UNIVERSITY OF OKLAHOMA
Information Technology
Security Policies

Subject: Information Security Password Management Policy	**Coverage:** OUHSC
Policy #: Information Security-P#11.3.1	**Version:** 2.0
Regulation: HIPAA, GLB, State of Oklahoma	**Approved:** 04/11/07
Effective: 04/11/07	**Revised/Reviewed:** 11/18/2014

Policy Summary:

The University must implement a formal documented process for the appropriate creation, modification, and safeguard of information system passwords.

Purpose:

This policy reflects the University's commitment to identify and implement security controls that will keep risks to information system resources at reasonable and appropriate levels.

Policy:

The University shall develop, implement, and regularly review a formal, documented process for appropriately creating, modifying and safeguarding passwords used to validate a user's identity and establish access to the University's information systems and data. All University workforce members must be regularly trained and reminded about this process.

At a minimum, the University's password management processes must:

- Require the use of individual passwords to maintain accountability.
- Where appropriate, allow workforce members to select and change their own passwords.
- Require unique passwords that meet the standards defined by the University.
- Require regular password changes.
- Not display passwords in clear text when they are being input into an application.
- Require the storage of passwords in an encrypted form.
- Require passwords to be given to users in a secure manner.
- Require the changing of default vendor passwords following installation of software or hardware.
- Require temporary passwords to be randomly generated and force password change at first log-on when possible.

The University's password management training and awareness must involve requirements for use of information systems including, but not limited to:

- The importance of keeping passwords confidential and not sharing them with anyone.
- The need to avoid maintaining a paper record of passwords, unless the record can be stored securely.
- Changing passwords whenever there is any indication of possible information system or password compromise.
- The University's password standards.
- The importance of not using the same password for personal and business accounts.
- The importance of changing passwords at regular intervals and avoiding re-using old passwords.
- Changing temporary passwords at the first log-on.
- Not including passwords in any automated log-on process (e.g. stored in a web browser, macro or function key).
- Ensuring that University workforce members understand all activities involving their User ID and password will be attributed to them.

Documentation:	All data collected and/or used as part of the Risk Management Process and related procedures will be formally documented and securely maintained.
Scope/Applicability:	This policy is applicable to all OUHSC workforce members.
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 (‘‘G–L–B Act’’) State of Oklahoma Information Security, Policy Procedures Guidelines
Definitions:	See the Information Security Policy Definitions document for definitions
Responsible Department:	Each organizational unit within the University of Oklahoma that manages its own information systems is responsible for complying with this policy.
Enforcement/Audit:	The University’s Internal Auditing department is responsible for monitoring and enforcement of this policy.
Related Policies:	Risk Analysis, Data Classification, Resource Identification, Resource Classification
Procedures:	Contact the appropriate campus IT Service Desk for questions about password management procedures for IT accounts.
Renewal/Review:	This policy is to be reviewed and updated as needed by IT Information Security Services.