CYBER STANDARDS DOCUMENT

NCSP Passwords standard

ABSTRACT:
This Standard supports the principles set out in the National CSP, providing detailed guidance to those implementing and managing PDS & policing systems. This Standard applies to all passwords created for use on PDS & policing systems, including those for user-level accounts, system-level accounts, and any device-specific passwords.

ISSUED	April 2024
PLANNED REVIEW DATE	February 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 Framework and associated documents sets out National Policing requirements for passwords.

Introduction

This standard supports the National Community Security Policy System Access requirements with respect to defining requirements for the use and selection of a password / passphrase-based method of authentication. It should be read in conjunction with the System Access, Identity & Access Management and Privileged Access Management standards and the Biometric guidance. Note that these documents will be fully available within 3 months of issue of this standard.

Passwords represent only one method of authentication (something that you know) and should be combined with other methods such as something you have (token) or something you are (biometric). It is not always possible especially with legacy applications or services to utilise multi-factor authentication, and this is where this standard can help to ensure that risks are effectively managed.

A strong passphrase / password will help to ensure lawful business access to applications, mobile devices, systems and networks when combined with an agreed access control policy and supported by an Identity and Access Management (IAM) system.

Threats to systems using passwords include brute force / dictionary attacks and offline attacks following a breached or leaked password database. Password / passphrase complexity affects the time it takes adversaries to guess them using commonly available tools however this should be considered alongside other technical controls such as account lock-out, throttling, alerting and protective monitoring. The complexity requirements described serve to complement these technical controls and help to delay

exposure of passwords that are subjected to offline attacks. See NIST Special Publication 800-63b Appendix A.

Undertaking a business impact assessment (BIA) is important to determine specific information security requirements to support proportionate risk management.

This standard is aligned with the NCSC's password guidance and NEP blueprints.

Owner

National Chief Information Security Officer (NCISO).

Purpose

This Standard supports the principles set out in the National CSP, providing detailed guidance to those implementing and managing PDS & policing systems.

This Standard applies to all passwords created for use on policing systems, including those for user-level accounts, system-level accounts, and any device-specific passwords.

This Standard document applies to all those implementing password solutions (outside of the National Identity & Access Management solution) within PDS & policing, System Designers, administrators, and users of such systems.

Once implemented correctly this standard will ensure that PDS & National policing systems will be adequately reduce the risk of password compromise.

This standard 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.

Audience

Members of the Policing Community of Trust.

More specifically the standard is targeted at, architects, developers, and security experts tasked with designing and building solutions, applications and services that will process or store policing information assets.

The following should also be aware of the content of this standard, in order that they can provide appropriate oversight and governance of the use of technology within policing:

- Senior Information Risk Owners (SIROs)
- Information Asset Owners (IAOs)
- Information & Cyber risk practitioners and managers
- Auditors providing assurance services to PDS or policing.

Finally, Policing's reliance on third parties means that suppliers acting as service providers or developing products or services for PDS or policing, should also be made aware of and comply with the content of this standard, in relation to their work on Policing systems and data.

Scope

1. This standard applies to systems handling policing 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 ICT systems, applications, or service implementations.

Requirements

Accounts within the PDS & policing must be protected by passwords that follow rules, dependent on their intended use. The types of account recognised are described in the table below:

Reference	Minimum requirement	Control reference	Compliance Metric
Defaults **CSP-PWD-01**	All initial / default passwords must be changed to comply with this standard before operational use.	ISO/IEC 27002:2022 5.17 ISO 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev.5 AC-1, AC-2	Process in place for provisioning new assets / systems which includes changing default passwords. Formal IT Health Check to verify no manufacturer default passwords in use.
User Account **CSP-PWD-02**	Applies to all user accounts, such accounts shall have no administration privileges or the ability to escalate account privileges. **Complexity** **Minimum Length: 17 characters** Composition: Minimum of 3 unconnected dictionary words ideally of irregular length (minimum 4 characters per word) separated by a hyphen or other supported character. NOTE: If a short word is used (4 characters), then a	ISO/IEC 27002:2022 5.17, 6.2 ver 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev.5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.

Reference	Minimum requirement	Control reference	Compliance Metric
	longer word will be needed to make up the length. Format examples: Word-Word-Word WordWordWord Word!Word!Word! **Examples:** • Sunny-lazy-nights • Donut-keyboard-house • Early-yellow-donkeys Users choose the words to use. Noting that personnel awareness campaigns should deter the use of What3Words word combinations that could be exposed through Open Source Intelligence (OSINT) techniques for example. **The use of Passwords;** Where the solution cannot use a passphrase then a password can be used that follows the following standard. Minimum Length: 10 character highly complex password/ passphrase;		

Reference	Minimum requirement	Control reference	Compliance Metric
	Composition: 4 character types (Upper Case, Lower Case, Special Character, Number); Or the maximum allowable by the target system. Note: this should be documented as a risk. Denylist: Any leaked or known weak passwords shall be blocked as will previously used passwords. Passwords that contain common strings (e.g. “Abc”,”123” etc) or that contain multiple sequential or repeated letters (3 or more). Generation: User generated, passwords must not include personal information (e.g. Mother’s Maiden name, favourite holiday destination, football teams, information readily available on-line (social media) etc.).		

Reference	Minimum requirement	Control reference	Compliance Metric
Local Administrator (where not managed by a PAM solution) **CSP-PWD-03**	1) Use Local Administrator Password Solution (LAPS) to ensure each Windows 10 computer has a random, complex 14-character local administrator password which is unique to the device, and which is automatically changed every 30 days. Or where LAPS not available use Minimum Length, either: 2) 20 character highly complex password. 3) 25 character passphrase composition Or the maximum allowable by the target system. Note: this should be documented as a risk. Where the password / passphrase cannot be machine generated, passwords must not include; personal information (e.g. Mother's Maiden name, favourite holiday destination etc.). Deny list: Any leaked passwords shall be blocked as will previously	ISO/IEC 27002:2022 5.17 ISO 27001:2013 9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.

Reference	Minimum requirement	Control reference	Compliance Metric
	used passwords. Passwords that contain common strings (e.g. "Abc","123" etc) or that contain multiple sequential or repeated letters (3 or more). MFA: Not possible on local admin accounts Remote Access: Prohibited. Password Reset: By System administrator only Account unlock: By System administrator only		
Application Administrator (where not managed by a PAM solution) **CSP-PWD-04**	As per local administrator and unique to account. MFA: Required Remote Access: May be required depending on where the application is hosted.	ISO/IEC 27002:2022 5.17 ISO 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.

Reference	Minimum requirement	Control reference	Compliance Metric
System Administrator (where not managed by a PAM solution) **CSP-PWD-05**	As per local administrator and unique to account. MFA: Required Remote Access: May be required depending on where the application is hosted.	ISO/IEC 27002:2022 5.17 ISO 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.
Privilege access accounts **CSP-PWD-06**	These types of accounts are to be deprecated. Minimum Length: 15 character highly complex password; Composition: 4 character types (Upper Case, Lower Case, Special Character, Number); Or the maximum allowable by the target system. Generation: User generated, passwords must not include personal information (e.g. Mother's Maiden name, favourite holiday destination etc.).	ISO/IEC 27002:2022 5.17 ISO 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.

Reference	Minimum requirement	Control reference	Compliance Metric
	Remembered passwords: (Cannot use the last) 24 Minimum password age: 3 days (Not always suitable for software applications and other uses) Deny list: Not applicable. MFA: Not applicable. Remote Access: Prohibited. Account Unlock: System administrator only Privileged access: That is the purpose of these accounts		
Root account **CSP-PWD-07**	Minimum Length: 24 characters or maximum allowable by the System Composition: Incorporates all 4-character types. 2 of each. (Upper Case, Lower Case, Special Character, Number). Generation: Machine generated random password which meets or exceeds complexity requirements.	ISO/IEC 27002:2022 5.17 ISO 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.

Reference	Minimum requirement	Control reference	Compliance Metric
	Deny list: Not applicable. MFA: Required where possible. Remote Access: Not possible. Password Reset: By System administrator only. Account unlock: By System administrator only		
Break Glass **CSP-PWD-08**	Minimum Length: 24 characters or maximum allowable by the System. Composition: Incorporates all 4-character types. 2 of each. (Upper Case, Lower Case, Special Character, Number). Generation: Machine generated random password. Which is changed after use. Deny list: Not applicable. MFA: Recommended where possible. Note: NEP blueprint currently states that break glass accounts are not required to register	ISO/IEC 27002:2022 5.17 ISO 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.

Reference	Minimum requirement	Control reference	Compliance Metric
	for MFA as they are exempt from the conditional access policies. Remote Access: May be required depending on where the application is hosted. MFA strongly recommended. Password Reset: By System administrator only. Account unlock: By System administrator only		
PAM User Account **CSP-PWD-09**	As per User Account (above) with the following variations: Multifactor Authentication (MFA) - User: Used to authenticate to the PAM tool for access to privilege access management functions. Privileged Access: No direct privilege however is allowed access to PAM tooling. See also: Privileged Access Management standard	ISO/IEC 27002:2022 5.17 ISO 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.

Reference	Minimum requirement	Control reference	Compliance Metric
PAM System Managed Account **CSP-PWD-10**	Minimum Length: 20 characters. [20 characters of a complex nature has been chosen for the cases when the password has to be manually typed in]. Composition: Incorporates all 4-character types. 2 of each (Upper Case, Lower Case, Special Character, Number). Complex. Generation: Machine generated random password. Deny list: Not applicable. MFA: Not applicable. Remote Access: Prohibited. See also: Privileged Access Management standard	ISO/IEC 27002:2022 5.17 ver 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.
Privilege access accounts for Microsoft 365 **CSP-PWD-11**	Minimum Length: 15 character highly complex password; Composition: 4-character types (Upper Case, Lower Case, Special Character, Number);	ISO/IEC 27002:2022 5.17 ISO 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AC-1,	Formal IT Health Check can confirm that the appropriate password policy & standard have been implemented.

Reference	Minimum requirement	Control reference	Compliance Metric
	Generation: User generated passwords must not include personal information (e.g. Mother's Maiden name, favourite holiday destination etc.) Remembered passwords: (Cannot use the last) 24 Minimum password age: 3 days (Not always suitable for software applications and other uses) Deny list: Not applicable. MFA: Uses Microsoft MFA Remote Access: May be required depending on where the application is hosted. MFA strongly recommended. Password Reset: Not Applicable. (PAM resets the password on a regular basis.) Account Unlock: System administrator only.	AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	

Reference	Minimum requirement	Control reference	Compliance Metric
	Privileged access: That is the purpose of these accounts See also: Privileged Access Management standard		
Communication & Awareness (Specifically relating to password / passphrases compliance.) **CSP-PWD-12**	All persons with access to any IT system or application should complete regular training including the following password specific aspects; (These can be included in a security awareness programme.) • How to choose effective passwords / passphrases that are compliant with this standard • How to recognise weak / poor passwords – may signpost online resources. • The importance of using different work and personal passwords • The need to always keep their passwords / passphrases private to themselves.	ISO/IEC 27002:2022 5.17, 6.2 ISO 27001:2013 A9.2.4, A9.3.1, A9.4.3 NIST SP 800-53 Rev. 5 AT-1, AT-2,	% Force / organisation coverage of induction training delivered Number of personnel who receive regular information security awareness briefings per annum % of personnel with privileged (inc IT admins) access who have received targeted information security awareness. Number of stolen / disclosed password incident reports per annum

Reference	Minimum requirement	Control reference	Compliance Metric
	• That passwords / passphrases shall never be shared or disclosed. • How to safely protect passwords – may include password managers where available • Internal IT helpdesk procedures for engaging IT support (and the fact that they will never ask for passwords) • Awareness of proper password reset procedures. • An awareness of 'social engineering' techniques that might be used by threats. • The need to report the suspected disclosure of their work passwords		

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.

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

For external use (outside PDS), this standard should be distributed within IT and information security 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.

The effective use of passwords / passphrases depends upon personnel engagement and awareness. It is therefore important to ensure that this standard is party of internal security awareness programmes, targeted campaigns, and induction training. The communication & awareness section of this standard signposts some key awareness objectives to include.

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	Tim Moorey	Initial version	05/10/22
0.2	Tim Moorey	Template updated following National Policy & Standards Working Group review	06/10/22
0.3	Chris Tiller	Drafting of password standard	01/12/22
0.4	Tim Moorey	Minor amendments for NCPSWG review	06/12/22
0.5	Tim Moorey & Chris Tiller	Updated following NCPSWG review and agreed by NCPSWG on 11/01/23	06/01/23
1.1	Chris Tiller	Annual review and migration to new template	Jan/24

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National Authority for approving Cyber Standards	26/01/23
1.1	National Cyber Policy & Standards Board	National Authority for approving Cyber Standards	21/03/24

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
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021
NEP 2022-05 Design Set (IAM and PS – v8.4)	V8.4.0	
NCSC Cyber Assessment Framework (CAF)	V3.1	11/04/2022
Password administration for system owners - NCSC.GOV.UK		