University of Missouri
Information Security Requirements

Vendors must demonstrate compliance with the security criteria listed below by responding in writing to every statement and question in the identified categories. Validation of the answers provided by the vendor may be conducted during the review/audit process. Any erroneous information could limit the vendor's ability to finalize implementation of a new solution or place a hold on continued use of a current solution. Vendors are expected to maintain an awareness of the laws and regulations applicable to the use of the solution in a University environment.

Data Classification

The University assigns data classification levels for all University owned or hosted IT-based systems. This system will have a DCL level of 4 . Security requirements for all DCS levels can be found at: https://www.umsystem.edu/ums/is/infosec/classification . The University of Missouri reserves the right to periodically audit any or all hardware and/or software infrastructure provided by the vendor to ensure compliance with industry standards and best practices as well as the requirements of the University's DCS. When applicable, the University of Missouri requires compliance with the Health Insurance Portability and Accountability Act (HIPAA), FERPA, GLBA, PCI specifications, and all other applicable state, local and federal laws and regulations.

The University considers security to be an ongoing responsibility and as a result, these information security criteria are subject to additions and changes without warning. When appropriate, the vendor will be expected to work in good faith with the University to maintain compliance with new laws and regulations and/or to improve the security of the solution.

Compensating Controls and Descriptions

All statements and questions below are mandatory unless they are not applicable. The vendor must clearly explain why a given question is not applicable. For all other questions, if a requirement cannot be met, the vendor still has an opportunity to meet the requirement by the use of compensating controls. Compensating controls must be described in full in the appropriate column, including a full explanation of the compensating control detailing how the control meets the intent of the original question. In some instances, the University has requested that the vendor provide a description to accompany their response to a particular statement or question below. Descriptions are requested when a "Meets or Exceeds" answer alone could be deceptive without further detail.

When more room is needed to fully explain the compensating control or provide further detail, attachments can be included so long as such attachments are labeled and cross-referenced in the "Comments or Explanations of compensating controls" column. The University has the sole right to determine if a proposed compensating control is acceptable and if the details provided describe a solution that truly meets or exceeds the University's needs.

Vendor/Product Information (MUST BE COMPLETED)

Vendor Name and Contact Information _____

Product Name and Brief Description _____

_____

Does this solution store and/or transmit any of the following types of restricted and/or highly restricted data? Check all that apply.

☐ Protected Health Information (PHI) ☐ Payment Card Industry (PCI) ☐ Gramm-Leach-Bliley Act (GLBA) ☐ Social Security Numbers (SSN) ☐ Federal Educational Rights & Privacy Act (FERPA)
☐ Biometric Data (fingerprints, handprints, etc.) ☐ Personally Identitiable Information (PII) ☐ Intellectual Property ☐ Confidential Research

Vendor represents and warrants that their responses to the above questions are accurate and that the system configuration will continue to conform to these answers unless mutually agreed upon by the University and the Vendor. Vendor further agrees to work with the University in good faith to to maintain compliance with new laws and regulations and/or to improve the security of the system.

Agreed this _____ day of _____, 20__

_____
Company Name

_____
Signer's Name and Title

_____
Signature

University of Missouri
Information Security Requirements

Requirements	Response or approved compensating control required if product falls within the specified DCS Level: https://www.umsystem.edu/ums/is/infosec/classification/	Meets	Does Not Meet	Comments/Compensating Control
1. The vendor must acknowledge and agree to allow the University, at its discretion, to inspect/assess all or portions of the proposed solution prior to placing the system into production. The University does not need the vendors "code" to perform such assessments, however, the University will use web application (IBM AppScan, HP WebInspect) and network vulnerability tools (Nessus) in coordination with the vendor's technical team when appropriate. The results of the assessment(s) will be provided to the University customer (i.e., the department) and to the vendor.	All			
1.a The vendor must agree to remediate high risk security vulnerabilities that are identified by such assessments within a reasonable time frame and at no cost to the University. Medium and low risk vulnerabilities should also be remediated but will be scheduled for remediation based on a mutually agreeable timeframe. (This applies to generally accepted security vulnerabilities within the industry, NOT changes or modifications that would be considered customer-requested improvements or functionality enhancements.)	All			
2. Upon request, details of any third party reviews related to industry or regulatory compliance must be made available for University review. Vendor MUST include third party web application and server vulnerability and/or penetration tests if available. Redacted reports are acceptable. Please check all that are available: ☐ SOC2 Report ☐ HiTrust Certification ☐ Other ☐ None available	DCL3 and DCL4			
3. Vendor must comply with applicable industry standards and best practices for system administration and application development (i.e. OWASP). Indicate which industry standards are utilized by the vendor.	All			
4. If applicable, Payment Card Industry - Data Security Standard (PCI-DSS) or Payment Data Security Standard (PA DSS) compliance is required. The vendor can comply with this item if it has attained PCI certification for the overall set of products/services being proposed or by having one or more system implementations that are currently PCI certified. Provide evidence of such certification attached to the response. If available, the vendor must provide a guide for PCI-compliant implementation of their product.	DCL4			

University of Missouri
Information Security Requirements

Requirements	Response or approved compensating control required if product falls within the specified DCS Level: https://www.umsystem.edu/ums/is/infosec/classification/	Meets	Does Not Meet	Comments/Compensating Control
Authentication, Authorization and Password Security				
1. The University requires that the vendor allow authentication to their system through existing University authentication methods. For on-campus systems, Shibboleth/SAML2.0 (preferred) or Microsoft Active Directory (AD) is required. For vendor-hosted systems, Shibboleth/SAML 2.0 (SP initiated) is required. Vendor must provide their Shibboleth/SAML 2.0 integration documentation. Please check all that are supported: ☐ Windows AD ☐ LDAP ☐ Shibboleth/SAML 2.0 ☐ Other	DCL2, DCL3 and DCL4			
2. For vendor-hosted systems that are unable to implement or are not required to use Shibboleth/SAML 2.0 (SP initiated) at the University's discretion, the vendor must meet the following University Password Standards: • Passwords requirements must be enforced and meet the University Password Standard https://www.umsystem.edu/ums/is/infosec/standards-password. • Passwords must be stored in a manner such that they are not decryptable. (This usually means a one-way hash and salt). • Password recovery mechanisms must be in place for users who forget their password. • The authentication session must be encrypted. (HTTPS for web applications). • Support for SSL v2/v3 and TLS 1.0 must be disabled. Only TLS 1.2 should be supported, 1.1 if necessary.	DCL2, DCL3 and DCL4			
Application Security				
1. The database must be segregated from front-end systems (i.e web and application servers.) Please describe how this is accomplished.	DCL3 and DCL4			
Cryptography/Encryption				
1. Except for the viewing of static Web pages, the vendor must ensure that all other transmissions to and from the system, including file transfers, data in process, authentication mechanisms, end-user and administrator access, etc. are handled via encrypted protocols.	All			
2. Any data stored at rest on a hard drive, on a file server and/or in a database MUST be encrypted or granted an exception by the appropriate Information Security Officer at https://www.umsystem.edu/ums/is/infosec/admin/	DCL4			

University of Missouri
Information Security Requirements

Requirements	Response or approved compensating control required if product falls within the specified DCS Level: https://www.umsystem.edu/ums/is/infosec/classification/	Meets	Does Not Meet	Comments/Compensating Control
Answer These Additional Questions If The Proposed Solution Will Be Vendor Hosted				
1. The vendor must immediately disable all or part of the system functionality should a security issue be identified.	All			
2. The University requires notification of actual or suspected security incidents/breaches within **24** hours of the vendor's first knowledge of such an event.	All			
3. The proposed solution must be behind a firewall to protect and limit access to the system.	DCL3 and DCL4			
4. The vendor must ensure that University of Missouri owned or provided data is segregated and protected from other customers. Please describe how this is accomplished.	All			
5. The vendor must always change vendor-supplied defaults before installing a system on the network.	All			
6. The vendor must remove or disable unnecessary default accounts before installing a system on the network.	All			
7. The vendor must prohibit group, shared, or generic accounts, passwords, or other authentication methods as follows: • Generic user IDs and accounts are disabled or removed; • Shared user IDs for system administration activities and other critical functions do not exist; and • Shared and generic user IDs are not used to administer any system component.	All			
8. The vendor must configure user password parameters to require passwords meet the following: • Minimum password length of 8 characters • Contain both alphabetic and numeric characters	All			
9. The application/system/environment must be monitored consistently (24x7) for integrity and availability. Data center is hosted by: ☐ Vendor ☐ Third party (please specify)	All			
10. The system must provide user access logs: • Will you provide on-line access to query the logs?; • If not, can you SFTP the log to our Splunk instance?; • If not, can you provide a report on a schedule or on demand?; • What security events are logged?; • How long are access and security logs retained?; • Describe backup recovery and resiliency of information system; and • Do logs contain ePHI? If yes, which identifiers are collected?	DCL3 and DCL4			