Information Security Incident Reporting Policy

1. Purpose

This policy serves to minimize negative consequences of information security incidents by providing prompt reporting of such incidents to the appropriate University official. Prompt reporting improves the University's ability to prevent unauthorized access, use, disclosure, modification or destruction of information systems that are affected by security incidents.

2. Policy

This policy establishes the requirement that all OUHSC faculty, staff, students, residents, volunteers, and other entities or person who perform work for the University are obligated to report information security and privacy incidents to the appropriate individuals with delegated authority as identified below.

What to Report

- Any event in which access to University data might have been gained by an unauthorized person
- Any event in which a device containing University information has (or might have been) lost, stolen or infected with malicious software (viruses, Trojans, etc.)
- Any event in which an account belonging to a person that has access to the data might have been compromised or the password shared with unauthorized person (responding to phishing emails, someone shoulder surfing and writing down your password, etc.)
- Any attempt to physically enter or break into a secure area where University data is or might be stored
- Any other event in which University data has been or might have been lost or stolen
- Any event in which University or information system policies, standards, or practices are violated

Reporting and Responding to IT Security Incidents

Individuals

- Should attempt to stop any IT security incident as it occurs.
- First, **DO NOT TURN OFF OR UNPLUG THE COMPUTER.**
- **Second, unplug the network cable from the back of the computer and turn off any wireless internet connection**.
- Report IT security incidents to the appropriate OUHSC campus IT Service Desk or Tier 1. The Service Desk will help you assess the problem and determine how to proceed.
    - Oklahoma City campus IT Service desk: servicedesk@ouhsc.edu, (405) 271-2203 or Toll Free (888) 435-7486
    - Tulsa campus IT Service desk: tulsait-servicedesk@ouhsc.edu, (918) 660-3550
- If the incident has potentially serious consequences and requires immediate attention, individuals can report the security incident by calling 405-271-2476.
- Following the report, individuals must comply with directions provided by IT Support staff or IT Security to repair the system, restore service, and preserve evidence of the incident.

IT Service Desk and Tier 1s

- Respond quickly to reports from individuals.
- Take immediate action to stop the incident from continuing or recurring.
- Collect appropriate information about the information systems affected.
- Report incidents to the appropriate delegated authority.

IT Security

- Assess the nature and scope of the incident and identify what data or information systems are involved.
- Create an Incident Report that will document the facts surrounding the incident; the steps taken to mitigate any immediate threat, the steps taken to ascertain the scope and nature of the breach; the nature of the breach itself; the list of affected individuals and any other relevant information relating to the incident.

How to Report

Delegated Authority for Information Security Incidents	Area of Responsibility	Contact Information
Information Security	All information, information systems, and infrastructure technology except for the areas specifically listed below.	IT-Security@ouhsc.edu 405-271-2476
HIPAA Security Officer	Electronic PHI for OUHSC Healthcare Components	Valerie Golden 405-271-8001 x46456
FERPA Official	Incidents involving student information protected by the Family Educational Rights and Privacy Act (FERPA)	Lori-Klimkowski@ouhsc.edu Registrar, Office of Admissions & Records 405-271-2359 x48900

3. Scope

This policy applies to all users of information systems or data at the OU Health Sciences Center and Health Care Components.

4. Regulatory References

- HIPAA Standards for Safeguarding Customer Information
- Section 501(b) of the Gramm-Leach-Bliley Act (“G–L–B Act”),
- Payment Card Industry Data Security Standard (PCI DSS)
- Family Educational Rights and Privacy Act (FERPA): 20 U.S.C. §1232g; 34 CFR Part 99

5. Authorization/Enforcement

This policy is authorized and approved by the OUHSC Dean’s Council and Senior Vice President and Provost, and enforced by the 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.

6. Policy Maintenance

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

7. Revision, Approval and Review

7.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	03/14/2007	OUHSC IT	Baseline Version
2.0	09/29/2015	OUHSC IT	Revised purpose statement, added definition
3.0	11/14/2016	OUHSC IT	Revised policy statements to clearly define roles and responsibilities. Updated enforcement statement.
3.1	12/13/2016	OUHSC Information Security Review Board	Added contact information for the OU Tulsa IT Service Desk
3.2	01/27/2017	OUHSC IT	Added contact information for the FERPA official

7.2 Approval History

Version	Date	Approved By
1.0	03/14/2007	OUHSC Deans' Council and Senior Vice President and Provost
3.1	12/13/2016	OUHSC Information Security Review Board
3.2	01/11/2017	OUHSC Deans' Council and Senior Vice President and Provost

7.3 Review History

Date	Reviewed By
11/18/2014	OUHSC IT
09/29/2015	OUHSC IT
11/14/2016	OUHSC IT
11/14/2016	OUHSC Legal Counsel