The University of Memphis
Campus Cyberinfrastructure Plan
Revised September 2023

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 main components of the organization for CI includes 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

In 2013, UofM centralized its CI support in a unified ITS division. Where the institution had hosted numerous support specialists, competing directions and plans, and multiple technological initiatives, the reorganization established planning and services for most segments of the university. The impact on the research agenda was significant and long lasting since investments in personnel, technologies, and strategies could be mutually beneficial and sustainable.

The University of Memphis
Campus Cyberinfrastructure Plan
Revised September 2023

Internal Partnerships

ITS enjoys a vibrant relationship with the campus research community through a liaison program of local support specialists, dedicated research computing 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 experiences as suppliers and users from across the campus. Additionally, ITS maintains a high-performance computing (HPC) advisory team consisting of key staff members from ITS and researchers who utilize the on-premises enterprise HPC service. This advisory team provides advice on HPC configurations and performance that best support the research community. Finally, in 2022, ITS created a Research Computing department to provide support and outreach to the campus research community. The ITS Research Computing department provides researchers with HPC support and collaborates with PIs on technical requirements of sponsored projects.

UofM's cyberinfrastructure enables diverse 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 upgraded to 100Gb in 2023.

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, Aruba, 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 access. Simulated phishing campaigns are conducted annually to assess the effectiveness of training efforts.

The University of Memphis
Campus Cyberinfrastructure Plan
Revised September 2023

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 330 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 serves as the central networking hub and Internet2 gateway for these entities.

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 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 09/18/2023 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 University of Memphis
Campus Cyberinfrastructure Plan
Revised September 2023

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 center, 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 the addition of these paths and the implementation of this design, all buildings are dual homed to a minimum of 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 to the fiber-optic network is the creation of a Science DMZ (Science Demilitarized Zone), which will serve as a backbone for the secure transmission of large datasets both within and external to the UofM research community. The Science DMZ will be a dedicated network segment designed to optimize the transfer of large-scale datasets and ensure that researchers can efficiently move and share data. One goal of the Science DMZ deployment 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, making over 1.5 PB available for storage. The central Data Center and Disaster Recovery sites currently offer high-speed storage for rapid recovery of research data. ITS continues to review 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 AWS Glacier and other dark archive services.

The data center houses a $1.5M high-performance computing cluster that maintains a constant, monitored 85-90% usage. Due to consistent demand growth for computing capacity, the university may add nodes to the cluster or, as it has on occasion, turn to cloud resources to meet temporary, high-intensity computing needs. Additionally, 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 the cyberinfrastructure. The centralized nature of the cyberinfrastructure means, as well, that the deployment of these tools 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 as its standard security framework and ITS regularly assists researchers in their compliance planning and attestations. All employees are required to complete annual IT Security Awareness Training, and all users are required to use multi-factor authentication. Regular vulnerability scans are conducted to identify collaborative opportunities with the research community to strengthen CI.

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