SACSF/G16.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 16.0: Privileged Access Management

Purpose

Cyber security is fundamental to the successful operations of the South Australian Government (SA Government). The South Australian Cyber Security Framework (SACSF) and supporting guidelines have been prepared to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of SA Government public sector agencies.

This guideline has been developed to assist agencies and applicable suppliers to understand and implement the privileged access management requirements of the SACSF.

Scope

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 2.5: 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.

Privileged access is defined as all logical access to systems and ICT services via privileged accounts, which include administrator accounts, user accounts with privileged access rights, service accounts, and access to privileged utility programs.

Background

Privileged accounts have higher access rights than those of a standard user. Privileged access is used to maintain, upgrade, and configure ICT infrastructure, servers, applications, and databases. Privileged access can be associated with human users as well as non-human users such as applications and machine identities. Examples of privileged access include root access, administrator access, or access to service accounts.

Privileged accounts are often the target of attackers so that they can gain broad access to information assets and escalate privileges in systems. Privileged access controls help organisations to reduce the attack surface and increase the difficulty for threat actors to penetrate a network and make further explorations.

Guideline

Administrative and technical measures should be implemented throughout the lifecycle of privileged access management and include the following processes and areas:

- Governance and awareness
- Secure environment
- Provisioning processes
- Secure use of privileged access
- Logging, monitoring, and access review
- Access change, expiration and termination

Refer to the table on the next page for guideline details.

Governance and Awareness

Security Principles

- Agencies should define the security principles for privileged access management to establish a robust and secure governance framework that effectively safeguards critical accounts and systems.
- Security principles should be adapted when defining and designing privileged accounts to minimise the risk of unauthorised access and credential loss.
- Following are example security principles for privileged access management:
  - Separation of duties – this principle requires more than one person to complete access management processes to reduce the risk of fraud, error, or misuse of privileged access.

    For example, people who request a privileged account should not be able to approve or grant the access.

  - Least privilege – this principle restricts access rights to only those required for performing their duties. Users should not be given privileged access by default.

    For example, if an IT administrator role was filled by a new contractor, that person should not be provisioned privileged access to systems until formally requested and approved through a documented process.

  - Need to know – this principle is related to the least privilege principle but focuses on granting users access only to the data and privileged rights they need in a more granular fashion.

    The Role-Based Access Control (RBAC) model is a good example of how the access rights between two administrators can be different. For example, a database administrator who is responsible for backing up a database may not need access to the data stored in the database, or be able to configure the database schema.

Policies and Procedures

- Agencies should define and document the security requirements and objectives for privileged access management in security policies or standards. The process of managing privileged access should also be defined, documented, and communicated to stakeholders. For example, password policies that outline the complexity, minimum length, and maximum age requirements for administrative accounts should be documented for all systems and applications.
- The agency's privileged access management policies, standards and procedures should be reviewed and updated regularly in line with agency policy frameworks, or when major changes occur to the environment.

Inventory of Privileged Accounts

- Agencies should establish and maintain an inventory of all privileged accounts in use, which includes system administrator accounts and services accounts.
- The inventory, at a minimum, should contain the account names, system or application names, provisioning and expiry dates, information classification of the systems accessed, and account

	owner names. The purpose of maintaining an inventory of accounts is to ensure that all accounts are validated, properly authorised, and removed when no longer needed. In addition, the up-to-date inventory of privileged accounts could also help to perform regular access reviews and implement other relevant security controls around critical information assets.
Awareness	• Agencies should provide targeted security training to administrators and users with privileged access rights to ensure they know how to perform administrative activities securely. • Measures should also be taken to ensure that users are aware of their privileged access rights and to make it clear when they are in privileged access mode. Possible measures include using specific user identities, security banners and warning signs (e.g. WARNING: PRIVILEGED ACCESS MODE - Authorised use only. Unauthorised access or misuse is strictly prohibited!), user interface settings and dedicated workstations. These controls help users to identify the privileged access has been established so that they can handle the access properly.

Secure Environment

Local Administrative Accounts Removal	• Local administrative accounts (e.g. Windows admin accounts, Linux root accounts) can be used to perform administrative tasks on the local devices, such as installing software or changing system settings. Local administrative accounts on workstations should be removed, disabled or otherwise secured against access from standard users to prevent misuse, policy breaches and lateral movement attacks.
Dedicated Privileged Access Workstations (PAWs)	• Consider providing a dedicated privileged access workstation that is used exclusively to carry out privileged activities. • Communication between this dedicated privileged workstation and the less trusted zones, such as regular user workstations, should be prevented. • Privileged access workstations should not have Internet or email access, as this may open the attack surface and increase the risk of compromise.
Segregation and Separation	• The privileged access workstations and infrastructure should be logically separated from other network zones, and only allowed communication with information assets designed for administrative tasks. • It is recommended to relay the communication through jump hosts (also known as bastion hosts or jump servers), which act as intermediaries between trusted networks and external or less secure networks. • Privileged access should not be established directly from unsecure networks or less privileged environments. • Unprivileged accounts should not be able to logon to privileged operating environments. • Privileged operating environments should not be virtualised within unprivileged operating environments.

	• Privileged accounts should be prevented from logging into lower trust and unprivileged locations (e.g. a server administrator should not be able to log into a workstation unless it is a privileged access workstation (PAW).
Secure Active Directory	• Active Directory (AD) plays a vital role in access management and requires proper security controls to prevent compromise. Secure configuration and hardening controls should be implemented to the agency managed AD tenancies (Best Practices for Securing Active Directory | Microsoft Learn), and Azure AD if applicable (Best practices to secure with Azure Active Directory - Microsoft Entra | Microsoft Learn).

Provisioning Processes

Provisioning Process	• Agencies should establish and follow a standard process, preferably automated, for granting privileged access to users upon formal request and approval. • An authorisation process should be maintained (for determining who can approve privileged access rights and ensuring privileged access rights are not granted until the authorisation process is complete) and records of all privileges allocated kept.
Account Creation	• System administrators should be assigned dedicated and unique administrative accounts to perform administrative tasks. • Specific rules should be established to avoid the use of generic administration usernames, such as root and admin, depending on systems' configuration capabilities. • The passwords of the administrative accounts should be complex, unique and at a minimum 14 characters long. • An expiry date should be assigned to the privileged account provisioned according to the business needs and third-party contracts. • Technical controls should be put in place to restrict the use of privileged accounts from reading emails, accessing the Internet, and obtaining files via online services (e.g. public cloud storage).
Securely Deliver Privileged Credentials	• Privileged credentials should be securely delivered to administrators and privileged users. • Credentials should never be transmitted in plain text or insecurely over communication channels. Instead, encryption should be applied to protect the confidentiality of credentials during transit. • A secure and reliable delivery mechanism should be established, such as a secure file transfer protocol (SFTP) or a password vault with strong access controls.
Multi-Factor Authentication (MFA)	• Authentication requirements for privileged access rights should be higher than the normal user access, and re-authentication or authentication step-up controls should be considered.

- Agencies should enable multi-factor authentication (MFA) for all administrative access accounts, where supported, on all systems and applications, whether managed internally or through a third party service provider.

Secure Use of Privileged Access

Centralised Account Management

- Privileged account management should be centralised through a directory or identity management solution, such as AD, Azure AD, or a Privileged Access Management (PAM) solution. A centralised PAM solution can enforce security policies, establish baselines, and monitor privileged access.
- Agencies should centralise the federated authentication processes for all privileged accounts through a directory service or Single Sign-on (SSO) solution, where supported.
- For legacy systems and applications where PAM or SSO measures are not supported, agencies should perform a risk assessment and manage the security risks associated with the legacy authentication access controls.

Just-in-time (JIT) Administration

- Agencies should grant temporary privileged access only for the time necessary to implement approved changes or activities (e.g. for maintenance activities or critical changes to systems and infrastructure), rather than permanently granting privileged access rights.
- Just-in-time (JIT) administration can be automated by a PAM solution.

Use of privileged utility programs

- Privileged utility programs are applications that require administrative privileges to perform specific tasks, which might be capable of overriding system and application controls. Examples include diagnostic tools, patching assistants, anti-virus programs, disk defragmenters, backup software, networking tools, and debuggers. In Windows operating systems, some common privileged utility programs are the Windows Task Manager, Windows Registry Editor, Windows PowerShell, and Windows Command Prompt.
- Controls to secure the use of privileged utility programs include:
    - Removing or disabling all unnecessary utility programs and limiting the use of utility programs to authorised users.
    - Use of identification, authentication, and authorisation procedures for utility programs, including unique identification for users.
    - Logical segregation of utility programs from other systems and applications. Where practical, segregating network communications for privileged utilities.
    - Using application control to prevent unwanted utility programs from running.

Logging and Monitoring

Logging and Monitoring	• All privileged access to systems should be logged for audit purposes and to monitor administrative actions for unusual activity. This includes administrative access from internal and third-party users. • Agencies should capture and store all event logs and audit logs for all administrative activities, privileged access, privileged account changes, and security group management events. • Where possible, agencies should centralise log management and protect the logs from unauthorised modification and deletion. • Administrative logs should not be able to be modified by users that are being monitored (e.g. the administrators should not be able to modify or delete their administrative logs). • Logs should be stored separately from application databases and write access from users should be restricted. • Agencies should monitor logs for signs of compromise and investigate when any signs of compromise are detected.

Access Review, Change, Expiration and Termination

Access Review	• Agencies should regularly, and after any critical system and personnel changes, review privileged access rights to verify if the privileged users' duties, roles, responsibilities and competence still qualify them for working with privileged access rights. • The review frequency should be, at a minimum, every six (6) months, or every three (3) months for critical systems. The review results should be properly documented and reported to management to address identified issues.
Change of Access	• Agencies should monitor for any privileged users who change their job roles and review their privileged access rights. If users change roles but retain former privileges or request new privileged access without proper justification or revocation, they may accumulate access rights beyond their job responsibilities, which may lead to privilege creep and security breaches. • All requests for additional privileged access should be assessed separately. Access should not be granted based on existing approved access. • An example control to minimise the risk of privilege creep is to maintain an up-to-date RBAC matrix based on users' job roles access rights, and keep records of any changes to the matrix.

Access Expiration	• Requirements for expiry of privileged access rights should be defined and implemented. • Privileged access to systems and applications should be automatically disabled after 12 months unless revalidated.
Disable Dormant Accounts	• If an account is no longer needed or if the owner confirms its inactivity, take appropriate action to disable or remove the account. This ensures that the account cannot be misused or targeted by unauthorised individuals. • Agencies should disable dormant administrative accounts after 45 days of inactivity, and automate the processes where supported.
Termination of Access	• Administrative access should be revoked immediately once there is no longer a specific business need for it. Agencies should establish and follow a standard process, preferably automated, for revoking privileged access, through disabling accounts immediately upon termination, rights revocation, or role change of a user. • Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails. However, it is essential to be aware of the potential security risks associated with disabled accounts, including insider threats and account exploitation.

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this guideline. There is no specific impact on Aboriginal people.

Related documents

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls
- South Australian Cyber Security Framework (SACSF)
- Australian Cyber Security Centre - Information Security Manual (ISM)
- Australian Cyber Security Centre – Essential Eight

Definitions

Term	Definition
Privileged account	Privileged accounts are considered to be those which can alter or circumvent a system's controls. This can also apply to users who have only limited privileges, such as software developers, but can still bypass controls. A privileged account often has the ability to modify system configurations, account privileges, event logs and security configurations for applications. Privileged accounts include privileged user accounts and privileged service accounts.
Privileged operating environment	An operating environment used exclusively for administrative activities.
Privileged utility program	An application that requires elevated (administrative) privileges to perform a specific task, e.g. software updates, or firewalls.
Service account	User accounts that are used to perform automated tasks without manual intervention, such as machine to machine communications.
Virtualisation	Simulation of a hardware platform, operating system, application, storage device or network resource.

Acronyms

Acronym	Words
SACSF	South Australian Cyber Security Framework
RBAC	Role Based Access Control
AD	Active Directory
PAM	Privileged Access Management
SSO	Single Sign-On

DOCUMENT CONTROL

Approved by: CIO Steering Committee	
Contact: Government Chief Information Security Officer	
Division: Office of the Chief Information Officer	Compliance: Optional
Review number: V1.0	Date of approval: 20 September 2023
Next review date: September 2024	Original approval: 20 September 2023

Licence