OM 9.1.7 - Outsourcing IT Services

[ Scope ] [ Reason for Policy ] [ Policy Statement ] [ History ]

Scope

All Clarkson University units and employees.

Reason for Policy

In some cases, it may be advantageous for the University to retain an outside firm to provide professional guidance, data processing or other services to the University rather than perform these tasks in house. Such services are often referred to as Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). This policy outlines the requirements of these external agreements or contracts from an Information Security perspective.

Policy Statement

- All agreements with external entities that may be exposed to University data classified as Clarkson Private are to complete the Higher Education Cloud Vendor Assessment Tool and provide the completed document to OIT for review and approval. The HECVAT can be obtained here https://library.educause.edu/~/media/files/library/2017/5/higheredcloudvendorassesstoollite.xlsx
- In cases where external entities will only be exposed to University data classified as Clarkson Public or Clarkson Confidential, OIT must review the project scope and proposed contract language before the contract is executed. OIT will be looking for security and operational requirements in these areas:
  - Service Availability
  - Service Level Reporting, Review and Resolution
  - Security Clearance of personnel
  - Security Roles and Responsibilities
  - Information Handling and Disclosure
  - Security Training and Competency
  - Secure Operations Requirements
  - Right to Audit
  - Incident Management and Response Plan
  - Business Continuity Plan
- For implementations that include some form of login accounts used to administer or otherwise access a remote system, the Office of Information Technology must be provisioned two administrative-level accounts. These accounts will be used to enable OIT to periodically review the data being processed via the service and to perform emergency account management when needed.
- Whenever possible, a service that includes some form of login accounts should use a centralized authentication mechanism such as Google Auth, LDAP, AD FS or SAML so that user authentication is performed against a University-controlled authentication method.

History

Revision 1.0 - 02/2018