16.4. Privileged Access Management

Objective

16.4.1. To ensure Privileged Access Management (PAM) is incorporated into IT Governance and that privileged accounts are managed in accordance with agency's PAM policy.

Context

Scope

16.4.2. This section provides information and guidance on the establishment and operation of an agency's Privileged Access Management policy and control mechanisms. This is sometimes also described as Privileged Account Management. In the context of this section the terms are synonymous.

16.4.3. Reference to other sections in this document is essential. In particular:

- 3.5 System Users;
- 5.1 Documentation Fundamentals;
- 6.3 Change Management;
- 9.1 Information Security Awareness and Training;
- 16.1 Identification, Authentication, and Authorisation;
- 16.2 System Access;
- 16.3 Privileged User Access;
- 16.7 Multi-Factor Authentication.

Background

16.4.4. **Privileged Access Management (PAM)** – sometimes also described as Privileged Account Management, refers to a set of processes and tools for granting, controlling, monitoring, and auditing privileged access.

16.4.5. A **Privileged Account** is a user account with high levels of access to systems, devices and data. Privileged accounts may, for example, be able to install or remove software, delete data, upgrade operating systems, or modify system or application configurations. They may also have access to data that is not normally accessible to standard users.

16.4.6. Privileged accounts invariably have direct or indirect access to most or all IT assets of an agency or organisation. When used improperly or maliciously, privileged accounts represent a significant security threat to operations, often exposing sensitive data, impeding operations or damaging IT systems. Any compromise of these accounts is, therefore, a significant business, operational and reputational risk.

16.4.7. Risks associated with privileged accounts have increased in recent years with the expansion of endpoints and use of new technologies including Cloud, Internet of Things (IoT) and the rapid and significant increase in remote and working from home environments.

16.4.8. Managing, controlling, monitoring and reviewing privileged access is fundamental to mitigating the risks posed by insider and external threats, privilege escalation threats, preventing unauthorised data access and data breaches, and meeting compliance requirements.

16.4.9. There are many types of privileged access including:

- **Root**, **Domain** and other **Administrator** accounts are typically used for installing, updating and removing software, changing configurations and administering system passwords.
- **Service Accounts**, which may include local or domain accounts, are typically used for running processes, such as web servers, database servers, and application servers. These may also include the ability to change passwords.
- **Emergency Accounts**, sometimes referred to as "DRP", "firecall", or "breakglass" accounts. These are highly privileged accounts that are critical for maintaining administrative access in case of emergency. While access to these accounts normally requires managerial approval as a security measure, they should only ever be used when normal administrative accounts are unavailable and when critically necessary.
- **System** or **Application Accounts** are characteristically used by devices and systems for running operating system components and owning related files.

16.4.10. Traditional administrative or management solutions are typically based on strong password management. Modern systems, especially in a cloud environment, require a more structured and robust means of access control and management. This should include the use of Multi-Factor Authentication (See Section 16.7 - Multi-factor Authentication) to provide access to privileged accounts.

16.4.11. In secure environments, privileged accounts should be reserved for network and system administrators to manage the access to and oversight of sensitive information and resources in support of normal agency or organisational operations.

16.4.12. The characteristics and capability of privileged accounts are described at 16.3.3. It is important to note that systems themselves, as well as human users, may have privileged account access. As such it is important to clearly and individually identify all real persons, systems and devices with privileged account access.

16.4.13. Access accounts or channels may have the following characteristics:

- **Regular access channels**—protected channels that are subject to standard IT controls;
- **Privileged access channels (PACs)**— channels that might circumvent regular controls but are deemed necessary and legitimate operational channels for reasons of practicality or cost;
- **Unintended channels**—not demanded by any technical or business requirement and represent a vulnerability.

Emergency accounts (Break glass accounts)

16.4.14. Emergency accounts (also known as break glass accounts) are highly privileged accounts and should only be used for maintaining access to an organisation's critical systems in emergencies. These accounts require additional layers of protection and should never be used for regular administrative functions.

16.4.15. Additional protections include:

- Break glass accounts are **only** used when normal authentication processes cannot be used, **and** when there is a critical need to access systems (or testing these for disaster recovery).
- **Use of non-expiring passwords**: passwords for break glass accounts should not expire. This helps prevent lockouts during emergencies.
- **No individual association**: ensure emergency accounts are not associated to an individual user.
- Central logging and auditing of all actions related to use of break glass accounts should be performed. Accounts are tested after credentials are changed.

16.4.16. Emergency accounts should be excluded from MFA policy. MFA on break glass accounts should be managed through other mechanisms outside system policy.

16.4.17. Emergency accounts should have MFA without being associated to any user. Examples of how this can be accomplished are:

- Utilisation of a password
    - Passwords can be split into two and stored in separate safes with strict limitations on authorised personnel accessing each safe.
- Use of FIDO2 security keys
    - Two separate keys can be registered and stored in separate safes with strict limitations on authorised personnel accessing each safe.
- Virtualisation, noting this option cannot be associated to an individual user.

16.4.18. It is important to consider adequate storage and access of break glass accounts in disaster recovery plans. Storage, including how (and when) to access these accounts should be included in disaster recovery planning (DRP) (Chapter 3).

Attacks on privileged accounts

16.4.19. Privileged accounts frequently allow unrestricted access the IT infrastructure, often including data residing on those systems. The very high level of access and capability associated with privileged accounts makes them a prime target for external attackers and malicious insiders. A compromise of a privileged account can be extremely damaging and may even take down systems, such as in ransomware attacks.

16.4.20. Compromised privileged accounts represent one of the largest security vulnerabilities an organisation. A compromise may allow attackers to take full control of an organisation's IT infrastructure, disable security controls, steal confidential information, commit financial fraud and disrupt operations. Stolen, abused or misused privileged credentials are identified in a very high proportion of successful breaches.

16.4.16. Common attack methods may include:

- Probes and scans;
- endpoint targeting;
- System and design vulnerability exploitation;
- Social engineering (including phishing, email spoofing, etc); and
- Malware implants.

16.4.22. These attack methods are essentially the same as attack methods on standard accounts. The difference, however, is the level of access an attacker gains once successful, and the increase of risk to entities and organisations.

Governance and Control

16.4.23. Privileged accounts are frequently used to deploy and maintain IT systems and necessarily exist in nearly every connected device, server, database, and application. Privileged accounts may extend beyond an agency-controlled IT infrastructure to include, for example, employee-managed corporate social media accounts. Most agencies and other organisations can typically have many more privileged accounts than employees, sometimes as many as two or three times the number of employees. It is not unusual for some privileged accounts to be unidentified, overlooked, unmanaged, and therefore unprotected.

16.4.24. Governance ensures that privileged accounts are properly approved, controlled, monitored and decommissioned throughout their entire lifecycle. A PAM policy defines the roles, policies and mechanisms for access requests, as well as the workflow for privileged access approvals and delivery. Monitoring and auditing ensure that account permissions and usage remain appropriate over time. PAM governance is a fundamental part of IT Governance as it can influence other IT security systems, such as identity and access management systems.

16.4.25. To support strong IT Governance, it is vital that security efforts are coordinated, and technology investment managed. This includes the integration of PAM into the Information Security Policy, Systems Architecture, IT Security Strategy and Risk Management Plan. The sensitivity of data and operations should be assessed by undertaking an impact assessment.

16.4.26. Underpinning any PAM is the principle of enforcement of least privilege. This is defined as the minimisation of access rights and permissions for users, accounts, applications, systems, devices and computing processes to the absolute minimum necessary in order to perform routine, authorised activities and maintain the safe and secure operation of agency or organisational systems.

16.4.27. Enforcing the principle of least privilege assists organisations in minimising their systems attack surface and supporting audit and compliance within agencies. This also can reduce risk, complexity, and costs for organisations.

16.4.28. Provision of unnecessary system privileges or data access rights will magnify the impact of misuse or compromise of that users account and can even be devastating. Account privileges should be established to provide a reasonable but minimal level of system privileges and rights needed in order to support the purpose and role. The granting of elevated or excessive system privileges should be carefully controlled and managed.

16.4.29. Risks associated with access to privileged accounts include:

- Misuse of privileges;
- Increased attacker capability;
- Circumventing established security and oversight controls;
- Severe system disruption or failure; and
- Significant data compromise and/or loss.

16.4.30. The principles of PAM controls are to:

- Establish and maintain an inventory of privileged accounts;
- Assess the risk(s) of each privileged account;
- Enforce the principle of least privilege;
- Use Multi-Factor Authentication for access to privileged accounts;
- Minimise access to only essential activities;
- Minimise the number of privileged access channels;
- Ensure each channel and user can be uniquely identified (prevent or minimise sharing of credentials, particularly with accounts such as “root” or “admin”);
- Ensure all logs are periodically reviewed;
- Ensure strong and strict change control procedures are implemented;
- Ensure the authorisation, activation and deactivation of privileged access channels is strictly enforced;
- Regularly audit and review PAM controls; and
- Reduce scope creep through regular reviewing of privilege user accounts.

16.4.31. It is also important to define all privileged accounts used by an agency or by other organisations, particularly where outsource arrangements are in place. It is fundamental for robust security to identify and record the business functions, related data, systems and access privileges. This is particularly important for agencies that create, store and process classified data.

16.4.32. Without a comprehensive privileged accounts inventory, agencies and other organisations may overlook **“backdoor”** accounts which allow users to bypass proper controls and auditing. These may have been created during system development, by malicious insiders or by external attackers. Such unregistered accounts may be undetected for months or even years and can create a means of unauthorised and unmonitored access. Such accounts may also be used to erase activity logs to avoid detection.

16.4.33. A privileged access inventory should include a description of the IT system, information asset, privilege description, privileged users and risk classification. This is essential information for assessing risk, the determining of controls and for identifying and managing use and misuse. Of note are:

- Local or Domain Server Admin accounts;
- Domain Admin accounts that typically control Active Directory users;
- System Admin accounts that manage databases;
- Root accounts that manage Unix/Linux platforms;

- Accounts that run and manage Windows applications, services, and scheduled tasks;
- IIS application pools (.NET applications);
- Networking equipment accounts that give access to firewalls, routers, switches, session border controllers, gateways and other similar devices, whether physical or virtual.

16.4.34. Privileged Access Management systems provide many of the capabilities and controls briefly described above and can facilitate PAM, as well as supporting strong IT Governance.

References

16.4.35. Additional information relating to Privileged Account and access management, including some policy examples, can be found at:

Reference	Title	Publisher	Source
	ISO/IEC 27001	ISO/IEC/ Standards NZ	Standards New Zealand
	Restrict Administrative Privileges	ASD	Restrict Administrative Privileges | ASD's Blueprint for Secure Cloud
	Identity and access management	NCSC - UK	Identity and access management - NCSC.GOV.UK
	Securing privileged access	Microsoft	Securing privileged access overview - Privileged access | Microsoft Learn
	Manage emergency accounts in Microsoft Entra ID	Microsoft	Manage emergency access admin accounts - Microsoft Entra ID | Microsoft Learn
	Privileged Account Management	MITRE Corporation	Privileged Account Management, Mitigation M1026 - Enterprise | MITRE ATT&CK®

Rationale & Controls

Policy Creation and Implementation

16.4.36.R.01. **Rationale**

The requirement for an agency security policy is discussed and described in **Chapter 5 – Information Security Documentation**. A fundamental part of any security policy is the inclusion of requirements for the treatment of Privileged Accounts. This is most conveniently contained in a Privileged Access Management (PAM) section within the agency's security policy. A PAM policy is a fundamental component of an agency's IT Governance.

16.4.36.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6835]

Agencies MUST establish a Privileged Access Management (PAM) policy.

16.4.36.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6836]

Within the context of agency operations, the agency's PAM policy MUST define:

- a privileged account; and
- privileged access.

16.4.36.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6837]

Agencies MUST manage privileged accounts in accordance with the agency's PAM policy.

The Principle of Least Privilege

16.4.37.R.01. **Rationale**

The Principle of Least Privilege is discussed in the **Context** part of this section. This principle stipulates the minimisation of access rights and permissions for users, accounts, applications, systems, devices and computing processes to the absolute minimum necessary in order to perform routine, authorised activities and maintain the safe and secure operation of agency or organisational systems.

16.4.37.R.02. **Rationale**

The implementation of the Principle of Least Privilege requires limitations on the number and use of privileged accounts as well as minimising the numbers of users with these privileges.

16.4.37.R.03.

Rationale

The use of privileged access should also follow the principle of least privilege by ensuring the use of two-factor or Multi-Factor Authentication for access to privileged accounts and ensuring that only activity requiring such access is undertaken. Refer to Section 16.7 – Multi-Factor Authentication. User accounts without privileged access should be used for all other activities. Refer to Section 16.3 – Privileged User Access.

16.4.37.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6842]

Agencies MUST apply the Principle of Least Privilege when developing and implementing a Privileged Access Management (PAM) policy.

16.4.37.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6843]

Agencies MUST use two-factor or Multi-Factor Authentication to allow access to privileged accounts.

16.4.37.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7550]

Agencies SHOULD consider the use of time bound revocation to privileged accounts.

Strong Authentication process

16.4.38.R.01. **Rationale**

The approval and authorisation process for the granting of privileged access should be based on the requirement to manage and protect organisational systems and assets or as an operational necessity only.

16.4.38.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6846]

As part of a Privileged Access Management (PAM) policy, agencies MUST establish and implement a strong approval and authorisation process before any privileged access credentials are issued.

16.4.38.C.02. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:6847]

Privileged Access credentials MUST NOT be issued until approval has been formally granted.

Suspension and Revocation of Privileged Access Credentials

16.4.39.R.01. **Rationale**

Because privileged accounts have high levels of trust associated with the issue of related credentials, any indication that credentials or accounts have been compromised or that credentials have been misused must be immediately investigated. Actions may include the immediate suspension of credentials. Revocation may follow depending on the outcome of the investigation.

16.4.39.R.02. **Rationale**

The privileged access credentials for staff and other users (such as authorised contractors) should be suspended or revoked as part of exit procedures when staff leave the agency and when other users no longer undertake duties for the agency. This ensures the numbers of credentials are controlled, credentials are revoked when no longer required for operational purposes and that the risk of unauthorised activities and access is minimised.

16.4.39.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6852]

Agencies MUST establish robust credential suspension and revocation procedures as part of the agency's Privileged Access Management (PAM) policy.

16.4.39.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7553]

Agencies MUST investigate any indication of compromise or misuse of systems credentials or accounts.

Privileged Account, Rights and Credential Inventory

16.4.40.R.01. **Rationale**

Account and credential "sprawl" is a continuing challenge as the number of users constantly changes and the number and variety of devices evolves and grows. The growing use of the Internet of Things (IoT) is a good example of this. A primary tool in the management and containment of sprawl is the creation and maintenance of an inventory of privileged accounts and the access rights and credential associated with those accounts together with a process of continuous discovery. This will assist in curbing privileged account sprawl, identifying potential insider abuse, and exposing external threats and malicious activity.

16.4.40.C.01.

Control System Classifications(s): All Classifications; Compliance: Must [CID:6855]

Agencies MUST create and maintain a comprehensive inventory of privileged accounts and the associated access rights and credentials.

Monitoring and Review

16.4.41.R.01. **Rationale**

Privileged Accounts have high levels of system and data access and are a "high value target" for malicious cyber-attacks and insider misuse. Access to privileged accounts can be extremely damaging to systems and can cause data and privacy breaches as well as data loss.

16.4.41.R.02. **Rationale**

A key control in the ongoing integrity of privileged accounts and their associated credentials is a robust system of monitoring and review in order to maintain the inventory of privileged accounts and implement a process of continuous discovery to curb privileged account sprawl, identify potential insider abuse, and reveal external threats. This includes continuous data and operations impact assessments.

16.4.41.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6859]

Agencies MUST create, implement and maintain a robust system of continuous discovery, monitoring and review of privileged accounts and the access rights and credentials associated with those accounts.

16.4.41.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6860]

Privileged account monitoring systems MUST monitor and record:

- individual user activity, including exceptions such as out of hours access;
- activity from unauthorised sources;
- any unusual use patterns; and
- any creation of unauthorised privileges access credentials.

16.4.41.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6861]

Agencies MUST protect and limit access to activity and audit logs and records.

Response and Remediation

16.4.42.R.01. **Rationale**

Because privileged accounts have high levels of system and data access, a rapid response to unusual or anomalous activity is fundamental to the maintenance of the integrity of an agency's systems and data. Any response must take urgent action to protect compromised accounts and systems based on defined policy and breach intelligence. This may include, for example, the immediate suspension of credentials, password rotation or deactivation of credentials.

16.4.42.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6864]

Agencies MUST develop and implement a response and remediation policy and procedure as part of an agency's Privileged Access Management (PAM) policy.

User Education and Awareness

16.4.43.R.01. **Rationale**

Privileged Account access may have procedures additional to or that vary from an organisation's usual account security and maintenance processes and procedures. As an agency will have established a Privileged Account Management (PAM) policy, this can be conveniently dealt with as a separate or additional component of user training and awareness. Refer also to Section 3.5 - System Users and Section 9.1 - Information Security Awareness and Training.

16.4.43.R.02. **Rationale**

User training and awareness is necessary to provide specific training to users of privileged accounts. This training should provide detailed information specific to users of privileged accounts. This includes awareness of the characteristics and value of privileged accounts, the additional responsibilities of users of these accounts, and the risk to organisations and systems if these accounts get breached.

16.4.43.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6868]

Agencies MUST implement a Privileged Access Management (PAM) policy training module as part of the agency's overall user training and awareness requirement.