MISR UNIVERSITY FOR SCIENCE AND TECHNOLOGY

MUST

POLICY ON

ANNUAL ICT SYSTEM REVIEW & UPGRADE

Information & Communication Technology Directorate

Policy Code	MUST-POL-ICT-ARU-2025
Policy Basis	Rector Regulation on ICT Governance & Digital Services
Approved By	Chief of Information Technology
Supervising Authority	Director General of Educational Technology
Implementation Scope	All Faculties and Administrative Units
Effective Date	1 September 2025
Review Cycle	Annual

Article 1 — Purpose

Misr University for Science and Technology (MUST) recognize that the reliability, security, and performance of its Information and Communication Technology (ICT) infrastructure are foundational to delivering high-quality education, advancing research, and ensuring efficient institutional administration. This Policy establishes a structured, evidence-based framework for the systematic annual review and planned upgrade of all ICT systems across the University, ensuring that technology assets remain fit for purpose, secure, and aligned with the University's strategic objectives and the evolving needs of the University Community.

This Policy is issued under the authority of the Chief Information Officer on ICT Governance and Digital Services and operates in conjunction with the University's Data Protection Policy, AI & Digital Transformation Policy, and Information Security Policy.

Article 2 — Scope of Application

2.1 Institutional Scope

This Policy applies to all ICT systems owned, operated, leased, or procured by MUST across all faculties, colleges, research centers, administrative directorates, affiliated hospitals, and any entity operating under the MUST charter, regardless of campus location or mode of operation.

2.2 Systems Covered

The Policy covers, without limitation, the following categories of ICT systems:

System Category	Examples
Network Infrastructure	Core switches, routers, firewalls, Wi-Fi access points, WAN/LAN cabling
Server & Data Centre	Physical and virtual servers, storage arrays, backup systems, UPS units
End-User Devices	Desktop PCs, laptops, tablets, printers, smart classroom equipment
Enterprise Applications	ERP, HRMS, LMS, Student Information System (SIS), finance and procurement systems

Cloud & SaaS Platforms	University-subscribed cloud services, email platforms, collaboration tools, storage solutions
Security Systems	CCTV, access control systems, intrusion detection/prevention systems, SIEM platforms
Telecommunications	IP telephony, video conferencing infrastructure, unified communications platforms
IoT & Smart Campus	IoT sensors, smart building management systems, digital signage, energy monitoring

2.3 Personal Scope

This Policy applies to all staff responsible for managing, operating, or procuring ICT systems, including: the IT Directorate, Departmental IT Coordinators, System Administrators, Procurement Officers, and all third-party vendors and contractors providing ICT services to the University.

Article 3 — Policy Objectives

- Ensure all ICT systems remain secure, performant, and operationally reliable through structured annual assessment.
- Identify and mitigate technology obsolescence risks before they impact academic, research, or administrative operations.
- Align ICT infrastructure investments with the University's Digital Transformation Roadmap and strategic priorities.
- Ensure compliance with applicable national laws, accreditation requirements, and internationally recognized ICT governance standards.
- Optimize total cost of ownership (TCO) through planned lifecycle management rather than reactive emergency replacements.
- Maintain up-to-date software, firmware, and security patches across all systems to reduce cyber risk exposure.
- Support continuity of service and minimize downtime through proactive capacity planning and upgrade scheduling.

Article 4 — Governance & Responsibilities

Role / Body	Key Responsibilities
Chief Information Technology Officer (CITO)	Overall accountability for ICT review and upgrade program; chair the ICT Review Committee; report to Rector.
ICT Review Committee (ICTRC)	Coordinate all annual review activities; evaluate system assessments; prioritize upgrade recommendations; publish the Annual ICT Review Report.
Director General of IT Infrastructure	Lead technical assessments of network, server, and data center systems; manage upgrade execution.
Director General of Educational Technology	Assess and upgrade learning management systems, smart classroom technology, and e-learning platforms.
Director General of Information Systems	Review and upgrade enterprise applications (ERP, SIS, HRMS); oversee data integrity and integration.
Information Security Officer	Conduct annual security assessments; ensure patches, vulnerability remediation, and security controls are current.
Departmental ICT Coordinators	Submit departmental ICT needs assessments; coordinate local system inventories; liaise with central IT.
Finance & Procurement Directorate	Process ICT procurement in accordance with the University Procurement Policy; manage vendor contracts.

Article 5 — Annual ICT Review Cycle

The annual ICT review shall follow a structured four-phase cycle, commencing each year on 1 October and concluding by 31 August of the following academic year:

Phase	Period	Key Activities	Responsible
1 — Inventory & Assessment	October – November	Full inventory audit of all ICT assets; performance benchmarking; age and lifecycle analysis; security vulnerability scanning; user satisfaction surveys.	ICT Coordinators + IT Directorate
2 — Analysis & Prioritization	December – January	Risk assessment of identified gaps; cost-benefit analysis; alignment with Digital Transformation Roadmap; classification of systems by urgency (Critical / High / Medium / Low).	ICTRC + CITO
3 — Planning & Budgeting	February – March	Draft Annual ICT Upgrade Plan; prepare Capital Investment Plan submission; initiate procurement processes; schedule maintenance windows; communicate to stakeholders.	CITO + Finance
4 — Implementation & Monitoring	April – August	Execute approved upgrades; conduct user acceptance testing (UAT); provide training; monitor system performance post-upgrade; document outcomes.	IT Directorate + Vendors

Article 6 — System Assessment Criteria

Each ICT system under review shall be evaluated against the following criteria to determine its upgrade priority classification:

Criterion	Assessment Questions	Weighting
Security Posture	Does the system have unpatched vulnerabilities? Is it end-of-support? Does it meet current cybersecurity standards?	30%
Performance & Reliability	Does the system meet current load and availability requirements? Are there recurring failures or downtime incidents?	20%
Age & Lifecycle Status	Is the system within its planned lifecycle? Is the vendor still providing support and updates?	15%
Compliance & Accreditation	Does the system comply with applicable data protection laws, accreditation requirements, and University policies?	15%
Strategic Alignment	Does the system support the Digital Transformation Roadmap and the University's current academic and research priorities?	10%
User Satisfaction	What is the level of end-user satisfaction? Are there persistent usability complaints or productivity impacts?	10%

Priority Classification

Priority	Score Range	Required Action
Critical	85 – 100	Immediate upgrade or replacement within the current academic year; escalation to CITO and Rector.
High	65 – 84	Upgrade scheduled within the current annual plan cycle; included in Capital Investment Plan.
Medium	40 – 64	Planned upgrade within the next 1–2 annual cycles; interim mitigation measures applied.
Low	Below 40	System adequately meets current needs; monitoring continued; scheduled for next full review.

Article 7 — Upgrade Standards & Requirements

7.1 Hardware Upgrades

- All hardware upgrades must comply with the University's approved hardware specification standards maintained by the IT Directorate.
- End-of-life hardware must be decommissioned in accordance with the University's IT Asset Disposal Policy, including secure data wiping and environmentally responsible disposal.
- New hardware acquisitions must include a minimum three-year vendor warranty and documented support commitment.
- Energy efficiency ratings must be considered in all hardware procurement decisions in line with the University's sustainability commitments.

7.2 Software & Application Upgrades

- All software must be maintained on vendor-supported versions; end-of-support software must be upgraded or replaced within the same annual cycle in which end-of-support status is identified.
- Security patches and critical updates must be applied within 72 hours of release for Critical systems, 7 days for High priority systems, and 30 days for Medium and Low priority systems.
- All major software upgrades must undergo user acceptance testing (UAT) in a staging environment before production deployment.

- Software licenses must be reviewed annually to ensure compliance with vendor terms and to optimize license utilization.

7.3 Network & Infrastructure Upgrades

- Network upgrades must maintain or improve current service level agreements (SLAs) for availability (target: 99.9% uptime for critical systems).
- All network changes must follow the University's Change Management Procedure, including pre-implementation testing, rollback plans, and post-implementation review.
- Bandwidth capacity planning must be reviewed annually to accommodate projected growth in users, devices, and data volumes.

7.4 Cloud & SaaS Services

- Annual review of all cloud subscriptions to assess value, security posture, contractual terms, and alignment with the Data Protection Policy.
- All cloud service providers must maintain a current Data Processing Agreement (DPA) with the University.
- Data residency and sovereignty requirements must be verified annually for all cloud-hosted University data.

Article 8 — ICT Asset Management & Inventory

The IT Directorate shall maintain a comprehensive, real-time University ICT Asset Register containing the following information for every asset:

- Unique asset identifier, description, and category.
- Location (building, room, department).
- Acquisition date, cost, and procurement reference.
- Current software versions and patch levels.
- Vendor support status and end-of-life date.
- Assigned custodian and departmental owner.
- Last review date and next scheduled review date.
- Current priority classification (Critical / High / Medium / Low).

The Asset Register shall be updated continuously and formally reconciled at the start of each annual review cycle. Discrepancies between the register and physical assets must be investigated and resolved within 30 days.

Article 9 — Budgeting & Procurement

9.1 Capital Investment Planning

The CITO shall submit an annual ICT Capital Investment Plan to the Finance Directorate by 1 Jule each year, based on the outputs of the assessment and analysis phases. The plan shall include:

- Itemized list of approved upgrade and replacement projects with cost estimates.
- Priority classification and justification for each project.
- Expected benefits: security improvement, performance gain, cost saving, compliance achievement.
- Proposed implementation timeline and responsible owner for each project.
- Total cost of ownership (TCO) analysis for major investments.

9.2 Procurement Requirements

- All ICT procurement above EGP 50,000 requires a formal competitive tendering process in accordance with the University Procurement Policy.
- Technical specifications for all ICT tenders must be reviewed and approved by the IT Directorate before issuance.
- Vendor selection must consider: technical compliance, security certifications, local support capability, total cost of ownership, and sustainability credentials.
- All ICT contracts must include clearly defined service level agreements (SLAs), data protection clauses, and exit provisions.

Article 10 — Security Review & Compliance

The annual ICT review shall incorporate a dedicated security assessment conducted by the Information Security Officer, comprising:

1. Vulnerability Assessment & Penetration Testing (VAPT): all externally accessible systems and critical internal systems.
2. Security Patch Audit: verification that all systems are running current, supported software versions with up-to-date patches.
3. Access Control Review: audit of user accounts, privileged access, and access control lists across all systems.
4. Backup & Recovery Testing: verification that backup systems are functional and recovery time objectives (RTOs) are being met.
5. Security Policy Compliance Audit: verification of adherence to the University's Information Security Policy across all departments.

6. Third-Party Security Review: assessment of the security posture of all external ICT service providers and cloud vendors.

Findings from the security assessment shall be incorporated into the Annual ICT Review Report and addressed within the upgrade plan according to the priority classification defined in Article 6.

Article 11 — Business Continuity & Disaster Recovery

All ICT upgrades and replacements must be planned and executed in a manner that maintains continuity of critical University services. The following requirements apply:

- Maintenance windows for critical system upgrades must be scheduled outside peak academic periods (examinations, enrolment, graduation) and communicated to affected users at least 14 days in advance.
- All major system upgrades must have a documented rollback plan tested prior to implementation.
- The Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) must be reviewed and updated as part of the annual ICT review cycle to reflect any changes in system architecture.
- Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) must be defined, documented, and tested annually for all critical ICT systems.
- Redundancy and failover capabilities must be assessed and upgraded where current arrangements do not meet defined RTOs.

Article 12 — Training & Change Management

The following training and change management requirements apply to all ICT upgrades:

- User impact assessment: all significant upgrades must include an assessment of the impact on end-users and a corresponding training plan.
- Training delivery: end-user training must be completed before the go-live date of any major system upgrade. Training materials must be made available on the University's intranet.
- IT staff upskilling: the IT Directorate must ensure technical staff receive appropriate training on all new systems and upgraded platforms within 60 days of deployment.

- Change communication: all planned system changes must be communicated to affected staff and students at least 14 days in advance through official University communication channels.
- Post-implementation support: enhanced helpdesk support must be available for a minimum of 30 days following any major system upgrade.

Article 13 — Reporting & Annual ICT Review Report

The ICTRC shall produce and publish an Annual ICT Review Report by 31 October each year, covering the preceding academic year. The report shall include:

- Executive summary of ICT system health across the University.
- Full inventory status and asset lifecycle summary.
- Summary of upgrades and replacements completed during the year, with outcomes and benefits realised.
- Security assessment findings and remediation status.
- Key performance indicators (KPIs) for ICT service availability, incident rates, and user satisfaction.
- Recommended priorities and budget requirements for the forthcoming annual cycle.
- Compliance status with this Policy and applicable regulatory requirements.

The Annual ICT Review Report shall be submitted to the CITO, the Vice-Rector for Administrative Affairs. A summary version shall be shared with all faculty deans and administrative directors.

Article 14 — Key Performance Indicators (KPIs)

KPI	Target	Measured By
Critical system availability (uptime)	≥ 99.9%	IT Monitoring Platform
Security patch compliance rate	100% within defined timelines	Patch Management System
End-of-life systems in active use	0 (zero tolerance)	Asset Register
Annual review completion on schedule	100% of phases on time	ICTRC Progress Reports

- Change communication: all planned system changes must be communicated to affected staff and students at least 14 days in advance through official University communication channels.
- Post-implementation support: enhanced helpdesk support must be available for a minimum of 30 days following any major system upgrade.

Article 13 — Reporting & Annual ICT Review Report

The ICTRC shall produce and publish an Annual ICT Review Report by 31 October each year, covering the preceding academic year. The report shall include:

- Executive summary of ICT system health across the University.
- Full inventory status and asset lifecycle summary.
- Summary of upgrades and replacements completed during the year, with outcomes and benefits realised.
- Security assessment findings and remediation status.
- Key performance indicators (KPIs) for ICT service availability, incident rates, and user satisfaction.
- Recommended priorities and budget requirements for the forthcoming annual cycle.
- Compliance status with this Policy and applicable regulatory requirements.

The Annual ICT Review Report shall be submitted to the CITO, the Vice-Rector for Administrative Affairs. A summary version shall be shared with all faculty deans and administrative directors.

Article 14 — Key Performance Indicators (KPIs)

KPI	Target	Measured By
Critical system availability (uptime)	≥ 99.9%	IT Monitoring Platform
Security patch compliance rate	100% within defined timelines	Patch Management System
End-of-life systems in active use	0 (zero tolerance)	Asset Register
Annual review completion on schedule	100% of phases on time	ICTRC Progress Reports

IT helpdesk average resolution time	≤ 4 hours (critical) / ≤ 24 hours (standard)	Helpdesk Ticketing System
User satisfaction with ICT services	≥ 80% satisfaction score	Annual User Survey
ICT Capital Plan delivered on budget	Within ±10% of approved budget	Finance Directorate
Backup & DR test success rate	100% annual test completion	IT Directorate

Article 15 — Compliance, Violations & Sanctions

All members of the University Community involved in ICT management, procurement, or operation are obliged to comply with this Policy. Non-compliance shall be addressed as follows:

Breach Type	Examples	Consequence
Minor Breach	Failure to submit departmental inventory on time; use of unsupported software without authorisation.	Written warning; mandatory compliance training; remediation required within 30 days.
Significant Breach	Procuring ICT systems without IT Directorate approval; bypassing security patch requirements.	Formal disciplinary proceedings; loss of ICT procurement authority; mandatory audit.
Serious Breach	Operating critical systems in end-of-life status causing a security incident; deliberate circumvention of review processes.	Referral to Disciplinary Board; potential contract termination; escalation to Rector.

Article 16 — Policy Review & Amendment

This Policy shall be reviewed annually by the ICTRC in conjunction with the annual ICT review cycle. An extraordinary review shall be triggered by:

- A major cybersecurity incident affecting University ICT systems.
- Significant changes in applicable Egyptian ICT or data protection legislation.
- Material changes to the University's ICT architecture or strategic direction.
- Feedback from accreditation bodies indicating policy deficiencies.

All proposed amendments shall be subject to a 14-day consultation period with faculty deans and administrative directors before submission to the Chief Information Technology Officer for approval. All Policy versions shall be archived and publicly accessible on the University Policy Portal.

Article 17 — Contact Information

Contact	Details
Policy Queries	info@must.edu.eg
IT Helpdesk	info@must.edu.eg
Security Incidents	info@must.edu.eg | Ext. 1199 (24/7)
CITO Office	IT Building, 5th Floor, Main Campus | info@must.edu.eg
Policy Portal	www.must.edu.eg/policies

Official Endorsement

Chief of Information Technology Officer (CITO)

Name: _____

Signature: _____

Date: _____