MAHE IT Team;
- Firewall configuration shall be audited and verified half yearly;
- Strict physical access controls shall be in place to secure the firewall;
- Logical access to the firewall shall be controlled and authorized by Assistant/Deputy Director, IT;
- Necessary controls shall be implemented through configuration hardening of the Firewall;
- Necessary failover or redundancy mechanism as applicable shall be in place as per business needs and criticality;
- Firewall logs shall be stored and maintained as per the log retention matrix defined by MAHE (for a month) or based on internal customer requirements;


Manipal A...
[Follow Page](#)


Manipal Academy of Higher Education
on Thursday

The Federation of Indian Chambers of Commerce and Industry (FICCI), in collaboration with Manipal Academy of Higher Education (MAHE), initiated the third batch of the Leadership Development Program (LDP) today. This exclusive three-day residential program is hosted at the MAHE

- Firewall logs shall be analysed on a regular basis and any discrepancies will be logged and acted upon;
- Firewall configuration shall be backed up as per the 'Backup' Section (daily backup) in Operations Security Policy;
- Changes to firewall configuration shall be streamlined and authorized as per the Change Management process; and
- Firewall Management responsibilities shall be listed and assigned.

Network Security

- Network security controls shall be documented and implemented at MAHE for logical segregation of MAHE networks and for the protection of critical networks, information systems, and applications from unauthorized access, modifications, or destruction by internal or external users;
- The wireless infrastructure of MAHE shall be logically separate from the wired LAN and further secured with adequate levels of strong user authentication, encryption levels, detection of rogue access points and appropriate physical security controls;
- All critical applications shall be protected by a firewall from both external users and internal users of MAHE;
- The firewall shall be configured and managed to permit access to University data from authorized users only and for authorized network services only;
- Intrusion prevention systems shall be deployed, as appropriate, to detect / prevent any intrusions and any unauthorized or malicious activities; and
- Network Architecture documentation shall be maintained and access to it shall be restricted.

Instant and Social Messaging

- MAHE reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the IM system(s) for any purpose;
- The contents of IM messages may be disclosed within MAHE to and among authorized personnel without permission of the affected IM user, if reasonable suspicion exists of activities that may violate this or any other MAHE Policy;
- Social Media platforms and/ or Messaging platforms such as but not limited to Facebook, Twitter, Whatsapp, WeChat, SnapChat, Hike etc. shall not be used by the MAHE faculty members, students and third-parties for any official/ professional communication; Users need to use official social media channels and handles only.
- Any communication on social media platforms shall be carried out by a function or employee only post authorization from HIO/HOD/Functional Head, Registrar, MAHE and Director IT & Digital;
- MAHE shall consider proactively scanning for and blocking or flagging any transmissions, via the MAHE network, that contain phrases of profanity or violence, confidential information, or other sensitive data that may expose the organization to operational, legal, reputation, or physical risks.

Clock Synchronization

All clocks of MAHE, including servers, desktops, laptops, etc. shall be synchronized with a Network Time Protocol (NTP) server or equivalent.

Developed and Maintained by Department of Digital & Information Technology, MAHE, Manipal
No of online users:4
muportalweb2