Information System Storage and Data Policy

Current Version	Compliance Date	Approved Date
3.3	12/31/2018	11/13/2018

1. Purpose

The University of Oklahoma Health Sciences Center has established enterprise data centers to assist Business Units in providing technical and physical safeguards to protect University data and associated 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
- Available data backup and restore services
- Available data replication and warm site services

Using established enterprise data centers and services along with the appropriate safeguards to house servers and store University data is the expected practice at OUHSC that assists Business Units in mitigating risks to reasonable and acceptable levels.

2. Policy

University data must be shared or stored only in one of the services or locations that have completed an Information Security Risk Assessment, as indicated in the *OUHSC Information System Storage and Data Sharing Standard*. Note that data types that are not included in the Standard may still be considered University data, and users are responsible for complying with OUHSC's Information Technology, HIPAA, State of Oklahoma Records Retention policy and other relevant policies regarding information security requirements for those data types.

Use of Peer to Peer (P2P file) sharing for University academic, research, or clinical purposes that does not violate the law or University policy or compromise network integrity or security may be permitted *with prior approval* of OUHSC's Information Security Review Board.

2.1 Category A or Category B Information Systems or Data Storage

Servers or data classified as Category A or Category B Information Systems (IS) must be stored in the University's designated enterprise data centers or approved service/solution. IS such as third party cloud services that have completed the Information Security Risk Assessment process and have the appropriate legal agreements in place may reside off campus and do not have to be housed in 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:

1. The Business Unit must assign and document current employee to fill the IS Owner role, as part of the *OUHSC Information Security Risk Assessment Process*.
2. 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. IT Security will assist with classification, during the Information Security Risk Assessment process.

3. All data and IS servers classified as Category A or Category B, stored on campus, must be stored in University's designated enterprise data centers.
4. Category A IS and data stored in the enterprise data centers, must reside in the University's data center Business Zone.
5. Category B IS and data stored in the enterprise data centers, must reside in either the University's data center Business or General Zone.
6. Category A or B data must not be permanently stored on desktop computers, laptop computers, USB drives, or other portable media. Procedures must be created by the IS Owner and/or IS Administrator to transfer Category A or B data to an approved location on a nightly basis.
7. Category A or B data may be temporarily stored on encrypted USB drives or other encrypted portable media, in accordance with the *OUHSC Information System Data in Motion* and *Portable Computing Device Security* Policies.
8. OUHSC Information Technology will assess appropriate cost recovery charge-backs for all resources moved into the data center.

Information Systems classified as Category A, and temporarily storing data outside of the University's designated enterprise data centers must be encrypted to prevent unauthorized access. In addition, the IS Owner or IS Administrator must develop and implement a process to relocate data from the local storage device to an OUHSC Data Center on a nightly basis.

2.2 Category C Information Systems or Data Storage

It is recommended but not required that servers or data classified as Category C should be in the University's designated enterprise data centers or approved service/solution.

Portable computing devices and/or portable storage media storing Category C data must be encrypted in accordance with the *OUHSC Portable Computing Device Security Policy.*

2.3 Category D Information Systems or Data Storage

Servers or data classified as Category D are intended for public access. It is recommended that but not required that servers or data classified as Category D are stored in the University's designated enterprise data centers or an approved service/solution.

Portable computing devices and/or portable storage media storing Category D data must be encrypted in accordance with the *OUHSC Portable Computing Device Security Policy.*

2.4 Other Information System Storage and Data Sharing Services

It is the responsibility of OUHSC Business Unit to ensure that all external services used to store Information Systems and/or data, are done so in compliance with University Policy and Standards through the use of the *OUHSC Information Security Risk Assessment*. The *OUHSC Information System Storage and Data Sharing Standard* provides a complete list of currently acceptable facilities and services for the storage of Information Systems and Data sharing, as well as any additional requirements that must be met in order to use such services.

2.5 Information Security Risk Assessment (Product Review)

Departments evaluating the purchase and/or use of services must request an Information Security Risk Assessment, prior to purchase or use of services. The Risk Profile Summary generated during the Information Security Risk Assessment will document the shared security model these services employ, providing security requirements to the IS Sponsor, IS Owner, and IS Administrator, and the OUHSC Risk Subcommittee, as necessary, to make appropriate risk decisions as Information Security risk is identified.

2.6 External Sharing

If confidential or regulated University information such as (1) data subject to PHI, FERPA, PCI laws or (2) data that is not legally regulated but for which an expectation of privacy or confidentiality exists, or (3) data protected by contractual obligations, must be shared with external parties over an external network (e.g., the Internet), the intent to share must first be reported in an *OUHSC Information Security Risk Assessment* and data transmission must be encrypted. Intention to share information with external parties must be reported during the Information Security Risk Assessment to verify the security of transmitted information.

3. Definitions

See Information Technology Policy Definitions Document at
http://it.ouhsc.edu/policies/documents/infosecurity/Information%20Security%20Policy%20Definitions.pdf

4. Scope

This policy is applicable to all OUHSC Information Systems and Data. Norman Health Care Components should contact their local Information Technology department for information regarding server and data storage for each category of data.

5. Regulatory References

- Payment Card Industry (PCI) Data Security Standard
- HIPAA 45 CFR 164.310(d)(2), 164.308(a)(7), 164.312(a)(2)
- 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act ("GLB Act"), Standards for Safeguarding Customer Information
- State of Oklahoma Information Security, Policy, Procedures, and Guidelines – Information Availability, Backup of Information
- HITRUST 03.b Performing Risk Assessments
- HITRUST 05.i Identification of Risks Related to External Parties
- HITRUST 06.c Protection of Organizational Records
- HITRUST 06.d Data Protection and Privacy of Covered Information
- HITRUST 06.e Prevention of Misuse of Information Assets

6. Authorization

This policy is authorized and approved by the OUHSC Senior Vice President and Provost, and enforced by the IT Chief Information Officer. Internal Audit and other authorized departments of the University may periodically assess Business Unit compliance with this policy and may report violations to the University Administration and Board of Regents.

7. Policy Maintenance

This policy is scheduled to be reviewed, updated and modified as necessary at least every two (2) years.

8. Revision, Approval and Review

8.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	03/28/2005	OUHSC IT	Baseline version
2.0	12/12/2014	OUHSC 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.

2.1	01/15/2015	OUHSC 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.
3.0	12/9/2016	OUHSC IT	Applied new template. Updated policy statement to indicate the business unit designates the IS Sponsor and that IT Security will assist with IS and data classification.
3.1	07/10/2018	OUHSC IT	Renamed Policy to Information System and Data Storage Policy. Added encryption requirement for Category A IS storing data outside of approved data center. Added recommendation and requirement for Category C IS and data.
3.2	09/10/2018	ITRC	Added Category D Minor revisions
3.3	09/11/2018	Jill Raines	Minor revisions

8.2 Approval History

Version	Date	Approved By
1.0	05/12/2005	Dean's Council and Senior Vice Provost and Provost
2.1	01/26/2015	Dean's Council
3.3	11/13/2018	Information Security Review Board

8.3 Review History

Date	Reviewed By
01/15/2015	ISRB
12/9/2016	OUHSC IT
07/10/2018	OUHSC IT
07/12/2018	Randy Moore
09/06/2018	ITRC