One Campus Security Posture Policy

Statement of Policy
Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations, and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective
The policy and associated guidance provide an organized approach for safe and secure network segments based on information classification.

Applicability
This policy is applicable for all WashU network segments except those designated by Office of Information Security (OIS) and WashU Information Technology Networking.

Audience
The audience for this policy is all WashU faculty, staff, and students. It also applies for all other agents of the university with access to WashU information and network for contracted services. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “WashU community”.

Roles & Responsibilities

Background
The OIS has provided security guidance to shared services to provide safe and secure computing to the community of educators, researchers, clinicians, etc. Given the multiple classifications of information within the community, how to handle it within the offered services, and safely make it available to those who need it resulted in a network restructuring known as “One Campus”.

The One Campus design presents a shift in protection responsibilities of the required and necessary controls. As upcoming threats emerge and risks are identified, the design lends itself to the applications of controls without impacting other networks that present less
risk. Information and assets are to be grouped together based on their functions and the information they use.

The recommendation to divide or segment the enterprise network into secure network segments or “Trust Zones” is a step to create a secure layered network infrastructure that is consistent with moving security controls closer to the data they are intended to protect.

The concept of Trust Zones is an IT industry, widely accepted best practice for establishing security boundaries, control points, and accountabilities. A Trust Zone is a logical entity containing one or more types of services or entities. Trust Zones group together those entities with similar security requirements and levels of risk. Further segmentation within the Zones may be supported to allow each service and businesses program the level of security isolation they require.

Multiple zones are required for the protection of IT assets and information which coincides with the different classes of information (Protected, Confidential, and Public) in which the class is used to place the information into the appropriate zone. Controls within the zones are important, since weaknesses and vulnerabilities can be exploited at each one to affect the confidentiality, integrity, or availability of the information.

**One Campus Roles and Responsibilities**

- The OIS will classify departments and schools personnel, groups, and resources into the applicable zones based on information access and usage.
- WashU Information Technology will run the discovery process to ascertain the necessary information required to classify and implement the minimal controls and access.
- WashU Information Technology and the school business unit’s IT staff will implement the minimal controls on the endpoints.
- WashU Information Technology Networking will provision the applicable access into and out of the control zones.

**Policy**

All university computing networks will be placed into the One Campus network design and meet the required minimal controls designated as High, Moderate, and Low. All other networks will be designated as untrusted.

**Exceptions**

All exceptions to this policy are to be escalated to the CIO and CISO for review and consideration of alternatives.

**Policy Compliance**

The OIS will measure the compliance to this policy through various methods, including, but not limited to - reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the OIS in advance. Non-compliance will be addressed with
management, Area Specific Compliance Office, Human Resources, or the Office of Student Conduct.

**Related Policies**
Information Classification Policy

**Reference**
System Classification Standard
Control Zone Standard
Network Security Standard
Minimal Control Zone Standard

**Policy Review**
This policy will be reviewed at a minimum every three years.

**Title:** One Campus Security Posture Policy  
**Version Number:** 1.0  
**Reference Number:** SC-01.04  
**Creation Date:** October 3, 2018  
**Approved By:** Security and Privacy Governance Committee  
**Approval Date:** November 15, 2018  
**Status:** Final  
**Scheduled Review Date:** March 1, 2022  
**Revision Date:** February 26, 2019  
**Revision Approval Date:** March 15, 2019  
**Policy Owner:** WashU Information Technology