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.

Background

The Information Security Office (ISO) 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 that 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.

Applicability

All Washington University Networks except those designated by ISO and WashU Information Technology Networking

Roles and Responsibilities

The ISO will classify departments and school 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 EUS/School 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 networks will be placed into the "One Campus" network design with the required minimal controls for control zones designated as High, Moderate and Low. All other networks will be designated as un-trusted.

Exceptions

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

Reference

Information Classification Policy
System Classification Standard
Control Zone Standards
Network Standard
Minimal Control Zone Standards

Title: One Campus Security Posture Policy
Version Number: 1.0
Creation Date: 10/03/2018
Approval Date: 11/15/2018
Applicability: WashU Networks
Reference Number: 02.10
Status: Final
Policy Owner: WashU Information Technology