6.30 – CAMPUS DIGITAL INFRASTRUCTURE AND EQUIPMENT

Effective: May 15, 2025

Purpose: To establish guidelines and responsibilities for the development, maintenance, use, and enhancement of digital campus infrastructure and equipment at Emporia State University. The policy aims to ensure that the digital infrastructure and equipment meet the educational, research, and operational needs of the University while ensuring safety and compliance with applicable laws, regulations, and policies.

This policy outlines ESU's commitment to adopt standard methods and procedures when altering the information technology environment in order to minimize the risk of negative impacts to information and technology services offered and managed by Information Technology (IT).

Scope: This policy applies to all campus digital infrastructure and equipment on the University's campus and other owned property including digital intellectual property on premise and cloud bases. It applies to the digital infrastructure based outreach locations. It applies to all University employees, students, contractors, visitors, and third-party service providers involved in the planning, development, maintenance, or use of University digital infrastructure or facilities. Digital Infrastructure includes but is not limited to Network systems, IT systems, and related electronic and digital facilities and equipment under the purview of the Information Technology Department.

Responsible Office: Information Technology

Policy Statement: At the direction of the President and Executive Vice President of Operations and Economic Development, the Director of University Facilities bears ultimate responsibility and accountability, for all University physical infrastructure (buildings, tunnels, parking lots, sidewalks, etc.), including all owned auxiliary assets (student housing, recreational center, memorial union, athletics facilities, health and wellness center, etc.).

Scope of Authority

The CIO is responsible for all University digital infrastructure and has the authority to oversee and manage the day-to-day operations related to:

- Patching and Updates:
  - Physical and cloud-based servers.
  - Campus-wide desktop computers and University-owned software and systems.

- Network Technology:
  - Campus wireless network.
  - University firewalls, switches, and other network equipment.

- Delegation of Operational Duties:
  - While the CIO is ultimately accountable for these functions, they may delegate specific operational responsibilities at their discretion.

- Implementation:
  - The CIO is responsible for ensuring all delegated duties are conducted in a timely, secure, and efficient manner, maintaining compliance with University policies and relevant regulations.

Maintenance and Operations

The University will engage in long-term digital and facilities infrastructure planning to align with the University's strategic goals. This planning will be overseen by the University Facilities unit, in collaboration with University administration.

The allocation of space within University digital infrastructure will be determined based on institutional priorities, including academic and administrative needs.

New IT infrastructure and system upgrades must meet data security and privacy requirements, including compliance with NIST, FERPA, HIPAA (if applicable), and relevant cybersecurity standards.

The University Information Technology Department will manage allocation of digital resources, such as server capacity, storage, and bandwidth, based on institutional priorities. Including cloud storage, compute and hosted services.

In the event of emergency situations, the Information Technology Department will respond promptly to critical failures or cybersecurity incidents affecting University systems or networks, coordinating with external experts as necessary.

IT will manage digital infrastructure requests including troubleshooting through the University's IT helpdesk.

Use of Infrastructure

Access to digital resources is governed by IT, with priority given to academic and research needs Use of digital resources may not violate university policies and local ordinances or state and federal laws.

Unauthorized use of digital infrastructure is strictly prohibited. Any requests for modifications must be formally submitted to the Chief Information Officer for approval.

Safety and Security

The Information Technology Department will conduct regular security audits on digital systems to identify and address potential vulnerabilities across hardware, software, and research-related data. Additionally, the department will perform an annual physical inventory of all IT assets.

Definitions: All words and phrases shall be interpreted utilizing their plain meanings unless otherwise defined in another University or Board of Regents policy or by statute or regulation.

Digital Infrastructure – Includes IT systems, data centers, network components, cloud compute, cloud storge, cybersecurity frameworks, and digital facilities essential to University operations.

University Information Technology Department – The University unit responsible for the day-to-day maintenance, repair, and management of the University's digital infrastructure.

Procedures: All procedures linked and related to the policies above shall have the full force and effect of policy if said procedures have first been properly approved by the University's administrator in charge of Information Technology.

[Hyperlink to Information Technology procedures]

Related Policy Information: [Include here any supporting information for this policy]

History: Adopted: 05/XX/2025 [Policy approved and included in UPM as 6.30 -
Campus Digital Infrastructure and Equipment]