SYSTEM ADMINISTRATION AND CYBER SECURITY POLICY

[Document subtitle]

FEBRUARY 27, 2025

DR. C.V. RAMAN UNIVERSITY, KHAMDWA, MP
BALKHANDSURA, Post Chhegaon Makhan, Indore Road, Khandwa

Policy Research Wing, Vice Chancellor' Secretariate, CVRUK

System Administration and Cyber Security Policy

1. PURPOSE

This Cyber Security Policy outlines the guidelines and provisions for preserving the security of the university's data and technology infrastructure. As digital dependency grows, so does the risk of cyber threats, including data breaches, financial fraud, and reputational damage. A cyber-attack can compromise university operations, violate legal obligations, and erode trust with students, faculty, and partners. This policy establishes preventive measures to safeguard sensitive information and mitigate cyber security risks.

2. SCOPE

This policy applies to all university employees, faculty, contractors, students, and any individual granted permanent or temporary access to university systems, hardware, or networks.

3. POLICY ELEMENTS

3.1 Confidential Data

Confidential data includes any information whose unauthorized access, disclosure, modification, or deletion could cause severe harm to the university and its stakeholders. Examples include:

- Unpublished financial information
- Credit card details
- Data of students, faculty, partners, or vendors
- Human resource records
- Research and intellectual property data
- Examination and Database data.

All employees and authorized users are responsible for securing confidential data.

3.2 Device and Network Security

- Employees should only access university emails and systems on university-issued devices.
- University devices must not be used for accessing personal emails or accounts.
- Personal and university-issued devices should be kept secure at all times.
- Secure and private networks should be used to access university system.
- The university opts for a premium subscription to E-Scan Bot Security.

4. SECURITY MEASURES

4.1 General Cyber Security Practices

- Use strong passwords (at least 12 characters, including uppercase and lowercase letters, numbers, and symbols).
- Avoid clicking on unknown email links or attachments.
- Be cautious of click bait, phishing emails, or fraudulent websites.
- Keep antivirus software updated.
- Never leave devices unattended in public areas.
- Do not share personal or confidential information via email, phone, or text.
- Install security updates for browsers and operating systems as soon as they are available.
- Log in to university accounts only through secure, encrypted connections.
- Avoid using public Wi-Fi for university-related work.

4.2 Password Management

- Passwords must be complex and unique for each account.
- Avoid reusing old passwords.
- Store passwords securely (preferably in an encrypted password manager).
- Change passwords every 30 days.
- Exchange credentials only when necessary and via secure channels.

4.3 Secure Data Transfer

- Avoid transferring sensitive data unless absolutely necessary.
- Encrypt sensitive data before sharing.
- Use only university-approved file-sharing platforms.
- Ensure recipients of confidential data are authorized and follow security protocols.
- Store sensitive data in secured, access-controlled drives.

4.4 Reporting Security Incidents

- Employees must report suspicious emails, phishing attempts, or suspected data breaches immediately to the IT security team.
- The IT team will investigate and, if necessary, issue security alerts to all users.
- Any security compromise must be documented, assessed, and rectified promptly.

5. SYSTEM ADMINISTRATOR RESPONSIBILITIES

System administrators must:

- Install and maintain firewalls, anti-malware software, and access authentication systems.
- Conduct regular security audits and vulnerability assessments.
- Organize mandatory cyber security training for all employees.
- Keep employees informed of emerging cyber threats and security best practices.
- Investigate and mitigate security breaches effectively.

6. REMOTE WORK SECURITY GUIDELINES

Employees working remotely must comply with all security policies, including:

- Using only university-authorized devices and VPNs for remote access.
- Ensuring a secure work environment free from unauthorized individuals.
- Regularly updating security software and system patches.

7. COMPLIANCE AND DISCIPLINARY ACTIONS

All employees and authorized users must adhere to this cyber security policy. Failure to comply will result in disciplinary action, based on the severity of the security breach:
(a) **First-time, unintentional breaches**: Verbal or written warning, up to termination depending on the severity.
(b) **Intentional, repeated, or large-scale breaches**: Severe disciplinary measures, including legal actions or termination.
Each case will be assessed individually.

8. DATA SECURITY COMMITMENT

Every member of the university community shares responsibility for securing sensitive data. Trust in our digital infrastructure depends on vigilance, proactive security measures, and adherence to this policy.

9. DISCLAIMER

This document is intended for internal reference and does not constitute a legally binding agreement. Dr. C. V. Raman University, Khandwa, does not assume legal liability for its application. This policy may be revised periodically to align with evolving cyber security standards and regulatory requirements.

Cyber Policy

1. Introduction

The Cyber Policy of Dr. C.V. Raman University, Khandwa, aims to establish a legal framework for electronic transactions, data protection, and cybersecurity in compliance with prevailing laws and regulations. This policy outlines guidelines for addressing cyber-related issues such as cybercrime, data privacy, intellectual property rights, social media governance, and responsible digital platform usage by students, faculty, and staff.

This policy is based on the provisions of the **Information Technology Act, 2000 (IT Act, India), the IT (Amendment) Act, 2008**, and other relevant laws such as the **General Data Protection Regulation (GDPR)** to address evolving challenges in the digital ecosystem.

2. Key Aspects of Cyber Law in the University Context

I. Cybercrime and Cyber security

The university enforces cyber laws to safeguard its digital systems from hacking, data breaches, and other cyber security threats.

II. Privacy Protection

The university ensures compliance with privacy protection laws, including the **IT Act, 2000, and GDPR**. The personal data of students, faculty, and stakeholders must be protected, and explicit consent must be obtained for data collection and processing.

III. Intellectual Property Rights

All content shared on university platforms must comply with intellectual property laws. Unauthorized use or distribution of copyrighted materials is prohibited. Ethical and lawful use of digital platforms must be upheld.

IV. Fake News and Disinformation

The dissemination of false information or disinformation on university-affiliated platforms is strictly prohibited. The university will implement preventive measures to curb misleading information.

3. Scope of the Policy

This policy applies to:

- Students
- Faculty and staff
- Administrative personnel and stakeholders
- Any third party engaging with the university's digital systems or platforms

4. Policy Guidelines

4.1 Cybercrime

- Identity theft, impersonation, and fake profiles of any university member are prohibited.
- Cyberbullying, online harassment, and stalking will lead to disciplinary action.

4.2 Cyber Law Policies Related to Social Media Use

1. **Identity Hacking and Fake Profiles** – Impersonation on digital platforms is a punishable cybercrime.
2. **Cyberbullying and Harassment** – Offensive or defamatory language online is prohibited.
3. **Sharing of Photographs and Content** – Permission must be obtained before sharing media captured on university premises.
4. **Prohibition on Photographing in Restricted Areas** – Capturing media in sensitive areas such as washrooms and classrooms is forbidden.
5. **Defamation** – Spreading false or offensive content about individuals will result in disciplinary action.
6. **Violation of Privacy** – Sharing private images or content without consent is strictly prohibited.
7. **Unauthorized Access and Hacking** – Any form of hacking or unauthorized access to university systems is punishable.
8. **Plagiarism** – Unauthorized use of intellectual property without attribution will face strict action.
9. **Misrepresentation** – Falsifying identities or credentials online is a violation of policy and cyber law.
10. **Fake News and Disinformation** – Spreading misleading information on university-affiliated platforms is prohibited.

5. Enforcement of Cyber Law Policies

Institutional Structures

The university's **IT Department, Administration, and Disciplinary Committees** will oversee policy enforcement.

Security Practices

- Regular audits and security checks will be conducted.
- All digital transactions and communications involving university data will be monitored.

Consequences of Violations

Violations may result in warnings, suspension of digital privileges, or legal action based on severity.

6. Disciplinary Measures

Violations may result in:

1. **Warning or Counseling** – For minor infractions.
2. **Suspension or Expulsion** – For severe violations by students.
3. **Termination or Legal Action** – For employees or external stakeholders involved in unlawful activities.

7. Responsibilities for Social Media Accounts

- Official university social media accounts will be managed by designated personnel.
- Students and staff must ensure their personal social media use does not harm the university's reputation.

8. Conclusion

This policy aims to ensure a safe, ethical, and lawful digital environment at **Dr. C.V. Raman University, Khandwa**. Regular awareness programs and grievance redressal mechanisms will be implemented to uphold compliance.

Note: This policy will be periodically reviewed to align with emerging cyber laws and challenges.

9. Incident Reporting and Response

I. Reporting Mechanism

- Cyber incidents can be reported to the **university's Cyber Cell Helpdesk** via email, phone, or in-person.
- Anonymous reporting is allowed for sensitive cases.

II. Investigation Process

- Incidents will be investigated by the **university's Cyber Cell** in collaboration with IT professionals.
- Cases involving legal breaches will be escalated to law enforcement.

III. Resolution

- Actions may include warnings, disciplinary action, or legal proceedings, depending on severity.

10. Training and Awareness

The university will conduct:

1. **Cybersecurity Workshops** – Training on phishing prevention, password security, and safe online practices.
2. **Guest Lectures** – Sessions by legal and cybersecurity experts.
3. **Digital Literacy Campaigns** – Awareness programs on privacy laws, intellectual property rights, and cyber ethics.

11. University Social Media Accounts: Best Practices and Code of Conduct

Content Management

- All posts on official social media must align with university values and policies.
- Content must be **accurate, verified, and plagiarism-free**.

Access and Authorization

- Only designated personnel may manage official accounts.
- Account credentials must be safeguarded against unauthorized access.

Prohibited Activities

- Posting unverified or offensive content.
- Engaging in online disputes that may harm the university's reputation.

Monitoring

- A dedicated team will oversee compliance with social media guidelines.

12. Special Provisions for Students

Social Media Conduct

- Students must not defame the university, staff, or peers.
- Discriminatory or inciteful content will lead to disciplinary action.

Content Usage

- Written permission is required before using the university's name, logo, or event details online.

Cyber bullying

- Trolling, body shaming, or spreading false rumors will be investigated and penalized.

13. Grievance Redressal Mechanism

1. **Cyber Cell Team** – Comprising IT specialists, legal advisors, and student representatives.
2. **Support System** – Psychological counseling services for cyberbullying victims.
3. **Resolution Timeline** – Complaints will be addressed within **24 hours** and resolved within **15 working days**.

14. Compliance with Legal Standards

The university ensures compliance with:

1. **Information Technology Act, 2000 (India)** – Governing all digital activities.
2. **GDPR and Privacy Laws** – For international collaborations and students.
3. **Copyright and Intellectual Property Laws** – To uphold academic integrity.

15. Penalties for Non-Compliance

For Students

- Warnings for minor infractions.
- Suspension or expulsion for repeated violations.

For Staff

- Written reprimands for minor breaches.
- Termination or legal action for severe violations.

Legal Consequences

- Cybercrime cases will be referred to law enforcement.

16. Review and Updates

This policy will be reviewed **annually** to:

1. Address emerging cybersecurity challenges.
2. Align with updates in national and international laws.
3. Enhance security practices and enforcement mechanisms.

ANNEXURE-1

SOP- Maintenance of Computers (Hardware & Software) and Networking:

Purpose: The purpose of this Standard Operating Procedure (SOP) is to form guidelines and procedures to be adopted for maintenance of computers (Hardware & Software) and networking.

Scope: This procedure is applicable for maintenance of computers in all the Departments, Sections and Computer Centre's.

Responsibility: System administrator.

Activities/ Information:

• General Procedure

• Repair Request

• Policies and Procedures

1) General Procedure:

Whenever there is a problem with computer hardware or software the respective lab-in charge/individual has to submit the repair request to the director through respective HODs.

The copy of same to be retained in the department.

Policies and Procedures:

- The repair request letter has to be signed by the concerned lab-in charge and by the HOD.
- After duly signed by the HOD and lab-in charge the repair request letter comes to Director.
- The Director will mark to the System administrator.
- System administrator will maintain a log book for repair request letter.
- Priority is assigned according to the order of entry in the log register.
- As per the order of entry in the log register, the System administrator will attend the problem.
- The request letter is seemed to be closed once the problem is solved.
- In due course of repair, if the need for purchase of spare parts arises, the request from system administrator is raised and the same is submitted to director through Registrar/ VC Office for its approval.

Guidelines for the users:

For utilization of computers, the users have to make an entry in the log register.

- The user is not allowed to plug in their external drives without prior permission.
- The respective user will be held responsible for any damage or malfunction of the computer.

- There will be no claim for loss of data saved on desktop.
- The user should not delete/uninstall any data or software.
- Only necessary documents are allowed to print on nominal charge basis.

Records to be maintained:

- Repair Request letters
- Log book containing repair request.
- User log-in registers at respective places

ANNEXURE-2

Cyber law

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books

Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

- **Cybercrime**

Cyber law applies to the internet and internet-related technologies, including cybercrime and cyber security.

- **Privacy protection**

Laws like the Information Technology Act, 2000 (IT Act India) , IT (Amendment) Act 2008 and the General Data Protection Regulation (GDPR) protect user privacy on social media.

- **Intellectual property rights**

Users must respect intellectual property rights when sharing content on social media.

- **Fake news and disinformation**

Governments are concerned about the spread of fake news and disinformation on social media.

What cyber law policies include:

- **Data protection**

  Policies that protect data from cyber threats, such as data breaches and phishing attacks.

- **Cyber security**

  Policies that help to prevent and respond to cyber threats, such as by establishing security practices and processes.

- **Information infrastructure**

  Policies that protect the infrastructure that supports the university's information systems.

- **Digital rights**
  Policies that protect the digital rights of university employees and students.

How cyber law policies are enforced:

- **Institutional structures**: Policies are enforced through a combination of institutional structures, people, and processes
- **Security practices**: Policies are enforced through security practices that apply to the design, procurement, development, and use of information resources.