# Villanova University

# Campus Cyberinfrastructure (CI) Plan

# Revised November 2021

1. **Executive Summary**

The Villanova University (VU) 2020-2030 Strategic Plan [1] highlights the commitment to advance research and student engagement with scholarship activities. The strategic plan includes investments in research infrastructure that will improve administrative support and research computing services. This Villanova Campus Cyberinfrastructure (CI) Plan further supports the research goals of the university. Specifically, the proposed HPC cluster is a key component of VU’s robust research computing infrastructure and will significantly advance current and future research.

Villanova’s CI plan has these significant priorities:

1. Create a secure, segmented network that can be configured to ensure end-to-end performance and support data transfer requirements.
2. Implement two perfSONAR nodes to ensure network performance.
3. Expand our current College of Engineering (COE) and College of Liberal Arts & Sciences (CLAS) research computing facilities with the proposed HPC resource to support all researchers on campus and provide greater access to compute resources off-site.
4. Develop a central model for administering research computing resources to ensure reliability, accessibility, and efficiency.
5. Provide students with access to research infrastructure in support of Villanova’s commitment to offering high-impact student research opportunities.
6. Continue investment in the security of our cyberinfrastructure with appropriate controls for critical resources. Implement network segmentation to mitigate risk.
7. Enhance the Villanova relationship with InCommon to provide identity authorization as an InCommon federated entity and meet the Baseline Expectations for Trust in Federation and Research and Scholarship Entity category specifications.
8. Villanova is a member of the Mutually Agreed Norms for Routing Security (MANRS) and meets the recommended best practices.

# Security and Resilience

Villanova University has a Campus Security Awareness program that is mandated for all employees (faculty/staff) and incorporated into new employee onboarding.

The Information Security office, led by the Chief Information Security Officer (CISO), provides cybersecurity services and practices including vulnerability management, identity and access management policies, threat and risk assessment, antivirus strategies, managed detection and response, incident response, vendor security risk assessments, vendor access management, firewall policy management, process review, policy enhancements, and system and service guidance and recommendations.

The university employs an outsourced security information and event management (SIEM) service for advanced threat detection and rapid response to security incidents.

Villanova is a member of InCommon, providing certificate services and eduroam connector service. Villanova plans to provide identity authorization as an InCommon federated entity and meet the Baseline Expectations for Trust in Federation and Research and Scholarship Entity category specifications. This InCommon upgrade will enable Shibboleth authentication.

Villanova has joined the Mutually Agreed Norms for Routing Security (MANRS) community as a participant and meets the requirements that MANRS recommends.

Current security challenges related to the proposed HPC research activities include (1) security requirements of various types of research data, (2) changes to privacy regulations and compliance requirements, and (3) networking and bandwidth requirements.

# Current Campus Infrastructure

The campus technology infrastructure is an essential resource that supports all active research. Villanova University has strategically invested in the campus cyberinfrastructure to meet growing needs of the academic community.

VU has a multiyear contract with an offsite third-party data center hosting solution provider, which houses production and research systems in a Tier III facility with 24/7 managed services and N+1 fault tolerance.

VU, through its membership with Association of Independent Colleges and Universities of Pennsylvania (AICUP), is a member of the Keystone Initiative for Network Based Education and Research (KINBER), an interconnected network resource for Pennsylvania colleges and universities. KINBER is also a member of Quilt. Villanova’s partnership with KINBER provides Internet/Internet2 connectivity via PennREN. The PennREN connection is also available for direct high-speed connections to other PennREN-connected organizations via the KINBER Member Exchange. Villanova University works closely with KINBER and is guided by their best practices regarding delivering services, data management, operation support, and monitoring.

The campus data network has dual scalable 10 Gb Internet/Internet2 connectivity (burstable to 20 Gb) via PennREN. A secondary 10 Gb Internet connection via CenturyLink is available. The campus network bandwidth between all campus buildings to the core is 20 Gb/s. Redundant connections from the edge switches to the core provide a more reliable network connection and double the available bandwidth. The VU Wi-Fi network was upgraded in 2018 and is composed of 3,100 Access Points using protocol 802.1ac.

VU has a secure cyberinfrastructure that includes security architecture, SIEM service for managed detection of threats and response, antivirus strategy, mandatory security awareness program, and identity and access management. End-user authentication is required for network access. Key university router locations are backed up with uninterruptable power supplies, and most have generator backup.

Villanova is an InCommon eduroam connector institution.

**D. Sustainability and Future Cyberinfrastructure Development**

The 2020–2030 Villanova University Strategic Plan [1] includes initiatives to support faculty research and scholarship aspirations. Villanova will advance opportunities for creation of new knowledge through robust support of the research enterprise. Specific initiatives toward this end include (1) more optimized workload for research-active faculty; (2) continuing efforts to build and maintain a research infrastructure, including staffing and support commensurate with a national university; (3) institutional investment for high-potential research and scholarship; and (4) enhanced undergraduate and graduate student engagement on scholarly and research endeavors with faculty. The proposed HPC resources, therefore, are directly applicable to advancing these initiatives, and the university is committed to ensuring a sustainable HPC enterprise on campus. As part of this effort to achieve financial sustainability, the cluster will acquire income from indirect cost (IDC) return from funded projects that use the cluster, optional user fees, and condo computing.

Villanova University is committed to maintain and expand the university’s IT infrastructure to meet future needs. A sustainable, central business model for budget and administration of research computing resources will be developed that ensures ongoing operation and availability of research computational facilities and services. The HPC oversight committee will establish university-wide best practices that will improve the operation of existing HPC clusters on campus.

As part of the fourth listed strategic plan initiative above, students will be engaged within the advancement of IT infrastructure as part of this HPC initiative. First, the HPC Oversight Committee will contain a rotating student member to accomplish two goals: (1) the student will learn about the technical and non-technical intricacies of HPC management, and (2) the committee will be guaranteed the perspective of a frequent HPC user. This holistic approach will ensure that HPC management includes a diverse array of views and opinions. Second, students will be heavily engaged in the Southeastern Pennsylvania HPC Consortium as they run training sessions, present research, and help with symposium organization.