MANAV RACHNA INTERNATIONAL UNIVERSITY

(Deemed to be University under section 3 of the UGC Act 1956)

Policy No. MRIU-IQAC-PL-IT/2016-17

MRIU POLICY FOR IT USAGE AND MAINTENANCE AND its SOPs
(Effective from AY 2017-18)

Notified vide MRIU/REGR/2016-17/127/1 dated: 3rd October 2016

MANAV RACHNA INTERNATIONAL UNIVERSITY

Sector-46, Surajkund Badkhal Road, Aravali Hills, Faridabad 121004
HARYANA

MANAV RACHNA
vidyanatariksha

MANAV RACHNA INTERNATIONAL UNIVERSITY, FARIDABAD

Deemed-to-be-University
Accredited by NAAC with A Grade in the First Cycle

Policy for IT Usage and Maintenance and its SoPs

Number: MRIU-IQAC-PL-IT/2016-17

Committee Constituted for Preparation of draft on 18.03.2016

1. Mr. Atul Kalra, Director-Admin
2. Mr. Sabyasachi Sen, GM-IT
3. Mr. K.S. Mishra, Project Manager

Reviewed by IQAC: May 31, 2016

Approved by: Vice- Chancellor, MRIU

Date of BoM Approval: September 28, 2016

Date of Release: October 3, 2016

INDEX

A. The computing resources 1-7

1. Rights and responsibilities
2. Acceptable use of IT infrastructure and resources
3. Fair share of resources
4. Adherence with central, state and local laws
5. Privacy and personal rights
6. Privacy in e-mail
7. User compliance and liability

B. Definition of terms 8-23

1. Acceptable use
2. Prohibited activities
3. Network connection policy
    - A. Appropriate connection methods
    - B. Network registration
    - C. Responsibility for security
    - D. Security standards
    - E. Centrally-provided network-based services
    - F. Protection of the network
4. Handling of MRIU restricted information
5. Access, storage, transmission & back-up of restricted information access
    - A. Access
    - B. Storage
    - C. Transmission
    - D. Backups
    - E. Release of information
    - F. Confidentiality agreement
    - G. Special statement on the collection, storage, and use of personal identifications
    - H. Special statement on research data
    - I. Policy enforcement
    - J. Computing passwords policy
    - K. General password guidelines
    - L. Account administration standards
    - M. Shared accounts

6. Data protection roles & responsibilities
7. Violation or breach of policies
8. Revisions to policy
9. Further information / grievance

HARDWARE PROCUREMENT, USAGE AND MANAGEMENT........................24-33

A. Definitions
- Technology
- University-owned

B. Technology equipment purchasing
C. Computers for active faculty & professional staff
D. Ownership and sale of university-purchased equipment
E. Hardware replacement policy
  1.Newly-hired faculty
  2.Existing faculty
  3.Part-time faculty
  4.Shared computers
F. Policy for loss and damage of equipment
  1. Damage to equipment
  2. Loss of equipment
G. Disposition of replaced equipment
  1. Computer return at time of departure
  2. Data retention when employees depart

E-WASTE MANAGEMENT..34-39

1.Introduction:
2.Definition of e-waste
3.E-waste disposal sop

SOFTWARE PROCUREMENT AND USAGE 40-46

1.Software licensing compliance
2.Software inventories
3.Software purchasing
4.Storage of software media and licenses
5.Authorized installation of software
6.Software audit and use of audit tools
7.Disposal of software
8.Role and responsibilities

A. IT help desk

B. IT services staff authorized to install software

C. University staff using workstations

9. Breach of this policy

10. Revisions to policy

11. Grievances

DATA MANAGEMENT 47-55

1. Purpose

2. Definitions

2.1 Data

2.2 Data controller

2.3 Data owner

2.4 Data custodian

2.5 Data user

2.6 Processing

2.7 Data subject

2.8 Personal data

2.9 Staff

2.10 Student

2.11 External parties

2.12 Sensitive personal data

3. Scope

4. Data management policy

4.1 The data controller

4.2 The data owner

4.3 The data custodian

4.4 The data users

4.5 Storage media

4.6 Disposing of equipment/storage media

4.7 Breach of this policy

4.8 Revisions to policy

5. **EXIGENCY, IF ANY** 56

MRIU POLICY FOR IT USAGE AND MAINTENANCE AND its SOPs

In pursuance of the provisions of Section 26 of the Bye Laws of Manav Rachna International University, the Board of Management of the Manav Rachna International University hereby makes the following Policy for ICT Usage and maintenance and its Standard Operating Procedure

SHORT TITLE AND APPLICATION

This Policy shall be called Manav Rachna International University Policy No. MRIU-IQAC-PL-IT/2016-17 and titled as ‘‘MRIU POLICY FOR IT USAGE AND MAINTENANCE AND its SOPs”.

APPLICABILITY: This policy and procedures shall apply to mainly to entire faculty, staff and students of the university.

This Policy framework shall govern the stakeholders’ for usage of all the IT facilities available in the campus and the maintenance processes. It broadly covers the Computing Resources, Definition of Terms, Hardware Procurement Usage and Maintenance, E-Waste Management, Software Procurement and Usage and Data Management.

A. The computing resources

The computing resources at Manav Rachna International University (MRIU) support the educational, instructional, research, and administrative activities of the University and the use of these resources is a privilege that is extended to members of the MRIU community. As a user of these services and facilities have access to valuable University resources, sensitive data, and internal and external networks. Consequently, the user needs to behave in a responsible, ethical, and legal manner.

This document establishes specific requirements for the use of all computing and network resources at MRIU are called “IT Policy” (or as Policy / Policies elsewhere in this document).

This policy applies to all users of computing resources owned or managed by MRIU. Individuals covered by the policy include (but are not limited to) MRIU faculty and visiting faculty, staff, students, alumni, guests or agents of the administration, external individuals and organizations accessing network services via MRIU's computing and computer network facilities with due written permission or without violating the protocols etc. it should complete)

Computing resources include all university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

These policies apply to technology administered in individual departments, the resources administered by central administrative departments (such as the University Libraries and Computing and Information Services), personally owned computers and devices connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the University's network services.

“Acceptable use” means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements.

1. Rights and Responsibilities

Use of MRIU's computing facilities and services for those activities that are consistent with the educational, research and public service mission of the University and are not “Prohibited Activities”.

As a member of the University community, MRIU provides use of scholarly and/or work-related tools, including access to the Library, certain computer systems, servers, software and databases, the campus telephone and voice mail systems, and the Internet. It is expected from University Community to have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (may vary depending on whether user association/ role in the University), and of protection from abuse and intrusion by others sharing these resources. Authorized users can expect their right to access information and to express their opinion to be protected as it is for paper and other forms of non-electronic communication.

It is the responsibility of the University Community to know the regulations and policies of the University that apply to the appropriate use of the University's technologies and resources. University Community is responsible for exercising good judgment in the use of the University's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action.

As a representative of the MRIU community, each individual is expected to respect the University's good name in user electronic dealings with those outside the University.

2. Acceptable Use of IT Infrastructure and resources

An authorised user may use only the computers, computer accounts, and computer files for which he/she has authorization.
Usermay not use another individual's account or attempt to capture or guess other users' passwords.

The user is individually responsible for the appropriate use of all resources assigned to the user including the computer, the network address or port, software and hardware. Therefore, user is accountable to the University for all use of such resources. As an authorized MRIU user of resources, the user may not enable unauthorized users to access the network by using an MRIU computer or a personal computer that is connected to the MRIU network. [Please refer to Network Connection Policy]

The university is bound by its contractual and license agreements respecting certain third party resources; the user is expected to comply with all such agreements when using such resources.

User should make a reasonable effort to protect user passwords and to secure resources against unauthorized use or access. User must configure hardware and software in a way that reasonably prevents unauthorized users from accessing MRIU's network and computing resources.

User must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.

You are must comply with the policies and guidelines for any specific set of resources to which use have been granted access. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

User must not use MRIU computing and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

On MRIU network and/or computing systems, do not use tools that are normally used to assess security or to attack computer systems or networks (e.g., password 'crackers,' vulnerability scanners, network sniffers, etc.) unless user have has specifically authorized to do so by the MRIU-IT Information Security Group.

3. Fair Share of Resources

The campus network, computer clusters, mail servers and other central computing resources are shared widely and are limited, requiring that resources be utilized with consideration for others who also use them. Therefore, the use of any automated processes to gain technical advantage over others in the MRIU community is explicitly forbidden.

The University may choose to set limits on an individual's use of a resource through quotas, time limits, and other mechanisms to ensure that these resources can be used by anyone who needs them.

The users using the Computing and Information Services, and the IT department which operates maintain computers, network systems and servers, will maintain an acceptable level of performance and assure that frivolous, excessive, or inappropriate use of the resources by one person or a few people does not degrade performance for others unless the users found to be inappropriate and not adherence to this IT policy.

4. Adherence with Central, State and Local Laws

As a member of the MRIU Community, user is expected to uphold local ordinances and state and federal law. Some MRIU guidelines related to use of technologies derive from that concern, including laws regarding license and copyright, and the protection of intellectual property.

As a user of MRIU's computing and network resources user must:

i. Abide by all federal, state, and local laws

ii. Abide by all applicable copyright laws and licenses. MRIU University has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements

iii. Observe the copyright law as it applies to music, videos, games, images, texts and other media in both personal use and in production of electronic information. The ease with which electronic materials can be copied, modified and sent over the Internet makes electronic materials extremely vulnerable to unauthorized access, invasion of privacy and copyright infringement

iv. Do not use, copy, or distribute copyrighted works (including but not limited to Web page graphics, sound files, film clips, trademarks, software and logos) unless user have a legal right to use, copy, distribute, or otherwise exploit the copyrighted work. Doing so may provide the basis for disciplinary action, civil litigation and criminal prosecution

See the Copyright Infringement Policy, which details the policies and procedures MRIU follows in responding to notifications of alleged copyright infringements on the University network.

5. Privacy and Personal Rights

All users of the university's network and computing resources are expected to respect the privacy and personal rights of others.

Do not access or copy another user's email, data, programs, or other files without the written permission of MRIU's Registrar or General Manager IT, who is bound to the procedures outlined at Emergency Access to Accounts and Information.

Be professional and respectful when using computing systems to communicate with others; **the use of computing resources to libel, slander, or harass any other person is not allowed and could lead to university discipline as well as legal action by those who are the recipient of these actions.**

While the University does not generally monitor or limit content of information transmitted on the campus network, it reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that MRIU is not subject to claims of institutional misconduct.

Access to files on University-owned equipment or information will only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come from the

GM IT in conjunction with requests andor approvals from Registrar and or Head of Departments (HoDs) of the University, as found in the document Emergency Access to Accounts and Information. External law enforcement agencies and MRIU Public Safety may request access to files through valid subpoenas and other legally binding requests. All such requests must be approved by the Registrar. Information obtained in this manner can be admissible in legal proceedings or in a University hearing.

6. Privacy in e-mail

While every effort is made to insure the privacy of MRIU email users, this may not always be possible. Since employees are granted use of electronic information systems and network services to conduct University business, there may be instances when the University, based on approval from authorized officers, reserves and retains the right to access and inspect stored information without the consent of the user.

7. User Compliance and Liability

When an individual use MRIU computing services and accept any University issued computing accounts, means that individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep up-to-date on changes in the computing environment, as published, using University electronic and print publication mechanisms, and to adapt to those changes as necessary. User shall be liable to hold responsibility for any unlawful activities or communications made from his / her device and account.

B. Definition of Terms

1. Acceptable Use

"Acceptable use" means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements.

2. Prohibited Activities

The activities that are not consistent with the educational, research and public service mission of the University are called "Prohibited Activities". Prohibited activities include:

a) Activities that would jeopardize the University's UGC and NAAC status
b) Use of MRIU's computing services and facilities for political purposes
c) Use of MRIU's computing services and facilities for personal economic gain
d) Use of MRIU's computing services for any unlawful activities, racial activities, threat to nation or any individual, hoax calls, impersonation etc.

3. Network Connection Policy

The purpose of this policy is to define the standards for connecting computers, servers or other devices to the University's network to protect the MRIU campus network and the ability of members of the MRIU community to use it.

The standards are designed to minimize the potential exposure to MRIU community from damages (including financial, loss of work, and loss of data) that could result from computers and servers that are not configured or maintained properly and to ensure that devices on the network are not taking actions that could adversely affect network performance.

MRIU must provide a secure network for educational, research, instructional and administrative needs and services. An unsecured computer on the network allows denial of service attacks, viruses, Trojans, and other compromises to enter the university's campus network, thereby affecting many computers, as well as the network's integrity. Damages from these exploits could include the loss of sensitive and confidential data, interruption of network services and damage to critical MRIU University internal systems. Universities that have experienced severe compromises have also experienced damage to their public image. Therefore, individuals who connect computers, servers and other devices to the MRIU network must follow specific standards and take specific actions.

This policy applies to all members of the MRIU community (faculties, employees, students etc.) or visitors who have any device connected to the MRIU network, including, but not limited to, desktop computers, laptops, servers, wireless computers, mobile devices, smart-phones, specialized equipment, cameras, environmental control systems, and telephone system components. The policy also applies to anyone who has systems outside the campus network that access the campus network and resources. The policy applies to university-owned computers (including those purchased with grant funds), personally-owned or leased computers that connect to the MRIU network.

a. Appropriate Connection Methods

Devices can be connected to campus network at appropriate connectivity points including voice/data jacks, through an approved wireless network access point, via a VPN or SSH tunnel, or through remote access mechanisms such as DSL, cable modems, and traditional modems over phone lines.

Modifications or extensions to the network can frequently cause undesired effects, including loss of connectivity. These effects are not always immediate and not always located at the site of modifications. As a result, extending or modifying the MRIU network must be done within the MRIU-IT published guidelines. Exceptions will be made by MRIU-IT for approved personnel in departments who can demonstrate competence with managing the aforementioned hardware.

b. Network Registration

Users of the university network need to be required to authenticate when connecting a device to it. Users may also need to install an agent on their computers before they are allowed on the network. The role of such an agent would be to audit the computer for compliance with security standards as defined in this document.

MRIU-IT maintains a database of unique machine identification, network address and owner for the purposes of contacting the owner of a computer when it is necessary. For example, MRIU-IT would contact the registered owner of a computer when his or her computer has been compromised and is launching a denial of service attack or if a copyright violation notice has been issued for the IP address used by that person or found to be indulged in unlawful and mollified activities.

c. Responsibility for Security

Every computer or other device connected to the network, including a desktop computer has an associated owner (e.g. a student who has a personal computer) or caretaker (e.g. a staff member who has a computer at their office). For the sake of this policy, owners and caretakers are both referred to as owners.

Owners are responsible for ensuring that their machines meet the relevant security standards and for managing the security of the equipment and the services that run on it. Some departments may assign the responsibility for computer security and maintenance to the Departmental Computing Coordinator or the Departmental Systems Administrator. Therefore, it is possible that one owner manages multiple departmental machines along with his or her own personal computer. Every owner should know who is responsible for maintaining his or her machine(s).

d. Security Standards

Security standards apply to all devices that are connected to MRIU network through standard university ports, through wireless services, and through home and off campus connections.

Owners must ensure that all computers and other devices capable of running anti-virus/anti-malware software have MRIU-licensed anti-virus software (or other appropriate virus protection products) installed and running. Owners should update definition files at least once per week.

Computer owners must install the most recent security patches on the system as soon as practical or as directed by Information Security. Where machines cannot be patched, other actions may need to be taken to secure the machine appropriately.

Computer owners of computers that contain MRIU Restricted Information should apply extra protections. MRIU-IT's central Group will provide consultations on request to computer owners who would like more information on further security measures. For instance, individuals who are maintaining files with Social Security information or other sensitive personal information should take extra care in managing their equipment and securing it appropriately.

e. Centrally-Provided Network-Based Services

MRIU-IT, the central computing organization, is responsible for providing reliable network services for the entire campus. As such, individuals or departments may not run any service which disrupts or interferes with centrally-provided services. These services include, but are not limited to, email, DNS, DHCP, and Domain Registration. Exceptions will be made by MRIU-IT for approved personnel in departments who can demonstrate competence with managing the aforementioned services. Also, individuals or departments may not run any service or server which requests from an individual their MRIU-IT-maintained password.

f. Protection of the Network

MRIU-IT uses multiple methods to protect the MRIU network:

a) monitoring for external intruders

b) scanning hosts on the network for suspicious anomalies

c) blocking harmful traffic

All network traffic passing in or out of MRIU's network is monitored by an intrusion detection system for signs of compromises. By connecting a computer or device to the network, user are acknowledging that the network traffic to and from user computer may be scanned.

MRIU-IT routinely scans the MRIU network, looking for vulnerabilities. At times, more extensive testing may be necessary to detect and confirm the existence of vulnerabilities. By connecting to the network, user agree to have user computer or device scanned for possible vulnerabilities.

MRIU-IT reserves the right to take necessary steps to contain security exposures to the University and or improper network traffic. MRIU-IT will take action to contain devices that exhibit the behaviours indicated below, and allow normal traffic and central services to resume.

a) imposing an exceptional load on a campus service
b) exhibiting a pattern of network traffic that disrupts centrally provided services
c) exhibiting a pattern of malicious network traffic associated with scanning or attacking others
d) exhibiting behaviour consistent with host compromise

MRIU-IT reserves the right to restrict certain types of traffic coming into and across the MRIU network.

MRIU-IT restricts traffic that is known to cause damage to the network or hosts on it, such as NETBIOS. MRIU-IT also may control other types of traffic that consume too much network capacity, such as file sharing traffic.

By connecting to the network, it is expected that the individual has acknowledged that a computer or device that exhibits any of the behaviours listed above is in violation of this policy and will be removed from the network until it meets compliancy standards.

4. Handling of MRIU Restricted Information

MRIU University is dedicated to ensuring the privacy and proper handling of private and restricted information of its students, employees, and individuals associated with the University. The primary purpose of this policy is to ensure that the necessary policy and awareness exist so that University employees and students comply with all applicable laws and regulations. This document establishes minimum requirements for the proper handling and protection of MRIU Restricted Information. All departments shall limit access to MRIU Restricted Information to those individuals with a university and/or business need to the information in order to do their job.

This policy applies to all MRIU Restricted Information, which includes but is not limited to: Personal identifications, credit card numbers, medical records, dates of birth, driver's license numbers, addresses, and passport information.

Restricted information is not meant only for university operational, business and student data. Research data also utilizes highly sensitive, confidential, restricted and regulated information. Many Data use Agreements stipulate and dictate strong security measures for the use of the data.

The restricted information is covered in any tangible format, including but are not limited to, paper, photographs, film, audio and videotapes, microforms, drawings, databases, email, and any other electronic records.

All members of the MRIU community, including staff, faculty, students, affiliates, volunteers, and third party vendors or contractors shall complywith this policy. Vendor contracts should include a clause referencing this policy.

5. Access, Storage, Transmission & Back-up of Restricted Information Access

a) Access

Access controls to all MRIU Restricted Information must be documented. MRIU Restricted Information must have a designated Data Owner who authorizes such access.

b) Storage

MRIU Restricted Information in electronic format must be stored on a server centrally managed by Computing and Information Services (MRIU-IT) or in an environment that is under strict legal contracts with the university that meet this policy, and not on a workstation, laptop, portable storage device, or locally managed server. Exceptions must be reviewed and approved in writing by the GM IT

An approved local machine must be in a physically secure location and require a unique logon with a strong password for each individual with authorized access (i.e. shared accounts and passwords are prohibited). Security logs must be enabled and periodically reviewed by the locally approved department.

MRIU Restricted Information must be housed on a server or approved workstation that meets current operating system, hardware and software support levels.

MRIU Restricted Information in any hard copy format must be stored in locked cabinets or offices, and not be able to be accessed by unauthorized persons.

c) Transmission

MRIU Restricted Information should never be transmitted over the network "in the clear” rather it should always be transmitted using an Information Security Group-approved encryption mechanism.

MRIU Restricted Information should never be transmitted via unencrypted email. Password-protected documents or spreadsheets can be used as attachments in certain cases, with approval of the Chief Information Security Officer.

d) Backups

It is the responsibility of everyone entrusted with MRIU Restricted Information to back it up and store it in a secure and controlled location by themselves. Backup of MRIU Restricted Information should be encrypted if technically feasible.

The backup of central server and databases will be taken on tapes on rotation basis, there should be an incremental backup to be taken every day and full back up need to be taken twice a week. The back-up data should be kept in two copies. One copy will be stored locally for any emergency restoration and other copy will be stored physically apart out of the campus premises but may be within the city.

e) Release of Information

Restricted information concerning individual students or employees may be released only if the release of such information has been authorized by the Data Owner (the University employee identified as being responsible for the classification and data oversight for a functional area, or certain type of protected information).

The Data Owner is responsible for theprotection, confidentiality, and release of the information assigned to them, in accordance with University Policy, regulatory mandates, and legal obligations to release.

Additional information on the roles of the Data Owner can be found in the Data Protection Roles and Responsibilities Section of this document.

f) Confidentiality Agreement

Data Owners, who authorize access to MRIU Restricted Information, should ensure that those with access sign a Confidentiality Agreement. All authorized users of MRIU Restricted Information are also required to successfully complete the "Protecting MRIU Information" class (contact Computing Accounts and Passwords for details).

g) Special Statement on the Collection, Storage, and Use of Personal Identifications

While it is recognized that a small number of areas, departments, and processes have a need to utilize personal identifications, any use of this identifier puts members of the MRIU community at a greater risk of identity theft. As a result, any Department of MRIU that currently uses, or wishes to collect, store, or use personal identifications in any format must:

1) Show institutional need
2) Receive approval from the Data, Privacy, and Records Management Steering Committee
3) Permit audits (including server and application security) at least annually to ensure safe SSN handling

Additional information specific to personal identifications can be found in the Personal identifications – Usage and Protection Requirements.

h) Special Statement on Research Data

As a research institution, MRIU collects, stores and utilizes large amounts of research data which may be restricted, confidential and protected information. In addition to the stipulations on handling such information as outlined in this policy, guidance and oversight is provided by the Office of the Director of Research (ODR). ODR assists faculty in ensuring that research complies with institutional and federal standards, beginning with proposal preparation and review, and extending throughout the performance of the research and into evaluation and reporting of research project results.

i) Policy Enforcement

Violation of this policy may result in disciplinary action, up to and including termination of employment

j) Computing Passwords Policy

Computing Passwords Policy describes the University's requirements for acceptable password selection and maintenance to maximize security of the password and minimize its misuse or theft.

Passwords are the most frequently utilized form of authentication for accessing a computing resource. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are very often also the weakest link in securing data. Password use must therefore adhere to the policy statement found below.

This policy applies to anyone accessing or utilizing MRIU network or data. This use may include, but is not limited to, the following: personal computers, laptops, MRIU-issued cell phones, and hand-held factor computing devices (e.g., PDAs, USB memory keys, electronic organizers), as well as MRIU electronic services, systems and servers. This policy covers departmental resources as well as resources managed centrally.

k) General Password Guidelines

All passwords (e.g., email, web, desktop computer, laptop etc.) should be strong passwords and follow the standards listed below. In general, a password's strength will increase with length, complexity and frequency of changes.

Greater risks require a heightened level of protection. Stronger passwords augmented with alternate security measures such as multi-factor authentication, should be used in such situations. High risk systems include but are not limited to: systems that provide access to critical or sensitive information, controlled access to shared data, a system or application with weaker security, and administrator accounts that maintain the access of other accounts or provide access to a security infrastructure.

Central and departmental account managers, data trustees, and security and/or system administrators are expected to set a good example through a consistent practice of sound security procedures.

All passwords must meet the following minimum standards, except where technically infeasible:

1) be at least ten characters in length (for Brown network passwords, eight for Google mail)
2) contain at least one lowercase character
3) contain at least one number
4) contain at least one special character
5) contain at least one uppercase character
6) cannot contain user first name, last name, or username
7) cannot match user last three passwords
8) To help prevent identity theft, personal or fiscally useful information such as Social Security or credit card numbers must never be used as a user ID or a password
9) All passwords are to be treated as sensitive information and should therefore never be written down or stored on-line unless adequately secured
10) Passwords should not be inserted into email messages or other forms of electronic communication without the consent of the Information Security Group (ISG)
11) Passwords that could be used to access sensitive information must be encrypted in transit
12) The same password should not be used for access needs external to Brown (e.g., online banking, benefits, etc.)
13) It is recommended that passwords be changed at least every six months
14) Individual passwords should not be shared with anyone, including administrative assistants or IT administrators. Necessary exceptions may be allowed with the written consent of ISG and must have
15) a primary responsible contact person. Shared passwords used to protect network devices, shared folders or files require a designated individual to be responsible for the maintenance of those

16) passwords, and that person will ensure that only appropriately authorized employees have access to the passwords.

17) If a password is suspected to have been compromised, it should be changed immediately and the incident reported to the Departmental Computing Co-ordinator (DCC).

18) Password cracking or guessing may be performed on a periodic or random basis by ISG or its delegates with the cooperation and support from the appropriate system administrator. If a password is guessed or cracked during one of these scans, the password owner will be required to change it immediately.

l) Account Administration Standards

In addition to the general password guidelines listed above, the following apply to desktop administrator passwords, except where technically and/or administratively infeasible:

1) Passwords must be changed at least every six months
2) Where technically and administratively feasible, attempts to guess a password should be automatically limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes
3) Failed attempts should be logged, unless such action results in the display of a failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities or compromises should be immediately reported to the Information Security Group

m) Shared Accounts

In addition to the general password standards listed above, the following apply to server administrator passwords, except where technically and/or administratively infeasible:

a) Passwords for servers must be changed as personnel changes occur

b) If an account or password is suspected to have been compromised, the incident must be reported to

ISG and potentially affected passwords must be changed immediately

c) Where technically or administratively feasible, attempts to guess a password should be limited to ten incorrect guesses. Access should then be locked for a minimum of ten minutes, unless a local system administrator intercedes

d) Uniform responses should be provided for failed attempts, producing simple error messages such as "Access denied". A standard response minimizes clues that could result from hacker attacks

e) Failed attempts should be logged, unless such action results in the display of the failed password. It is recommended that these logs be retained for a minimum of 30 days. Administrators should regularly inspect these logs and any irregularities such as suspected attacks should be reported to the Information Security Group

Note: Log files should never contain password information

6) Data Protection Roles & Responsibilities

There are four basic roles for proper data management and protection at MRIU:

a) Data Owner
b) Manager of Policies & Procedures for access to that data
c) Manager of the infrastructure and account access
d) Data user

It is important that

a) All MRIU Restricted Information should have an identified owner
b) Anyone who has been entrusted with sensitive information has a responsibility to the data's owner for its proper use and protection.

The following chart breaks out above roles and defines their responsibilities. The listed example is for the handling of financial business information and illustrates one combination of roles and responsibilities.

Responsible Position or Individual	**Key Responsibilities**	**Example *(Financial Data)***
Registrar(Chairperson)	• Data owner for their functional area, responsible for its management and participating in establishing policies. • Promotes data resource management for the good of the entire University.	University Controller
Departmental Heads	• Manage access to their functional area's data. • Provide input in policy implementation and resulting procedures • Awareness/ training for those individuals who have access to "MRIU sensitive information" in the course of their jobs.	Assistant Controller
Zone Leaders	• Provide a secure infrastructure in support of the data, including, but not limited to: physical security, backup and recovery processes as well as secure transmission of the data. • Grant/ Revoke access privileges to authorized system users and maintain records. • Ensure individuals have access only to that information for which they have been	Technical Support / System Administrator

	authorized, and that access is removed in a timely fashion when no longer needed. • System Administrator and/or Departmental Computing Coordinators are accountable for data within their specific areas or departments. • Computing and Information Services for centrally held data.	
Manager ICT	• Protecting the security and integrity of the data as detailed in the Policy on the “Handling of MRIU Restricted Information” • Report weakness in the protection of data to IT Security	User of Workday Financials System

7) Violation or Breach of Policies

If an individual is found to be in violation of the Acceptable Use Policy, the University will take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could result in more serious consequences, up to and including suspension or termination from the University. Individuals are also subject to central, state and local laws governing many interactions that occur on the Internet. These policies and laws are subject to change as state and local laws develop and change. (Violation sub section comes in the end.

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Helpdesk at intercom No. 4444 or email at team-helpdesk@manavrachna.net. On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user’s access to University’s Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of

Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

8) Revisions to Policy

The University reserves the right at any time to revise the terms of this Policy. Any such revisions will be noted in the revision history of the policy, which are available on the MRIU website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

9) Further Information / Grievance

If user have any queries in relation to this policy, please contact:

General Manager IT

Email: gm.it@mriu.edu.in

POLICY FOR IT USAGE AND MAINTENANCE

HARDWARE PROCRUREMENT, USAGE AND MAINTENANCE

Abstract

This Data Management Policy is designed to help the MRIU understand their responsibilities with regards to the protection of electronic data. In particular electronic data and information belonging to, held or used by, MRIU

Policy

The University has entrusted IT Department with responsibility for the support and timely maintenance of the University network, servers and workstations to include University owned computer hardware, software and peripherals. This policy establishes expectations for the purchase, use and re-use of technology hardware that assures, as a community, as responsibilities towards the University resources, aware of security considerations and consistent in MRIU practices.

Definitions

Technology

“Technology” means a cable or small digital camera to a desktop computer/ laptop or printer or Network Active Components like Switches, Routers, Firewall etc. Throughout this policy the word “technology“ when not otherwise qualified refers only to computers, monitors, tablets, printers and most devices that connect to the University’s network. While IT department will gladly offer advice and guidance and/or facilitate making other types of purchases, this policy is not aimed at those needing small peripherals (for example cables, an adaptor, a specialized mouse, a thumb drive, a small webcam, a voice recorder, microphone or speaker.)

University-Owned

A “University-owned” computer is defined as a computer that is optimally configured for the general activities associated with being a staff or faculty member and optimized to work on the MRIU network with associated adequate security provisions. This may be new or used equipment depending on circumstances.

Technology Equipment Purchasing

To achieve the best possible and most effective service levels for all MRIU-owned technology, technology hardware purchases are made under the suggestion of IT department through central procurement department.

By working through IT department, faculty and staff can expect assistance and guidance that helps to assure purchases are sustainable, compatible with existing systems, and can be adequately supported. To aid in this endeavour, IT department in association with the central procurement department has negotiated purchasing agreements with hardware, software, network, and telecommunication vendors, service agencies, multimedia companies, software developers, and others. Involving IT department in technology purchases and taking advantage of pre-negotiated purchasing agreements helps assure the needs of our campus users are met, such as:

a) Compatibility with MRIU network environment.
b) Compliance with MRIU security requirements and policies.
c) Suitability, based on needs assessment.
d) Licensing compliance for any bundled software purchases that accompany hardware devices.
e) Hardware that can be efficiently supported.
f) All equipment is entered into the University's asset management system

Standardizing equipment purchased allows the MRIU to efficiently select and manage technology, obtain better technology pricing, reduce maintenance costs and increase access to training and assistance. These standards are re-evaluated periodically based on common needs, vendor offerings, cost, reliability, supportability, quality, sustainability, compliance with recycling policies and timeliness of vendor response.

C. Computers for Active Faculty & Professional Staff

Standard technology purchases are part of MRIU Annual computer replacement cycle which focuses on the primary computer provided to active faculty and staff.

a) Manav Rachna International University (MRIU)will provide one "University-owned" computer to each member of the faculty and professional staff of the University, including visiting faculty for official use.
b) In case, a faculty member requests for a primary computer above the standard configuration, the requests are typically reviewed by the IT Core Committee. If approved, the faculty member may have to use his or her

department, grant or endowed fund to cover the additional cost. It is not allowable for an individual’s to use their own personal resources to pay for this cost differential.

c) Computers and equipment should be returned to IT TRC (Technical Repairing Centre) at the end of their useful life and are not automatically eligible for replacement. Depending on age and condition, IT TRC may use for parts, properly remove data and/or recycle retired equipment. “Beyond the end of its useful life“ is generally defined by IT TRC as equipment that is: broken, unable to run a newer operating system, requires an operating system that is considered end of life, or lacks necessary storage or memory to apply critical security patches, browser or software updates.

d) Computer purchases cannot be made for individual’s personal use. IT department will, from time to time, make information available from some vendors that offer special incentives to employees for their personal use but those transactions are carried out directly between the vendor and the employee.

e) Departmental computer purchases may not be charged to an individual’s University provided purchase card or reimbursed through an expense voucher. MRIU will not reimburse nor support the purchase of any technology-related item, unless that purchase was made through and/or with the knowledge and approval of IT and core committee..

f) Should an individual’s position require more than 1 computer, the individual’s department

g) bears the cost of the additional equipment from their allotted annual budget. That additional equipment will be given to IT Help Desk when it is no longer needed, or when it reaches the end of its useful life. IT staff will work with departments to determine whether equipment is no longer needed.

h) Additional desktop or laptop computers or desired peripherals such as docking stations or external monitors for laptops (either for individuals or to share within a department) are purchased through central procurement department, but charged to departmental annual budget.

i) Because of data security concerns, administrative departments are strongly discouraged from purchasing extra shared equipment for their department (for example a shared travel laptop that is only periodically used.)

j) The majority of faculty and staff have their primary computer issued by IT department. There are a few exceptions to this. Despite this exception for primary issuance source, all other policies remain in effect.

D. Ownership and Sale of University-purchased equipment

All technology equipment, regardless of how the purchase was originally funded (departmental funds, IT funds, endowed funds, etc.) remains the property of Manav Rachna International University. MRIU does not consider requests for sale or retaining for non- University uses of equipment to faculty, staff, retirees or students; for example at the time of departure from MRIU. This is true regardless of how the equipment purchase was originally funded. For a variety of reasons including information security, restrictions of software licensing contracts and general interest of fairness to all who might want to buy used goods from the University, IT department is not authorized to sell or give away equipment directly to individuals. Other questions about purchase or sale of University equipment should be directed to the University IT Core Committee.

E. Hardware Replacement Policy

University-owned individual-use computers are “generally” replaced every five years. This is done for several reasons, like:

- to provide community members with the current operating systems and sufficient power for the latest software applications
- to protect our campus network by updating the security protections that come with more recent operating systems
- to maintain a reasonable number of hardware configurations that can be well supported by limited staff

IT department will engage in an Annual replacement plan by examining existing inventory of all University-owned hardware, making an initial recommendation for replacement based on the needs of various faculty and staff members and the funds that are available for hardware replacement. The Academic Head and or Management heads will then review these recommendations to make the necessary adjustments to arrive at the final plan. Depending on the adjustments made, allocations of hardware are likely to be changed, particularly if there are funding constraints within the department.

Individuals will be notified prior to the replacement of their computer and will be given an option to request delaying their replacement by no more than one year. This extension will be granted if the computer meets the needs of the individual for another year, and if the operating system and other software will be supported for another year.

The plan will take into consideration the budget constraints and the academic cycles of various academic and administrative departments to schedule the purchase and replacement of hardware. IT staff will contact the Academic Head and or Management in advance of replacement for consultation, scheduling and training.

IT Staff will assist users in the transfer of data from the old computer to the new one. IT Staff will also assist in the installation of any custom applications that the user needs. However, IT Staff cannot assist in transferring any custom applications that are not supported by the University that the user had installed on their own on the older computer. In many cases, these installations will require original CDs or DVDs and serial numbers for which the user is responsible. Therefore, any reinstallation of these applications is the responsibility of the user. After the data has been transferred to the new computer and the user confirms that everything has been transferred correctly, IT staff will remove the older hardware usually within a day or two.

IT Help Desk maintains customized software images for the following standard configurations:

- Thin Clients - Appropriate for administrative staff that use the computer for basic use such as email, Office applications, basic Banner access and the web.
- Intermediate Windows Desktop Computer - This will be the standard computer for faculty who want a Windows desktop computer. This is also appropriate for an administrative user
- Windows Laptop - Ideal for anyone who travels a lot, and for use in both office and home.
- In addition, IT Help Desk will recommend advanced, custom configurations for Windows PC Desktop, Windows PC Laptop, If requested. If a faculty or staff member eligible for replacement needs an advanced configuration, the same shall be routed through their HoDs to IT department for further actions.

1) Newly-hired Faculty

Each new tenure-track faculty member will be provided with a standard desktop or laptop Windows or Mac computer at the beginning of their first year depending on his requirements as decided by the department head.

2) Existing Faculty

All tenured professors of the practice and lecturers on continuing appointments are eligible for an appropriate Windows notebook or desktop computer when their existing computers are due for replacement.

3) Part-time Faculty

Faculty working part-time are eligible for a desktop computer only or they are allowed to use their own laptop / tablet devices cleared by central / zonal IT department duly verified for legitimate software and virus / malware cleaned environment and installed with antivirus application.

4) Shared Computers

There are many offices that require additional computers for their student employees, temporary employees, or teaching assistants. IT Help Desk will assess the need in these areas and provide the minimum number of shared computers. IT department will manage these requests by recommendations purchasing some of the base desktop configurations as well as use some of the computers that are being replaced for this purpose. In the long run, we will use Thin Clients for this purpose, resulting in a far more functional and cost effective solution.

F. Policy for Loss and Damage of Equipment

1) Damage to Equipment

Faculty & Staff who receives a University owned computing device (such as a computer or laptop) are expected to return it to University at the end of its life cycle or before moving from the university. In the event a computer is damaged, the individual or department will be responsible for the repair or replacement of the computer. In these cases, IT TRC will provide the most cost-effective solution taking into consideration factors such as the age of the computer and the extent of the damage.

2) Loss of Equipment

If the equipment is lost on University property, it should be reported to the Campus security and Police immediately and IT Help Desk will find an appropriate replacement computer for the faculty or staff who lost the computer. If the equipment (such as a laptop or tablet) is lost outside the University property, then the individual or department is responsible for the cost of replacing the equipment with an appropriate device.

G. Disposition of Replaced Equipment

When a new computer is delivered by IT, and the recipient has worked with the delivering technician to assure it is working satisfactorily, the old computer will be returned to IT. IT can typically derive several years of service from a computer beyond its first years as a faculty/staff primary workstation, thereby optimizing the lifetime service an individual computer can provide to the campus. IT will gladly pick up other unused older computer equipment that was previously purchased by the University. This equipment may be repurposed on campus, responsibly recycled, or donated to worthy local and international causes after being cleaned of data and software or dispose-off as per local govt body for safe disposition of electronic goods.

1) Computer return at time of departure

When an employee departs, IT is typically alerted several weeks in advance by weekly automated reports provided by Human Resources and will arrange to pick up the departing employee’s computing equipment when they depart. If a device needs to be reassigned to a different user, even within the same department, IT must retrieve the device, scrub it of data, update the University's asset database and deliver it to the new user.

2) Data retention when employees depart

For liability reasons, it is considered bad business practice to allow a department to retain a departing colleague’s computer in order to retain or retrieve files for departmental operations. Under normal departing circumstances, a department should work with their colleague to relocate files from an employee’s computer to an accessible and shared location prior to their last day of work. IT Staff is happy to advise and assist. In circumstances where an employee departs suddenly or unexpectedly, IT Staff will work with colleagues in that department to retrieve and retain relevant files before removing the computer. Departments are urged to establish operating practices that avoid creating and maintaining critical operational files on an individual employee office computer.

Asset Management

IT Help Desk will affix MRIU asset tag (typically a small sticker with a unique number on it) on each asset subject to this policy and will maintain an inventory database with I T Manager to include a description of the device and who it is assigned to, and how it was paid for if it was funded outside of IT Department.

IT Help Desk may install software to track information about the device, which is essential for locating equipment when it is lost or stolen; and in some cases being able to reliably remove data from a stolen asset. IT may also periodically conduct a physical inventory to ensure asset records align with the physical location and individual we believe has possession of them. IT may also work with departments to retrieve and re-distribute equipment that is not being utilized.

Revisions to Policy

The University reserves the right at any time to revise the terms of this Policy. Any such revisions will be noted in the revision history of the policy, which are available on the MRIU website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

Further Information

In case of any queries in relation to this policy, please contact:

General Manager IT - gm.it@mriu.edu.in

POLICY FOR IT USAGE AND MAINTENANCE

E-WASTE MANAGEMENT

MANAV RACHNA

॥vidyanatariksha॥

1. Introduction:

Manav Rachna International University, stands committed to the ideals of Late Dr. O P Bhalla – Right Philosophy, Right Knowledge, and Right Conduct – in branches of the knowledge tree a cloud of knowledge activity (Vidyanatariksha) and aspires to be recognized as the ultimate destination for world-class education.

After the University was established in 2002, Dental, Engineering, Management, Law, Sciences, Physiotherapy, Hotel Management, Graphical Design, Architecture, Journalism, Fine Arts, Language Studies, have been established to meet rising aspirations of the use. The campus is laid out with picturesque landscape, numerous buildings of various designs and wide road network. It presents a spectacle of harmony in architecture and natural beauty. The University is equipped with all modern facilities such as road networks, water supply, street lighting, electricity supply and parks/ lawns including Purified drinking water and highly efficient effluent / sewage treatment system.

With expansion, over a period of time and growing ICT demands, the need was felt of a systematized E-waste management system.

2. Definition of E-waste

Electronic waste (e-waste) means waste electrical and electronic equipment whole or in-part or rejects from their manufacturing and repair process, which are intended to be discarded.

Steps followed by the University to dispose-off E-waste:

- Collection of all unserviceable computers and accessories at TRC stores
- Scavenging the good working parts out of the dead devices and used them for
  repairing.
- Salvaging the body and other peripherals to build fully working computers for

facilitating to poor students and schools. This includes children of EWS staff at university.

- Salvaging peripherals to some extent is workable.
- Declaring the rest of the metal and circuits as scrap and writing off them from the asset list and dumping them to closed IT dump yard.
- Sending information to Govt and pollution control board (both Delhi NCR and Haryana) certified vendors to visit the dump yard and quote.
- Quotes submitted by vendors are required to submit latest license and passbook for eligibility.
- List of eligible vendors with their quotes are sent to purchase department for negotiation.
- Sale price approved by management.
- The University awards the contract for Electrical/Electronic goods recycling and disposal to the govt. authorised vendor selected by the IT committee includes central purchase department.
- After disposal Vendor need to submit the certificate that they have processed the recycle as per NGT and pollution control board prescribed norms.
- The categorisation of the E-waste is being followed as below.

Category	Nature	Items	Useful/productive life
1	Immediate obsolescence/use and throw products	Printing consumables(ink toners),floppies, CDs, DVDs, Digital Audio Tapes(DAT), UPS Batteries	As per usage. No. residual value determined. However, proper inventories of purchase, issue and final use/disposal etc. would be maintained in order to keep an accounting system.
II	Low life/Fast obsolescence products	Mobile phones	Two years
		Laptops, pen drive, External Hard Disk	Three years in case of Laptops, pen Drive, HDD etc.

		Drive(HDD) etc.	For replacement, residual values determined separately
III	Medium obsolescence/ medium life products	Desktops, multifunctional scanners, projectors, UPS system etc. printers, devices, multimedia projectors, UPS etc	Five years for replacement
IV	Slow obsolescence/long life products	Fax, cameras, TVs, DVD players, etc.	Seven years
V	Software	Software like MS office, Oracle, MS-SQL,MS- Windows, Antivirus etc.	Please refer to the explanation given in (software) policy
Note:	The above mentioned items can be used beyond the mentioned/specified life till such time these items continue to serve the purpose.		
	Before obsoleting / disposal / condemnation of equipment, all university colleges / departments / branches will consider the following steps.		

- The following equipment will be considered for obsoleting/disposal/ condemnation

The equipment will be covered under electronic e - waste equipment like TV, air conditioners and information technology/ telecommunication equipment like centralized data processor mainframe, servers, minicomputers, personal computer, notebook, printer, cartridge, scanner, multifunctional printer, electrical and electronic typewriter, user terminal and system, FAX, telephone, cordless phone, UPS batteries, UPS, Stabilizers, DVD players, CVTs, DVD, CD, Floppies, pen drive, internal and external HDD, RAM, LCD & DLP projector, Head phones, computer speakers, computer MIC, VGA cable, data cable, networking items like Switch, hub, router, Modems, LAN card and other electronics cards like sound, graphics, PCI cards etc.

3. E-WASTE DISPOSAL SOP

1. University will send its details of all e-waste equipment through IT department in association with central purchase committee

2. All obsolete / condemned material will be verified / inspected by the inspection committee. Inspection committee will work up to the completion of first phase inspection of equipment under consideration of obsolete/ disposed / condemned e- waste material. Written elsewhere in this document on e-waste

3. Ininitialstage,allthedepartmentswillcondemn/write-offtheirelectronic/electrical items in the follow disposal processing steps.

    - They will submit the details of the items as shown below to the IT department.

S#	Item description	Date of purchase or year of purchase	Stock register page No.	Qty	Unit price	Total price	Purchase details	Status(working or not working)

4. The colleges / departments /branches will submit it to the IT department. The lists prepared and duly signed within ten days from the date of letter issued by the respective college / department

5. Further, a letter will be issued by the IT department with the date and time of visit of inspection committee to inspect / verify the equipment of all concerned college / departments / branches as submitted in their obsolete / disposed / condemned equipment list.

6. All obsolete / disposed / condemned equipment and stock register will be presented and shown by all colleges / departments /branches to the inspection committee during the time of the inspection visit

7. Inspection committee will verify the condition of all equipment as submitted by the colleges / departments /branches on the site.
8. After approval from the competent authority, IT department MRIU will send the University consolidated list of obsolete / disposed / condemned material to the vendor and obtain govt certificate for authorised disposal of the goods.
9. Allcolleges/departments/brancheswillretainthisobsolete/disposed/condemned material at their site and it will be picked by the e-waste vendor.

NOTE: This E – Waste management system will be implemented on disposition of replaced equipment under Hardware Acquisition, Disposition and Replacement Policy.

POLICY FOR IT USAGE AND MAINTENANCE

SOFTWARE PROCURMENT AND USAGE

MANAV
RACHNA
||vidyanatariksha||

1. Software Licensing Compliance

The scope of this Policy on Software Licensing applies to the following:

1. University staff , faculties and students those who are in use of university or individual computers, laptops, tabs or any other IT related devices.
2. Software on workstations (e.g. PCs and laptops) as well as servers.
3. Software on workstations in either of the following categories:
    - Workstations which belong to the University.
    - Workstations which are privately owned, but which are being used for University business and supported by the University.
4. The University has a responsibility to ensure that all software used by members of the University using hardware supplied or supported by the University, is appropriately licensed.
5. Individual users of software applications have a responsibility to ensure that:
    - Software installed on workstations for which they have some responsibility is licensed.
    - The software is either named on the list of University/College list of approved and supported software, or otherwise use of the software has been agreed with/notified to the College IT department.
    - The software is not named on the list of prohibited software maintained at the University/College level.
    - They are complying with the conditions of use of respective licenses

A central list of supported software approved for use within the University will be maintained by IT Services and College IT Managers, as well as a list of specifically prohibited software (e.g. on security grounds or inappropriate use of University resources). Use of software which may not require a license, e.g. Freeware or Shareware, may only be used if it is on the list of officially approved software. Usage of approved screensavers will be specified at the College level.

- Each user must take responsibility for their own particular use of software, in accordance with the license terms and End User License Agreement.
- The University's Conditions of Use of Computing and Network Facilities contains the following stipulations concerning use of licensed software – failure to comply with these could constitute a disciplinary offence:
- The University reserves the right for access to be granted to computer audit staff
- without notice to enable them to check against an inventory of licensed software and hardware. Any unlicensed software or hardware or illicit copies of documentation will be removed by such audit staff and reported b.to the
- General Manager IT/ committee, who may initiate disciplinary proceedings."
- Where software has been electronically downloaded from IT Services computer systems requiring user authentication by means of a username and password, the user must read and comply with the licensing conditions for that software, and the act of downloading indicates acceptance of the licensing conditions pertinent to that software.
- All persons who are licensed to use software or who control access to any computing and/or network resources are obliged to take all reasonable care to prevent the illicit copying and use of software and documentation.
- No one shall introduce on to computer systems any software or other material requiring a license for which a valid license is not in place.

2. Software Inventories

a. A software inventory must be set up and centrally maintained at the University/College level, with responsibility for this taken by the IT Manager, and similarly a nominated IT Services manager being responsible for the software inventory within Corporate Services. The format should be as close as possible to the University standard format specified by IT department.

b. This software inventory will be used to match the number of software licenses purchased against the number of staff licenses in use; also to check that the software licenses are current, i.e. have not expired. This monitoring must be carried out on a regular basis, and licenses purchased appropriately if required to rectify any discrepancies identified.

c. The inventory must take account of staff leavers, i.e. identifying software licenses that are no longer being used. Unused software licenses remain the responsibility of the College IT Manager. Any transfer of such licenses between Colleges should be recorded within the inventory.

d. The same Managers/Staff responsible for the software inventory are also responsible for maintaining copies of the software licenses relating to the inventory.

e. Use of Freeware/Shareware software should also be monitored in order to ascertain firstly that use of the software is actually free for use for business use within the University, and secondly that the use of such Freeware/Shareware does not pose any security risks. Beyond carrying out these checks, it is not necessary to either record the usage of such software, or maintain copies of software licenses.

3. Software Purchasing

a. Software purchasing must be limited just to IT staff themselves or in association with central purchase department, together with any other nominated individuals authorized by the College Management. A list of such additional authorized individuals must be documented and maintained by the College IT Manager.

b. These authorized members of staff must also sign off individual software purchases.

4. Storage of Software Media and Licenses

a. Software and media must be stored in a suitably secure and accessible location, and take into account the Business Continuity requirements, including for the case of loss of a server, or even potential loss of a building.

b. The location of the software media should be recorded on the software inventory, preferably in software library.

c. Similar consideration must be given to software which has been electronically downloaded, and it should be stored on an appropriate server. A hard copy of the licence or certificate should also be stored.

5. Authorized Installation of Software

a. Only authorized IT Staff within IT Services or University/College IT support staff are permitted to undertake installation of software. Other non-IT staff will be permitted to undertake installation of software only if authorized on the exception list maintained by the University/College IT department (or equivalent).

b. The same IT installation staff (or other staff specifically authorized to install software) are also responsible for ensuring that the software which they are installing is appropriately licensed and recorded in the relevant software inventory.

6. Software Audit and Use of Audit Tools

a. Wherever possible, access to the use of software by individuals should be controlled by Active Directory, thereby enabling both potentially automatic distribution of software applications, as well as automated use of audit tools

b. Support staff, either in IT services centrally, or within Colleges, have the responsibility for using these automated audit tools to ensure compliance by the University, i.e. confirmation that the number of licenses held corresponds with the actual number of users of the software as specified by the license conditions

c. An exception list of those devices which are excluded from such an audit must be specified at the College level, e.g. laptops and devices on the wireless network.

d. All University workstations and servers must have the standard corporate tools installed on them as part of their build to enable the software monitoring to take place. Any exception to this must be authorized and documented at the College level.

e. If suitable automated tracking software is available, support staff should use this in order to identify any software which may no longer be required within the University, with a view to either re-utilizing such software, or arranging for its disposal if redundant.

7. Disposal of Software

When permanently disposing of equipment containing storage media, all licensed software must be irretrievably deleted either before the equipment is moved off-site, or by utilizing an approved 3rd party off-site service.

8. Role and Responsibilities

A. College IT Help Desk

Responsibilities of the College IT HELP DESK in respect of software licensing staff can be summarized as follows:

a. Maintaining a University/College list of approved/supported software.

b. Maintaining a University/College list of prohibited software.

c. Maintaining a software inventory for the College (or Corporate Services).

d. Maintaining copies of the software licenses relating to the inventory.

e. Ensuring that IT support staff carries out a regular automated audit of software in use on workstations.

B. IT Services Staff Authorized to Install Software

Responsibilities of IT Services staff authorized to install software in respect of software licensing can be summarized as follows:

a. Ensuring, with the user, that software being used on the workstation is licensed, and approved/not prohibited.

b. Ensuring, with the user, that they are complying with the conditions of the software license.

c. Ensuring that the installed software is recorded in the software inventory.

C. University Staff Using Workstations

Responsibilities of University staff using workstations in respect of software Licensing can be summarized as follows:

a. Ensuring that software being used on the workstation is licensed, and approved/not prohibited.

b. Ensuring that they are complying with the conditions of the software license.

c. Disposing of redundant software appropriately

9. Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT Helpdesk or respective zone leaders On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user’s access to University’s Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

10. Revisions to Policy

The University reserves the right at any time to revise the terms of this Policy. Any such revisions will be noted in the revision history of the policy, which are available on the MRIU website and by continuing to use the University’s IT Resources following any update it is considered acceptance on the revised terms of this Policy.

11. Grievances

In case of any queries in relation to this policy, please contact:

General Manager of IT Services

DATA MANAGEMENT

1. Purpose

The purpose of this Data Management Policy is to protect the electronic data and information belonging to, held or used by, MRIU. It aims to provide a framework within which the roles and responsibilities of those who manage or use the data and information are defined. The intention of the Policy is to enable access to data and information held by MRIU, to the greatest extent possible, consistent with legislation and relevant MRIU policies, whilst ensuring that electronic data is protected from unauthorized use, access and breaches of privacy.

2. Definitions

2.1. Data

"Data" means information in a form which can be processed and is a general term meaning facts, numbers, letters and symbols collected by various means and processed to produce information.

2.2. Data Controller

"Data Controller" means the organization or body which ultimately controls the content and use of data. Under this policy, the Data Controller means the University, rather than any individual, department, school, college, administrative unit or research unit, as for legal purposes it ultimate owns and controls all Data held by the University.

2.3. Data Owner

"Data Owner" means the most senior person/individual in the department/school/college/ administrative unit/research unit within which the data is created. An exception can be made if this role has been explicitly and formally delegated to someone else by the most senior person in the aforementioned areas. Data owners have overall responsibility for the quality and integrity of the data held in their area. Further explanation of this term is provided below.

2.4. Data Custodian

"Data Custodian" means an individual or department/school/college/ administrative unit/ research unit (e.g. IT Services) to which data is entrusted on behalf of the Data Controller for the purposes of storage and/or processing.

2.5. Data User

"Data User" means any person who uses, processes, stores, manipulates data held by the University

2.6. Processing

"Processing" means performing any operation or set of operations on data, including:

a) Obtaining, recording or keeping data;

b) Collecting, organizing, storing, altering or adapting the data;

c) Retrieving, consulting or using the data; e.g. reports generated from centrally held databases

d) Disclosing the information or data by transmitting, disseminating or otherwise making it available;

e) Aligning, combining, blocking, deleting or destroying the data.

2.7. Data Subject

A "data subject" means an individual who is the subject of or identified in the data.

2.8. Personal Data

"Personal data" means data related to an individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into the possession of the Data Controller. Personal data would include the age of the individual, their home address, their educational and employment history, information relating to their financial affairs, marital status. Users taking personal data outside of the University need to adhere to the Encryption guidelines, as set out in the Guidelines to encryption standards.

2.9. Staff

"Staff" means all full-time and part-time employees of the University, including staff funded externally but under contract to the University.

2.10. Student

"Students" mean all full-time and part-time registered students of the University.

2.11. External Parties

"External Parties" means all the University's subsidiary companies, contractors, researchers, visitors and/or any other parties who are granted access to the University's IT Resources.

2.12. Sensitive Personal Data

"Sensitive personal data" means personal data relating to:

a) The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject.

b) The physical or mental health or condition or sexual life of the data subject;

c) The commission or alleged commission of any offence by the data subject; or

d) Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

3. Scope

This Policy governs any electronic Data held by the University. The Policy has been formulated on the basis of the following principles:

Data generated and/or held by the University are key strategic assets that must be correctly managed and controlled so as to ensure their availability, integrity and confidentiality and to protect the University's resources, reputation, legal position and ability to conduct its business. In addition to its legislative responsibilities, the University values the privacy of the individual and the management of Data must be handled in way that protects that privacy.

4. Data Management Policy

4.1. The Data Controller

It is the data controller's responsibility to ensure that appropriate data management policies are in place so that the data owners can ensure they are compliant with legislation to the best of their ability.

4.2. The Data Owner

Every set of data must have a Data Owner. The Data Owner has overall responsibility for the quality and integrity of the data. Specifically, the Data Owner is responsible for:

a) Deciding the criticality and sensitivity of the data and classifying the data accordingly Authorizing access to Data

b) Authorizing the use of the data, e.g. what processing takes place on the data

c) Regularly reviewing access privileges

d) Assessing the risks to the data. Risks could include but are not limited to:

    i. Theft
    ii. Data Loss – due to lack of proper backups
    iii. Neglect – Old hardware being recycled without proper data sanitization
    iv. Online File Share

e) Data Users and Data Custodians need to be made aware of the potential consequences of data theft or loss so the relevant parties can act so as to mitigate these risks;

f) Ensure that appropriate contingency plans are in place to safeguard the data and ensure that they or the Data Custodian have the appropriate backup and disaster recovery plans in place.

The Data Owner is the most senior person in the area within which the data is created unless this role has been explicitly delegated to someone else.

Functional Area	Student Data	Staff Data	Financial data	Data warehouse	Research Data
Data Owner	Registrar	HR Director	Accounts	IT Director	Principal Investigator

An inventory will be maintained of all the University's major electronic information assets and the ownership of each asset will be clearly stated. Within the information inventory, each information asset will be classified according to sensitivity and criticality.

Sensitivity has three categories:

a. Public data
b. Data for Internal Use Only
c. Confidential data (including Personal Data and Sensitive Personal Data)

4.3. The Data Custodian

In many cases data will be entrusted to an individual or a department/school/ college/administrative unit/research unit (e.g. IT Services) for the purposes of storage and/or processing in which case they take on the responsibilities of the Data Custodian. This relationship between owner and custodian is often managed by a contract or service level agreement which clarifies specific responsibilities for each party, typical Data Custodian responsibilities include:

a. Maintaining the integrity and confidentiality of the data entrusted to them.

b. Ensuring that access to the data is restricted to those individuals authorized by the data owner.
c. Ensuring that processes undertaken on the data have been authorized by the data owner.
d. Having adequate backup and recovery procedures in place for the data, taking into account the sensitivity and criticality of the data as characterized by the Data Owner.
e. Providing any information necessary for the Data Owner to fulfil their responsibilities.

4.4. The Data Users

Anyone using or processing University Data must ensure that they do so in a manner that safeguards and protects the integrity, confidentiality and availability of the data at all times. They must comply with the relevant policies of the University (as may be amended from time to time) and with all applicable legal requirements, particularly in relation to data protection and copyright. The data should only be used for the purposes approved by the data owner.

a. Data Users are responsible for protecting their access privileges – Usernames and Passwords for University Systems should not be shared
b. Data generated from central systems that cannot readily be accessed externally, e.g. DMIS, ITS, and HRIS etc. should not be removed from campus without first seeking permission from the Data Owner. Data from these systems is both personal and sensitive so care should be taken when looking to access the information externally.
c. Users should be especially vigilant in complying with this policy when transferring data to mobile equipment such as laptops, tablet devices, phones, USB memory sticks, PDAs, DVDs etc., as they have a greater risk of being lost or stolen.

    a. Anyone accessing information systems remotely to support the business activities of the University must be authorized to do so by the Data Owner of this data.

d. (Permission can be implied given the fact that the system allows the Data User to log in remotely) The strategic importance and sensitivity of the data being accessed needs to be considered and common sense should be used in these situations.

e. Removal off-site of Confidential Data must be properly authorised by the Data Owner. The potential fallout from the theft or loss of said Confidential Data should be considered by both the Data User and Data Owner before removing the data off-site. If necessary, the Data Custodian (e.g., IT Services) can be consulted to ensure all possible safe guards are being used e.g. laptop encryption.

f. Confidential Data or information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured throughout the transfer.

g. Unsolicited electronic mail (aka SPAM) should not be acted upon or forwarded.

h. Email addresses should be checked carefully prior to dispatch to avoid sending information to unintended users.

    a. Where the information contains data of a personal nature, extra vigilance is required. While it is acknowledged some users will need to process (including transmit) personal data as part of their job, all Data Users are required to comply with standard Data Protection Policy.

4.5. Storage Media

Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved. IT Services will advise Data Owners and Data Users as to the appropriate media type.

4.6. Disposing of equipment/storage media

When permanently disposing of equipment containing storage media, all Confidential Data and licensed software must be irretrievably deleted before the equipment is moved off-site.

Any third party used for external disposal of the University's obsolete data-bearing equipment must be able to demonstrate compliance with the University's information security policies. Where appropriate and/or where the data being disposed of contains Confidential Data, as categorised by the Data Owner, the third party will enter into a service level agreement which documents the performance expected and the redress available in case of non-compliance and, where it contains personal data, the data protection contractual commitments required to be given to the University by law.

4.7. Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the IT department. On receipt of notice (or where the University otherwise becomes aware) of any suspected breach of this Policy, the University reserves the right to suspend a user's access to University's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the University's disciplinary procedures.

4.8. Revisions to Policy

The University reserves the right at any time to revise the terms of this Policy. Any such revisions will be noted in the revision history of the policy, which are available on the MRIU website and by continuing to use the University's IT Resources following any update it is considered acceptance on the revised terms of this Policy.

In case of any queries in relation to this policy, please contact: General Manager IT.

5. EXIGENCY, IF ANY

Notwithstanding anything stated in this Policy and Procedures, for any unforeseen issues arising, and not covered by this Policy and Procedures, or in the event of differences of interpretation, the Vice-Chancellor may take a decision, after obtaining if necessary the opinion/advice of a Committee constituted for this purpose. The decision of the Vice-Chancellor shall be final.