SACSF Guideline 10.0: Password Management

Introduction

Cyber security is fundamental to the successful operations of the South Australian (SA) Government. Cyber security risks are evolving, as rapid technological advances lead to an increased reliance on technology to perform critical business functions. The management and effective sharing of information and information technology resources is essential to maintain legal and regulatory compliance, reputational image, and meet the objectives of the SA Government.

The South Australian Cyber Security Framework (SACSF) has been prepared to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of SA Government agencies.

Applicability

The SACSF applies to:

- all South Australian Government Public Sector agencies and personnel operating on behalf of the agencies (as defined in ICT Policy Statement 1 – Compliant Authorities)
- non-government suppliers and personnel that access SA Government information and resources.

Background

Government agencies depend on information to provide services to citizens, businesses and the community. This information is accessed by many internal and external users through applications and networks.

To meet expectations in terms of service delivery, while maintaining information security, agencies are expected to undertake management of passwords for their personnel. Should any government-owned assets or systems be accessed by non-government suppliers or personnel, the same password policies may be inherited.

Password management is a mechanism by which access to information and systems can be controlled. This guideline aims to assist agencies in suitable practices, controls and other mechanisms for effective password management.

Scope

This guideline provides recommended considerations for password management, is provided as a guide only and cannot be used for audit purposes.

The guidance was prepared using national and international best practice[1]. Agencies should take a risk-based approach to password management. This includes performing a risk assessment to assist in determining a password policy.

The SACSF policy statement related to this guideline is:

South Australian Cyber Security Framework (SACSF) ***Policy Statement 2.4: Access to Information****, which states that:*

> Access to agency systems, applications and information must be based on business need, authorised by the information owner or delegated custodian and be limited to the minimum required for personnel to undertake their duties. Secure authentication mechanisms must be in place to control access to agency systems, applications and information.

It also relates to ***Policy Statement 2.5: Administrative Access***, which states that:

> Administrative access to agency systems, applications and information must be restricted to personnel with a specific business need which is validated on a periodic basis.

This guideline also aligns with the *Code of Ethics for the South Australian public sector*, *Professional Conduct Standards* in relation to *Handling Official Information,* which stipulates that:

> Public sector employees will maintain the integrity and security of official information for which they are responsible.

Considerations

Governance

It is important that personnel understand the role and responsibilities they have when managing passwords within an agency.

Agencies should develop a password policy and supporting standard or procedure, including (but not limited to):

- password complexity requirements for standard user, privileged, local and service accounts. Including the storing of plain text passwords or secrets in source code
- promote the use of passphrases consisting of four or more random words
- passwords across standard user, privileged, local and service accounts are not re-used

[1] refer to the Related documents section[2]Passwordless protection RE2KEup (microsoft.com)

- the incorporation of process to manage the storage of passwords, password alternatives and authentication methods
- the management of standard user, privileged, local and service accounts passwords when staff leave the agency or experience a compromised account
- document risk-based decisions for password management in a register
- provide regular password management awareness to all staff and promote the use of passphrases.

Password management considerations

To protect information against unauthorised access, agencies should set appropriate password controls, such as:

- Setting a password requirement to access all systems and services
- Enforcing the maximum password reuse period, to ensure unique passwords are created across standard user, privileged, local and service accounts
- Set the maximum age to six (6) months to ensure the system enforces a password reset
- Set the minimum password age to one (1) day
- Set the user account to be locked after a minimum of five (5) unsuccessful password attempts
- Force passwords changes if:
    - they are directly, or suspected of being, compromised
    - they appear in an online data breach database
    - they have not been changed in the past six (6) months
    - it is a first-time log on
- Never store passwords in clear, readable format (encryption should be used)
- Limit cached credentials to one previous login
- Check new or updated passwords against a list of commonly used, expected, or compromised passwords to ensure they cannot be easily guessed
- Upon account recovery, request immediate selection of a new password (for example, in situations when a password is forgotten)
- Protect passwords using organisation-defined controls
- Protect the collection of passwords by encrypting them and storing the collection offline in a token
- Do not display passwords on screen while being entered
- Only transmit credentials over secure channels
- Provide an agency-defined password management/storage tool to generate and manage passwords, to ensure that the same password is not used on multiple systems
- Enable Multi-factor authentication for critical systems and services.

Specific password requirements for user accounts and privileged accounts

An agency should increase the time on average it takes an adversary to compromise a credential by continuing to increase its length over time. Such increases in length can be balanced against useability with the use of passphrases rather than passwords.

In cases where systems do not support passphrases, and as an absolute last resort, the strongest password length and complexity supported by a system should be implemented. Agencies should consider the enforcement of:

- A minimum of ten (10) characters for standard user accounts
- A minimum of fourteen (14) characters for privileged user accounts.

Specific password requirements for local and system accounts

- Enforce a minimum of fourteen (14) characters
- Ensure credentials are unique, unpredictable and managed
- Ensure physical credentials are stored separately from systems to which they grant access
- Ensure credentials stored for systems are protected by a password manager, a hardware security module; or by hashing, salting and stretching them before storage within a database.

Enforce multi-factor authentication

Multi-factor authentication is a method of increasing the security of password management. Enabling multi-factor authentication as part of our agency policy adds an additional layer of security.

Multi-factor authentication requires you to prove your identity in two or more ways before you can access sensitive features of password management. It typically requires a combination of at least two of:

- something you know (e.g., a password or PIN)
- something you have (e.g., an authenticator app or physical token) or
- something you are (e.g., your fingerprint or face scan).

Password authentication alternatives

Passwordless authentication is a form of Multi-factor authentication (MFA) that can be used to replace passwords with secure password alternatives.

Agencies should consider:

- Alignment to Web Authentication API (WebAuthN) and Fast Identity Online (FIDO2) standards as a form of authentication[2].
- Passwordless sign-in options, such as the Microsoft Authenticator. Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a user's device, where the device uses an alternative password authentication method, i.e., your fingerprint or face scan.

Password manager

Password managers provide the option for employees to store all their passwords behind a master password. This enables users to store a range of complex passwords or passphrases in a secure platform, without having to remember them all.

As per the standard process for introducing any new platform, a risk assessment should be conducted by agencies before implementing or recommending a password manager to staff.

Related documents

- South Australian Cyber Security Framework (SACSF)
- ICT Policy Statement 1 – Compliant Authorities
- Code of Ethics for the South Australian public sector
- Information Security Manual (ISM) | Cyber.gov.au
- Microsoft Policy Recommendations
- Security and Privacy Controls for Information Systems and Organizations (nist.gov)
- Australian Cyber Security Centre (ACSC) – Creating strong passphrases
- ISO/IEC 27002-2013

[2]Passwordless protection RE2KEup (microsoft.com)

Document control

ID	SACSF/G10.0
Version	0.1d
Classification/DLM	OFFICIAL
Compliance	Discretionary
Original authorisation date	N/A
Last approval date	June 2022
Next review date	June 2023