The University of Memphis
Campus Cyberinfrastructure Plan
Revised November 2021

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-level CI experts to engage in, and drive, new CI capabilities and approaches in support of the institution's research ambitions.
- Providing stewardship of the campus CI plan within which the proposed improvements are conceived, designed, and implemented in the context of a coherent campus-wide strategy that is integrated horizontally intra-campus and vertically with regional and national CI investments.
- Safeguarding the sustainability of the plan considering operational, financial, security, and technological risks.

The components of this coherent 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 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 ambitions, 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

Seven years ago, 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 coherent planning and services for all 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.

ITS also facilitates the University's partnership with Internet2. UofM has been a member of Internet2 since its inception and participates on service advisory boards and service validation programs. Internet2 operates the nation's largest and fastest, coast-to-coast research and education network that serves 319 U.S. universities, 60 government agencies, 43 regional and state education networks and through them supports more than 100,000 community anchor institutions, close to 1,000 InCommon participants, 64 leading corporations, and 70 national research and education network partners that represent more than 100 countries.

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). 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.

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 on behalf of GEANT and Internet2.

External Partnerships

UofM is a founding member of the Memphis Research Consortium (www.memphisresearch.org). The Memphis Research Consortium (MRC) promotes collaboration among The University of Memphis, The University of Tennessee Health Science Center, 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.[1]

UofM is also a long-time participant of the InCommon Federation with support for the Research and Scholarship category. Campus visitors enjoy the benefits of Eduroam, and UofM researchers enjoy the same when collaborating at partner institutions. UofM meets "Baseline Expectations for Trust in Federation".[2]

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 and the need to develop breadth as well as depth in the CI planning process.

---

[1] See https://www.manrs.org.

[2] See https://spaces.at.internet2.edu/display/BE/Baseline+Expectations+Adherence+by+Organization.

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 a 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.

UofM has undertaken a thorough refresh of its networking hardware from the edge to the core, replacing every wireless access point, distribution switch, and controller as well as the core switches, security gateways, perimeter and internal firewalls, and routers.

We have embarked on the process of making the campus network fully compliant with IPv6, running IPv6 in limited application and procuring equipment, including the security gateway, firewalls, and routers. As is common practice, the university is implementing the plan in two phases – first, to host both IPv4 and IPv6 ensuring 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.

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 Disaster Recovery site currently offers high-speed storage for rapid recovery of research data, and in the coming year the university will migrate 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 $1.2 M high-performance computing cluster that maintains a constant, monitored 80% usage. Should consistent demand grow 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.

In anticipation of the need to meet highly elastic demand, ITS has begun a thorough redesign of its CI architecture to migrate the Data Center and the DR site to the cloud. Among the CI benefits to researchers is the anticipated establishment of self-service server-based resources, eliminating the typical wait between demand and supply.

The Safeguards

Safeguarding the sustainability of the plan requires consideration of operational, financial, security, and technological risks. The mainstay of safeguards for the CI program is performance monitoring.

Performance Monitoring

UofM uses commercial and open source tools for monitoring and securing main CI components. Significant investments in Splunk, Zabbix, Nessus, Palo Alto, and Airwave are the cornerstones of a multi-perspective approach to ensuring 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 sp800-171 as its standard security framework and 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 have been the focus of division activity over the past year and will remain a priority as research activity increases.