The University of Memphis
Campus Cyberinfrastructure Plan
Revised March 2026

Introduction

The Information Technology Services (ITS) division of the University of Memphis (UofM) provides the institution with the cyberinfrastructure (CI) planning and support services to meet the needs of a burgeoning portfolio of research activities by:

- Promoting internal partnerships among campus CI experts to engage in, and drive, new CI capabilities and approaches in support of the institution's research requirements.
- Coordinating alignment of the CI plan horizontally with other campus plans and vertically with regional and national opportunities.
- Safeguarding the sustainability of the campus cyberinfrastructure considering operational, financial, security, and technological risks.

The components of this campus cyberinfrastructure plan are:

1) The Organization
    a) The ITS Division
    b) Internal Partnerships
    c) External Partnerships
2) The Technological Elements
    a) The Network – Fiber and Electronics
    b) The Data Center and Disaster Recovery Site
3) The Safeguards
    a) Performance Monitoring
    b) Security and Data Privacy

The Organization

The organization's main components for CI include the ITS division, its internal partnerships, and its external partnerships. By promoting internal partnerships among campus-level CI experts to engage in, and drive, new CI capabilities and approaches in support of the institution's research requirements, ITS extends and strengthens the reach of its support capabilities. Through external partnerships, the university performs well beyond the extent supported by internal resources.

The ITS Division

Centralized CI support in a unified ITS division, under the division of Business and Finance, at UofM for well over a decade has established planning and services across most segments of the university. The impact of this unity on the research agenda is significant and long-lasting since investments in personnel, technologies, and strategies are mutually beneficial and sustainable.

Internal Partnerships

ITS enjoys a vibrant relationship with the campus research community through a liaison program of local support specialists, dedicated research computing personnel and resources, and the regular meeting of the Research Technology Advisory Committee (RTAC), which is a task force of the university's Research Advisory Council. RTAC considers the effects of divisional strategies for meeting needs associated with emerging research programs and offers valuable insight into the advantages and disadvantages of competing options. The committee is composed of researchers with CI experience as suppliers and users from across the campus.

The ITS Research Computing department provides support and outreach to the campus research community. Research Computing provides researchers with HPC support and collaborates with PIs on technical requirements of sponsored projects including hardware and software needs and experiment design. It also provides a forum for seminars and a symposium focusing on advanced computing topics.

UofM's cyberinfrastructure enables different types of academic and research collaborations. For example, UofM has been active in LOLA, hosting demonstrations of real-time musical performance and instruction utilizing the university's Internet2 circuit that was recently upgraded to 200Gb.

External Partnerships

Government Agencies

UofM collaborates with MS-ISAC and REN-ISAC to access threat intelligence, vulnerability notices, best practices and to facilitate information sharing and access to resources for cyber defense. These partnerships promote sector-wide cyber resilience. In cooperation with local, state, and federal law enforcement agencies and using established protocols, the UofM assists in the investigation and prosecution of cybercriminals on their attempts to exploit CI for nefarious purposes.

Cybersecurity Vendors

Mandiant and Microsoft are contracted to provide 24/7 monitoring, threat detection, and incident response services. These partnerships enable a proactive response to cyber threats. Cisco, Palo Alto, and Splunk technologies are deployed to stay up to date with the latest security technologies and solutions. Regular assessments of our technology stack and procedures are conducted to support compliance with applicable security frameworks.

KnowBe4 is contracted to provide the UofM faculty and staff with cybersecurity awareness training to promote the safety and security of the institution's digital assets. Simulated phishing campaigns are conducted annually to assess the effectiveness of training efforts.

Academic and Research Associations

UofM has been a member of Internet2 since its inception and ITS facilitates the university's partnership by participating on service advisory boards and management of infrastructure related to this key service. Internet2 operates the nation's largest and fastest, coast to coast research and education network that serves over 345 higher education institutions, 50 affiliate and government members, 46 regional and state networks, over 80,000 community anchor institutions, over 1,000

InCommon participants, over 50 industry members, and over 100 countries and research networks connections.[1]

Internet2 membership provides opportunities for the UofM to collaborate with The University of Tennessee Health Science Center and St. Jude Children's Research Hospital, the medical device industry, and Memphis hospitals. UofM provides administrative oversight and support for dedicated managed fiber circuits that connect UofM, The University of Tennessee Health Science Center, and St. Jude Children's Research Hospital, and UofM serves as the central networking hub and Internet2 gateway for these entities. Also, UofM has recently added a second 100Gb I2 circuit for redundancy.

Additionally, the UofM CI enables Internet connectivity and Internet2 access to K-12 institutions throughout the West Tennessee region. As a long-time Internet2 member, UofM has followed with interest the emerging best practices in network routing security for network operators, including route origin validation (ROV), as expressed in the Mutually Agreed Norms for Routing Security. [2]

UofM is also a long-time participant of the InCommon Federation with support for the Research and Scholarship category. Campus visitors enjoy benefits of Eduroam, and UofM researchers enjoy the same when collaborating at partner institutions. UofM meets "Baseline Expectations for Trust in Federation".[3]

UofM has experienced dramatic growth in external collaboration with other universities, community partners, and industry partners. Partnerships incubated through the UofM Research Foundation Research Park (https://www.umrfresearchpark.org) have led to collaborative efforts that underscore the need for continual CI planning.

_____

[1] Retrieved 03/03/2026 from https://internet2.edu/community/about-us/.
[2] See https://www.manrs.org.
[3] See https://spaces.at.internet2.edu/display/BE/baseline-expectations-2

The Technological Elements

ITS provides stewardship of the campus CI plan within which the proposed improvements are conceived, designed, and implemented in the context of the coherent campus-wide strategy that is integrated horizontally intra-campus and vertically with regional and national CI investments. The main technological elements composing this plan are the network, the data centers, and the disaster recovery site.

The Network – Fiber and Electronics

UofM maintains a comprehensive fiber-optic network connecting all buildings by dual paths to increase fault tolerance and throughput. The university has complemented this redundancy through the development of a distributed core architecture. With these paths added and this design implementation, all buildings are dual homed at 10Gb to at least two of the four core switches.

Approximately every 7 years, UofM undertakes a refresh of its networking hardware from the edge to the core, replacing wireless access points, distribution switches, and controllers as well as the core switches, security gateways, perimeter and internal firewalls, and routers to ensure the infrastructure remains viable for supporting critical services throughout campus locations.

We will embark on the process of making the campus network fully compliant with IPv6, planning a pilot of IPv6 in limited applications and procuring equipment, including the security gateway, firewalls, and routers. As is common practice, the university will implement the plan in two phases - first, to host both IPv4 and IPv6 to ensure that network devices may join either - and second, to permit edge devices to connect to the network through exclusive IPv6 connections. This common two-phase plan should provide a smooth transition for all devices while alerting engineers to potential obstacles.

An upcoming addition in support of research computing is the creation of a Science DMZ (Science Demilitarized Zone), which will serve as a backbone for secure access to large datasets both within and external to the UofM research community. The Science DMZ will be a dedicated network segment designed to optimize data transfer and ensure that researchers can effectively utilize data wherever it is stored. The primary goal of this endeavor is to provide researchers with the reliable and high-capacity network needed to advance discovery and innovation while maintaining the highest standards for security and data integrity. The investment in our cyberinfrastructure will expand our research capabilities and encourage collaboration across disciplines and institutions.

The Data Center and Disaster Recovery Site

The university has recently refreshed its central Data Center and Disaster Recovery site. The central Data Center and Disaster Recovery sites currently offer high-speed storage for rapid recovery of research data. ITS continues to review the feasibility of migrating its disaster recovery resources to a cloud provider disaster-recovery-as-a-service (DRaaS). Finally, the university has offered researchers cloud-based storage resources, such as Wasabi, AWS Glacier and other archive services.

Going live in January 2024, the data center houses a $1.6M high-performance computing cluster (HPC). Merged with the previous HPC, the cluster has 9000 CPUs, 45TB of RAM, 20 GPUs and

600TB of high-speed storage. Additionally, grant funding brought another $1M 96-GPU HPC cluster to the data center in the summer of 2024. Also, ITS is collaborating with leading national researchers to facilitate high-speed access to federal research computing facilities.

The Safeguards

Safeguarding the sustainability of the plan requires consideration of operational, financial, security, and technological risks.

Performance Monitoring

UofM uses commercial and open-source tools for monitoring and securing main CI components. Significant investments in SIEM, firewalls, vulnerability scanning, and performance monitoring are the cornerstones of the multi-perspective approach to ensure the availability and security of our cyberinfrastructure. The centralized nature of the cyberinfrastructure means that these tools' deployment is not divided among organizational units or unequally deployed but uniform and continuous.

Security and Data Privacy

The UofM information security program includes components that address CI risks for security and data privacy. A multi-layered approach is used to protect the CI including patch requirements, multi-factor authentication, encryption requirements, and data storage guidelines. The university has adopted NIST SP 800-171 R3 as its standard security framework, and ITS regularly assists researchers in their compliance planning and attestations. The university has also adopted NIST SP 800-223 as its standard for HPC security. All employees must complete annual IT Security Awareness Training, and the use of multi-factor authentication is required. Regular vulnerability scans are conducted to identify collaborative opportunities with the research community to strengthen CI.

These aspects of cyberinfrastructure are the focus of ITS activity and will remain a priority as research activity increases.