INFORMATION SECURITY POLICY

Madanapalle Institute of Technology & Science

(UGC- AUTONOMOUS)

Mr. G. R. Hemanth Kumar, SAO (Systems)

PRINCIPAL

1. PURPOSE

The Purpose of this policy is to define the Acceptable Usage of Internet, Intranet including Emails, Systems, Storage Media, Operating Systems, and Application Software etc in MITS.

2. SCOPE

This policy applies to employees, business visitors, vendors and consultants working at MITS , including all personnel affiliated with third parties in relation to maintenance of IT equipment, application software's that are owned or leased by MITS . The users shall understand and agree to this policy by signing the policy at the time of joining or during the start of the engagement to ensure they bind to the same.

3. GLOSSARY

ISF Head	Information Security Forum Head
DISO	Department Information Security Officer
ISF	Information Security Forum

4. POLICY STATEMENT

Acceptable use of MITS Facilities includes:

- Conducting MITS business.
- Sending and receiving work-related e-mail during normal business hours.
- Collaborating with work-related professional contacts.
- Participating in discussion groups on subjects of professional interest.
- Enhancing the knowledge

With the exception of the above-mentioned purposes, any other use of MITS Facilities is unacceptable. For the sake of clarity, some examples of the unacceptable usage of MITS Facilities are defined in **Appendix A** of this policy.

List of assets at function level are maintained in RARTP

4.1 Email Usage Policy

- Each employee is responsible for the contents of his / her e-mail. All e-mails must be identified with a user's name or e-mail id to allow for individual tracking.
- Employees shall be responsible to keep their email passwords secure and strictly confidential to avoid misuse of the login ids. These passwords shall be changed as per the MITS Password Policy
- Employees shall be aware that Electronic mail is vulnerable to unauthorized access through the Internet and modification by third parties.
- All employees shall use the assigned MITS / MITS client e-mail address for official communication. On no account, shall the employees use their personal third party e-mail addresses as their contact address for conducting company business.
- Individuals accessing the e-mail services of MITS must not use or access an e-mail account assigned to another individual to either send or receive messages.
- When sending e-mails with attachments, all attachments must be compressed if the size exceeds 5 MB to the external domains, and 20 MB in case of internal circulation within same domain
- Employees must treat e-mail messages and files as confidential information. E-mail must be handled as a confidential and direct communication between a sender and a recipient.
- In case a backup of Individual's PST folder (mails) is required, then an approval shall be obtained from the respective reporting Manager of the Individual.
- In the legitimate business interest of the company, any communication sent or received via electronic mail, may be monitored or reviewed by persons authorized by the Company, at any time with or without notice to employees.
- The MITS email system shall not be used for the creation or distribution of any disruptive or offensive messages, including but not limited to offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any MITS employee should report the matter to their reporting manager immediately.

Specific non-business e-mails should be avoided as below. Misuse of the same may lead to disciplinary actions.

- Chain letters
- Joke emails
- Pornography of any type
- Solicitation to sell personal property

- Users must not employ a scanned version of a hand-rendered signature to give the impression that an e-mail message or other electronic communications were signed by the sender as another person could misuse the signature. Hence it is prohibited.
- Users should not use their official email ID to subscribe to non-technical, non-business newsgroups that generates heavy amount of mail traffic. However the subscription shall be allowed on specific request and approval from ISF head.
- E-Mail attachment shall be scanned before downloading for viewing.

4.2 Internet Usage Policy

- Only employees who have legitimate business requirements shall be allowed to access Internet
- Internet access exceptions shall be based on a specific request from the employee and shall be routed through the Department Head who shall authorize the same.
- Internet shall be accessed through MITS approved sources only. Usage of Individual Dial up or Cable Modem shall not be allowed.
- Employees who have the access to Internet shall not share the same with those who are not allowed with that privilege.
- All kinds of Internet Chat sites such as Skype, GTalk, AOL, Yahoo, and MSN etc. can be accessed only with Program Manager's/Department Head/Network Admin specific business case approvals.
- The access to Internet shall always be used for Business requirements only. Personal Hosting of Web Pages, Establishing Personal Business links is construed to be deviations of this policy.
- All information downloaded through Internet shall always be screened through the Official Anti Virus Scanner before being used.

- The employees shall not indulge in unlawful activities such as accessing unauthorized resources, hacking, introducing any computer virus, committing acts which may disrupt use of the resources aiding or abetting any of the above.
- Users using MITS resources, on discovering that they have been connected with a web site which contains potentially offensive material must immediately disconnect from such a site.
- Users should be aware that MITS accepts no liability for their exposure to offensive material that they may access via the Internet.
- The ability to connect with a specific web site does not in itself imply that users of MITS are permitted to visit that site.
- The Company has the right to monitor and log any and all aspects of Internet usage including, but not limited to monitoring Internet sites visited by users, Chat and newsgroups, file downloads, and all communications sent and received by users.

4.3 Systems Usage Policy

- Only legally valid and business related Applications Software to be installed.
- Based on the level of the end user & specific business cases, USB ports shall be enabled.
- Users shall make sure that their desktops are installed with Anti-Malware software with real time scan enabled

4.4 Associated Document

ISMS Manual

4.5 Roles and Responsibilities

Roles	Responsibilities
Department Head / DISOs/ISF member	Responsible for executing and implementing the policy
ISF Head and MR	Monitoring the Implementation of the policy

4.6 Maintenance and Update Trigger

MITS PMO department shall be responsible for document control, any changes; updates shall be discussed in the ISF under the guidance of ISF Heads. MR shall forward the recommendations of ISF to the MF for approval.

Any change in the organizational strategy, business model, technology, organizational policies/process or any major event impacting the organization can trigger an update for this document.

MR shall forward the recommendations to the MF for approval.

APPENDIX A

Examples of the unacceptable usage of MITS Facilities

Internal rules

- Interferes with the own productivity or work performance or that of another employee.
- Adversely impacts the smooth operation of the computer system (s) and MITS network.
- Violates any provision of this policy, any additional policy adopted by MITS , or any other policy, regulation, law or guideline set forth by provincial or federal Laws of other countries where MITS conducts business.
- Uses MITS facilities for private or personal gain.
- Standard configuration of software/hardware on MITS computers provided to MITS employees, contract employees and business partners without the authorization of the IT department.

Criminal and civil offence

- Child pornography, copyright violation, defamation, computer hacking and other crimes related to computer security, harassment, hate propaganda, lewd remarks, etc.
- Provision or transmission of material that violates laws pertaining to sexual harassment or hostile work environments in the user's local jurisdiction.

Sensitive information

- Disclosing sensitive information pertaining to the government or trade secrets after leaving MITS .
- Disclosing sensitive information pertaining to personal privacy that MITS has received, processed and/or stored, in a manner which violates the provisions of the country, province, or state where MITS employees, contract employees and business partners work after leaving MITS .
- Providing information or lists pertaining to MITS employees, contract employees, business partners and clients to third parties outside of MITS , unless such an action is part of the employee's responsibilities after leaving MITS .

Copyright and trade law

- Copying copyrighted material including, but not limited to, the digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which MITS does not have an active and legally valid license.
- Exporting software, technical information, and encryption technologies which violate laws.

Malicious act

- Causing security breaches to the network or system. Security breaches include, but are not limited to, the unauthorized access to data by MITS employees, contract employee, or business partner, or the unauthorized access to a server or a system by a MITS employees , contract employee or business partner unless they are within the scope of regular duties.
- Causing congestion and disruptions of the network or system. Congestion or disruption includes, but are not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Introducing malicious programs in the network or computer (e.g. viruses, worms, Trojans, e-mails, bombs, etc.).
- Sending spam or junk mail (e.g. chain letters, pyramid systems, gambling activities, etc.).
- Executing port scanning or security scanning on a computer when these actions are not within the scope of regular duties.
- Conducting any form of network monitoring outside the scope of regular duties.
- Circumventing user authorization or the security of any host, network or account.
- Interfering with or denying service to any user (e.g. saturation attack).
- Using any program, script, or command, or sending messages of any kind, with the intent to interfere with or disable a user's session through any means, locally or via the Internet, intranet or extranet.
- Revealing account password (s) to third parties or allowing unauthorized third parties to use personal accounts (this includes family members when a user works at home).

APPENDIX B

Media Destruction Guidelines

Considerable information is obtained from computing equipment and media, which have either failed or outlived the purpose for which they were acquired. In general, there is no known method short of total destruction, which will completely remove all traces of the information borne by memory devices (including volatile storage such as Random Access Memory (RAM)) or magnetic media.

However, some sanitization measures can significantly reduce the risk of information being recovered from used media.

Proper procedural measures has to be incorporated when old physical assets, which are having confidential data, are being discarded or destroyed as e-waste through third party vendors. Control measures have to be taken to make sure that such third parties are authorized legally and statutorily to perform such activities.

Different Methods

Sanitization

Sanitization is the process of erasing as far as is possible the information from the media or equipment. The process of sanitization does not automatically change the classification of the media or equipment. Note that sanitization does not involve destroying the media or equipment. Low level formatting of hard disk is proved to be one way of sanitization for data erasure.

Declassification

Declassification is the removal or reduction in the classification of the media or equipment. The decision to declassify should be preceded by an assessment of the risk of improper disclosure of any information remaining on the media or equipment, should the declassification take place. In considering risk associated with declassification, it is important to take into account the resale value of the asset(s), the destination of any released media (and therefore the likelihood of compromise), the serviceability of the media which may directly relate to the resale value, and any contractual obligations.

Degaussing

Degaussing or demagnetizing is a procedure that reduces the magnetic flux density to zero by applying a reverse magnetizing field. Degaussing renders any previously stored data on magnetic media unreadable. Degaussing is the most reliable method of purging magnetic media short of destruction.

Magnetic Media Overwrite

The standard method used to declassify by overwriting is to write over every addressable location with one pattern (usually binary 'ones') and then with the complementary pattern (E.g. binary 'zeros'). This cycle of overwriting is then repeated a number of times, where the number is based on the requirements for declassification and/or the risk assessment. Note that any binary pattern can be used, as long as the opposite or complementary pattern is written alternately, for the given number of

cycles. In order to ensure that the media overwrite procedures are correctly undertaken, the following steps are recommended:

- Overwrite all the data bit locations with a pattern such as binary zeros, and verify that it has occurred.
- Overwrite all the data bit locations with binary ones (or the complement of whatever pattern was used in the previous step), and verify that it has occurred. Verification of the overwriting may be accomplished by reading all or a sample of the information (proportion based on a risk assessment), and ensuring that no other characters can be detected.
- Repeat the above steps a number of times, based on the requirements for declassification and/or the risk assessment.

Volatile Media

Memory devices and other volatile storage retain some information even after the power has been lost, although at such a low level that sophisticated methods are needed to recover it. A very highly classified, volatile memory may be sanitized sufficiently by the removal of all power (including all battery power). A decision on whether to release the item to outsiders or destroy it must be based on a risk assessment taking into account the quantity and classification of the data the device bears.

Physical Security and Destruction Methods

Paper, Microfilm, CDs and related storage media cannot be sanitized and must be destroyed in an approved disintegrator or by burning/smelting under the direct supervision / control of a suitably cleared person. Destruction of hard disk, floppy disk and volatile memory should occur by melt, smelt, grind, or smash.

Grades of Sanitization

The following grades of sanitization have been included to assist in determining the level of effort that should be allocated to such a task. These are not exhaustive / definite but only guidelines. There are three categories of media included in the following grades, which are generally the most common. These are "magnetic media", "laser printer/copier drums" and "volatile memory". Volatile memory includes solid-state memory that loses data when power is removed (e.g. RAM), but does not include devices that do not lose data (e.g. EPROM).

Grade 0

- Magnetic media not sanitized.
- Laser printer/copier drums not sanitized.
- Volatile memory devices not sanitized.

Grade 1

- Magnetic media sanitized via an EPL approved degausser or single overwrite method.
- Laser printer/copier drums not sanitized.
- Volatile memory devices not sanitized.

Grade 2

Magnetic media sanitized via an EPL (EVALUATED PRODUCTS LIST) approved degausser configured as per DSD recommendations; or double or triple overwrite method, subject to the outcomes of a risk assessment. The risk assessment should take into account the cost (or resale value) of the media, the amount of classified information stored on the media and the serviceability of the media. A declassification decision following sanitization should be no more than two levels of classification below the original classification of the media.

- Laser printer/copier drums sanitized via approved method.
- Volatile memory devices sanitized via approved method.

Grade 3

- All magnetic media destroyed
- Laser printer/copier drums sanitized via approved method.
- Volatile memory devices sanitized via approved method, subject to the outcomes of a risk assessment. The risk assessment should take into account the cost (or resale value) of the media, the amount of classified information stored on the media and the serviceability of the media.

Grade 4

- All magnetic media destroyed.
- All laser printer/copier drums destroyed.
- All volatile memory devices destroyed.

1 PURPOSE

The purpose of the procedure is to protect sensitive and confidential business information data of MITS from disaster, damage, theft, and system failure.

2 SCOPE

This Policy & Procedure applies to all employees of MITS, Vendors, Consultants, Employees of Third Parties affiliated with MITS.

Further these procedures apply to the following information resources.

- All data residing in Critical Servers including the Operating System files and application
  software files
- All business critical data managed and handled by various departments and MITS managed projects
- Configurations and Operating system files (IOS) of all network devices, Security products, communication equipments
- Error Log files generated from all critical servers, devices and communication equipments etc
- Software, Utilities / Scripts, Manuals - developed in house, provided by external vendors etc.

3 GLOSSARY

ISF	Information Security Forum
ISF-Head	Information Security Forum - Head

4 POLICY STATEMENT

- To evolve appropriate procedures for backing up information required for business functions on a predefined and regular basis.
- Review the backup and retrieval logs by the respective System Administrator to ensure proper backup.
- Have proper documented procedures in place.

4.1 Information to be backed up

MITS IT TEAM will back up all the business critical information as per agreed upon RPO, which could include:

- Operating System's software and files
- Configurations of Network & Security Devices
- Log Files
- Departmental folders are provided for copying the critical data of respective departments. Full backup is done for these folders once in a week on Friday.

4.2 Backup and Retention Scheme

4.2.1 File Services

- Backup retention scheme is applicable for business critical data
- The backup of business critical data is retained for a period of at least week.
- The weekly full backup is performed on every week.

4.2.2 Mail Services

- Google apps used for Mail services for all Employees.

4.3 Phasing out old media

All back up media must be phased out after the recommended number of cycles.

If a media has outlived its recommended shelf life or the number of backup cycles has exceeded the recommended number or has defects then the media shall be taken out of the process. IT team will maintain a tracker based on which shelf life will be tracked.

This shall be recorded in a register Media Removal Register

4.4 Storage of Media

All media whether used in backup process or new shall be kept safely under restricted access.

All media either used or new shall always be stored in the following environmental conditions.

Temperature - 15° to 45° Centigrade

Humidity - 30% to 60% Relative Humidity

Backup media will be transported to an offsite location using tamper proof container/cover so that it is not mishandled during the transit. Same will be maintained inside a Fire Proof/Resistant Cabinet, the details will be recorded in the Media Movement Register.

All media shall be labeled as per the Information classification policy.

4.5 Backup Restoration

Files that are accidentally damaged or deleted can normally be restored from backup tapes within three to seven working days depending on type, size, aging of data and priority. Files can only be restored to the state they were in at the time of the most recent backup. Files older than 30 days shall not be available for restoration.

Test Restoration shall be done quarterly by IT TEAM and other recovery restoration as per routine requests received from data owners.

Depending upon the retention period and the availability of media at Onsite or Offsite, of the concerned backup, the backup shall be restored subject to the following:

- Whether the person requesting the backup is authorized?
- Whether he/she is required to access the data – Need to know basis?
- Whether there is approval from function head/program manager for restoring the required information?

All restoration shall be done to a different location.

Backup logs shall be reviewed by the respective System Administrator to ensure proper backup.

4.6 ASSOCIATED DOCUMENTS/ RECORDS

- Backup Policy
- Backup Restoration Register
- Media Removal Register
- Media Movement Register
- Backup Restore Request
- Information Handling and Classification Policy and Procedure.

4.7 ROLES AND RESPONSIBILITIES

Roles	Responsibilities
Manager – IT	Responsible for executing and implementing the procedures across MITS
ISF-Head	Monitoring the Implementation of the procedures across the organization
ISF	Assist in Monitoring the Implementation of the procedures across the organization

4.8 MAINTENANCE AND UPDATE TRIGGER

MITS PMO department shall be responsible for document control, any changes; updates shall be discussed in the ISF under the guidance of ISF Heads. MR shall forward the recommendations of ISF to the MF for approval.

Any change in the organizational strategy, business model, technology, organizational policies/process or any major event impacting the organization can trigger an update for this document.

MR shall forward the recommendations to the MF for approval.

IT SERVICE DESK ACCEPTABLE USE POLICY

1. Policy Statement

To bring standards in IT SERVICE DESK. This standardization is essential to IT Department in analyzing call for corrective actions and improving quality of service by stopping reoccurrence of problem, enhancing Uptime, Availability and business continuity.

2. Scope

This guideline applies to all employees, contractors, Vendors, Employees of Third Parties and Consultants having business relationships with MITS.

3. Definition

The IT Service Desk serves as the primary point of contact for MITS staff to get assistance for Infrastructure & Support related questions or problems. The following policy definition will standardize support process, brings in transparency, and enhances high availability, timely support and continuous service improvement.

4. Guidelines for Users (DO's)

- IT Service Desk has been setup to act as one point contact for IT Infra Support & Service.
- IT Service Desk has been setup through service desk tool Spice works
- Service Request can be initiated in 3 ways :-

WEB REQUEST	http://helpdesk:333/portal will take you to the online request form. You can use your credentials to login to raise and view tickets. **The most preferred mode.**
WALK IN	During Service Desk operating hours 9:30AM to 11.00 PM IST
PHONE CALL	Calls to Service Desk @ 167 during operating hours 9:30AM to 11.00 PM IST
E-Mail	To the support email ID nssg@MITStech.com

- **Users shall cooperate and mandatorily practice online request form http://helpdesk:333/portal before reaching out IT for any kind of support.**
- User shall follow Walk IN / Phone Call/ Instant Messing mode only during emergency.
- Call will be attended in the priority order of **SEVERITY1** to **SEVERITY4.** Please refer Annexure-1 for details.
- User shall escalate the call to 133, if calls are not attended within stipulated resolution time. Appendix-II attached for Escalation matrix details.
- Service Desk Tool is programmed for Auto email replies such that users receive an email when the ticket is raised and closed.
- User shall be clear in explaining the problem and error screen shots where ever possible to help IT support to quickly debug and resolve the problem.

5. Guidelines for Users (DONT's)

- Don't use office communicator or other Instant Messenger to raise a Service Request.

- Follow process of raising Service Request first. Don't walk in or phone Call unless there is an Emergency or show stopper.
- Don't send support emails directly to IT support staff. Instead, mark an email to the reporting authority looping the IT support team (**nssg@MITStech.com**).
- Use IP messenger only for support related communication and not for any general communication.
- Use only online request form **http://helpdesk:333/portal** for raising fresh Service Request. Don't duplicate or resend the support mail if ticket is already raised.

6. Guidelines for IT Department (DO's)

- IT Department Shall be focused to achieve 100% call loggings & timely Resolutions.
- IT department shall review the Call & Resolution database for taking corrective action towards stopping reoccurrence of the issue; enhance Uptime Availability & Business Continuity.
- IT department shall not attend any support call without the service ticket being raised.
- IT Engineer shall attend the call based on order of default SEVERITY set for the call.
- IT engineer shall take due care in rightly updating the Service Desk for call classification, prioritization.
- IT Manager shall analyze calls on weekly/Monthly basis for corrective actions

7. ANNEXURE – I

PRIORITY MATRIX				
PRIORITY	**CRITERIA**	**RESPONSE TIME**	**RESOLUTION TIME**	**EXAMPLES**
SEVERITY1	Mission Critical, Emergency, Widespread Impact, Power user issues	<=15 minutes	<= 1 Hours (if no external dependency)	• Network Down • Server Down • Virus Attack • Power Issue • Equipment Failure during Critical Meeting
SEVERITY2	System Down, Cannot carry on work responsibilities	<=30 Minutes	<=4 Hours If no external dependency)	• Network Issues • Email Issues • System Crash
SEVERITY3	System or component is down or degraded, but requestor can carry out normal work responsibilities and/or a temporary alternative is available	<=2 Hour	<= 1 Business Days	• Application errors • Computer slow • Minor equipment failure (sound card, local printer, etc.) • Permission changes • Network printer down
SEVERITY4	Enhancement, planned change, general application questions	<=1 Business Days	<=2 Business Days	• New software installation • Office move • Provide new phone/network connection • Routine purchase of new • software/equipment

8. ANNEXURE – II

SUPPORT ESCLATION MATRIX			
Role	**Contact Person**	**Time Lines**	**Remarks**
System Administrator	Mohammed Maqdoom Basha/ mohammed.basha@MITStech.com	**>=2hr**	
Manager	Rajat Goel/ rajat.goel@MITStech.com	**>=4hr**	

9. SERVICE REQUEST PROCESS FLOW CHART