

Data Security Policy Review for Cloud Services Providers

Created by Townsend, Jeremy W, last modified on Sep. 30, 2024

University of Maryland Eastern Shore

Administrative Computing

Standard Operating Procedure

June 3, 2019

Name: Data Security Policy Review for Cloud Services Providers

Prepared By: Jerome F. Waldron

Revised:

Description:

The University of Maryland Eastern Shore is utilizing a growing number of third-party cloud-based software products. These tools are used by many administrative departments across the campus. The university is concerned about the security of all faculty, student, and staff data and reviews the data security policies annually. As new products are purchased, Information Technology requires providers to submit their data security policy.

Procedures:

1. A list of third-party cloud-based software product is maintained by the Department of Information Technology. This list is updated as new products are added or discontinued. The list contains the product name, URL, brief description, responsible department, type of data stored, and related information.
2. Vendors provide a SOC2 report or a corporate policy that states that security, availability, processing integrity, confidentiality and privacy of UMES data are insured.
3. Data security policies from each vendor are reviewed to ensure that UMES data is used for the expressed purpose of providing a service to the university. The review focuses on how UMES personally identifiable information (PII) data is collected, accessed, used, stored, backed up, and/or shared with other entities.
4. Verification links and/or documents are stored on the Information department Wiki.
5. IT will advise the UMES sponsoring department regarding the vendor's ability to meet security best practices at the time of purchase or in the event of any breach.

Review schedule:

Follow-up reviews are made every three years starting in 2019 or on the condition of a security policy update or a breach of the company.