Statewide Learning Management System: Section 6 - Reliability and Security Requirements

Functional Area		Detailed Functionality	Ability to Meet Requirement				
			As Delivered	w/ Third Party	w/ Customization	Only Partially Meets	Not Available
Proposal Section 6	**6-1.0**	**Reliability and Security Processes**	0	0	0	0	0
	6-1.1	Provide a hosted, web-based Software as a Service (SaaS) solution (include the underlying technology of the application platform and details of the ASP provider)					
	6-1.2	Data must be stored/retained on a secure server environment that uses firewall and other advanced technology to prevent interference or access from non-authorized users; requires unique login ids; and meets at a minimal a level 7 data center rating as outlined in the Delaware Data Center Policy: http://dti.delaware.gov/pdfs/pp/DataCenterPolicy.pdf					
	6-1.3	Solution is available to users 99.9% of the time, excluding scheduled maintenance, and the State is notified when the solution is unavailable					
	6-1.4	Scalable to support current and future usage					
	6-1.5	Allow administrators (at Statewide and agency levels) to accept/decline features for a system upgrade					
	6-1.6	Upgrades must not interfere with customizations or modifications					
	6-1.7	Functional role-based authorizations to control levels of access to information - agency defined roles include (but not limited to): User (learner, employee), Manager, Administrator, Instructor/facilitator, and agency-defined roles which are specific to the agency					
	6-1.8	Solution must be responsive to users with metrics provided during peak and off-peak hours of operations					
	6-1.9	Solution must manage transactions and resource contention					
	6-1.10	System must be modular, allowing administrators to configure the deployment of only relevant functionality as needed					
	6-1.11	Internet security must be provided using Delaware's Encryption standards: http://dti.delaware.gov/pdfs/pp/WebApplicationSecurity.pdf					
	6-1.12	Must allow access to reports as determined by user's access level					
	6-1.13	Solution must provide an efficient mechanism to authenticate users, manage and update their permissions, and passwords cannot be sent in clear text email					
	6-1.14	SCORM and course repository management w/version control at both course and object levels					
	6-1.15	Alert to administrator with an email when course name is changed and track changes to course names over time					

Statewide Learning Management System: Section 6 - Reliability and Security Requirements

Functional Area		Detailed Functionality	Ability to Meet Requirement				
			As Delivered	w/ Third Party	w/ Customization	Only Partially Meets	Not Available
	6-1.16	Solution must meet State of Delaware Department of Technology and Information standards; http://dti.delaware.gov/information/standards-policies.shtml					
	6-1.17	Solution meets all data security practices in RFP Section III, C.					
	6-1.18	Securely transport all data files with confidential or higher classification as outlined in Delaware's File Transport standard http://dti.delaware.gov/pdfs/pp/SecureFileTransport.pdf and http://dti.delaware.gov/pdfs/pp/SecureFileTransport.pdf					
	6-1.19	Provide ongoing dedicated toll free number for call center support					
	6-1.20	Disposal of electronic information storage devices (hard drives, tapes, diskettes, compact disks, USB, multifunction peripherals, etc) in accordance with Delaware's policy DTI-005.01, Disposal of Electronic Equipment/Storage Media when the assets are considered no longer suitable of use and completion of (http://dti.delaware.gov/pdfs/pp/DisposalOfElectronicEquipmentAndStorageMedia.pdf) and then completion of a data destruction certification form is required.					
	6-1.21	Email communication cannot contain data classified as confidential or secret such as employee id number or social security number					
	6-1.22	Provide audit reports (SOC 2, etc) that capture user level interaction such as login/logoff with the system					
	6-1.23	Encrypt all State non-public data on all vendor devices including mobile					
	6-1.24	Restrict direct user access to the database layer of the solution					
Desired	6-1.25	Solution utilizes authenticating with Delaware's identity access management system for state employees and external learners					
Desired	6-1.26	Encrypt State data at rest using industry standard key management					
Desired	6-1.27	Ability to run on mobile devices using the State's Mobile Device encryption protocols					