CYBER STANDARDS DOCUMENT

System Access

ABSTRACT:
This standard defines the requirements which, when applied, will prevent unauthorised access to national policing IT systems. Areas considered include account management, access control mechanisms e.g. biometrics and customer access.

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.

This standard also relates to other PDS standards passwords and IAM, which the audience should also consider.

ISSUED	JULY 2024
PLANNED REVIEW DATE	JUNE 2023
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 Framework and associated documents, sets out National Policing requirements.

Introduction

The System Access standard specifies requirements regarding system access processes, actions, and configurations. It aims to provide PDS and policing with clear direction for preventing unauthorised access to policing systems and data.

The ISF Standard of Good Practice for Information Security 2024 (SoGP) defines access control as:

“Restricting access to business applications, mobile devices, systems and networks to authorised individuals and services (entities) for specific business purposes, as defined in a formal access control policy and supported by an Identity and Access Management (IAM) system.”

Examples of how these restrictions may be achieved are:

- Principle of least privilege
- Segregation of duties
- User accountability
- IAM services
- MFA

These examples and other related actions that ensures robust system access are the focus of this document and are detailed throughout.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to establish formal requirements, which detail system access processes, actions and configurations that can be applied to policing systems. Applying system access controls should enable authorised users to perform their roles appropriately, whilst ensuring confidentiality, integrity and availability of policing systems and data is protected. This concept is echoed in National Policing CSP principles 4, 5 and 6, which specifically address confidentiality, integrity, and availability as integral to the foundation of all information security activity.

In addition, the requirements stated in this standard are mapped across the following industry standard frameworks:

- ISO 27002:2002
- CIS Controls
- NIST Cyber Security Framework
- Information Security Forum (ISF) Statement of Good Practice (SoGP)

NEP design documents have also been considered for the System Access standard, which, together with the frameworks listed above, ensure that the stated requirements are comprehensive and relevant to policing when applied.

Audience

This standard must be read and adopted by all staff across PDS and policing who build and implement IT systems, either on behalf of National Policing or at a local force level. It must also be read and adopted by the user community, including those who have escalated privileges to provide administrative functions.

Scope

1. This standard is to cover systems handling data within the OFFICIAL / OFFICAL-SENSITIVE tier of the Government Security Classification Policy (GSCP). National policing IT systems, applications, or service implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

2. 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.

3. Additional controls may be applicable based upon the security classification of the information being processed by the external supplier's IT systems, applications, or service implementations.

Requirements

Reference	Minimum requirement	Control reference	Compliance Metric
1. System Access Policy	Each policing community member must establish a local System Access Control Policy. The policy must describe *who* should have access to systems, data, devices and processes, *why* access should be granted and under *what* circumstances. The System Access Control Policy must enforce only lawful business needs for access. The System Access Control Policy must describe security	ISF SoGP: AC1.1, AC1.2, AC1.3, AC2.1, AC3.2 ISO 27001/2: 9.1.1	Internal audit and review will confirm if a system access policy exists. Refer to the NCSP Privileged Access Management standard for more information.

Reference	Minimum requirement	Control reference	Compliance Metric
	requirements which are underpinned by: • Principle of Least Privilege • Segregation of duties • Security Vetting Clearance • Access control models such as RBAC, MAC, DAC • Data classification schemes • Legal and regulatory obligations • The IAO's/PAO's vision and approach Privileged / administrator accounts must be subject to enhanced management and control, but control selection will vary according to the architecture being considered. For cloud services, users should be assigned a single account with PIM or PAM applied. This will allow the appropriate permissions for administrative activity to take place.		

Reference	Minimum requirement	Control reference	Compliance Metric
	Refer to the NCSP Privileged Access Management standard for more information. For on-premises systems or for situations where PIM or PAM is unsuitable, the following controls must be considered: • Unique, dedicated accounts for administrator duties • If possible, limiting access to email & Internet access • Multi-factor authentication • Enhanced auditing of actions performed • Increased security vetting for account holders. Stated requirements must have documented processes and procedures to support implementation.		

Reference	Minimum requirement	Control reference	Compliance Metric
2. Account Management	**JML.** There must be Joiners-Movers-Leavers (JML) procedures which verify user identity and provides or revokes the correct permissions for individual accounts. Access should be assigned according to the principle of least privilege. When provisioning accounts for joiners, the process must also consider initial logon actions for new users, for example, secure passing of credentials, out-of-the-box setup. **Account provisioning.** Account provisioning should be subject to individuals having their security vetting clearance confirmed by the Force / Organisational vetting unit. Accounts must be provisioned to individuals, as opposed to groups of individuals or shared accounts, so that system actions can be accounted for correctly.	ISF SoGP: AC1.3, AC2.1, AC2.2, AC2.3, AC2.4, AC3.1 ISO 27001/2: 7.3.1 9.2.1 9.2.2 9.4.3 CIS v8.1: 4.7 5.2 5.3 3.4 NIST: PR.AC.1 PR.AC.4 NIST SP 800-53 Rev 4: DE.AE.3 DE.CM.3 DE.CM.6 DE.CM.7	Internal audit and review will confirm if a JML process exists. A formal IT Health Check can confirm that the appropriate system access controls have been implemented. Protective monitoring logs can highlight system access violations. Refer to: • NCSP IAM standard • NCSP Vetting requirements • NCSP People Security Management standard • NCSP Privileged Access Management standard for further information.

Reference	Minimum requirement	Control reference	Compliance Metric
	For system accounts, often referred to as 'Service Accounts,' refer to the NCSP Privileged Access Management standard. These accounts must also be included in the accounts inventory. Default accounts must be managed in accordance with the local Access Control Policy. **Account administration.** Policing community members should refer to the NCSP IAM standard in the first instance. The NCSP IAM standard details several requirements, including: • Account parameters e.g. lockout, session lockout • Privileged account use • Remote access • Account Review • Segregation of duties **Account audit and review.** An up-to date inventory of all accounts should be maintained and reviewed on a regular		

Reference	Minimum requirement	Control reference	Compliance Metric
	basis, in partnership with system owners / PAOs / IAOs. This must ensure that user access still meets lawful, business need. Redundant, inactive, or disabled accounts should be removed in accordance with the local Access Control Policy. All account management actions should be auditable.		
3. Access control Mechanisms	**BIA and Information Risk Assessment.** A Business Impact Analysis (BIA) and Information Risk Assessment (IRA) must be completed with the approval of the Platform Asset Owner (PAO) or IAO. **Access Control Mechanisms.** Using the BIA and Information Risk Assessment, appropriate access control mechanisms for systems and data must be identified. These mechanisms must be based on factors:	ISF SoGP: AC2.1, AC3.2 ISO 27001/2: 9.4.1 9.2.6 9.2.5 9.2.3 CIS v8.1: 3.3 4.7 5.1 5.4 5.5 5.6 NIST SP 800-53 Rev 4: PR.AC.1 PR.AC.4	Internal audit and review will confirm if a current, approved IRA & BIA exists.

Reference	Minimum requirement	Control reference	Compliance Metric
	• Something the user knows • Something the user has • Something the user is / does For certain circumstances geo-fencing or conditional access controls should be applied. For example, to prevent access from overseas or from unapproved devices.	PR.AC.7	
4. Access Control Mechanism: Password Management	Unique passwords or passphrases shall be in place for all accounts including service and privileged accounts. These should meet the requirements of the NCSP Password standard. Systems and applications must be configured to enforce the NCSP Password standard. Password obfuscation must be employed at system and application entry points.	ISO 27001/2: 9.4.2, 9.4.3 CIS v8.1: 5.2 NIST SP 800-53 Rev 4: PR.AC.7	Refer to NCSP Password standard for detailed information.

Reference	Minimum requirement	Control reference	Compliance Metric
5. Access Control Mechanism: MFA Management	**Application.** MFA must be applied to accounts used for: • Online services • Privileged / administrative access Community members must ensure MFA is applied to any situation where there is a need to authenticate a user and decide how this will be implemented for each service, for example: • Logging on to a service from a new device or location. • Performing an action such as changing a password. A choice of factors to authenticate should be offered where possible. For example, 'app' / token-based authentication is considered stronger than simple text based. **Registration / enrolment.** A process must be created to detail registration / enrolment	ISF SoGP: AC2.3, AC2.4 ISO 27001/2: 9.4.2 CIS v8.1: 6.3, 6.5 NIST SP 800-53 Rev 4: PR.AC.7	A formal IT Health Check can confirm that appropriate system access controls have been implemented. A review of documented processes and procedures outlined including (enrolment/fallback)

Reference	Minimum requirement	Control reference	Compliance Metric
	methods for mechanisms such as token access or biometric access. **Fallback process.** A fallback process must be developed for situations where an authentication factor fails or, for example, a token is lost. Procedures must also be developed for users to report any lost or stolen hardware, if issued.		
6. IAM	**IAM arrangements.** Policing community members should refer to the NCSP IAM standard in the first instance. The NCSP IAM standard details several requirements, including: • Assigning unique IDs. • Use of identity stores. • Administering privileges and permissions. **FIAM arrangements.** Federated IAM can be utilised by community members, but documented FIAM procedures must:	ISF SoGP AC3.2	Refer to NCSP IAM standard for detailed information. A formal IT Health Check can confirm that the appropriate system access controls standard has been implemented.

Reference	Minimum requirement	Control reference	Compliance Metric
	- Build on existing IAM arrangements. - Use agreed protocols eg SAML, OpenID. - Use approved FIAM connection software. Utilise MFA for access.		
7. Customer Access	Customer access refers to any 3rd party access, vendor access or supplier access. Customer access to policing community systems is acceptable. The following considerations must be formally documented in standards and procedures: - Actions to be performed before granting customer access. - Security vetting clearance requirements - Contractual measures to protect information, assets, systems in accordance with requirements.	ISF SoGP: AC3.2, BA2.1, BA2.2, BA2.3	Internal audit and review will confirm if a customer access controls exist including on/off boarding procedures and records. TPAP and / or Risk Ledger may provide additional information on customers. A formal IT Health Check can confirm that the appropriate system access controls standard has been implemented. See also the NCSP Vetting requirements for policing. Refer to NCSP IAM standard for detailed information

Reference	Minimum requirement	Control reference	Compliance Metric
	• Recording of customer connections. • Access control requirements. • Customer access arrangements. • Legal and regulatory requirements. • Security awareness required for customers. • Selecting and undertaking proportionate, regular auditing of all access. • Reviewing customer access arrangements. • Revoking customer access where appropriate. Customer access is also referred to in the NCSP IAM standard and can be used for further guidance.		
8. Monitoring	**Monitoring** • All user, device and system access is logged and monitored (including both successful and unsuccessful sign in attempts). • Access logs are reviewed and correlated for	NIST CSF v1.1: DE.AE.2, DE.AE.3, DE.CM.3, ISF SOGP: SE1.1, SE1.2	Onboarding to NMC or similar service including validation of log sources / use cases.

Reference	Minimum requirement	Control reference	Compliance Metric
	expected behaviour with other access records. • Lawful business monitoring & protective monitoring is established to detect suspicious/unusual behaviour and trigger an alert for investigation.		
9. Communication and Awareness	All personnel should be briefed on a regular basis regarding: • Lawful business use (access) • Process for requesting and revoking access including who is the authority for access. • Third party access requirements. • Choosing and managing passwords • Online safety including anti-phishing awareness • Social engineering awareness • Reporting security incidents	ISO 27001/2: 7.2.2	The following records can evidence communication and awareness maturity: • Records of individuals received awareness training • Records of induction training delivered • Records of targeted awareness • Records of ad-hoc awareness delivered • Records of security incident reports

Reference	Minimum requirement	Control reference	Compliance Metric
	Additionally, IAOs, PAOs, or system owners may provide additional specific security awareness for their assets / systems.		

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

The implementation of this standard should include a local Equality Impact Assessment. Complex password or access rules could exclude individuals with various disabilities, and these should be considered carefully as part of the impact assessment.

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
1.1	PDS Cyber Specialist	Annual review	12 Jun 24

Approvals

Version	Name	Role	Date
1.1	NCPSB	National Cyber Policy & Standards Board	25/07/24

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	07/2024

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
10 Steps to Cyber Security - NCSC.GOV.UK	**Web Page**	**05/2021**