COLLEGE OF SCIENCE LOGGING AND MONITORING POLICY

Policy Number: COS-1002

Policy Subject: Logging and monitoring of events on COS servers

Responsible Office: Director of I.T. and Security, College of Science

Related Policies:

- University Policy 1312 Physical and Logical Access Security
- University Policy 1305 Reporting Electronic Security Incidents

I. SCOPE

This Policy applies to all 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 is ancillary to University Policy number 1312 and governs requirements and implementation of IT system logging on COS assets. In the event that any component of this policy is found to be in conflict with University Policy, University Policy supersedes COS Policy.

II. POLICY STATEMENT

College of Science research centers, departments, and faculty employ various servers in their course of operation. While the vast majority of these systems are not critical and do not contain sensitive data, they can be targeted for use as agents in cybercrimes and present risk to the reputation and security of the University. This policy is created in order to establish logging requirements in order to:

- Centralize logging of COS servers for the forensic needs of the University.
- Establish log monitoring requirements for the identification of suspicious activities.
III. DEFINITIONS

System Administrator: Anyone who has the responsibility to maintain, configure, operate, or repair COS computing resources.

Server: A server is a system that responds to requests across the Mason network 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.

System Owner: The system owner is the ultimate responsible party for operation and maintenance of an IT system.

Electronic Security Incident: Electronic Security Incidents are activities, such as “hacking” or a compromised or abused computer, that result in damage to or misuse of the Mason network or a device connected to it. Routine detection and remediation of a “virus,” “worm,” or similar issue that has little impact on the day-to-day business of the University is not considered an Incident under this policy.

IV. RESPONSIBILITIES

The COS office of the Director I. T. and Security will maintain a central syslog server available for log forwarding from COS servers preserving all forwarded logs for 13 weeks.

For any serve space assignment request, The COS office of the Director I. T. and Security will require log forwarding to the COS log server, the installation of log review software such as logwatch, and the assignment of a responsible a system administrator for log review before approval.

The system administrator will review logs on a routine basis.

The system administrator will report Electronic Security Incidents per University Policy 1305.

V. COMPLIANCE

Failure to honor the requirements set forth in this policy may result in the revocation of serve space IP address privileges.

VI. REVIEW and UPDATE

This Policy will be reviewed annually in July.

VII. EFFECTIVE DATE

The policies herein are effective March 24, 2014

Approved:
Justin Brown
Director I.T. and Security, College of Science
Date approved: March 24 2014