CYBER STANDARDS DOCUMENT

NCSP Privileged Access Management standard

ABSTRACT:
This standard defines the requirements and best practice for privileged access management which should be adopted to manage elevated access consistently and securely across national policing IT systems.

This standard adheres to the National Policing Community Security Policy Framework and is a suitable reference for community members, notably those who build and implement IT systems on behalf of national policing.

ISSUED	May 2024
PLANNED REVIEW DATE	May 2025
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This standard is due for review on the date shown above. After this date, this document may become invalid.

Cyber Standard users should ensure that they are consulting the currently valid version of the documentation.

CONTENTS

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This standard in conjunction with the National Policing Community Security Policy (NPCSP) Framework and associated documents sets out National Policing requirements for Privileged Access Management.

Introduction

Privileged Access Management (PAM) is an integral part of Identity and Access Management (IAM) with specific focus on protection, monitoring, detection and prevention of unauthorised privileged access to critical resources, sensitive data, business applications, networks and computing devices.

This standard defines additional and complementary security requirements to the NPCSP Identity and Access Management standard, which should be followed and implemented to effectively and securely, control and manage privileged access. Security controls defined in this standard are based on industry frameworks and security best practice and should be used as baseline security requirements for protecting privileged access across National policing systems.

The defined set of controls presented in this document could be easiest and most effectively met by the use of a dedicated PAM solution but can also be achieved without. It is expected that strategically, forces will strive toward maturing privilege access management by adoption of a dedicated PAM.

Owner

National Chief Information Security Officer (NCISO).

Purpose

This standard alongside the NPCSP System Access and Identity & Access Management standards, helps organisations demonstrate compliance with the following NCSP policy statements:

System Access

- Restrict access to applications, mobile devices, systems and networks to authorised individuals and services (entities) for specific lawful business purposes, as defined in a formal access control standard and supported by an Identity and Access Management (IAM) system.
- Ensure individuals are only granted access privileges in line with their role; authenticated using access control mechanisms (e.g. password, token or biometric); and subject to a rigorous sign-on process before being provided with approved levels of access.
- Ensure additional robust controls to limit privileged access to systems, networks or data.
- Ensure 3rd party access is strictly controlled.
- This document establishes a set of security requirements for Privileged Access Management that PDS / Forces / suppliers should work to, to ensure consistent security controls are followed when designing, implementing and managing privileged access local and national policing systems and data.
- Complement the NPCSP Identity and Access Management standard.

Audience

This standard is aimed at:

- Staff across PDS and policing who build, implement and maintain ICT systems, either on behalf of National Policing or at a local force level.
- The user community, including those who have escalated privileges to provide administrative functions.
- Suppliers acting as service providers or developing products or services for PDS or policing.
- Auditors and penetration testers providing assurance services to PDS or policing.

Scope

1. The requirements of this standard are the foundation for National policing IT systems, applications, or service implementations. The requirements should be applied to new and existing installations.
2. This standard is applicable to any infrastructure, system, application, or IT solution that processes or stores policing information assets.
3. This standard is applicable to all systems used by community members to process, store and transmit policing data, more specifically data classified as OFFICIAL or above by the UK Government Security Classification Policy (GSCP). Note: systems processing data classified above OFFICIAL will attract additional controls.

4. The security control requirements laid out in this standard are vendor agnostic and applicable for all IT systems, applications, or service implementations that are provisioned for policing community of trust use.

Definitions

Privileged account
These exist in many different forms across an organisation and have the ability to make configuration changes, modify permissions, manage and access services, that a standard user is not capable of.

Privileged service account – applicable to both on-premises and cloud environments, are special type of accounts that represent a non-human entity such as an application, API or other services.

Privilege Interface
Can be also defined as an administration interface and typically allow privileged accounts inbound connections to different technologies to perform privileged/elevated tasks and operations. Privileged interfaces may come in different forms:

- Browser-based interface such as cloud service/application (e.g., AWS portal, Office 365)
- Management protocols such as SSH, PowerShell, RDP and VNC
- API management interface
- Thick clients allowing administration via dedicated software (API, protocol)

Privilege Tiers
Tier classification helps organisations to group different level of privileged access and privilege systems as not all administration is the same. NCSC's tier classification is based upon risk to organisation should a privileged account be compromised or misused. The classification is as follows:

- Tier 0 – Root administrators, root cloud accounts and highly privileged accounts, highly privileged systems such as PAM or systems to generate cryptographic material.
- Tier 1 – Highly privileged roles that can conduct operations on critical infrastructure, critical services within cloud services and important systems that contain sensitive data that other systems depend on.
- Tier 2 – Privileged roles that can carry out privileged functions but more isolated in scope, allowing administration across smaller number of components. This could include a root administrator access to manage a specific application, single component or a front-end web server, that would be part of a wide architecture.
- Tier 3 – Privilege roles that allows to execute constrained privileged actions such as password resets, manage single/small number of cloud services of lower significance.

Note – The Privilege tier table has been extended with the addition of the "Emergency Tier" that includes a Tier 0 type account, Break Glass account, for emergency access to privileged systems.

Privilege Tier	Privilege Functions	Security Controls
Emergency Tier	• Break Glass account	• Should follow process controls rather than technical security controls • Usage must be specifically monitored • Password should be split and stored in two places • Approval for an appropriate group for the highest privileged accounts
Tier 0	• M365/AWS Root admin • Microsoft Entra ID (Azure AD) Global Administrator • PAM root administrator • Enterprise or Domain administrators	• PAW • Dedicated Intermediary • JITA with limited duration elevations • JEA (RBAC) • MFA • Enhanced Conditional Access (e.g., continuous evaluation) • Enhanced Session Monitoring
Tier 1	• Core service administrator (e.g., security, backup service) • Administration of a critical business system (Command and Control, Records Management System) • Teams Administrator • SharePoint Administrator • Exchange Online Administrator	• PAW • Intermediary • JITA • JEA (RBAC) • MFA • Enhanced Session Monitoring
Tier 2	• Application administrator accounts that have full access to specific applications and the data stored in them • Server Service Administrator • Privileged user password reset	• PAW (could be optional for least privileged roles within Tier 2, risk-based) • Intermediary (could be optional for least privileged

		roles within Tier 2, risk-based) • JITA • JEA (RBAC) • MFA • Session Monitoring
Tier 3	• Low privileged role within Azure to managed specific service or specific privilege task such as password reset of non-privileged user account • Workstation support • SharePoint Site Owner	• JITA • JEA (RBAC) • MFA • Session Monitoring

Note – MFA above means that an MFA prompt must be displayed upon login to the privileged interface. Tier 3 administration will still require MFA as part of a user's normal workstation authentication process.

Privileged Access Workstation (PAW)
Dedicated workstation (physical or virtual) to perform administrative access, typically focusing on the highest privileged system and roles, that is hardened, strictly monitored and provides segregation from an environment through security and technological controls. PAW is an important component of Privileged Access Management strategy.

Password Vault
Centralised digital store that protects all types of passwords, secrets and credentials that control access to business privileged interfaces. This could include cloud-based vault (e.g., AWS/Azure) that could operate independently or integrate with PAM solutions.

Zero Trust
Zero trust architecture is an approach to system design where there is no implicit trust granted to assets and users on the network. Instead, every session within Zero Trust architecture is authenticated and authorised prior establishing connection to a target based on an access policy.

Requirements

1. *Privilege Discovery*

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
1.1	Privileged Identity Discovery	All privileged accounts and credentials, both human and machine, with access to systems, infrastructure and applications must be discovered, recorded, and tier-classified (refer to Privilege Tier classification in the Definitions section) across all platforms. Examples include, but not limited to: • Domain and local administrative accounts • Break glass accounts • Root accounts • Cloud accounts • Service accounts • Accounts with embedded/hard-coded credentials • Automation accounts to run workloads (Security tools like Tenable, Dev Ops) • Infrastructure accounts • IoT Where possible, discovered privileged accounts should be automatically onboarded to a privilege management solution.	NIST CSF ID.AM-1, ID.AM-5, ID.GV-4, PR.AC-1, PR.AC-4, DE.CM-7 CIS 6.6 ISO 27001:8.2a	Documented configurations and processes. Outputs from identity/asset discovery tools that can confirm that the discovery process has implemented and followed.

		Continuous privileged account discovery should be enforced. Where possible, the process should be automated.	NIST CSF ID.AM-1, ID.AM-2, ID.GV-4, PR.AC-1, PR.AC-4, DE.CM-7 CIS 6.6 ISO 27001:8.2a	Documented configurations and processes. Outputs from identity/asset discovery tools that can confirm that the discovery process has been implemented and followed.
1.2	Privilege Interface Discovery	All business-critical assets/interfaces must be discovered and classified accordingly. Those may include: • Domain controllers • PAM servers • Hypervisors • CI/CD servers and services (GitHub, Azure DevOps) • Databases • Core service consoles • Network devices • Cloud services e.g., Azure and AWS portals, SaaS applications like Office365 or SailPoint • Other	NIST CSF ID.AM-1, ID.AM-2	Documented configurations and processes. Outputs from identity/asset discovery tools that can confirm that the discovery process has been implemented and followed.
		Continuous and automated discovery of all privileged interfaces should be employed.	ISO 27001:8.2a, ID.AM-1, ID.GV-4, PR.AC-1, PR.AC-4, DE.CM-7 CIS 6.6	Documented configurations and processes. Outputs from identity/asset discovery tools that can confirm

				that the discovery process has been implemented and followed.
1.3	Privileged Identity Classification	Define tiers of privilege access, Emergency tier for break glass accounts, Tier 0 being the most privileged account with ability to control the entire environment or with access to most sensitive system and Tier 3 being the least privileged account and enforce appropriate control set/polices for each tier. Please refer to Definitions section for reference.	NIST CSF ID.AM-5, PR.AC.4 SOGP SA1.3.1, SA1.3.2	Documented privileged identity classification with security controls and polices defined and enforced as per each tier.
1.4	Privilege purge	Root and administrative privileges should be removed from endpoints and replaced with PAM controlled access where possible.	NIST CSF PR.AC-1, PR.AC-4	Documented processes and procedures. Output from tools managing privileged accounts on endpoints. Internal IT health check.

2. *Privileged Accounts*

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
2.1	Privileged Account Separation	Privileged accounts must not be used for day-to-day business (such as email and internet browsing) and only dedicated for activities requiring elevated access.	NIST CSF PR.AC-4, PR.PT.6 SOGP – SA1.1, 1.2, 1.3, 1.4 NCSC CAF – B2.c	Documented design decisions and enforced system policies. Internal IT health check.
2.2		Privileged tasks should not be permitted from less trusted system/environments/network boundaries to more trusted system to ensure privilege task integrity. Browse-down approach should be followed and/or dedicated PAW should be provided. Tier 3 privileged access may be an exception from this rule, where a risk assessment has been carried out for a specific use case.	*NIST CSF PR.AC-5, PR.PT.3*	Documented design decisions and enforced system and security policies. Internal IT health check.
2.3		Privileged accounts should not be permitted to perform elevated operations from untrusted devices. Tier 3 privileged access may be an exception from this rule, where a risk assessment has been carried out for a specific use case.	*NIST CSF PR.AC-5, PR.PT.3*	Documented design decisions and enforced system and security policies.

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
2.4	Unique credentials	Systems should have unique passwords assigned to prevent reuse from system to system Single Sign-On authentication should be prioritised where possible, with a password manager solution injecting passwords as required during an authentication session.	NIST CSF PR.AC.1, PR.AC.4, PR.AC.7	Documented design decisions and enforced system policies. Internal IT health check.
2.5	Service accounts	Privileged service accounts must be only associated with one service or service cluster (a group of the same applications/tasks under the same service). • Conditional access polices should be applied to further secure privilege services and their scope. • Interactive log-on sessions must not be permitted and any logon attempts must be logged and monitored. All service accounts must have an owner allocated who is responsible for maintaining the account.	NIST CSF PR.AC.1, PR.AC7, DE.CM-3	Documented design decisions and enforced system policies. Internal IT health check.

3. Privileged Access

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
3.1	Zero Trust	Zero trust approach should be implemented and followed for users and devices when managing privileged access to continuously verify the requester's identity and role as well as the requesting device's health posture and credentials.	*NIST CSF PR.AC-5, PR.AC-7*	Documented architectural design decisions and enforced system polices.
3.2	Least privilege	Privilege requestor should be automatically provided with "Just In Time Administration - JITA" temporary credential to complete the required task when accessing system's privileged administration interfaces and subsequently remove them once the task is complete or the window or context for authorised access has expired. • Requests must justify intended actions each time privileged access is required. • Risk-based approach should be considered to determine access time frame and controls for JITA policies. • All privilege JITA requests should be	ISO 27001:8.2j,d NIST CSF PR.AC-4, PR.DS-5, NIST 800-53v5 AC-3(6), NCSC CAF – B2.c	Documented design decisions and enforced system and security policies. Output from tools managing privilege access.

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
		audited and monitored. • Any requests should be integrated with a workflow tool to capture requested change and change resolution. • JITA should not be applied to privileged service accounts.		
3.3		Privilege requestor must be provided with "Just Enough Administration - JEA" permissions to complete the required task when accessing system's high privileged administration interfaces. • Requests must justify intended actions each time privileged access is required. • Risk-based approach should be considered to determine access time frame and controls for JEA policies. • All privilege JITA requests should be audited and monitored.	ISO 27001:8.2j,d NIST CSF PR.AC-4, PR.DS-5, NIST 800-53v5 AC-3(6), NCSC CAF – B2.c	Documented design decisions and enforced system and security policies. Output from tools managing privileged.

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
		• Any requests should be integrated with a workflow tool to capture requested change and change resolution. • If a 'built in' role's permissions exceed the principle of JEA, then a custom permissions role should be created and used in favour.		
3.4	Dynamic privilege management	Privileges should be dynamically and automatically managed where possible, allowing automatic adjustments based on defined criteria and/or rules. The following should be considered: • Operation out of hours • Emergency access • Recertification • JML • ABAC • Geolocation • Threat intelligence • Risk	NIST CSF ID.AM-6 PR.AC-1,4,6 NCSC CAF – B2.c	Documented design decisions, configurations and enforced system polices. Output from tools managing privileged.
3.5	Authentication	Authentication for privileged requests must be in line with IAM standard.	NIST CSF - PR.AC-1,3,6,7 SOGP – SA1.9	Documented design decisions, configurations and enforced system policies.

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
		Multi-factor authentication (MFA) must be enforced when the privileged credentials are requested excluding emergency break glass accounts.		Alignment with IAM standard and Volume 2 IAM blueprint.

4. Privilege Governance

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
4.1	Define Privileged Roles	RBAC privilege roles must be carefully and granularly defined based on business requirements and risk-based approach to privileged system/application/service as per defined privileged Tier classification.	NIST CSF ID-AM-5,6 PR.AC-1, 4,6 SOGP-SA1.1, 1.2	Documented RBAC process. Documented risk-based decisions.
4.2	Approve Privileged Role	Process must be defined for creation and approval of new or modification of existing roles. • Multi-party approval from Information Security for the highest privileged roles Tier 0, Tier 1, approval should be considered. • A simplified approval process could be considered for least privileged roles – Tier 2, Tier 3. Approval process for allocation of people to privileged roles should also be defined.	NIST CSF PR.AC-1, 4,6 ID.GV-2 SOGP – SA1.1, 1.2, 1.3, 1.4 NCSC CAF – B2.c	Documented privilege governance process. Output from tools managing privileged access.
4.3	Assign Privileged Roles	Role assignment should be in line with the NEP IAM and PS LLD – Volume 8 – IAM Governance utilising an	NIST CSF PR.AC-1, 6 SOGP – SA1.1, 1.2, 1.3, 1.4	Documented privilege

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
		identify governance tool and align with IAM standard.	NCSC CAF – B2.c	governance process. Output from tools managing privileged access. Alignment with IAM standard and Vol 8.
4.4	Revoke Privileged Roles	Role revocation should be automated where possible and in line with the NEP IAM and PS LLD – Volume 8 – IAM Governance utilising an identify governance tool and align with IAM standard.	NIST CSF PR.AC-1, 6 SOGP – SA1.1, 1.2, 1.3, 1.4 NCSC CAF – B2.c	Documented privilege governance process. Output from tools managing privileged access. Alignment with IAM standard and Vol 8.
4.5	Review Privileged Roles	The membership of all privileged roles, including non-human and application identities, must be reviewed: • Every 30 days • On demand (e.g., in response to an incident or during assessment) Please refer to the IAM standard for requirements details.	NIST CSF PR.AC-1, 6 SOGP – SA1.1, 1.2, 1.3, 1.4 NCSC CAF – B2.c	Documented privilege governance process. Output from tools managing privileged access. Alignment with IAM standard.

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
4.6	Change process	A change process should be defined to record any modifications to roles and assignments by administrators responsible for managing privileged roles (e.g., new role created, scope of role expanded, or users/systems added or removed) and approval.	NIST CSF ID.GV-1, ID-GV-2 SOGP – SA1.3	Documented privilege governance process. Output from tools managing privileged access. Change process records.
4.7	Access Approval	An approval process must be accessible and timely enough to enable requestors to complete their task. The process should be proportional to the risk-based tier approach and adequate approval mechanism should be applied. Those should include: • Approval for an appropriate group for the highest privileged accounts – Emergency tier, Tier 0 and/or Tier 1 • Rule-based auto approval for least privileged account – Tier 2, Tier 3. • Elevation notifications to relevant stakeholders	NIST CSF PR.AC-1,6,7 SOGP – SA1.1, 1.2, 1.3, NCSC CAF – B2.c	Documented privilege governance process. Output from tools managing privileged access.

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
4.8	Access removal	Automatically remove privileges from privilege management system/records when the infrastructure is de-provisioned.	NIST CSF PR.AC-1,6,7 SOGP – SA1.1, 1.2, 1.3 NCSC CAF – B2.c	Documented privilege governance process. Output from tools managing privileged access.

5. Secrets and Passwords Management

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
5.1	Secrets and Passwords Complexity	Password complexity should align with the Password standard.	NIST CSF PR.AC-1,5,6,7, PR.DS-5 NIST 800-53v5 IA-5(1) SOGP – SA1.5	Alignment with Password Standard. Documented password policies.
5.2	Secrets Obfuscation	Privileged passwords, credentials, and secrets should be never revealed to requesting users and should be passed/proxied via an intermediary solution upon user/service/application being authenticated.	NIST CSF PR.AC-1,5,6,7, PR.DS-5 NIST 800-53v5 IA-5(1) SOGP – SA1.5	Documented design decisions and enforced system policies. Security testing. Output from a tool managing secrets rotation.
5.3	Secrets Management	Privileged passwords, credentials, and secrets (e.g., API keys, Tokens, Certificates, JSON files, XML files, private keys, others)	NIST CSF PR.AC-1,5,6,7, PR.DS-5 NIST 800-53v5 IA-5(1)	Documented design decisions and enforced system policies.

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
		for applications, services and devices should be centrally secured (e.g., Azure Vault), managed and protected in a tamper-proof vault and released upon authorised request to human and non-human (applications/services) identities. Non-human credentials should never be revealed.	SOGP – SA1.5	Security testing. Output from a tool managing secrets rotation.
5.4	Hard-coded Credentials	Credentials must never be hard-coded and applications/services should be using secure and authenticated APIs to safely request credentials/secrets from the secrets vault.	NIST CSF PR.AC-1,5,6,7, PR.DS-5 NIST 800-53v5 IA-5(1) SOGP – SA1.5	Documented design decisions, processes and enforced system policies. Code review report.
5.5	Secrets Rotation	Automatic rotation of passwords, credentials or secrets should be based on workflows, tier classification and based on risk. • Break glass account upon every use • Non-human accounts to rotate based on Tier classification (e.g., 30 days for Tier 0, 90 days for Tier 3)	NIST CSF PR.AC-1,5,6,7, PR.DS-5 NIST 800-53v5 IA-5(1,18) SOGP – SA1.5	Documented design decisions and enforced system polices. Output from a tool managing secrets rotation.

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
		• Privilege user account should not be regularly rotated as in line with NCSC guidance		
5.6	Secrets Deployment	Rotated credentials should be automatically propagated, where possible, to all services and/or systems.	NIST CSF PR.AC-1,5,6,7, PR.DS-5 NIST 800-53v5 IA-5(1,18) SOGP – SA1.5	Documented design decisions and enforced system policies. Output from a tool managing secrets rotation.
5.7	Vault Security	Access to the password vault must be specifically protected and be approved upon the following: • Approval for an appropriate group for the highest privileged accounts. • Multifactor authentication (MFA) must be enforced upon access to the vault. • Access from PAW and by privileged accounts only.	NIST CSF PR.AC-1,5,6,7, PR.DS-5 NIST 800-53v5 IA-5(1,18) SOGP – SA1.5	Documented design decisions, processes and enforced system polices. Penetration testing.

6. Privilege Session

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
6.1	Session management	All privileged session management must be controlled, monitored and recorded.	NIST CSF PR.PT-4 DE.CM-1,3,4 NIST 800-53v5 AC-12 SOGP – SY1.1	Documented configurations, processes and enforced system policies.
6.2	Session policies	Privilege session policies must be defined to determine what tools, programs, activities, executed commands and controls should be enforced and permitted per defined roles.	NIST CSF PR.PT-4 DE.CM-1,3,4 NIST 800-53v5 AC-6(3)	Documented configurations and enforced system policies.
6.3	Session Isolation	All established privileged sessions (e.g., RDP/SSH/web session) that end-user establishes to a privileged target interface should be isolated from the end-user's workstation.	NIST CSF PR.PT-4 DE.CM-1,3,4 NIST 800-53v5 AC-6(3)	Documented configurations and enforced system and security policies. Output from a tool managing privileged sessions.
6.4	Session Protection	All established privileged sessions must be protected from sessions hijacking, unauthorised file downloads, access to clipboard and other malicious attacks.	NIST CSF PR.PT-4 DE.CM-1,3,4 NIST 800-53v5 AC-6(3)	Documented configurations and enforced system and security policies. Output from a tool managing

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
				privileged sessions. Penetration testing.
6.5	Session Analytics	Privileged sessions should be automatically analysed to detect any abnormal/malicious activities and paused or stopped until session legitimacy is proven.	NIST CSF PR.PT-4 DE.CM-1,3,4 RS.AN-3 NIST 800-53v5 AC-6(3)	Documented configurations and enforced system and security policies. Output from a tool managing privileged sessions.
6.6	Session Recording	Automated privileged sessions with a target resource/system should be recorded. • Risk-based approach should be applied to determine how session should be recorded (e.g., video/ keystrokes).	NIST CSF PR.PT-4 DE.CM-1,3,4 RS.AN-3 NIST 800-53v5 AC-6(3)	Documented configurations and enforced system policies. Documented risk-based decisions.
6.7	Session Replay	Replaying of recorded privileged sessions should be possible for training, event review and investigations.	NIST CSF PR.PT-4 DE.CM-1,3,4 RS.AN-3 NIST 800-53v5 AC-6(3)	Documented configurations and enforced system policies for session replay. Output for a tool managing

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
				privileged sessions.

7. Break Glass Account

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
	Emergency Access	Each critical system must have at least two break glass accounts. • Break glass process must be defined. • Notification upon break glass use must be sent to dedicated members. Break glass passwords must be changed upon every use. • Break glass accounts must not be stored in a location which depends on the same authentication provider.	NIST CSF PR.AC-1,6,7 SOGP – SA1.1, 1.2, 1.3 NCSC CAF B2.c	Documented processes, configurations and enforced system polices.
	Audit Trail	Use of break glass accounts must be recorded and provide full audit trail, clearly showing who and when accessed emergency credentials and what actions were performed.	NIST CSF PR.PT-1 SOGP – TM1.2 NCSC CAF C1.a	Audit reports. Output from a tool managing break glass accounts. auditing controls have been implemented.

	Alternative	Any break glass processes should be routinely updated and manually tested to ensure effectiveness and change control.	NIST CSF PR.AC-1, ID.GV-1, ID-GV-2 SOGP – SA1.3	Documented processes and reports from tested procedures.

8. Record and Audit Requirements

Reference	***Control Name***	***Minimum requirement***	***Control reference***	***Compliance Metric***
8.1	Auditing	Auditing rules in SIEM should be configured to automatically notify upon defined suspicious events such as: • Command injection • Unauthorised code execution • Attempt to make unapproved and unauthorised changes and modifications. • Attempt to modify credentials. • Access to credentials vault • Unusual privileged access schedule (out of hours, weekend) • Break glass account use • Failed login attempts • Non-UK login attempts,	NIST CSF, DE.CM-1, DE.CM-3 SOGP – TM1.2, TM1.3	Documented configurations and enforced polices to capture defined events. Output from a protective monitoring tool/SIEM. Audit reports.

		including unusual threat sources		
8.2	Audit Logs Security	Audit logs must be adequately protected to prevent unauthorised access and ensure integrity.	NIST CSF, DE.CM-1, DE.CM-3 SOGP – TM1.2, TM1.3	Internal IT Health check or security testing confirming that adequate controls are implemented to protect audit logs.

9. PAM Security Requirements

Reference	***Control Name***	***Minimum requirement***	***Control reference***	***Compliance Metric***
9.1	Authentication	Single Sign-On (SSO) should be enforced on access to PAM solution as the primary authentication mechanism. (excluding break-glass accounts)	NIST CSF PR.AC-1,6,7 SOGP – SA1.9	Documented design decisions, configurations and enforced system policies.
9.2		Multi-factor authentication (MFA) must be enforced for all administrators to access PAM solution. (excluding break-glass accounts)	NIST CSF - PR.AC-1,6,7 SOGP – SA1.9	
9.3	Least Privilege	PAM administrators must follow the least privilege principle.	ISO 27001:8.2j,d NIST 800-53v5 AC-6, NCSC CAF – B2.c SOGP – SA1.1, 1.2, 1.3, 1.4	Documented design decisions, configurations and enforced system policies. Internal IT Health check.

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
9.4	Device Access	Only trusted, authorised and/or dedicated privileged devices must be used to access PAM (e.g., PAW).	NIST CSF PR.AC-7, PR.PT-1	Documented design decisions, configurations and enforced system policies. Internal IT Health check.
9.5	Protocols	Connections to PAM must employ encryption in transit.	NIST CSF PR.AC-5, PR.DS-2	Formal IT Health Check can confirm that appropriate PAM controls have been implemented.
9.6	PAM Hardening	PAM system should be continuously tested for vulnerabilities and hardened.	SOGP – BA1.1.3, PA1.1.10, PA1.2.1, PA1.2.9	Internal IT Health check. Reports from penetration testing and vulnerability testing.
9.7	PAM Protective Monitoring	All administrative connections to PAM must be actively monitored with sessions security controls applied.	NIST CSF PR.PT-4 DE.CM-1, DE.CM-3 SOGP – TM1.2, TM1.3	Documented configurations and enforced security policies. Output from a protective monitoring tool/SIEM. Audit reports.
9.8		All PAM logs must be actively monitored within SIEM Logs must be securely stored and always available. Audit policies should align with the NMC auditing requirements to provide maximum situational awareness within the deployed	NIST CSF PR.PT-4, DE.CM-1, DE.CM-3 SOGP – TM1.2, TM1.3 NIST CSF DE.CM-1,3,4	

Reference	*Control Name*	*Minimum requirement*	*Control reference*	*Compliance Metric*
		environment and to avoid excessive log storage costs.	NIST 800-53v5 AC-6(3)	
9.9	PAM Managed Account credentials	For PAM account credentials complexity refer to Password Standard.	NIST CSF PR.AC-1	Alignment with Password Standard.
9.10	PAM break-glass account credentials	Break-glass account credentials must be: • Master credentials complexity (Refer to Password Standard) • Master PAM credentials should be stored encrypted in an alternative secure location (e.g., physical safe or another credentials vault).	NIST CSF ID.GV-1,3 PR.AC-1,3,4,7 DE.DP-2	Alignment with Password Standard. Internal IT Health check.

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Presentation to the National Cyber Policy & Standards Board (NCPSB) for approval.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

For external use (outside PDS), this standard should be distributed within IT teams to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with force SIROs / Security Management Forum. Consideration should also be given to raising awareness amongst force personnel of the implementation of this standard where it may affect them.

Measurables generated by adopting this standard can also form part of regular cyber management reporting.

Review Cycle

This standard will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the standard continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Cyber PDS	Initial version	25/09/23
0.2	Cyber PDS	Updates following NCPSB review.	12/03/24

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	23/05/24

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
CSA Cloud Controls Matrix	v4	01/2021

Document Name	Version	Date
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021
NPCSP Identity and Access Management Standard	Current	05/23
NPCSP Password Standard	Current	01/23
NPCSP NEP IAM and PS LLD – Volume 2 - IAM	Current	04/23
NPCSP NEP IAM and PS – Volume 8 – IAM Governance	Current	05/22