CYBER GUIDELINE DOCUMENT

NCSP Biometric and PIN Guideline

ABSTRACT:
The Biometric & Pin Guidance provides recommendations and best practices for securely implementing and managing biometric authentication and PIN systems.

APPENDIX A: If none, please delete

ISSUED	AUGUST 2025
PLANNED REVIEW DATE	JUNE 2026
DISTRIBUTION	Community Security Policy Framework Members

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

Cyber guideline 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 guideline in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements.

Introduction

Threats and risks associated with biometrics include potential data breaches, identity theft through spoofing or replication of biometric data, unauthorised access to biometric databases, system vulnerabilities to hacking or cyber-attacks, and privacy concerns related to the collection and storage of sensitive biometric information. This guidance document offers recommendations and strategies for implementing robust and secure biometric authentication and PIN systems.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guideline is to provide clear, actionable recommendations for securely implementing biometric authentication systems, aligning with national Cyber Security Principles and Policy. By adopting this standard, readers will gain insights into mitigating cyber threats, protecting sensitive data and ensuring compliance. Specific outcomes include:

- Enhancing security measures for Biometric and PIN system design
- Supporting the use of authentication mechanisms
- Safeguarding privacy and preventing identity theft
- Mitigating risks associated with biometric data storage and processing
- Supporting compliance with legal and policy requirements
- Optimising user experience and system usability
- Strengthening overall cyber security posture.

This guideline aims to raise awareness of the importance of robust authentication mechanisms, aligning with IAM and password standards to bolster cyber security defences and protect against evolving threats.

Audience

This standard is aimed at:

- Staff across PDS & policing to any person who builds & implements or maintains IT systems, either on behalf of National policing or at a local Force level
- IT System managers, administrators and those who have escalated privileges to provide administrative functions
- Information & cyber risk practitioners and managers
- Information Asset Owners (IAOs), Platform Asset Owners (PAOs), and Senior Information Risk Owners (SIROs.)
- Suppliers acting as IT service providers or developing products or services for PDS or policing
- Auditors providing assurance services to PDS or policing.

Scope

This guidance applies to any member of the Policing Community of Trust. It is also applicable to third parties to the policing community.

When

This guidance should be referred to as part of any decision-making in relation to the selection, procurement, deployment and use of biometric and PIN technologies within the law enforcement arena.

Where

The guidance should be applied in any scenario involving biometric and PIN technologies, and it is not geographically restricted.

What

The guidance applies to the use of any biometric and PIN technologies deployed to authenticate, send, receive, store, or otherwise process any policing data. This includes, but is not limited to:

- Mobile / smart phones with biometric or PIN authentication
- Tablets with biometric or PIN authentication
- Body worn technology with biometric or PIN authentication
- Access control systems utilising biometric or PIN authentication
- Computers and laptops with biometric or PIN authentication
- Secure databases and data storage systems requiring biometric or PIN access
- Devices with integrated biometric sensors (e.g. fingerprint, facial recognition)
- Any other device or system that employs biometric or PIN technologies for secure access and data processing.

Biometric Authentication relates to “something you are”: Biometric authentication relies on unique biological or behavioural characteristics of individuals for identification. It can include fingerprint recognition, facial recognition, iris scanning, voice recognition etc. (Please refer to the Identity & Access Management Standard, *Authentication* & System Access Standard).

PIN authentication relates to “something you know”: Once firmly a “Personal Identification Number", often associated with credit cards, PIN authentication now commonly refers to a knowledge based credential used in conjunction with a physical item (“something you have”), such as a hardware security module built into a device.

Biometric and PIN secrets are commonly used locally on a portable device to permit access to locally stored credentials used to authenticate elsewhere. Examples include Windows Hello and Android lock screens.

Threats to PIN & Biometric Authentication

General Guidance:

- Biometrics should not be used as the sole factor for authentication. It is advisable to combine biometric data with other forms of authentication for enhanced security.

Real-life Case Studies and Incidents:

- 2015 U.S. OPM Data Breach:
  - Personal information of over 21 million individuals was compromised, including fingerprint records of 5.6 million people.
  - The breach highlighted significant risks such as identity theft and other malicious activities.
- 2016 Fake Fingerprints Demonstration:
  - Researchers from Michigan State University successfully created fake fingerprints using gelatine and inkjet printers, which were able to deceive fingerprint scanners on smartphones and laptops.
- 2017 Android Device Vulnerability:
  - A vulnerability in Android devices allowed the extraction of fingerprint data, which enabled the creation of 3D-printed replicas due to the absence of encryption, facilitating unauthorized access.

Injection Attacks:

Overview:

- Injection attacks involve inserting unauthentic biometric data into a security system to gain unauthorised access.

Techniques:

- Use of virtual cameras or browser plugins to present fraudulent biometric data.
- Creation of virtual replicas that convincingly mimic real biometric data.

Examples:

- Fingerprint Spoofing:
  - Attackers lift latent fingerprints from surfaces and recreate them using materials like wood glue, silicone, or gelatine. Advanced methods include 3D printing fingerprints.
- Deepfake Video Injection:

    - Attackers use AI to generate realistic deepfake videos that deceive facial recognition systems.
- Voice Authentication Bypass:
    - Exploitation of voice conversion technology and text-to-speech algorithms to create convincing voice deepfakes.
- Vein Pattern Forgery:
    - Crafting counterfeit hand vein patterns using high-resolution images and materials like wax.

Replay Attacks:

Description:

- Attackers record genuine biometric data and reuse it to gain unauthorised access. For instance, replay attacks can involve the use of recorded fingerprint data.

Weak PIN Vulnerabilities:

Weak PINs (e.g., "1234", "0000") are easily guessable. PINs derived from personal information, like birth dates or phone numbers, also increase vulnerability. Weak PINs significantly contribute to the rise in cyber-attacks.

Smudge Attacks:

Smudge attacks rely on analysis of oily smudges left behind on touchscreens or PIN entry mechanisms to identify the location of commonly used numbers. Similar attacks can be effective against mechanical PIN entry systems as commonly used digits visually wear faster than other digits, or mechanical systems exhibit.

Requirements

Guidance Area	Description	References
1. Biometric and PIN System Design	Biometric and PIN System Design Biometric and PIN authentication are authentication methods that provide a faster way of verifying a user's identity. The system design should encompass the following: Types / Methods of Acceptable Biometric Authentication: Fingerprint Recognition: Using unique patterns in a person's fingerprints for identification. Facial Recognition: Analysing facial features to identify individuals. Iris Scanning: Scanning the unique patterns in the iris of the eye. Voice Recognition: Identifying individuals based on their voice characteristics. Biometrics should be used only as part of multi-factor authentication, such as when combined with credentials stored in a hardware security module on a managed device. Establish a secure, authenticated communication channel between the sensor (or an endpoint housing the sensor that is designed to prevent unauthorised sensor	ISO27002:2022, NIST SP 800-63B (Digital Identity Guidelines, Authentication and Lifecycle Management), System Access Standard, Password Standard, Identity & Access Management Standard

Guidance Area	Description	References
	replacement) and the verifier. The sensor or endpoint should undergo authentication procedures before capturing the biometric sample from the claimant. Biometric implementations must use hardware security features such as a Trusted Platform Module (TPM) as part of the system design. TPMs should be independently certified; FIPS 140-2 is the 'current' scheme for this but certifications will expire in 2026 and new certifications must meet FIPS 140-3. Certifications should be at least level 2 overall, and consideration should be made of the use-case and any requirement for level 3, particularly with regard to physical security. PINs can be used as an alternative to biometric authentication for a local device. PINs must consider complexity requirements such as length, repeated or patterns of characters, but many PIN systems will not be configurable to meet the NCSP Password Requirements. Avoid PINs comprised of single digits i.e. 1111 or digits in numerical order i.e. 1234. Consider key layout when selecting PINs to avoid straight-line or pattern-forming combinations. Implement regular PIN change requirements as a good security practice. Treat PINs as personal private information and do not share them.	

Guidance Area	Description	References
2. Risk Assessment and Mitigation	Risk Assessment and Mitigation Each type of Biometric / PIN authentication has its own set of risks and vulnerabilities. A comprehensive risk assessment should be performed and mitigation strategies implemented. Threats & Vulnerabilities: Spoofing Attacks: The risk of attackers using fake fingerprints or facial images to gain unauthorised access. Biometric Data Theft: The potential for biometric data to be stolen and misused if not adequately protected. PIN Guessing: The risk of attackers guessing or brute-forcing PINs. To ensure the security of biometric data, the following principles and practices should be followed: Principles: Informed Consent: Obtain explicit consent from users before collecting biometric data. Purpose Limitation: Collect biometric data only for authorised and specific purposes.	ISO27002:2022, CIS Controls, NIST SP 800-63B (Digital Identity Guidelines) ISO27002:2022, NIST SP 800-63B ISO/IEC 24745:2011 – Information technology – Security techniques – Biometric information protection

Guidance Area	Description	References
	Retention Limitation: Store biometric data for the minimum necessary time required for authentication. For more detailed guidance on the above principles please refer to the *NIST SP 800-63B, Digital Identity Guidelines – Authentication and Lifecycle Management* (https://pages.nist.gov/800-63-3/sp800-63b.html#intent). Legal Requirements: Compliance with Data Protection Laws: Ensure compliance with relevant data protection laws, such as General Data Protection Regulation (GDPR) or the Data Protection Act. Good Practices: Biometric Data Encryption: Encrypt biometric data during transmission and storage. Secure Storage**:** Store biometric data in secure, access-controlled databases. Data Anonymisation: Anonymise or pseudonymise biometric data to protect the identity of users. Privacy and User Control:	

Guidance Area	Description	References
	Biometric Processing: Consider implementing solutions that allow users to retain control over their biometric data by keeping it on their devices. Template-Only Storage**:** Implement systems that exclusively store biometric templates rather than raw biometric data (fingerprints etc.), preventing the reconstruction of the original biometric image.	
3. Biometric and PIN Integration	Biometric and PIN Integration Implement secure and validated biometric matching algorithms to ensure accurate authentication and prevent spoofing or tampering attempts. Where using vendor supplied systems, evaluate the system and the vendors' best practice guidance for implementation.	ISF, ISO27002:2022, CIS Controls, NIST SP 800-63B, "Digital Identity Guidelines: Authentication and Lifecycle Management.", NISTIR 8238, "Ongoing Facial Recognition Vendor Test (FRVT)," CSA
4. Actions in the event of compromise	In the event of a suspected or actual compromise or breach of biometric data, it is crucial to follow the Cyber Threat & Incident Management Standard. Below are specific actions tailored to the management of biometric data breaches: **Immediate Response:**	NCSP Cyber Threat & Incident Management Standard

Guidance Area	Description	References
	• **Notification**: Notify the Information Security Officer and relevant stakeholders, including NMC Incident Response as soon as possible. **<u>Communication:</u>** • **Internal Communication**: Implement the Incident Communication Plan to keep all internal stakeholders informed about the breach, its impact, and the ongoing response efforts. • **External Communication**: Notify affected individuals if there is a risk that their biometric data has been compromised. Follow any legal or regulatory requirements for breach notification. • **<u>Documentation and Reporting:</u>** • **Incident Log**: Ensure that all actions taken during the incident are recorded in an incident log or ITSM system. This log should include the categorisation, classification, and reference of the incident, a description of the impact, actions taken, and evidence gathered. • **Review and Report**: Review all documented information related to the incident. Report the findings and actions taken to senior management and any relevant oversight bodies.	

Guidance Area	Description	References
	For comprehensive guidance, refer to the ***Cyber Threat & Incident Management Standard***, which outlines the full spectrum of actions and protocols to follow during security incidents.	
5. User Awareness and Training	User Awareness and Training Conduct regular user awareness and training programs to educate users about the proper use and security considerations of biometric and PIN authentication. Promote good security practices, such as safeguarding PINs, recognising potential threats and reporting any suspicious activities.	ISF, ISO27002:2022, CIS Controls, NIST SP 800-63B, Section 10, CSA, 10 Steps to Cyber Security (ncsc.gov.uk)

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.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

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

Review Cycle

This guideline 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 guideline 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

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
1.0	PDS Cyber	Updates after initial peer review	28/06/2024
1.1	PDS Cyber	Annual review	09/07/2025

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	5/06/24
1.1	NCPSWG	National Cyber Policy & Standards Working Group	20/08/25

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	03/2024
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