


UNIVERSITY OF MIAMI 	Information Technology	
	Security Assurance & Compliance Email: ciso@miami.edu Phone: 305-243-0281	Page 1 of 5
Document Title: IT Security Assessment Questionnaire		

Complete all *required fields* to the best of your knowledge; incomplete forms will not be reviewed.

Project Summary

Subject Matter Expert (SME) Information	
Name:	Email:
Telephone Number:	Job Title:
Project Name:	
<u>Required Field</u> <Provide Project Overview>	

Regulatory Compliance

Will the application store, process, and/or transmit any of the following regulatory compliance data:

- Protected Health Information (PHI)? e.g. HIPAA Yes No
- Credit Cardholder Data (CHD)? e.g. PCI-DSS Yes No
- Personally Identifiable Information (PII)? Yes No
- Personally Identifiable Student Education Records? e.g. FERPA Yes No
- Clinical Research Data? e.g. FDA CFR 21 Part 11 Yes No
- Federally Funded or Contracted? e.g. FISMA Yes No
- Personally Identifiable Financial Information? e.g. GLBA Yes No

Auditing and Reporting


Does the application support audit/logging capabilities to a syslog/SIEM solution? Yes No

Solution Infrastructure

Provide a data flow diagram (DFD), which includes the following information:

1. Source and Destination IPs of all hosts involved in the solution
2. Any web page URLs
3. Ports involved with the solution
4. Any encryption being used
5. Any interfaces involved
6. Any crash report/metadata

Required Field <Provide data flow diagram below (DFD) or attach as a separate document>

UNIVERSITY OF MIAMI 	Information Technology	
	Security Assurance & Compliance Email: ciso@miami.edu Phone: 305-243-0281	Page 3 of 5
Document Title: IT Security Assessment Questionnaire		

Please enumerate all data points/fields (e.g. SSN, First Name, Last Name, etc.)

<Required Field or attach as a separate document>

Data Encryption

Will the application data be encrypted at-rest using AES-128, RSA-3072, or SHA-256?

Yes No

<If No, provide compensating controls>

Will the application data be encrypted in-transit using SSL, TLS, or VPN?

Yes No


<If No, provide compensating controls>

Does the application leverage a back-end database? (Oracle, MS-SQL, MySQL, etc.)

Yes No

- If Yes, Can the database be encrypted at-rest?

Yes No

	Information Technology	
	Security Assurance & Compliance Email: ciso@miami.edu Phone: 305-243-0281	Page 4 of 5
Document Title: IT Security Assessment Questionnaire		

Support

Will the application require remote access for technical support? Yes No

Does the application use an embedded support tool that communicates in/outbound?
(e.g., GoToMyPC, Team Viewer, VNC, etc.) Yes No

<If Yes, what is the name of the support tool?>

What is the best time of the day for us to conduct periodic vulnerability scanning?

<Provide details>


Access Controls and Security

For web based solutions, can it leverage UMIT SAML based authentication? Yes No

Required Field *<If No, provide description of authentication mechanism and its security controls>*

For on-premise solutions, can it leverage Active Directory Federation Services (ADFS)? Yes No

Required Field *<If No, provide compensating controls>*

	Information Technology	
	Security Assurance & Compliance Email: ciso@miami.edu Phone: 305-243-0281	Page 5 of 5
Document Title: IT Security Assessment Questionnaire		

Cloud Specific Questions

Can you provide a third-party 3rd audit report describing the security features in place at the organization?
e.g. Service Organization Control (SOC) 2 Report, or equivalent attestation report

Yes No

<If you or your infrastructure provider are working towards any of these certifications please state that and give us a timeframe by which this certification will be accomplished.>

Has the Contract/Agreement been reviewed and approved by UM General Counsel Office? Yes No

<Provide specifics>

Who is your Cloud Service Provider (CSP)?

What is your Cloud Computing Architecture?

- SaaS Single-Tenancy SaaS Multi-Tenancy
 PaaS
 IaaS

How is our data secured and segregated from that of other customers?

In which country (or countries) will the data reside?

USA Other, please indicate:

Upon termination of the contract, will data be transition back to UM? Yes No, explain:

Upon termination of the contract, will your process completely purge University information from your organization's/infrastructure provider's systems and backups?

Yes No, explain:

Do we have the right to audit, annual site visit?

Yes No, explain: