IT and Surveillance Policy

Internal Quality Assurance Cell

RAMA DEVI WOMEN'S UNIVERSITY

Vidya Vihar, Bhubaneswar-751022, Odisha

E-mail: iqac@rdwu.ac.in, Website: https://rdwu.ac.in

Director IQAC
Rama Devi Women's University
Bhubaneswar

Registrar
RD Women's University
Bhubaneswar

1. **Vision**

   Providing state of the art for Information Technology (IT) infrastructure and make all necessary content and services towards IT enabled.

2. **Mission**

   i. To update and upgrade the IT infrastructure regularly and remain at the cutting edge of Technology.

   ii. To conform to the legalized use of software systems and applications.

   iii. To ensure secure and robust IT infrastructure that can support teaching-learning, research and smooth administration.

3. **Objectives of the Policy**

   i. IT Policy of Rama Devi Women's University (RDWU) aims at providing the best state of the art IT resources to its stake holders on campus. The stake holders on campus which includes:

   - Students: UG, PG, and Research Scholars (Ph.D.)
   - Employees (All staffs including Teaching, Non-teaching, Visiting, Guest etc.)

   The IT Resources includes:

   - Desktop / laptops / server computing facility
   - Documentation facility (Printers/Scanners)
   - Power back-up devices
   - Access through Firewall
   - Internet Access
   - Bio-metric devices
   - Network Devices
   - Data Storage devices
   - Smart Class room devices
   - Surveillance camera devices

   ii. Computerization of administrative procedures and digitalization of data for ease of access and organization of information at all level with due protocols in place.

   iii. Providing continuous availability of high-speed data to all the stake holders.

   iv. Ensure use of licensed software applications and encourage the use of open-source software wherever possible.

   v. In line with the University's policy, provide all the IT resources totally free of cost to all stakeholders.

   vi. Recommend the adoption of cloud computing, wherever possible, to reduce dependence on physical hardware and take benefit of efficient use of computing.

vii. Strategic planning for IT infrastructure up gradation to stay abreast of the times and obsolescence remediation for safe electronic waste disposal.

4. Establishment and Maintenance Mechanism for the IT Infrastructure

a) The IT infrastructure at RDWU is to be established conforming to the existing IT infrastructure and information security standards.

b) The establishment, expansion and maintenance of IT infrastructure is to be carried out by the Computer Science department with the approval of university administration.

c) Procurement of hardware devices and software are to be procured using the recommended/applicable procurement rules of the University.

d) The IT support requirements of all departments of the University are to be routed through the IT cell to the University administration for necessary action.

e) All aspects of IT enabled services to be supported by Computer Science Department.

f) All aspects of IT enabled services to be properly documented.

g) The examinations related IT infrastructure is to be maintained separately from the other infrastructure so as to maintain confidentiality.

5. Implementation and Adherence to the Policy

University IT policy maintain certain protocols and precautions while getting IT resources and peripherals installed.

6. IT Resource User

The following Stake holders of the University are provided with computer facility. In this case, computer is installed and is primarily used by.

- Students Research Scholars
- Employees
- Faculty
- Administrative Staff (Non-Technical / Technical)

With respect to Internet facility, all the stakeholders of the University are provided with a unique user id and password for each academic building. This enables the University to trace academic building internet usage.

7. Hardware Purchase and Warranty

a) All the IT Resources purchased by any Section/Department/Project should preferably be with minimum 2-year on-site comprehensive manufacturer warranty.

b) After the expiry of warranty, IT Resources should be under annual maintenance contract.

c) Desktop, Laptops and Servers, maintenance should include OS re-installation and checking virus related problems.

8. Power back-up Connection

a) Uninterrupted regulated power supply will be provided to all IT resources. For long power outages a standby generator shall be made available.

b) All the IT resource should be connected to the electrical point strictly through UPS only.

c) Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging.

d) UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

9. Software Purchase

Only licensed software, both systems and applications, is used within the University. Respecting the antipiracy laws of the country, RDWU IT policy does not allow any pirated/unauthorized software installation in the University owned computers and the computers connected to the University campus network.

10. Network

Access to network resources is controlled by firewall authentication. Network connectivity provided throughout the University spread over the campus through an authenticated network access connection is governed under the IT Policy.

Any IP base device like smart TV, bio metric devices, Surveillance camera device, and Video conferencing device, to be install at any location, will be provided its unique IP Address based on its location and the available port. University uses Wi-Fi environments for quickly accessing the Internet services.

11. Internet

It is the responsibility of the stakeholders to access Internet in the ethical and legitimate manner. Stakeholders should keep in mind that the Internet facility should be used only for official and academic purposes. Users should avoid accessing non-SSL certificated Websites which are prone to infected with virus, malware, adware or expose vulnerability.

Usage monitoring, URL filters and gateway endpoint firewalls are used to check Internet misuse. Guest authentication id and password should be provided by respective department heads to the guest faculty and invitees for accessing Internet facility when they visit the campus for teaching and research purposes.

The IT policy ensures that Endpoint Protection and Network Security system is used to filter out non-academic blogs, Websites, social networking sites, non-academic blogs, video steaming site unsolicited or obscene sites, gaming sites and some shopping/multimedia streaming sites are blocked at firewall level to give a better ambience and conducive environment for academic progress.

The IT policy allocates 1 GBps NKN bandwidth and this bandwidth, with its associated services, is made available to the campuses over VPN. To ensure equity in Internet usage and prevent excessive usage by individuals, per day Internet usage quota is in place.

12. WIFI

Besides speed wired connection, Wi-Fi facility is implemented in all buildings and locations of the University. Personal Wi-Fi access devices are not allowed; as such devices may cause disturbance in IP allotment and security threat to University's Network. If found the personal devices will be confiscated.

13. Institute E-mail Account

In an effort to increase the efficient distribution of critical information, Faculty (Teaching, Non-Teaching) and administrative staff are provided with institute e-mail services, for formal communication and for academic & other official purposes.

The University provides email (@rdwu.ac.in) to the faculty and administrative staff. User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account. At end of tenure of the stakeholders mentioned above, the email id rights provided will be revoked and deleted for eternity.

14. Network Security

Campus LANs should be protected from public Internet with unified threat management boxes with enterprise level Firewall. The University will use an active and updated, Endpoint Protection and Network Security for the following purposes:

a) Individual user authentication for Internet access

b) Intrusion detection and prevention (Firewall)

c) Gateway malware detection

d) URL filtering based on use case profiles

e) Traffic and usage monitoring and reporting

f) Bandwidth management

15. Video Surveillance

The Surveillance system in the campuses comprises:

a) Fixed position cameras

b) Pan Tilt and Zoom cameras

c) Monitors

d) Digital recorders

Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings, examination rooms. Its mandatory that no

camera will be hidden from public view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

The Surveillance system's primary purpose is

a) Reducing the threat of crime

b) Protecting Universities premises

c) Helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy.

Images will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

16. IT Obsolescence remediation

Periodically the IT team of the campus will perform an IT audit and recommend disposal of IT resources. The disposal will depend on

a) end-of-life of the resource

b) replacement parts not available by vendors

c) availability of better resource and technology

d) economically not feasible to take up repair or replacement option

e) All concerned department Heads are asked to initiate the process of obsolescence removal and maintained a log book.

The IT policy mandates that the process of obsolescence removal should be conducive to the environment and also cost effective.

***