OM 9.1.3 - Application Security

Scope
All Clarkson University units and employees.

Reason for Policy
Computer applications must be configured and operated in a manner that minimizes risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration destruction or other compromise of such information.

Policy Statement
Because software systems are so complex, it is common for security-related problems to be discovered only after the software has been in widespread use. The period of time between the discovery of a problem and a patch being applied is referred to as the window of vulnerability. The magnitude of risk is directly proportional to the length of the window of vulnerability. By shortening this window, we are able reduce the risk to our data. As such, it is important that all software packages be patched on a regular basis, with security patches being applied within a reasonable time after they become available.

Several applications that are deployed as University standards should have default settings. Mandatory settings for these applications are found in the Anti-Virus and Updates Policies, respectively.

Many applications make use of encryption as an additional level of security; however often times the terms and settings relating to security can be confusing. Therefore, the guidelines set forth in the Acceptable Encryption Policy should be followed whenever encryption is used.

History
September 2014
February 2018