Policy Title: Information Technology Services – Digital Password Management Policy

Policy Number:

Established: December 2017

Approved by:

Last Approval Date:

Revision Date:

Position Responsible for Maintaining and Administering the Policy: Executive Director, Information Technology Services

Contact: Ryan Kenney, Executive Director, IT Services, (519) 253-3000 ext. 2740

Table of Contents

Policy Statement

This Policy defines the minimum standards governing the format and management of passwords used to access electronic services and accounts associated with the University of Windsor.

Purpose

Usernames and passwords are used as the keys to authenticate and authorize access to electronic services and accounts provided to the University community that are not for use by the general public or by unauthorized users. Ensuring that the passwords used are strong and managed appropriately is a key requirement to preventing the inappropriate use of electronic resources.

This Policy describes minimum standards for password format and strength, sets requirements for password management over time, and defines actions that can be taken to protect accounts from suspected attack or unauthorized use.

Scope

This Policy applies to all University or affiliated services that use an authentication scheme that involves the use of a username, password, pin and / or access code, with mandatory applicability to any system that utilizes an account with a UWinID or a uwindsor.ca email address as a username.

This Policy serves as the foundational password policy for the University community. Other systems may extend or strengthen the requirements described in this policy based on either additional capability or need for stronger security; however, systems may not weaken the requirements set forth in this Policy unless there are resource or other technical deficiencies that disallow its adoption

Responsibilities:

1. Information Technology (IT) Services has the responsibility to:
    - Enforce this policy and is authorized to set specific password creation and management standards for University systems and accounts
    - Provide cybersecurity awareness and password management resources to support a recommended approach to managing passwords
    - Secure an account as may be necessary when it is suspected that a password has been compromised
2. Client areas accessing University provided electronic services and corresponding accounts have the responsibility to:
    - Secure respective passwords and to expeditiously report a potential disclosure of their own or any other users' passwords
    - Only use a UWinID or uwindsor.ca email address and password as credentials for University-sanctioned services and not for personal or other non-University-sanctioned services
    - Implement, review and monitor internal policies, practices, etc. to assure compliance with this Policy
3. IT Steering Committee has the responsibility to:
    - Regularly review this Policy
    - Provide feedback and guidance on this Policy
    - Approve amendments to this Policy

Exceptions to Policy

Some legacy systems or specific / privileged services may not be capable to fully support all the requirements of this Policy. In these situations, the systems / services will be required to implement specific components of this Policy as may be reasonably possible, and IT Services must be notified in writing, describing the system / service and indicating the corresponding deficiencies, in order to ensure that an appropriate risk mitigation strategy can be proposed and / or adopted.

The Executive Director, IT Services may determine that certain situations or circumstances require exceptions to this Policy in order to best serve the interests of the University. Such requests should be communicated in writing to the Executive Director, IT Services and should include the exact nature of the exception and, if appropriate, the time period during which the exception should be granted.

Cross-References

None

Definitions

Item	Description
Account	Provides specific access to a resource and is usually comprised of a username and password. IT Services provisions a UWin Account for all users which consists of a UWinID and a password and has a corresponding email address to which it is associated. Encompasses all University system accounts, including those for guests and privileged users.
Authenticate	Process of identifying who is accessing a system or service
Authorize	Process of determining if an authenticated user is permitted to access a system or perform an action
Electronic Resource / Service	Function or information provided through the use of a computing device (e.g. desktop, laptop, tablet, smartphone, etc.), application (e.g. E-Mail, Student Information System, Learning Management System, etc.) or web site
Guest User ID	A sponsored wireless account for temporary use by campus visitors
Password	Typically a string of mixed characters or numbers used in conjunction with a username to authenticate a user; other mechanisms may exist, for example digital certificates or environmental factors such as physical location or the use of a specific piece of equipment like a fingerprint reader
Privileged Account	Provides a significant level of access and ability (e.g. administrator or super-user) to affect changes in electronic services and accounts. May be subject to additional policies or controls that supersede this Policy.
Special Character	Symbols that are not part of the standard alphanumeric characters (A-Z, 0-9), such as punctuation and units

Strong Password	Strength of a password is a measure of how well it can resist attempts to determine its value; generally longer and more random strings are stronger than shorter, dictionary-based words
UWinID	A unique, centrally-managed account name provided by IT Services to every University staff member and student

Procedures

Policy Requirements

All electronic resources not provided for public use by the University or where resource users need to be differentiated from one another must implement accounts that use a password

The following practices govern use and dissemination of passwords:

- Passwords are issued to one individual only and should not be shared
- Passwords must be changed by the user or reset by IT Services whenever there is doubt about account security. Where password change is not practical or timely, steps will be taken by IT Services to disable accounts in situations where unauthorized or inappropriate activities are suspected.
- If an account must be accessed by someone other than the user to whom it is assigned, the password must be changed for the new user. In the event this is not possible, role / group based authentication will be used to access the electronic resource / service.
- Electronic resources cannot store passwords in unencrypted form
- Electronic resources should record and monitor authentication and authorization attempts and generate alerts when abnormal activity is observed
- Users will be required to review and acknowledge this Policy during the process of activating a new UWin Account

Password Compliance Requirements

Passwords must comply with the following minimum requirements:

Requirement	**UWin Account Policy**
Minimum Length	10 characters
Upper and Lower Case Characters	At least 1 upper case and at least 1 lower case character
Numbers / Digits	At least 1 numeric character
Special Characters	At least 1 special character (no restrictions)
Not Trivial or Easily Guessable	Password cannot match User ID or e-mail address
Password Expiration	120 days
Password Expiration Notification (where possible based on application)	Initial = 30 days Reminder #1 = 14 days Reminder #2 = 7 days Reminders #3-9 = daily reminders from 6 days before and up until day of expiry
Password History to be Maintained	10
Inactivity Timeout	20 minutes (enforced by the application)
Account Lockout Upon Failed Logins	5 failed logins in 5 minutes, locked for 10 minutes
Purge User Profiles	Disabled or removed as per IT Services procedures

Review Process for Policy

This Policy will be reviewed at least every three (3) years. There may be certain circumstances that may cause for the review of the Policy prior to that date: changes in legislation that affect the Policy; a specific incident triggers a review of the Policy; there is a request made by Senior Management or the Board of Governors to review the Policy.

Process for Communicating Policy

The Policy will be posted on the University of Windsor's IT Services website, within two weeks of the approval. Separate notifications may also be sent via e-mail or other means to Departments directly affected by the Policy, or in some cases, the broader campus community if deemed applicable.

Contact Information

Inquiries regarding the policy should be directed to Executive Director, IT Services or appropriate individual in the Department where the Policy was developed, as per the contact information at the introduction of the Policy.