



SACSF/G10.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 10.0: Password Management

Purpose

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.

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 practice¹. 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 applies to:

- South Australian Government public sector agencies, that is, administrative units, bodies corporate, statutory authorities and instrumentalities of the Crown as defined in the Public Sector Act 2009.
- Suppliers to the SA Government and non-government personnel providing services to agencies.

The SACSF policy statements related to this guideline are:

- **SACSF Policy Statement 2.4: Access to Information** - 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.
- **SACSF Policy Statement 2.5: Administrative Access** - 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.

¹ Refer to the Related documents section.² Passwordless protection [RE2KEup \(microsoft.com\)](https://www.microsoft.com/en-us/identity/re2keup).

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 should be applied.

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.

Guidelines

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, that includes (but not limited to):

- password complexity requirements for standard user, privileged, local and service accounts
- prohibiting the storing of plain text passwords, or secrets in source code
- promoting the use of passphrases consisting of four or more random words
- prohibiting the re-use of passwords across standard user, privileged, local and service accounts
- processes 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
- documenting risk-based decisions for password management in a register
- providing regular password management awareness to all staff that includes promoting the use of passphrases, password managers, and good password hygiene such as not reusing passwords across multiple platforms.

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
- setting the maximum age to (6) months to ensure the system enforces a password reset

- setting the minimum password age to one (1) day
- setting the user account to be locked after a maximum of five (5) unsuccessful password attempts
- forcing password 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 storing passwords in clear, readable format (encryption should be used)
- limiting cached credentials to one previous login
- checking new or updated passwords against a list of commonly used, expected, or compromised passwords to ensure they cannot be easily guessed
- upon account recovery, requesting immediate selection of a new password (for example, in situations when a password is forgotten)
- protecting passwords using organisation-defined controls
- protecting the collection of passwords by encrypting them and storing the collection offline in a token
- not displaying passwords on screen while being entered
- only transmitting credentials over secure channels
- providing an agency-defined password management/storage tool to generate and manage passwords, to ensure that the same password is not used on multiple systems
- enabling multi-factor authentication for all cloud services and critical systems
- ensuring all successful and unsuccessful password log in events are centrally logged.

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 twelve (12) characters for standard user accounts
- a minimum of fourteen (14) characters for privileged user accounts
- alphanumeric passwords that also contain special characters
- not using previous or commonly used passwords.

Specific password requirements for local and system accounts

- Enforce a minimum of thirty (30) 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.

Enforcing multi-factor authentication

Multi-factor authentication (MFA) 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 2 or more ways before you can access sensitive features of password management. It typically requires a combination of at least 2 of:

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

Phishing-resistant multi-factor authentication is recommended.

Password authentication alternatives

Passwordless authentication is a form of 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 authentication²
- Passwordless sign-in options, such as the Microsoft Authenticator or Okta Verify. 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 (such as your fingerprint or facial recognition).

Password managers

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.

² Passwordless protection [RE2KEup \(microsoft.com\)](https://www.microsoft.com/en-au/re2keup).

Related documents

- [South Australian Cyber Security Framework \(SACSF\)](#)
- [Code of Ethics for the South Australian public sector](#)
- [Information Security Manual \(ISM\) | cyber.gov.au](#)
- [Microsoft password policy recommendations for M365](#)
- [Security and Privacy Controls for Information Systems and Organizations \(nist.gov\)](#)
- [Australian Cyber Security Centre \(ACSC\) – Creating strong passphrases](#)

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Government Chief Information Security Officer	
Division: Office of the Chief Information Officer	Compliance: Optional
Review number: V1.1	Date of approval: 24 April 2024
Next review date: May 2026	Original approval: June 2022

Licence



With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a [Creative Commons Attribution \(CC BY\) 4.0 Licence](#). To attribute this material, cite the Office of the Chief Information Officer, Department of the Premier and Cabinet, Government of South Australia, 2024.