Access to University Data Policy

1. Purpose

This policy defines roles and responsibilities for protecting OUHSC's non-public data and the Information Systems (IS) on which the data are maintained from unauthorized access, unauthorized disclosure, or misuse.

2. Policy

Access to University data and IS must be authorized by the IS Owner prior to granting access for business use. The following defines OUHSC's requirements for managing logical access to data and IS.

2.1 University Data Must Be Classified

OUHSC data shall be classified by the IS Owner and/or the IS Administrator and/or IT Security, in accordance with *OUHSC's Information System and Data Classification Policy*.

2.2 Information System Access Control Procedures

IS Owners must document and implement procedures for the authorization, establishment, modification, and removal of access to data and IS, to be maintained by the IS Owner. A template is available from IT Security to assist in these documentation efforts.

At a minimum, these procedures must include:

For All Category A and Category B data and Information Systems Only

1. The levels of access available in the IS.
2. Procedures for authorization and approval to grant new access, modify access, and delete access requests, in accordance with departmental Role-Based Access Worksheets or to only those with a "need to know", to prevent unauthorized access to IS.
3. Procedures for tracking access requests of any type (new, modify, delete).
4. Procedures and assigned roles/responsibilities for reviewing access levels, at least annually, and more frequent, as necessary.
5. How logical access to Category A or Category B data is logged, in accordance with *OUHSC's Activity Log Review Policy* and *Standard.*

2.3 Information Flow Enforcement

As part of the Information Security Risk Assessment process, IS Owners and/or IS Administrators are responsible for providing IT Security with the following information regarding an Information System's data flow prior to an Information System going into production use:

1. Network protocol (TCP/IP/UPD) ports necessary for IS communication
2. Encryption protocol used during transmission
3. Direction of information flow (inbound or outbound)
4. Source and destination IP addresses of IS
5. Business purpose for information flow

2.4 Separation of Duties

For Category A Information Systems Only

The principle of separation of duties is to eliminate conflicts of interest in the responsibilities and duties assigned to individuals. The following must be considered when assigning roles and responsibilities within an IS:

1. Ensure that audit functions are not performed by the same personnel who are responsible for administering access control.

2. Maintain a limited number of administrators, each of whom will have access to administrative functions based upon the minimum necessary or as-needed basis.

3. Ensure that the IS Owner and/or IS Administrator are not responsible for conducting information security testing of the IS.

2.5 Primary Authentication Method

OUHSC's preferred method of authentication is OUHSC's Active Directory Lightweight Directory Access Protocol (LDAP). IS must be configured to use this authentication method, wherever possible. If OUHSC's LDAP is unavailable as the authentication method, the following must be configured by the IS to automatically enforce:

1. IS accounts must meet the OUHSC Password Management Policy and Standard:
    a. Complexity of passwords
    b. Maximum 90-day expiration for passwords
    c. Account lock after 5 failed login attempts
    d. Session or application lock after fifteen minutes of inactivity
    e. Passwords must be kept private and not shared with others

See http://it.ouhsc.edu/policies/Password_Management_Policy.asp and http://it.ouhsc.edu/policies/Passwords.asp

For Category A and B IS Only

2. IS must be configured to display the following system use notification message or banner before granting access to the IS:

    "This system is for the use of authorized users only. Activities on this system may be monitored and/or recorded by systems personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible criminal activity or policy violation, system personnel may provide the evidence of such monitoring to law enforcement or University officials, as appropriate."

2.6 Permitted Actions Without Identification or Authentication

IS Owners, IS Administrators, or IS Suppliers are responsible for identifying user actions that can be performed on the IS without identification or authentication (public access). These actions should be supplied to IT Security during the IT Product Review/Risk Assessment Process for new products and upon requests for products in place prior to the adoption of the Product Review/Risk Assessment.

2.7 Remote and External Third-Party Access to OUHSC Data

Remote access into OUHSC's environment is authorized through the following mechanisms:

- OUHSC VPN (Requiring multi-factor authentication)
- OUHSC user-initiated web conference sessions for remote support purposes

For Category A Information Systems Only

Access by external parties to OUHSC Category A Data and the IS on which the data are maintained must be governed by the contract for goods or services, Business Associate Agreement , Memoranda of Agreement/Understanding (MOA/MOU), or other legally binding agreement that covers the access.

2.8 Information Sharing

IS Owners and/or IS Administrators are responsible for providing IT Security with pertinent details when University data is exchanged with OUHSC IS or External Parties as part of the technical configuration, requiring network firewall rules to permit the data exchange. The following information must be supplied to IT Security as part of the IT Product Review Process, prior to the IS being placed into production use:

1. The source and destination IP address of the communication path;
2. The specific data types being shared;
3. The network protocol ports used for data sharing;
4. The file format of the file being shared;
5. The frequency of the file transfer;
6. IT Contact for data recipient in the event of technical issues;
7. Business purpose for information sharing
8. Business contact for third party
9. Other information, as requested

2.9 Training

All Business Unit IS Owners and/or IS Administrators must undergo annual, and more frequently as needed, training to provide guidance for complying with the *Access to University Data Policy.*

3. Enforcement

This policy is authorized and approved by the OUHSC Dean's Council and 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.

4. Scope

This policy is applicable to all OUHSC faculty, staff, students, employees, Business Associates, contractors, vendors, OU Health Care Components, and others entrusted with data maintained in the University's information repositories.

5. Regulatory References

- FISMA Access Control Family
- 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''), Standards for Safeguarding Customer Information,
- State of Oklahoma Information Security, Policy, Procedures, and Guidelines
- Payment Card Industry Data Security Standard (PCI DSS)

6. Related Policies

- IT Information System and Data Classification Policy
- IT Access to University Data Standard

- IT Activity Log Review Policy

7. Review Frequency

This policy is scheduled to be reviewed, updated, and modified as necessary, but at least annually.

8. Revision, Approval and Review

8.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	03/14/2007	OUHSC IT	Baseline Version
2.0	08/24/2015	OUHSC IT	Revised purpose and scope. Added clear responsibility in the policy statement. Annual policy review by IT.
3.0	10/18/2016	IT Security	Updated Purpose statement. Updated Policy statements to include external parties and clearly define responsibilities.
3.1	10/31/2016	IT Security	
3.2	03/28/2017	OUHSC IT	Revised policy statements to align with FISMA Access Control families. • Added classification policy statement • Updated Access Control procedure policy statements • Added information flow enforcement policy statement • Added separation of duties policy statement • Added permitted actions without identification or authentication policy statement • Combined OUHSC Telework policy statements into section 2.7 policy statements • Added 2.8 Information Shareing policy statements
3.3	04/03/2017	OUHSC Director of IT Information Security	Added content from Password Standard and Login Banner policy.
3.4	04/04/2017	OUHSC IT	Consolidated comments received from IT Security team review. Updated language to include a template available from IT Security to meet procedural requirements.
3.5	05/11/2017	OUHSC IT Security	Consolidated feedback from IT and Legal Counsel review: • Updated references to IS to include “data” • Updated IT Product Review reference to IS Risk Assessment

8.2 Approval History

Version	Date	Approved By
1.0	03/14/2007	Deans' Council
3.5	08/08/2017	Information Security Review Board (ISRB)
3.5	10/10/2017	OUHSC Dean's Council and Senior Vice President and Provost

8.3 Review History

Date	Reviewed By
11/12/2014	OUHSC IT
08/24/2015	OUHSC IT
06/20/2016	OUHSC IT
10/28/2016	Legal Counsel
04/03/2017 04/04/2017	OUHSC IT
08/08/2017	ISRB