Physical and Information Security Policy

MSRUAS/REG/PIS POL/2014-15

ज्ञानं विज्ञानं च भक्तिसहितं

Pro Vice Chancellor
M.S. Ramaiah University of Applied Sciences
Bangalore - 560 054.

Registrar
M.S. Ramaiah University of Applied Sciences
Bangalore - 560 054

M. S. Ramaiah University of Applied Sciences
University House, New BEL Road, MSR Nagar, Bangalore – 560 054
www.msruas.ac.in

This Policy entitled "Physical and Information Security"

is applicable to all personnel and equipment on campus of MSRUAS

from the Academic Year 2014-15

(As per the SRAs of the respective Faculty)

Pro Vice Chancellor
M.S. Ramaiah University of Applied Sciences
Bangalore - 560 054.

Registrar
M.S. Ramaiah University of Applied Sciences
Bangalore - 560 054

Table of Contents

A. Physical and Information Security Policy

A.1 Preamble

Security at Higher Education Institutions is crucial for ensuring the safety of students, staff, visitors, protecting valuable assets, sensitive data including student records and research data, intellectual property, maintaining compliance with laws and regulations, and preserving the institutions' reputation. A well-secured and safe campus contributes significantly to the overall positive learning and working experience within the University community. It is important for institutions to review security periodically and to adapt to evolving threats, and technologies. Additionally, it is necessary to ensure that all the members are aware of and trained in effective security management.

MSRUAS has recognized that physical security is critically important to creating a safer environment for personnel, and significant physical assets, sensitive digital information, by preventing unauthorized access or theft. MSRUAS has acknowledged that measures such as well-lit pathways, presence of security personnel, installation of features such as firewalls, intrusion detection, antivirus and anti-malware, secure Wi-Fi networks, and the installation of CCTV cameras deter criminal activities like theft, assault, unauthorized access, and vandalism, contributing positively to the reputation of the University.

A.2 Scope of the Policy:

The security policy of MSRUAS covers all personnel, physical facilities, and equipment and seeks to formalize an organized and consistent approach in both the campuses without intending to impede upon any regular University activities.

This security policy covers the safety of the following"

- Personnel – Students, faculty and Staff, and visitors
- Buildings and Equipment
- Information or Cyber Security

For details related to security of Information and Communication Technology and related issues, the ICT Policy contained in the Chapter 12 of MSRUAS Employment Regulations may be referred to.

A.3 Objective

MSRUAS, with a view to providing security and safety to all campus residents including personnel, physical asset, information, and data of the University, has framed the following objectives:

1. To be compliant with regulatory authority requirements related to safety and security of Buildings and Equipment, Personnel, and Information.
2. To form a committee for sensitizing, overseeing, and investigating safety and security issues of MSRUAS
3. To frame security processes and implement them across institutions to reduce risk, respond faster to incidents, limit exposure to liability, and reduce financial losses.
4. To Regulate movement of personnel and traffic inside the campus.
5. To ensure peace and harmony in the campus always by maintenance of law and order.
6. To investigate unusual occurrences on the campus and to report the same to higher authorities.

A.4 Rules and Regulations for Ensuring Safety and Security on Campus

MSRUAS shall create a secure environment that promotes learning, research, and collaboration while safeguarding the well-being and information on campus. MSRUAS shall address evolving threats and maintain a high level of safety and security.

A.5 Safety and Security – Initiatives and Activities

1. With respect to safety and security of Personnel, the following shall be done:
    i. Develop and implement a system for identifying and verifying individuals accessing the campus, including students, faculty, staff, and visitors.
    ii. Establish protocols for registering and monitoring visitors.
    iii. Maintain updated emergency contact information.

iv. Conduct regular safety training sessions and emergency drills for personnel to make them aware of procedures and practices.

2. For Facility and Equipment Security, the initiatives shall be to:

i. Prepare an SOP addressing safety and security of Facilities and Equipment on Campus.

ii. Ensure all buildings and walkways are well lit and security cameras are installed at strategic locations to monitor and deter potential threats.

iii. Restrict access through usage of electronic access cards or biometric systems (wherever possible) to sensitive areas such as laboratories, data centers, and storage facilities.

iv. Conduct routine inspections of facilities and equipment to identify and address security weaknesses promptly.

v. Maintain inventory of equipment and assets and shall implement a system of tracking their location and usage.

3. Information Security shall be addressed as follows:

i. Encrypt sensitive information, both in transit and at rest, to protect it from unauthorized access or inception.

ii. Limit access to confidential data and shall provide role based accessed control.

iii. Establish protocols for the secure disposal of sensitive e-copies and printed documents and electronic devices.

iv. Develop a clear incident response plan handling data breach or security incidents.

4. Campus Safety shall be addressed as follows:

i. Ensure well-lit pathways and clear visibility across campus to deter abnormal activities.

ii. Develop and implement an effective emergency alert system to quickly disseminate information to the campus community during emergencies.

iii. Employ trained security personnel to patrol the campus and respond to security concerns promptly.

iv. Foster a cooperative relationship with local law enforcement agencies for mutual support during emergencies and security incidents.

5. Compliance and Reporting shall be address as follows:

i. Review and update relevant laws and regulations related to safety and security, and data protection.

ii. Provide awareness to all key personnel so that they shall adhere to and be compliant with the regulatory requirements.

iii. Establish a fool proof process for reporting security incidents and encourage all personnel to report any deviations.

6. Cybersecurity shall be addressed as follows:

i. Implement robust cybersecurity measures to protect the institution's network infrastructure, including firewalls, intrusion detection systems, and regular security audits.

ii. Provide cybersecurity awareness training to staff and students, educating them about security and safe online behavior.

iii. Regularly update software, applications, and security systems to address any form of weaknesses or liabilities.

7. Continuous Improvement shall be address as follows:

i. Conduct regular security audits and assessments to identify areas for improvement and address emerging security challenges.

ii. Develop and implement a feedback system for campus community to report to security concerns and suggestions for improvement