Authentication Management Standard

Version: 1.1
Published: April 21, 2021
First Published: Feb. 20, 2018
Published By: Information Security Office, Information Services
Approved By: UITSC
Approval Date: Jan. 5, 2018

1. Introduction

The University of Regina Password Management Policy (OPS-050-035) states that authentication mechanisms are critical controls permitting only authorized user access to University of Regina data and information systems.

Thus, the following standard establishes a minimum baseline for authentication mechanisms used at the University of Regina and is intended to provide direction and guidance to those responsible for the configuration, management, or design of applications or systems which control access to University information systems or data.

2. Scope

This Standard applies to all University of Regina users, identities and accounts utilized for authentication and access to University information, data, systems, and applications.

3. Standard

3.1. Password Construction

3.1.1. All information systems or applications which make use of passwords must do so in combination with a username.

3.2. Password Storage in Information Systems and Applications

3.2.1. Information systems and applications must never store passwords in clear text or any easily reversible form.

3.2.2. Whenever possible, stored passwords should use known secure encryption tools intended for passwords.

3.2.3. Passwords must not be stored or remembered by computer applications or systems that do not require authentication, or which are public or shared.

3.3. Password Change

3.3.1. Initial or default passwords included as a part of any system or account provisioning must be changed as soon as practical, and in all cases prior to the system being placed into production use.

3.3.2. Upon creation or reset of an account password, the application or system should prompt the user to create an initial password that complies with the Password Management Standard. In cases where this is not possible, the initial password must be unique and comply with the Password Management Standard. If the password does not comply with the Password Management Standard, the system should require that the user change the password upon the first use.

3.4. Password Transmission

3.4.1. Passwords must be encrypted when sending over any network. Systems or applications must not request or accept authentication over unencrypted channels.

3.4.2. When a new account is provisioned and provided to a user, passwords must not be emailed, nor included in Footprint tickets, or other means of unencrypted communications or storage, unless a password change is forced upon initial use.

3.4.3. When a new account is provisioned and there is a need to communicate a password to an authorized individual, ensure the password cannot be intercepted by unauthorized parties. Typically, this requires communicating a password out of band on secure channels to ensure that only the authorized user of a given account receives the associated password.

3.5. Password Sharing

3.5.1. Systems and applications shall support unique user accounts and passwords so that individual users are not required to share a password in order to use the system or application. Whenever possible, shared access should be handled with proxy/delegated access and/or aliases.

3.5.2. Passwords should never be revealed to anyone other than for the purposes of new account provisioning. All passwords are considered to be confidential to the owner. The University of Regina will never ask for passwords in an email or over the phone.

3.6. Application and System Configuration

3.6.1. Where technically practical, the minimum password standards found in the Password Management Standard shall be enforced by the application or system.

3.6.2. If a particular system or application will not support minimum strength attributes for the account category required, as per Password Management Standard Policy 4.3, then the strongest combination of password attributes allowed by that system shall be utilized in conjunction with an exception request.

3.6.3. Systems or applications should accept authentications only from networks, locations, or subnets which are required for business and academic reasons. For example, applications that are required to be available only on campus should not accept authentications from the public internet.

3.6.4. Whenever possible, systems and applications shall use the University of Regina centralized authentication system and its associated username and passwords for authenticating members of the University of Regina constituency instead of creating a separate, unique ID

or username. Supported mechanisms to integrate your system or application into the centralized authentication system include LDAP, RADIUS, SAML, and CAS.

3.6.5. Whenever possible, application creators and owners shall ensure that applications do not store passwords.

3.6.6. Applications and/or systems are required to lock, disconnect or require re-authentication after a reasonable period of idle.

3.6.7. For role management, applications or systems must allow one user ability to take over the functions of another user without having to share a password.

3.6.8. System and application owners shall avoid configuring systems and applications to allow or permit store or save password functionality in order to permit access without full re-authentication.

3.7. Multifactor Authentication (MFA)

3.7.1. The use of multifactor authentication mechanisms on systems and applications are recommended to strengthen authentication.

3.7.2. Whenever possible, systems and applications shall use supported mechanisms (Duo MFA) for multifactor authentication. Other means for multifactor authentication can only be used when supported methods are not compatible.

3.7.3. Supported second factors to be used for purposes of multifactor authentications include, in order of preference: push-based mobile application access token, supported time-based one-time password tokens (Duo D-series hardware tokens), supported HMAC-based one-time password tokens (such as Yubikey hardware tokens), temporary offline bypass codes, and backup codes. SMS should not be used as a second factor, except for multifactor authentication account enrolment/device provisioning, or where no other second factor is feasible.

3.7.4. Where hardware tokens are provided for second factors for purposes of multifactor authentications, the costs of additional, lost, damaged, or stolen tokens may be billable.

3.7.5. When an application or system is enabled, multifactor authentication is required on the first login of any new device, and at maximum every 15 days thereafter or upon suspicious authentication attempts.

3.8. Password Expiry

3.8.1. Passwords or multifactor authentication second factors (push-based mobile application access token, hardware token, bypass/backup codes, etc.) that have suspected use without authorization, lost, stolen, shared or publicly disclosed shall be reported to the IT Support Centre and associated accounts shall be locked/expired immediately.

3.8.2. Where technically practical, accounts which have passwords exceeding maximum age, or do not meet minimum password requirements (composition or length), shall be locked or expired.

3.8.3. Where technically practical, systems and applications shall implement brute force protection mechanism which limit the number of failed log on attempts. If an account exceeds the number of permitted failed attempts, the account shall be locked or expired for a minimum of the lockout duration.

3.8.4. If a user's relationship with the University ends, accounts must be expired or locked immediately.

3.9. Shared Accounts

3.9.1. Shared or generic accounts should not be utilized when an individual account can be utilized. Shared accounts should only be issued when technology requirements do not allow for individual accounts. Otherwise, the usage of shared accounts is strongly discouraged due to the difficulty of attributing individual actions through the accounting and auditing of shared accounts.

3.9.2. The passwords to system administrator and service accounts essential to the operation of an information system must be accessible to more than a single person. Any privileged account, such as root, super user, administrator, or any account that would be considered a master account should be escrowed to ensure availability for emergency access from authorized personnel.

3.10. Key Based Authentication Mechanisms

3.10.1. Where public private cryptographic key pairs are used as an authentication mechanism, the storage of private keys must be protected with passwords or passphrases commensurate with the level of system access or type of data access granted to the account secured with the key.

3.10.2. Passphrases applied to the private key are required for all interactive or user accounts. Wherever possible, passphrases applied to the private key are recommended where an SSH agent can be utilized.

3.10.3. Passphrases for a private key shall meet minimum password requirements for the account category.

3.11. This standard is subject to compliance audit, review and revision to ensure its effectiveness as authentication mechanisms, threats, and risks change.

4. Exceptions:

Exceptions to this standard require the written approval of the AVP Information Services or designate.

In determining if an exception to this standard is warranted, consideration will be given to any other security measures implemented or mitigating controls in place to manage the information security risk in a manner consistent with this standard.

Related Information

- Authentication Management Policy OPS-050-035
- Password Management Standard
- Password Guidelines

Revision History

Version	Version Date	Status	Summary of Change	Author
0.1	Feb. 11, 2017	Draft	Initial Draft	R. Jesse
0.2	Feb. 27, 2017	Draft	Include feedback from D. Wilson	R. Jesse
0.3	Mar. 25, 2017	Draft	Include feedback from ISET meetings	R. Jesse
0.4	April 10, 2017	Draft	Editorial corrections and feedback from UITSC	A. Exner
1.0	Jan. 5, 2018	Final	UITSC Approval	R. Jesse
1.1	April 21, 2021	Update	MFA Additions	R. Jesse