Information

Passwords

Effective

July 23, 2007

Number

ISO-008 v2.2

Applicability

This policy applies to all University workforce, faculty and student members (including, but not limited to: faculty, staff, students, temps, trainees, volunteers, and other persons as deemed appropriate) while conducting/performing work, teaching, research or study activity using University resources and includes all facilities, property, data and equipment owned, leased and/or maintained by the University or affiliates

Administrative Authority

Executive Vice President and University Provost

Responsible Unit

Information Technology Services

Miller IT Center, Louisville, KY 40292

502/852-7997

History

This policy is subject to change or termination by the University at any time. This policy SUPERSEDES all prior policies, procedures or advisories pertaining to the same subject.

This policy will be reviewed annually to determine if the policy addresses University risk exposure and is in compliance with the applicable security regulations and University direction. In the event that significant regulatory changes occur, this policy will be reviewed and updated as needed per the Policy Management process.

Approved July 23, 2007 by the Compliance Oversight Council
Shirley C Willihnganz, Executive Vice President and University Provost, Chair of the Compliance Oversight Council

Revision Date(s):

1.0 / July 23, 2007 / Original Publication

1.1 / January 31, 2011 / Revised special characters accepted

1.2 / November 16, 2011 / Add that passwords are to be known only by the owner of the account.

1.3 / January 29, 2013 / Content Review and update

1.4 / September 26, 2014 / Content update regarding length of time for password expiration

2.0 / March 8, 2016 / Review/update content and update to template format

2.1 / June 18, 2017 / Review and clarify (re-organize) password specifications

2.1 / June 30, 2018 / Update to replace should with must where needed

2.2 / October 11, 2024 / Review and update content to align policy with NIST guidelines and transfer responsible authority

Reviewed Date(s): March 8, 2016; June 18, 2017; June 30, 2018; October 11, 2024

Categories

Reason for Policy:

The purpose of this policy is to establish minimum requirements for the creation and protection of passwords which aligns with National Institute of Standards and Technology ("NIST") Cybersecurity Framework and Special Publication 800-63b.

Statement:

All computer accounts must be password protected to help maintain the confidentiality and integrity of electronic data as well as to help protect the University's computing resources and infrastructure. This policy establishes a minimum standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Responsibilities:

Policy Authority/Enforcement: The University's Chief Information Security Officer (CISO) is responsible for the development, publication, modification and oversight of these policies and standards. The CISO works in conjunction with University Leadership, Information Technology, Risk, Audit, and Compliance, and others for development, monitoring and enforcement of these policies and standards.

Policy Compliance: Failure to comply with these policies and standards and/or any related information security and/or information technology policy, standard or procedure may result in disciplinary action up to and including termination of employment, services or relationship with the University and/or action in accordance with local ordinances, state or federal laws.