NPCC
National Police Chiefs' Council

POLICE
DIGITAL
SERVICE

CYBER GUIDELINE DOCUMENT

NCSP Safe Deployment of High Risk Applications

ABSTRACT:
This guideline outlines approaches to follow for any use of high risk applications to reduce risk

ISSUED	August 2025
PLANNED REVIEW DATE	August 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....3
Introduction....3
Owner....3
Purpose....3
Audience....3
Scope....4
Requirements....4
Communication approach....5
Review Cycle....5
Document Compliance Requirements....5
Equality Impact Assessment....5
Document Information....6
  Document Location....6
  Revision History....6
  Approvals....6
  Document References....7

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

This document provides guidance to support the safe deployment of high risk applications by the policing community.

Adherence to this guideline will ensure that, where any high risk applications are required for genuine operational purposes, they can be used safely and with any impact resulting from potential compromise minimised.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guideline is to:

- Outline the three approaches that can be used to safely deploy high risk applications
- Provide clear guidance to segregate any use of high risk applications from the wider network (physically or virtually)
- Minimise the impact of any potential compromise

Audience

This guideline 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.

Scope

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

The risk level of an application can be identified via risk assessment completion.

The TikTok application (including the web version) has been identified as a high risk application (see Cabinet Office release 16 March 2023).

Requirements

Outlined below are three approaches to safely deploy high risk applications – local review is required to determine relevance on a case-by-case basis.

The approaches are:

- Network separation
- Use of a social media management platform
- Use of devices not connected to the force network

Network separation
A segregated environment can be used to allow staff to access services that would not otherwise be permitted on a police issued device. The use of remote desktop technologies, such as Azure Virtual Machines and Azure Bastion, removes the need for additional devices and allows access to the segregated area via a couple of mouse clicks. Commercially available solutions can also be procured that provide a segregated environment. These 'off the-shelf' solutions may also provide additional services and functionality, including tools for intelligence gathering and detailed auditing and logging that can support evidential submissions.
Use of a social media management platform
Social media management platforms can be used for posting to and monitoring various social media platforms from a single place, with the management platform interacting with social media applications via APIs. As there is no direct connection to the social media applications, a level of abstraction exists, thereby limiting the impact to privacy.

Use of devices not connected to the force network
Accessing applications from devices not connected to the force network mitigates risks associated to the use of high risk applications on networked devices, however there are associated risks in using such devices which would require further local review if this approach is to be employed.

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

National Standards Platform - About - National Standard Microsite

Revision History

Version	Author	Description	Date
0.1	Dean Cowe	Initial Version	19/05/23
0.2	Dean Cowe	Minor review following National Cyber Policy & Standards Board feedback	09/06/23
0.3	Dean Cowe	Minor refresh of guidance section following peer review	14/06/23
0.4	Dean Cowe	Template rebrand and wider change from TikTok to High Risk Applications	08/07/24
1.2	Ben Walker	Guidance annual review	10/07/25

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	07/06/23
1.1	NCPSWG	National Cyber Policy & Standards Working Group	21/08/24
1.2	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**	**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**
NIST Cyber Security Framework	V2.0	02/2024
CSA Cloud Controls Matrix	**v4**	**01/2021**
10 Steps to Cyber Security - NCSC.GOV.UK	**Web Page**	**05/2021**