ITP-38F Marshall University (MU) Office of Information Technology
Outsourcing Security Assessment Questionnaire for Hosting Service Provider

Service/Software/System Description	
Name of Service	
Short Description of Service	

Sponsoring MU Unit	**Name**
Unit/Department/Center Name	
Lead Project Administrator	
Lead Technical Contact	

Hosting Service Provider			
Company Name			
Contacts	**Name**	**Phone**	**Email Address**
Administrative Representative			
Technical Contact			
Reference URL			
Additional Information Needed			

Data Classification Definitions

<u>MU Restricted Data</u>: Data, which Marshall University is obligated by policy, law, or legal contract to protect against unauthorized disclosure.

Security Controls

1.0 HIGH LEVEL DESCRIPTION	
1.1	Please provide a brief description of the purpose of the system, including how the information will be used. If possible, include a simple diagram of the dataflow and where Restricted Data will be stored.

1.2	Does the vendor have a path for the University to recover any data from their solution once the contract is terminated? Are there additional costs involved? What is the process?
1.3	Who will own any works that have been created as a result of the relationship between the vendor and the University? Is that written into any contracts?

2.0 AUTHENTICATION			**YES**	**NO**
2.1	Will users of the hosted service be authenticated by MU systems? If yes, skip 2.2.		□	□
2.2	Will users be authenticated by the hosting service provider?		□	□
	2.2.1	Will userids assigned by the service provider match MU userids?	□	□
	2.2.2	Will each user have a unique userid?	□	□
	2.2.3	Can the service provider's system be configured to require strong passwords?	□	□
	2.2.4	Can MU dictate password criteria as needed to ensure compliance with MU security standards?	□	□
	2.2.5	Can the service provider's system be configured to expire user passwords periodically in accordance with MU security standards?	□	□
	2.2.6	Does the service provider provide a function to enable users to change their own password securely?	□	□
	2.2.7	Can accounts be locked after a MU defined number of unsuccessful login attempts?	□	□
	2.2.8	Can the service provider's system deauthenticate users after a MU defined period of inactivity?	□	□
	2.2.9	Does the hosted service provide a logout on-demand option?	□	□
	2.2.10	Are passwords entered in a non-display field?	□	□
	2.2.11	Are passwords encrypted during network transit?	□	□
	2.2.12	Are passwords encrypted in storage?	□	□
	2.2.13	Are all attempted and successful logins logged, include date/time, userid, source network address, and are maintained for at least one year?	□	□

3.0 DATA SECURITY		**YES**	**NO**
3.1	Is all network transfer of MU Restricted Data encrypted when traversing the service provider's network and the MU network or non-MU networks?	□	□
3.2	Is all network transfer of MU Restricted Data encrypted between multiple service providers' systems (e.g. web and database servers)?	□	□

3.3	Are there any provisions for notifying the customer prior to monitoring, or information being released?	□	□

5.0 RECOVERABILITY		**YES**	**NO**
5.1	Is the service provider fully aware of the MU Unit's recoverability objectives?	□	□
5.2	Does the service provider have and follow a data and system backup plan commensurate with the MU Unit's recoverability objective?	□	□
5.3	Does the service provider have an adequate hardware maintenance contract or hot spare inventory to meet the sponsoring MU Unit's recoverability objective after a hardware failure?	□	□
5.4	Does the service provider have the capability to execute a recovery from a security incident, complete system failure or destruction within the time-frame of the MU Unit's recoverability objective?	□	□
5.5	To what extent does the hosting service provider ensure system availability consistent with the MU Unit's recoverability objectives? (e.g. backup power systems, redundant network paths, use of virtual machines, etc)		

6.0 OPERATIONAL CONTROLS		**YES**	**NO**
6.1	Does the service provider outsource hosting of their application and data storage servers to a third-party?	□	□
6.2	Has the service provider taken measures to ensure the physical security of the data center(s) in which the application and data storage servers are housed, specifically addressing access controlled and audited entry ways, temperature monitoring and control, fire prevention and suppression, and use of a backup power source?	□	□
6.3	If the service provider is currently providing hosting services for other clients, is multi-client access effectively controlled to ensure users are restricted to only the data they are authorized to access?	□	□
6.4	Does the service provider maintain and apply host security standards on their servers and verify them whenever changes in configuration are introduced into the system?	□	□
6.5	Does the service provider have and exercise a process to maintain current patch levels of software running on their systems?	□	□
6.6	Does the service provider implement anti-malware controls on servers?	□	□
6.7	What methods are used to ensure that service provider employees, who have access to MU Restricted Data, have been properly vetted? (e.g. law enforcement background checks)		
6.8	Does the service provider have an effective procedure for timely termination of access of their staff and MU users (upon notification) who no longer need access to the service provider's system?	□	□
6.9	Is there a guaranteed throughput for the service? What are the penalties if the guarantee isn't met?	□	□

7.0 INCIDENT RESPONSE		**YES**	**NO**
7.1	Does the service provider have a documented process for reporting security incidents involving systems used to store/access/modify hosted MU data to the MU Unit contact or, if appropriate, law enforcement?	□	□
7.2	Will a third party ever have access to the service provider's hardware or systems that store MU Restricted Data?	□	□
7.3	Are the service provider's database and web server access and error logs regularly reviewed for anomalies that could indicate a compromise?	□	□
7.4	What process does the service provider have in place to identify security breaches on vendor managed systems (e.g. file integrity checks)?		
7.7	In the case of a security breach or unexpected exposure of MU Restricted Data, what are the hosting service provider's incident response procedures?		
7.8	What is the service provider's process for disclosing to MU any data requests, such as subpoenas or warrants, from a third party?		