CYBER STANDARDS DOCUMENT

NCSP Management of High Risk Applications

ABSTRACT:
This standard outlines the minimum requirements and controls that must be met to ensure the secure management of applications identified as high risk.

ISSUED	October 2024
PLANNED REVIEW DATE	September 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....3
Introduction....3
Owner....3
Purpose....3
Audience....4
Scope....4
Requirements....5
Communication approach....6
Review Cycle....6
Document Compliance Requirements....7
Equality Impact Assessment....7
Document Information....8
Document Location....8
Revision History....8
Approvals....8
Document References....9

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 in relation to the management of high risk applications.

Introduction

This Standard outlines requirements relating to the management of high risk applications by the policing community.

Adherence to this Standard will ensure that where there is a genuine operational requirement to use high risk applications, they can be used safely.

Legitimate use of high risk applications could include:

- Open source intelligence gathering
- Law enforcement investigations
- Authorised press or media relations

This standard should be read in conjunction with the NCSP Application Management standard.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to:

- Minimise the risk of data loss through the unfettered use of high risk applications;
- Ensure that Policing mirrors Cabinet Office direction to government departments, where applicable

Audience

This Standard is for the awareness of UK police force end users, in particular local Information Security and Assurance teams who have a remit to assess and manage local use of applications.

This Standard is also for the awareness to those within the community who may have cause to use a high risk application or have the ability to install a high risk application on policing technology.

Scope

This Standard is applicable to any use of high risk applications by the policing community, which includes web applications and native applications.

The risk level of an application can be identified by completing a risk assessment.

Typical indicators of a High level of risk for applications may include:

- Known or likely links to hostile nation state governments (Russia, China, Iran, North Korea)
- Lack of or unclear privacy policies or where the application operates or stores data in countries where there is no Data Protection Adequacy Decision (see the UK Information Commissioners website – ico.org.uk)
- Excessive permission requirements – such as requiring access to local files, camera, location etc.
- Higher level privilege requirements – such as admin / root access rights.
- UK Governmental sanctions / restrictions – see https://www.gov.uk/government/publications/the-uk-sanctions-list

Tik Tok

Tik Tok is perhaps the highest profile high-risk application and is worthy of special mention. This application (including the web version) has been identified as a high risk application (see Cabinet Office release 16 March 2023).

TikTok is a popular social media platform which has recently been restricted in its use by the UK Government. Adherence to this standard will ensure that where TikTok is required for genuine operational purposes, it can be used safely. Legitimate uses of TikTok could include:

- Open source intelligence gathering,
- Law enforcement investigations,
- Authorised press or media relations.

The TikTok application is deemed to be a significant risk due to overzealous permissions, which potentially include the monitoring of keystrokes, and due to concerns over the relationship of the parent company (ByteDance) to the Chinese Communist Party.

Requirements

This section details the requirements that this standard aims to deliver regarding the protection of policing assets from high risk applications. The minimum requirements outlined below are a baseline to minimise the risk of data loss through the unfettered use of high risk applications and, where applicable, to ensure that policing mirrors Cabinet Office direction to government departments. It is the responsibility of all community members and other in scope organisations to ensure that they are familiar with and adhere to this standard.

Reference	Minimum Requirement	Control Reference	Compliance Metric
1	All applications (including those accessed using web browsers, mobile devices or installed on endpoints) must be catalogued and risk assessed. See NCSP Application Management and Physical Asset Management standards	**NIST CSF:** ID.RA.5 ID.AM.1 ID.AM.2	Current application asset register including risk assessments.
1	High risk applications must not be installed on or accessed from police networked systems. Technical and policy controls must be in place to prevent the unauthorised installation or access of high risk applications.	**NIST CSF:** ID.BE-2 PR.IP-1 PR.PT-3	Information Security Policy, Baseline Configuration Documentation
2	Where there is an operational necessity to use high risk applications, a risk assessment must be documented and reviewed by the Senior Information Risk Owner (SIRO.) Note: where an application may access National Policing systems or information, this will require escalation to the National Cyber Audit, Risk & Compliance team. The application must be deployed and accessed in accordance with the NCSP Guidance document 'Safe Deployment of High Risk Applications'	**NIST CSF:** ID.AM-1 PR.DS-5 ID.RA-1 ID.RM-1	Asset Register, Low Level Designs, risk assessment and sign off by SIRO.

Reference	Minimum Requirement	Control Reference	Compliance Metric
3	Local Acceptable Use Policies (AUPs) must reflect the requirements of this standard	**NIST CSF:** ID.GV-1	Acceptable Use Policy, Cybersecurity Policy, Information Security Policy
4	The requirements of this Standard must be communicated as necessary to ensure compliance	**NIST CSF:** ID.GV-1 PR.AT-1	Information Security Policy, Security Training and Awareness Policy

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.

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

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

Revision History

Version	Author	Description	Date
0.5	PDS Cyber	Minor update following internal peer review	21/07/23
1.1	PDS Cyber	Template rebrand and wider change from TikTok to Management of High Risk Applications	16/07/24

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Board	National approving authority	28/09/23
1.1	National Cyber Policy & Standards Board	National approving authority	26/09/24

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