

SECURITY DOCUMENTATION DEFINITIONS

As part of the procurement process University Technology Services (UTS) requests various types of documentation to aid in evaluating the security of a product or solution. The following documents typically provide UTS with the vast majority of information required for an assessment and are the most efficient way to initiate a review.

- Higher Education Community Vendor Assessment Toolkit (HECVAT) Full
- Service Organization Control (SOC) Type II Report
- Software Bill of Materials (SBOM)
- [OU E-MAIL SECURITY QUESTIONNAIRE](#)

As not all parties involved with a purchase may be familiar with these documents and their importance we would like to address some commonly asked questions below:

- What is the [Higher Education Community Vendor Assessment Toolkit \(HECVAT\) Full](#)?
 - The HECVAT is a questionnaire framework specifically designed for higher education to measure vendor risk. There are two versions of this document, the 'Lite' and the more comprehensive 'Full' version. Completing the HECVAT Full allows an institution to evaluate that the information, data, and cybersecurity policies are in place to protect our sensitive institutional information and constituents' PII.
- What is a [Service Organization Control \(SOC\) 2 Type II Report](#)?
 - SOC compliance and audits are intended for organizations that provide services to other organizations and involve a third-party auditor validating the service provider's controls and systems to ensure that it can provide the desired services.
- What is a Software Bill of Materials(SBOM)?
 - The software bill of materials (SBOM) lists all component parts and software dependencies used in application development and delivery.
- What is the [OU E-MAIL SECURITY QUESTIONNAIRE](#)?
 - The [OU E-MAIL SECURITY QUESTIONNAIRE](#) is applicable to vendors / services that will be using OU to communicate with OU constituents. The purpose of the document is to gather information to ensure that email is delivered in accordance with OU standards and maximizes the likelihood email will be delivered properly (e.g. not flagged as junk, phishing).
- Why are these documents requested?

- To some extent all purchases require an ongoing partnership between OU and the vendor. This relationship can be limited in scope (for example from local usernames and passwords) to complex integrations that involve interconnecting applications and networks together. In order to ensure that university policies and legal & contractual obligations are being met UTS must thoroughly vet each proposed solution to ensure it meets minimum requirements and any risks are communicated, documented, and accepted.
- Are these documents required?
 - At this time these documents are strongly desired but not required for all purchases. However, as the HECVAT can be completed as a self-assessment UTS suggests that all vendors complete this document as it demonstrates a commitment to security awareness and best practices.

IT TECHNICAL COMPLIANCE
Attachment D

After conclusion of negotiations but prior to award of a contract (and/or release of funding to procure your solution) your solution/system will be submitted to UTS (University Technology Services). UTS will review your solution against a variety of metrics including, security, accessibility, ease/ability to integrate with existing systems, etc. The supplier must agree to submit their solution and submit any requested information to assist in the review process.

The supplier should submit any of the applicable documents below and be prepared to provide additional items as requested. *Non-Disclosure agreements will be completed if required.*

- Third Party Assessments - System and Organization Controls (SOC) Type II *preferred*
- Higher Education Community Vendor Assessment Toolkit (HECVAT) Full
- Software Bill of Materials (SBoM) *preferred*
- Data Integration Guides / Architecture Diagrams
- Email Integration Guides / Architecture Diagrams
- Voluntary Product Accessibility (VPAT) statement for ADA compliance
- Single Sign On (SSO) Integration / Configuration
- Implementation Guides / Architecture Diagrams
- Data retention, destruction, and return processes
- Service Level Agreement (SLA) language
- End User License Agreement (EULA)
- Any additional documentation or items requested during the review process

If the supplier is unable to provide applicable documentation, please include the rationale in the proposal.

Please indicate any of the following types of protected data the proposed solution will have access to:

☐ Health Information ☐ Credit Card ☐ Financial Aid ☐ Student Information
☐ Regulated Data ☐ Other _____

ACKNOWLEDGMENT; This Amendment must be signed and return

Signature

Date