UC SANTA BARBARA

Information Technology Services
Strategy, Academic & Research Support
4101 SAASB MC3020
Santa Barbara, CA 93106-3020
its.ucsb.edu

University of California Santa Barbara Cyberinfrastructure Plan (2024)

The core mission of the University of California Santa Barbara is to be a leading research institution that also provides a comprehensive liberal arts learning experience (UCSB Mission). To achieve that mission, UCSB must leverage technology in service of innovative teaching and groundbreaking research. In the past few decades, many research areas have achieved prominence at UCSB, even though it is a relatively young campus. Part of the success has come from the fact that faculty work collaboratively across disciplines, often changing the direction of their work quickly, without mind to administrative or other boundaries. UCSB's cyberinfrastructure has evolved within this model and in the 2024-2025 academic year, UCSB will undertake more changes to its technology landscape than at any other time in its history. Three significant initiatives are underway that will force multiply to make a whole that is greater than its substantial parts; integration and consolidation of information technology organizations on campus, a new campus technology strategic plan that will inform the institution's direction through 2028 that includes 13 new initiatives in the research domain for fiscal year 2025, and the *Secure UCSB* program, the institution's aggressive response to the University of California's Office of the President (UCOP) mandated cybersecurity enhancement for its campuses passed down to the disparate campuses in March of 2024. The latter initiative will be the cornerstone and impetus of the greatest investment the academy has put into the cyberinfrastructure for campus in its storied history as a technology and research leader.

Networking Capabilities

Local Area

Local Area networking at UCSB will see its largest migration into modernity in the coming year with *Secure UCSB*, the named response to the UCOP security mandate. The mandate prescribes its substantive changes to be completed by the end of May 2025, making it the most aggressive and demanding upgrade schedule in UCSB's history. As the campus infrastructure of networking has emerged in the past 50 years, at the home one of the four first nodes of

ARPANET to today, the shared governance culture of campus has informed a decentralized disparate collection of hardware with centralized management usually terminating at the building switch. The future state will see central network administration travel to the wall plate or wireless access point, bringing greater security controls as well as service delivery for endpoints including a standardized experience for clients that move about campus.
Once the redundant 100Gbps CENIC connection (see Metro & Wide Area) at the edge of campus passes into the university it continues at a rate of 100Gbps through the internal core. However, specific building switching at the hardware type varies widely in current state, but *Secure UCSB* will standardize the hardware layer using 1400 new Aruba 6300 & 6400 switches, mostly using the JL659a model, to bring, for the first time in the institution's history, a standard switch to all of campus. These devices will provide a uniform set of capabilities, including POE+ support for IoT and AP power and 25Gbps uplinks. The latter will be better enabled in a second phase of infrastructure upgrades to campus fiber plant. This standardization will present numerous benefits outside of a uniform hardware management console and asset catalog. One of the primary benefits to research will be the ability to further segment networks, local to use cases and populations, of which research and researchers will be a primary focus. Research areas have engaged at segmentation administered by local IT groups but will now inherit central management allowing for greater security controls. Disintermediation of interface layers will also be a target, allowing network administrators on campus to begin to relieve the stress of multiple protocols and services from the switch layer. This will allow for greater security as firewalls can now be better localized to network segments with lower overhead, as well as an increase in quality of service delivery to the endpoints of campus via services that now have headroom to operate in specialized hardware. Future state, in second and third phases of *Secure UCSB*, will see 200-400Gbps internal core rates as optics improve. For research, dedicated circuits for inter building connections for research focused properties such as the North Hall Data Center, Elings Hall, and Bren School, will see new rapid rates for storage replication and real-time access from client to server.

Metro & Wide Area

UCSB is a charter member of CENIC and acts as a host for CENIC networking in its coastal path. Established in 1997, CENIC is a nonprofit organization operating the California Research and Education Network (CalREN), a high-capacity computer network with more than 8,000 miles of optical fiber. The network serves over 20 million users across California, including the vast majority of K-20 students together with educators, researchers, and individuals at other vital public-serving institutions. Additionally, CENIC is closely involved with two important efforts to develop and expand networking capacity across the region, the nation, and the world. Pacific Wave is a wide-area distributed exchange platform that provides research and education

networks throughout the Pacific Rim and the world with access to state-of-the-art peering and exchange services, Science DMZs, software-defined exchange (SDX) and software-defined networking (SDN) capabilities. The National Research Platform (NRP) integrates Science DMZs into a high-capacity regional system that enables transfers of large scientific data sets. UCSB operates as a host for NRP with hardware supporting this effort located in the North Hall Data Center.

In addition to its participation in CENIC & CalREN, UCSB is a peer on the ESnet (Energy Sciences Network) offering faster connections for CERN data transfers. UCSB is also a Network Operator in the MANRS global initiative. This effort to enhance routing security is supported by the Global Cyber Alliance, and provides crucial fixes to reduce the most common routing threats.

Passive & Active Monitoring

SNMP monitoring for campus, both active and passive, is deployed via the Observium platform, an open source PHP tool licensed at the enterprise level for UCSB. With it, UCSB engages in netflow collection, polling all devices for port-level stats, statistics and system changes such as interface up/down, packet drops, alerts, i/o errors, etc. UCSB has multiple collectors for discovery and the RRD graphs and output are retained for up to 3 years. Observium also monitors syslog data and its uninterrupted power sources (UPS). UCSB is also increasing the use of Nessus and Trellix for its campus endpoints to mitigate cyber attacks and application and patch vulnerabilities.

IPv6 & InCommon

IPv6 is being routed on UCSB's campus in strategic pockets such as DNS, NTP, and in three subnets on campus such as Computer Science. These are used to saturate localities in need of greater addressing and multicasting. There is also a future state initiative that will begin in the Fall of 2024 that will reduce publicly facing IPv4 addressing in lieu of NAT addressing, or "10 dot" schema.

UCSB is registered with InCommon as supporting the Research and Scholarship (R&S) Entity Category and meets the InCommon Baseline Expectations for Trust in Federation.

Network and Information Security

The *Secure UCSB* program will act as an accelerator for many of the remediation areas UCSB deems important to move its cybersecurity forward. In 2024-2025, major investments and improvements in the mechanisms, administration, policies, and governance around endpoint management and protection via various platforms such as Trellix, MaaS360, JAMF, and others, will occur on campus Also, through advances in network uniformity and management, including an expansion of vision and management from the current state of core-to-switch to core-to-wall plate or access point, UCSB network administrators will be able to enable a services-to-the-endpoint model allowing for better role based onboarding and offboarding as well as opening scope for operational services to be deployed through network-borne policy. UCSB will implement a 100% compliance rate for cybersecurity training for all of its populations beginning in 2024 using its newly implemented SSO redirect to route non-compliant end users to the online training center prior to campus network access. The security team has also identified areas of need that will not be addressed by its response to the UCOP edict, and these areas include increasing staffing, redesigning organization in the campus cybersecurity office, enhancements in risk compliance toolsets, increases in governance in research security programs and teams, and efforts to acutely reduce attack surfaces through insights gleaned from internal and external penetration testing. All of these initiatives will assist UCSB in reducing its vulnerabilities and reduce the risks that can often lead to financial loss, academic disruptions, regulatory actions and fines, and reputational damage.

Three initiatives to note in the research domain for cybersecurity on campus are accelerated adoptions of NIST 800-171 standards for research security controls, increased attention to IS-3 standards to better incorporate protocols for electronic information security, and the aforementioned network segmentation benefitting both of the former programs while hardening storage, network traffic, and access control for research-specific activities.

Computational and Storage Capabilities

While the campus networking and administrative computing infrastructure are managed by the central ITS organization, research specific support is generally provided by specialized IT units, embedded in particular departments and research units. These groups operate in a federated model, and as part of the new UCSB Campus IT strategy, this federation is led by the Office of Research. Research intensive operations are directly supported in IT by several overarching groups, such as Engineering Computing Infrastructure (ECI), Life Sciences Computing Group (LSCG), Letters and Science IT (LSIT), General Research IT (GRIT), National Center for Ecological Analysis and Synthesis (NCEAS) as well as some individual departments. Several of these units operate large specialized workstation or virtual machine farms and specialized,

discipline specific storage. High Performance Computing (HPC) is operated by the Center for Scientific Computing (CSC) with both a campus available cluster, and a condo/buy-in cluster.. ITS employs a ‘research IT facilitator’ who is housed within the CSC to provide specialized programming and HPC support for researchers.

While Google Workspace storage and Box Drive storage are provided for collaborative work, the amount of storage is too low for many researchers who need to store research data. The Office of Research, as part of the new Campus IT strategy, is in the early stages of developing a plan for providing some level of faculty ‘birthright’ storage based on the existing local, low cost, research data storage and backups integrated with a collaborative ecosystem of compute infrastructure provided to researchers.

Collaboration / Outreach / Research Community

One of the research specific initiatives for FY25 in the Campus IT Strategic Plan is to create a research consultant community to support a range of research domains. This will be achieved by establishing a new position charged with creating a governance group and with leading the formation and implementation of a community of student and staff positions whose goal will be to support researchers in various ways ranging from basic introductions to research computing resources and skills to active involvement with specific research activities and projects and long term collaborations. When appropriate, this work will be partially funded by research grants and awards and, in non-engagement periods, these students and resources will be directed to tasks around the new research strategic plan and goals. A research consulting community provides benefits for a wide range of UCSB’s research population by expanding on the educational mission of UCSB, providing additional opportunities for students to gain new skills and experience, increasing opportunities for collaboration and cross-pollination, and providing opportunities for young researchers to explore alternative career paths without leaving research.

Author:
Kevin Watson, Campus IT & Data Strategist

Collaborators:
Michael Colee, Director, Research IT
Shea Lovan, Chief Technology Officer
Jackson Muhirwe, Chief Information Security Officer
Kevin Schmidt, Director of Network & Communication Services
Paul Weakliem, Co-Director Center for Scientific Computing

Key Stakeholders-
Josh Bright, Chief Information Officer
Kelly Caylor, Associate Vice Chancellor for Research