UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology
Security Policy

Server Consolidation Policy

Purpose:	The University of Oklahoma Health Sciences Center has established enterprise data centers that will aid Business Units in providing technical and physical safeguards to protect Information Systems (IS) and meet regulatory requirements and industry best practices. Safeguards may include, but are not limited to: • Enterprise-class data center firewall protection • Physical and Network Intrusion Prevention and Intrusion Detection features • 24/7 Security Operations Center monitoring and alerting Consolidating IS that function as servers into the enterprise data centers will aid departments in mitigating risks to reasonable and acceptable levels.
Policy:	Servers or data classified as Category A or Category B Information Systems (IS) must be consolidated into the University's designated enterprise data centers. IS such as third party cloud services which have completed the Product Review process and have the appropriate business agreements and approvals in place may reside off campus and would not be consolidated into the University's enterprise data centers. To ensure all IS are compliant with existing Information Technology policy, each Business Unit must comply with the following requirements as part of the mandatory server consolidation policy and process: 1. The IS Owner or IS Owner Representative must classify all IS and data stored on IS in accordance with the Information System and Data Classification Policy. The Dean or director must assign a current employee to fill the IS Owner role. 2. All data and IS servers classified as Category A or Category B must be consolidated into the campus enterprise data centers. The IS Owner must prioritize consolidation efforts to maintain compliance with the Server Consolidation Policy. 3. Campus IT will assess appropriate cost recovery charge-backs for all resources moved into the data center.
Scope/Applicability:	This policy is applicable to all OUHSC Business Units. Norman Health Care Components should contact Campus IT for information regarding server consolidation.
Regulatory Reference:	• HIPAA 45 CFR 164.308(a)(1)(ii)(B) • 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (''GLB Act'') • FERPA: 34 CFR Part 99 [Family Educational Rights and Privacy Act] • State of Oklahoma Information Security, Policy Procedures Guidelines • Payment Card Industry (PCI) Data Security Standard

Definitions:	Information Technology Policy Definitions **Business Unit:** As applied to the University, a Business Unit may be a department, a program or college, a support service or central administration function within the University. A business unit may extend across multiple locations. **Information System *(IS)***: A system and/or service, which typically include: hardware, software, data, applications and communications that support an operational role or accomplish a specific objective. *Note – An IS can reside on premise or off-premise. **IS Sponsor:** an individual responsible for providing the necessary funding and support for the IS Owner and Administrator to perform their roles and responsibilities. The IS Sponsor provides executive oversight of data and/or IS and assumes responsibility for policy compliance for the IS under his or her control. The IS Sponsor reviews high level risk items of the IS and makes risk treatment decisions for the Business Unit. **IS Owner*:*** the individual responsible for maintaining a current inventory of all ISs within the business unit, classifying the data and IS, establishing rules for disclosing and authorizing access to IS data, conducting access control reviews, coordinating with campus IT to conduct risk assessments and serving as the escalation contact for the IS Administrator. **IS Administrator*:*** An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device or system (e.g., system administrator or network administrator). At OUHSC the IS administrator role is typically performed by the business unit Tier One. The IS administrator role may be performed through an agreement between the business unit and Campus IT. **IS Owner Representative*:*** An individual designated by the IS Owner to act on his or her behalf. **Server*:*** An IS that receives, stores, processes, or transmits data over the OUHSC network to other computers. Servers function to share data, information, or any hardware and software resources. For additional Information Technology definitions, see Information Technology Policy Definitions Document at http://it.ouhsc.edu/policies/documents/infosecurity/Information%20Security%20Policy%20Definitions.pdf
Responsible Department:	Any entity within the University of Oklahoma managing an IS that processes, stores, transmits, and/or collects University data is responsible for complying with this policy.
Policy Authority/ Enforcement:	This policy is authorized and approved by the OUHSC Dean's Council and the Senior Vice President and Provost. Internal Audit may periodically assess Business Unit compliance with this policy and may report violations to the Board of Regents.

Table 1 Revision History

Revision Date	Version	Revised By	Changes Made
03/28/2005	1.0	Campus IT	Baseline Version
12/12/2014	2.0	Campus IT	Modified wording of purpose statement to reflect Category A and Category B. Added new policy statements to reflect process requirements. Added clarification to the scope statement.
01/15/2015	2.1	OUHSC Information Security Review Board (ISRB)	Added a sentence to the first paragraph of the policy for exclusion of third-party cloud services that have been through the Product Review process and have proper agreements and approvals to be hosted off premise.

Table 2 Approval History

Version	Approval Date	Approved by:	Title:
1.0	05/12/2005	Dean's Council and Senior Vice President and Provost	
2.1	01/26/2015	Dean's Council	

Table 3 Review History

Version	Review Date	Reviewed by:	Title:
2.0	01/15/2015	ISRB	See ISRB membership list