College of Science Server Policy

Policy Number: COS-1003

Policy Subject: Purchasing, installing, and configuration of servers by the College of Science (COS)

Responsible Office: Associate Dean for Research, COS

Related Policies:

- University Policy 1312 Physical and Logical Access Security
- University Policy 1114 Data Stewardship

I. SCOPE

This Policy applies to all centers, institutes, and academic and operational departments and offices of the College of Science at George Mason University. The policies and procedures provided herein apply to all College of Science faculty, staff, students, visitors and contractors.

This policy provides general requirements for purchasing, installing and configuring server resources in a secure manner as well as maintaining the security integrity of the hardware and application software.

II. POLICY STATEMENT

A departmental or college IT specialist must be consulted before systems are purchased. The Office of Research Computing also must be contacted prior to any HPC or cluster purchases. The college encourages the use of centralized shared resources whenever possible to maximize the return on investment and encourage long-term sustainable HPC assets for research.

System owners and administrators must ensure servers are configured and maintained in a manner in accordance with University Policy 1312, Physical and Logical Access Security. Whenever possible servers should be located in Aquia (university supported data center) unless other adequate facilities are available. Cooling, power and physical security requirements must be addressed.

Appropriate measures must be taken when configuring and managing server based resources to ensure the confidentiality and integrity of information in accordance with University Policy 1114, Data Stewardship.

In addition to university requirements, documented use of an applicable checklist from the National Checklist Program Repository (nist.gov), CIS Benchmark (cisecurity.org) or other governing authority will be used when configuring, securing and maintaining your server. A documented configuration change history must be maintained.

After a server is fully configured, ITSO should be contacted to scan the server for vulnerabilities. Any identified known vulnerabilities will be remedied if applicable. The use of centrally administrated vulnerability scanning is required.

III. DEFINITIONS
Server: A server is a system (software and suitable computer hardware) that responds to requests across the Mason network or the Internet, if hosted off campus, to provide, or help to provide, a network service. All systems that are intentionally configured to be accessible via the internet are considered to be servers. A system may only be accessible from the university network but provides a server service and therefore is a server.

System Owner: The System Owner is the person responsible for operation and maintenance of a university IT system.

System Administrator: A System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner. Their responsibilities can include administration at the system infrastructure layer and/or system application layer. Any given system may have more than one System Administrator depending on the size and complexity of the system. The System Administrator assists with the day-to-day administration of the IT systems, and implements security controls and other requirements of the IT security program on IT systems for which the System Administrator has been assigned responsibility. System Administrators are responsible for documenting and enabling user access.

IV. RESPONSIBILITIES
Departments and administrative offices shall develop, manage and review local operating policies and procedures to create the proper security practices for the logical and physical security of information resources.

V. COMPLIANCE
Documentation supporting checklist usage and configuration changes will be maintained until the server is retired and will be made available upon request for audit purposes.

VI. REVIEW AND UPDATE
This policy will be reviewed annually in July.

VII. EFFECTIVE DATE
The policies herein are effective February 15, 2018

Approved:
Peggy Agouris
Dean, College of Science
Date approved: