KSL Password Standard

Classification	INTERNAL
Document Reference	ITS0101
Document Version	1.0
Document Status	Final

Revision History

Version	Date	Change Number	Summary of Changes
1.0	16 Aug 2023	NA	First copy

Document Review

Date of Next Scheduled Review

Authors

Name	Title
Jonathan Ong	General Manager, Cybersecurity
Foo Tze Uei	Manager, IT Governance, Risk, Compliance

Contents

1. Objective

1.1 Introduction

Strong passwords are essential to prevent unauthorized access and data breaches, safeguarding sensitive information. A well-defined password policy reduces the risk of security breaches, enhances system reliability, and protects company and user data. Employees play a crucial role in maintaining security by adhering to password policies, thus contributing to the overall protection of the organization.

1.2 Purpose

This document outlines the password standards and best practices to ensure the security and integrity of user accounts for accessing KSL systems and applications.

Its purpose is to allow users to easily create passwords that are reasonably hard to guess, for systems access.

1.3 Background

Passwords are ubiquitous in modern society. It is the easiest form of computer security to implement. Having inconsistent password policies across different systems has often led to confusion and frustration for users.

This document aims to reduce those inconsistencies by defining a set of password standards for various types of systems and user accounts utilised in KSL.

2. Scope of Coverage & Applicability

All KSL systems and applications regardless of hosted on-premises or private/public cloud that perform any user, administrator, and/or system authentication should comply with this password standard. Entities or business systems that are unable to fully adopt this standard should seek approval for IT technology deviations from IT GRC.

3. Target Audience

This document is intended for staff:

- who use or manage accounts and passwords.
- who evaluate, recommend, and procure commercial hardware/software that require user, administrator, or system authentication.
- who manage, administer, or develop systems or applications that performs user, administrator, or system authentication.

4. User Authentication

Single Sign-On (SSO) to KSL's Azure Active Directory should be configured as the preferred method for authentication, where possible, as that will automatically enforce the standard KSL authentication controls.

If SSO could not be used, then having a strong password would provide an essential barrier against unauthorized access. Multi-Factor Authentication (MFA) should also be implemented, in such cases, where possible.

5. Password Requirements

Different types of user accounts and systems/applications have different levels of risks and capabilities. This document will describe the password requirements for the following types of accounts and systems/applications.

- Domain-joined interactive accounts and systems (AD, Azure AD, SSO)
- Local interactive accounts and systems (Servers, laptops, desktops)
- Non-SSO critical or high-risk applications
- Non-SSO non-critical applications
- Non-interactive service accounts

5.1 Domain-joined Interactive Accounts and Systems

This section describes the password requirements for accounts, systems or applications that are authenticated via **Active Directory**, **Azure Active Directory** or **Single Sign-On**.

Parameter	Setting
Minimum Length	12
Complexity	At least one uppercase At least one lowercase At least one number At least one symbol
Password History	5
Maximum Password Age	180 days
Account Lockout	5 incorrect attempts within 15 mins
Account Lockout Action	Re-enabled after 20 mins
Multi-Factor Authentication	Required

5.2 Local Interactive Accounts and Systems

This section describes the password requirements for accounts on Servers, Laptops and Desktops.

Parameter	Setting
Minimum Length	12
Complexity	At least one uppercase At least one lowercase At least one number At least one symbol
Password History	5
Maximum Password Age	180 days
Account Lockout	5 incorrect attempts within 15 mins
Account Lockout Action	Re-enabled after 20 mins
Multi-Factor Authentication	If supported

5.3 Non-SSO Applications (Critical / High Risk)

This section describes the password requirements for critical or high-risk systems and applications that are not SSO enabled.

Parameter	Setting
Minimum Length	12

Complexity	At least one uppercase At least one lowercase At least one number At least one symbol *(if supported)*
Password History	5 *(if supported)*
Maximum Password Age	180 days
Account Lockout	5 incorrect attempts within 15 mins *(if supported)*
Account Lockout Action	Re-enabled after 20 mins *(if supported)*
Multi-Factor Authentication	Required

5.4 Non-SSO Applications (Non-Critical)

This section describes the password requirements for non-critical systems and applications that are not SSO enabled.

Parameter	Setting
Minimum Length	12
Complexity	At least one uppercase At least one lowercase At least one number At least one symbol, if supported
Password History	5 *(if supported)*
Maximum Password Age	180 days
Account Lockout	5 incorrect attempts within 15 mins *(if supported)*
Account Lockout Action	Re-enabled after 20 mins *(if supported)*
Multi-Factor Authentication	Required, if external-facing

5.5 Non-Interactive Accounts

This section describes the password requirements for non-interactive accounts. Such accounts are typically used for by applications, rather than human users. E.g. Service Accounts.

Parameter	Setting
Minimum Length	14
Complexity	At least one uppercase At least one lowercase At least one number At least one symbol
Password History	5 *(if supported)*
Maximum Password Age	365 days
Account Lockout	5 incorrect attempts within 15 mins *(if supported)*
Account Lockout Action	Re-enabled after 20 mins *(if supported)*
Multi-Factor Authentication	If supported

6. Password Creation Guidelines

Adherence to the above password requirements does not guarantee a strong password. Users should also take into consideration the following guidelines to generate a strong password.

1. **Length is the most important characteristic of a good password**. In general, the longer the password, the better.

2. **Use pass-phrase, instead of pass-word**. A “phrase” made up of 4 or more smaller words is easier to remember than a single long “word”.
3. **Avoid patterns**. Do not use sequences of numbers, letters or keyboard patterns.
4. **Do not reuse a password or similar passwords on multiple systems**. Especially, between home and work accounts.
5. **Avoid words related to personal information or common interests**. Avoid using your birthdate, job titles, or things that people can find out about the user on the Internet.
6. **Limit using dictionary words**. Using dictionary words makes it easier for hackers to brute-force the password.

This page is intentionally left blank