جامعة مصر للعلوم والتكنولوجيا

Misr University for Science and Technology

NETWORK MONITORING SYSTEM POLICY
سياسة نظام مراقبة الشبكة

Document Reference	MUST-IT-NMS-POL-001
Version	1.0
Classification	Internal Use Only
Effective Date	January 2025
Review Date	January 2026
Owner	Information Technology Department
Approved By	Chief of Information Technology Department

INFORMATION TECHNOLOGY DEPARTMENT
قسم تكنولوجيا المعلومات

1. PURPOSE

This policy establishes the framework for monitoring network infrastructure at Misr University for Science and Technology (MUST). It defines the principles, responsibilities, and procedures for network monitoring activities to ensure the security, availability, integrity, and performance of university network resources.

2. SCOPE

This policy applies to:

- All network infrastructure owned or operated by MUST, including wired and wireless networks.
- All devices connected to the MUST network (university-owned and personal devices).
- All users of the MUST network including faculty, staff, students, contractors, and visitors.
- All network segments, including academic, administrative, research, and guest networks.

3. POLICY STATEMENT

MUST reserves the right to monitor all traffic passing through its network infrastructure for the purposes of security, performance management, and compliance. Network monitoring shall be conducted in accordance with applicable laws, regulations, and university policies. Users of the MUST network should have no expectation of privacy when using university network resources for non-personal purposes.

4. OBJECTIVES

The primary objectives of the Network Monitoring System (NMS) are:

- Detect and respond to security threats, intrusions, and policy violations in real time.
- Monitor network performance to ensure optimal operation and availability of services.
- Ensure compliance with applicable laws, regulations, and university policies.
- Support forensic investigation and incident response activities.
- Protect confidential, sensitive, and proprietary university data.
- Maintain accurate records of network activity for audit and compliance purposes.

5. MONITORING ACTIVITIES

5.1 Permitted Monitoring

MUST IT Department is authorized to conduct the following monitoring activities:

- Traffic analysis and packet inspection for security threat detection.
- Bandwidth utilization monitoring and capacity planning.
- Intrusion Detection and Prevention System (IDS/IPS) operations.
- Firewall logging and analysis.
- DNS query logging and analysis.
- Network device performance and availability monitoring.
- Wireless network monitoring includes rogue access point detection.
- VPN connection logging and analysis.
- Web filtering and content inspection.
- Email traffic metadata analysis (excluding content without legal authorization).

5.2 Prohibited Monitoring

The following monitoring activities are prohibited without explicit written authorization from the University President:

- Systematic decryption and reading of personal communications.
- Targeted monitoring of specific individuals based on protected characteristics.

- Sharing of monitored data with external parties without legal basis.
- Use of monitoring data for non-security or non-operational purposes.

6. DATA RETENTION

Network monitoring data shall be retained as follows:

Data Type	Retention Period	Access Level
Firewall Logs	12 Months	IT Security Team
IDS/IPS Alerts	24 Months	IT Security Team
Network Flow Data	6 Months	IT Operations
DNS Query Logs	6 Months	IT Operations
VPN Logs	12 Months	IT Security Team
Incident Reports	5 Years	IT Management
Audit Trails	3 Years	IT Security / Compliance

7. ROLES AND RESPONSIBILITIES

7.1 IT Department

- Implement, manage, and maintain the Network Monitoring System.
- Ensure monitoring tools are current, properly licensed, and securely configured.
- Respond to alerts and security incidents within defined SLA timeframes.
- Produce regular network monitoring reports for management review.
- Ensure monitoring data is protected against unauthorized access.

7.2 IT Security Team

- Define monitoring rules, thresholds, and alert criteria.
- Conduct analysis of security events and incidents.
- Maintain the IDS/IPS signature database and firewall rule sets.
- Coordinate incident response with relevant stakeholders.

7.3 Network Users

- Use network resources in compliance with this policy and all applicable university policies.
- Report suspected security incidents or unauthorized activity to the IT Help Desk.
- Refrain from attempts to circumvent network monitoring controls.

8. SECURITY CONTROLS

The Network Monitoring System shall implement the following controls:

- Role-Based Access Control (RBAC) for all monitoring systems and data.
- Multi-Factor Authentication (MFA) for access to monitoring platforms.
- Encryption of monitoring data in transit and at rest using AES-256 or equivalent.
- Tamper-evident audit logs for all access to monitoring systems.
- Regular vulnerability assessments of monitoring infrastructure.
- Physical security controls for network monitoring servers and equipment.

9. INCIDENT RESPONSE

Upon detection of a security incident through network monitoring, the following response process shall be followed:

- Detection: Automated alerts generated by monitoring systems.
- Triage: IT Security Team assesses severity within 1 hour of alert.
- Containment: Immediate steps to limit impact (within 2 hours for critical incidents).
- Investigation: Root cause analysis and forensic evidence collection.
- Eradication: Elimination of the threat from the network environment.
- Recovery: Restoration of affected services and monitoring validation.
- Lessons Learned: Post-incident review within 5 business days

10. COMPLIANCE AND ENFORCEMENT

Violations of this policy may result in:

- Temporary or permanent suspension of network access privileges.
- Disciplinary action in accordance with university HR policies.
- Academic disciplinary procedures for students.
- Legal action where violations constitute criminal offenses under Egyptian law.

This policy is reviewed annually or following significant security incidents, regulatory changes, or major changes to network infrastructure.

11. REGULATORY COMPLIANCE

This policy is designed to comply with the following frameworks and regulations:

- Egyptian Information Technology Law and cybersecurity regulations.
- ISO/IEC 27001:2022 – Information Security Management.
- ISO/IEC 27035 – Information Security Incident Management.
- NIST Cybersecurity Framework (CSF).
- University IT Acceptable Use Policy.

Official Endorsement

Chief of Information Technology Officer (CITO)

Name: _____

Signature: _____

Date: _____