Password Management Standard

Version: 1.0
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 states that poor password management or construction imposes risks to the security of University information systems and resources. Appropriate standards for construction and management of passwords greatly reduce these risks.

This Standards document is intended to provide direction and guidance to anyone who requires the use of passwords to authenticate access to University information systems or data.

2. Scope

The requirements in this standard apply to passwords for any computing account on any University computing or information resource, to the users of any such accounts, to application owners, and to system administrators and developers who manage or design systems that require passwords for authentication.

3. Definitions

- *Character Sets:* An enumeration of characters having the same attribute. Examples include lower case characters, upper case characters, digits, and the group of special characters found on common English language 'QWERTY' keyboards.
- *Institutional Data*: All data owned or licensed by the University.
- *Non-public Information:* Any institutional data that is considered as sensitive or restricted as defined in this standard.
- Privileged Access: Any service account or system administrator account, as defined in this standard, is deemed to provide elevated rights.
- *Restricted Data***:** Institutional data should be considered as 'Restricted' when the unauthorized disclosure, alteration or destruction of that data could reasonably cause material harm to the University or its affiliates. Significant harm occurs when the unauthorized disclosure, modification, destruction, or disruption of access to information could be expected to have severe adverse effect on finances, operations, assets or individuals. Restricted data includes data protected by University policy, legislation or privacy regulations, or data protected by confidentiality agreements. Examples of restricted data include health data, credit card numbers, or personally identifiable information on students, employees, donors, and alumni.
- *Sensitive Data***:** Institutional data should be classified as 'Sensitive' when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. Moderate harm occurs when the unauthorized disclosure, modification, destruction, or disruption of access to information could reasonably be expected to have a serious adverse effect on finances, operations, assets or individuals. By default, all institutional data that is not considered as Restricted or public data should be treated as Sensitive data. A reasonable level of security controls should be applied to sensitive data. Sensitive data is available only to those within the institution with a legitimate need to know. Examples may

include, de-identified research data, internal documents, or email messages not containing restricted data.

- *Service Account*: An account not intended for individual use which is required to run tasks on a scheduled basis, interact with an application or system, and may be privileged. Such an account may be a generic account which is used by applications to access databases, run batch jobs or scripts, or provide access to other applications. Service accounts may never be used interactively by system administrators or end users.
- *System Administrator*: An account specially privileged with rights to facilitate system or application administration. Examples include soft-install, supervisor, admin/administrator or root accounts. Such an account may permit configuration changes, changes in permissions, or otherwise elevated privileges above a normal end user.

4. Standard

4.1. Each person affiliated with the University of Regina has one or more security roles, levels of system access, or access to types of data with varying degrees of sensitivity. Each of these access roles, levels, or types will require application of the appropriate password complexity standard as defined below. If a user has an account with multiple degrees of access resulting in conflicting password complexity requirements, the strongest requirements will apply.

4.2. Accounts are assigned to one of the following categories, based upon the individual or account's security role(s), level of system access or classification type of data to which the account grants access.

Account Category	**Account Category Description**	**Example**
C1: Low	Accounts providing access to information about oneself, or provide data at about others at unit level, or access to sensitive data but no restricted data.	Typical shared network storage without access to restricted data, eDirectory or email account not containing restricted data.
C2: Medium	Accounts providing access to sensitive data at the institutional level, or access to restricted data, or privileged access to a system not containing restricted data.	Banner INB, CASPUR, Clockworks, StarRez, payment systems, eDirectory or email accounts with access to restricted data.
C3: High	Accounts providing access to control at the institutional level, privileged access to a system containing restricted data.	System Administrator Accounts, Service Accounts

4.3. Minimum password standards are assigned to each of the following Account Categories based upon the account's security role(s), level of system access or classification type of data to which the account grants access.

Password Attribute	Account Category		
	C1: Low	**C2: Medium**	**C3: High**
Minimum Length of Password	8	10	16
Maximum Length of Password	Not enforced.	Not enforced.	Not enforced.
Maximum Age of Password (Days)	365	365	365
Password Uniqueness History	10 Previous Passwords or 3 Years	10 Previous Passwords or 3 Years	Unlimited
Failed attempts before lockout	7	5	5
Lockout duration (minutes)	1	15	30
Minimum Character Sets Composition Requirements (lowercase letters, uppercase letters, numerals and special characters)	3 out of 4 character sets	3 out of 4 character sets	3 out of 4 character sets

4.4. Users are required to meet password attribute minimums in terms of complexity, length, age and other attributes for the appropriate Account Category when constructing a password.

4.5. Application and system owners are required to ensure applications and systems are configured to enforce the password attribute minimums in terms of complexity, length, age and other attributes for the appropriate Account Category when a password is set.

4.6. Where not practical for service accounts to be re-keyed or assigned a new password (i.e. resulting in a service outage), such an account can be exempted from maximum password age requirements. Service accounts must otherwise be sufficiently protected against exposure through access controls, encryption or other controls.

4.7. Users, systems, or applications *must not*:

4.7.1. construct passwords consisting of only a word found in a common dictionary.

4.7.2. create or utilize passwords or keys for University of Regina accounts that are or have been used for non-University accounts. Conversely, University of Regina passwords and keys must never be used on systems or services not associated with University of Regina services.

4.7.3. construct passwords containing 3 or more repeated characters (e.g. AAA, 111), or logical sequences (e.g. 1234, abcd, qwerty).

4.8. Users, systems, or applications *should not* create passwords which:

4.8.1. use any part of your first, middle, or last name, including maiden names, initials, or nicknames.
4.8.2. use any information that is known, published, or can be obtained about you such as pet names, names of friends or relatives, phone numbers, name of the street you reside on, etc.
4.8.3. utilize a username in any form as part of your password.
4.8.4. utilize dates, in any format, as part of a password.

4.9. If electronic password storage mechanisms, such as password managers or password vaults, are utilized, authentication to the password storage mechanism must be as least as robust as the highest category of password stored within. For example, if a password manager stores passwords for accounts within the high (C3) category, then the password manager's authentication must also meet the C3 category requirements or greater.

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

Exceptions

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

In determining whether an exception is warranted, consideration will be given to any comparable security measures in place or mitigating controls used to manage information security risks in a manner consistent with the intent of this standard.

Related Information

- Password Management Policy OPS-050-035
- Authentication 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 changes and UITSC feedback.	A. Exner
1.0	Jan. 5, 2018	Final	UITSC Approval	R. Jesse