UIndy Password Policy

Effective Date: December 2018

Office: Information Technology

PURPOSE:

Passwords are an important part of computer security. They are the first and sometimes last line of defense against would-be criminals. A poorly chosen password or mishandled password can result in a temporary denial of computer services, identity theft, theft of University services and even financial loss. Appropriate password security is necessary to protect the University's academic interactions, business and research.

This policy describes the requirements necessary for creating and maintaining password security on all UIndy Accounts.

REFERENCE DOCUMENTS/ RELATED INFORMATION:

Systems and Network Usage Policy

Social Media Account Policy

SCOPE:

All UIndy students, faculty, staff, partners, vendors and third party service providers.

POLICY HISTORY:

V1.0 – 11/09/2018

Policy Statement

All network devices and accounts must be secured with appropriate username and passwords. Whenever possible, systems will use UIndy Accounts stored in a central directory. All UIndy Accounts, including those used by faculty, staff, students, contractors and partners of the University, must be properly secured using the methods described in the following sections of this document.

Creating a Strong Password

The University of Indianapolis requires strong passwords on all UIndy Accounts. The University defines strong passwords as passwords that will take a computer at least six months to try all possible combinations of the letters, numbers and special characters contained in your password. The following are characteristics of a strong password:

- Is at least eight characters in length
- Contains at least 2 letters
- Contains lower case and upper case letters (a-z and A-Z)
- Contains at least 1 number
- Is not a word in any dictionary, English or other
- Contains at least 1 special character from the following list: !@#$%^&*()-+?/.
- Does not contain the user's first or last name
- Does not contain the username

Vendor Supplied Defaults

Vendor supplied default passwords must be changed upon implementation for all systems and services hosted by the University or hosted by a contracted third party.

Password Change Frequency

The University of Indianapolis requires all UIndy account passwords to be changed every six months. This reduces the likelihood of the password being discovered and reduces the length of time a compromised account can be unknowingly used for criminal activity. Exceptions are made for service accounts with limited access and must be approved by the Director of Network, Systems, and Security within Information Technology.

Password Storage

Choose passwords that are easy to remember so that it is not necessary to write it on any piece of paper. A password written on a post-it note is as good as no password at all. If passwords must be stored for any reason, contact Information Technology for assistance with tools which can aid in storing passwords securely.

Password Confidentiality

Never tell another person your UIndy Account password. Your UIndy Account password should be kept completely confidential. Supervisors, coworkers, friends and family should never know your password. Likewise, it is inappropriate to ask another user for their UIndy password. If a

person demands your password, refer the person to this document and/or contact the Director of Network, Systems, and Security in Information Technology.

Periodic Scans

University of Indianapolis Information Technology will periodically employ password cracking techniques to determine the effectiveness of this password policy. Any passwords found to be weak during these scans will be immediately changed and the user notified.

Encryption

All University computer systems will store passwords in an encrypted form. As such, the IT Help Desk cannot see or retrieve a password, only assist users in changing to a new password.

Compromised Accounts

If you suspect that a UIndy account has been compromised, change your password immediately and report it to the IT Help Desk and your supervisor.

Shared Accounts

There may be occasions when an account is shared among several employees, i.e., accounts for third party web sites, system service accounts, social media accounts and departmental email accounts. Access to such accounts must be tightly controlled. If an employee with knowledge of a shared account is terminated, the password must be changed immediately upon termination. Questions about how to securely manage account credentials should be referred to the IT Help Desk. Please note that an individual's personal UIndy account credentials should never be shared.