MIT World Peace University

Attack Research and Documentation
Fourth Year B. Tech, Semester 8

Developing a Cybersecurity Policy and Documenting its Implementation

Lab Assignment 7

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 15

April 5, 2025

Contents

1 Purpose and Scope

1.1 Purpose

The purpose of this Cyber Security Policy is to safeguard the information assets of MIT World Peace University, ensure compliance with applicable laws and regulations (e.g., IT Act 2000), and maintain the integrity, confidentiality, and availability of data critical to the university's operations, academic integrity, and reputation.

1.2 Scope

This policy applies to all information systems, networks, and data owned or operated by MIT World Peace University, including:

- Over 1,000 dual-boot (Windows and Ubuntu) systems, 100 Macs, and smart boards with Windows installed across the campus.
- The Enterprise Resource Planning (ERP) system managing student data, developed by a third-party vendor.
- Online payment systems and all associated infrastructure.
- Systems and networks used by employees, students, contractors, and third parties across the university's extensive campus and multiple buildings.

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

The CISO is responsible for:

- Overseeing the implementation and enforcement of this security policy.
- Managing cybersecurity risks and ensuring compliance with standards such as ISO 27001 and IT Act 2000.
- Leading the incident response team and coordinating security awareness programs.
- Reporting cybersecurity status to university leadership quarterly.

2.2 System Administrators

System Administrators are responsible for:

- Maintaining the security of all systems, including dual-boot systems, Macs, and smart boards.
- Applying security patches and updates promptly to mitigate vulnerabilities.
- Monitoring systems for incidents such as keylogger installations and reporting them immediately.
- Managing access controls and ensuring Kaspersky antivirus is updated on all systems.

2.3 Employees and Users

All employees, students, and other users are responsible for:

- Adhering to this policy and reporting security incidents (e.g., theft of systems or suspicious login activity).
- Participating in mandatory cybersecurity training and protecting their credentials.
- Avoiding unsafe practices, such as logging into systems with keyloggers present, and ensuring devices are secure.

3 Risk Assessment and Management

The university will:

- Identify threats, vulnerabilities, and risks, including:
  - Physical theft of systems (e.g., laptops, desktops, or Macs).
  - Installation of keyloggers on systems used by faculty and staff.
  - Vulnerabilities in the ERP system or online payment platforms.
  - Exploitation of smart boards as potential attack vectors.
- Conduct annual risk assessments to evaluate security controls and identify emerging risks.
- Implement mitigation strategies, such as physical locks for devices and advanced endpoint protection beyond Kaspersky.

4 Access Control and Identity Management

The university will:

- Implement role-based access controls (RBAC) to limit access to systems and data (e.g., ERP student records) based on user roles.
- Enforce multifactor authentication (MFA) for all critical systems, including ERP, online payment portals, and faculty logins, to prevent unauthorized access via keyloggers.
- Require strong passwords (minimum 12 characters, mixed case, numbers, and symbols) and review access privileges quarterly.

5 Data Protection and Privacy

The university will:

- Encrypt sensitive data, including student records in the ERP system and payment details, both at rest and in transit using industry-standard algorithms.
- Define data classification standards (e.g., Public, Internal, Confidential, Restricted) to categorize university data.
- Ensure compliance with the IT Act 2000 and other relevant privacy regulations through regular audits of data handling practices.

6 Incident Response and Management

The university will:

- Establish an Incident Response Plan (IRP) with the following steps:
  1. **Preparation:** Form an incident response team and equip it with necessary tools.
  2. **Detection and Reporting:** Monitor systems and encourage users to report incidents (e.g., stolen devices or keylogger detections).
  3. **Analysis:** Investigate incidents to assess scope and impact.
  4. **Containment:** Prevent incident escalation (e.g., isolating affected systems).
  5. **Eradication:** Remove threats (e.g., keyloggers or malware).
  6. **Recovery:** Restore systems securely.
  7. **Post-Incident Review:** Document lessons learned to improve future responses.
- Conduct cybersecurity drills biannually to test the IRP's effectiveness.

7 Security Audits and Compliance

The university will:

- Conduct annual security audits by external firms and quarterly vulnerability assessments to identify weaknesses.
- Ensure compliance with ISO 27001, IT Act 2000, and other standards through documented processes and controls.
- Deploy Security Information and Event Management (SIEM) tools for continuous monitoring of systems and networks.

8 Training and Awareness

The university will:

- Conduct annual cybersecurity awareness programs for all employees and students, focusing on risks like keyloggers, phishing, and device theft.
- Integrate cybersecurity best practices into employee onboarding and student orientation, emphasizing secure login habits and physical device security.
- Run phishing simulations and distribute regular updates via email or the university intranet.

9 Third-Party Security Management

The university will:

- Assess the security posture of third-party vendors, particularly the ERP system provider, before and during engagement.
- Include cybersecurity clauses in vendor contracts, mandating encryption, regular patching, and incident reporting.
- Audit third-party vendors annually to ensure compliance with university security standards.

10 Policy Implementation Plan

10.1 Establish Governance Structure

- Appoint a CISO to lead cybersecurity efforts, reporting to the university's executive leadership.
- Define roles for system administrators, security analysts, and faculty IT liaisons across multiple buildings.
- Form a cybersecurity steering committee with representatives from IT, administration, and academic departments.

10.2 Develop Security Baseline Controls

- Establish minimum security standards, including mandatory Kaspersky updates, firewalls, and physical locks for systems.
- Configure dual-boot systems and Macs with secure boot settings and encrypted partitions.
- Secure smart boards with restricted network access and regular software updates.

10.3 Monitoring and Incident Handling

- Deploy SIEM tools to monitor over 1,000 systems and smart boards for threats like keyloggers or malware.
- Establish an incident reporting hotline and online portal for students and staff.
- Train the incident response team quarterly to handle theft, malware, and ERP breaches.

10.4 Compliance and Reporting

- Review and update the policy annually or after major incidents (e.g., widespread theft or ERP compromise).
- Conduct internal compliance audits biannually, focusing on ERP access logs and payment system security.
- Report cybersecurity metrics (e.g., incident frequency, training participation) to university leadership semiannually.

References

[1] Information Technology Act, 2000.
Government of India. Website: https://www.meity.gov.in/content/information-technology-act

[2] ISO/IEC 27001: Information Security Management.
International Organization for Standardization. Website: https://www.iso.org/isoiec-27001-information-security.html

[3] Kaspersky Endpoint Security.
Website: https://www.kaspersky.com/endpoint-security

[4] Security Information and Event Management (SIEM) Tools.
Website: https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

[5] Enterprise Resource Planning (ERP) Systems.
Website: https://www.oracle.com/erp/what-is-erp.html

[6] Cybersecurity Awareness Training.
Website: https://www.cisa.gov/cybersecurity-awareness-programs