CYBER STANDARD DOCUMENT

USE OF TIK TOK ACROSS POLICING

ABSTRACT:
This standard provides direction on the use of TikTok across policing, in accordance with the latest guidance provided by the Cabinet Office.

ISSUED	August 2023
PLANNED REVIEW DATE	August 2024
DISTRIBUTION	Community Security Policy Framework Members
STANDARD VALIDITY STATEMENT This document is due for review on the date shown above. After this date, the document may become invalid. Members should ensure that they are consulting the currently valid version of the documentation.	

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	Initial draft	16/05/23
0.2	PDS Cyber	Internal peer review updates	23/05/23
0.3	PDS Cyber	Conversion into Standard template following NCPSWG feedback	12/07/23
0.4	PDS Cyber	Review following conversion to Standard template	17/07/23
0.5	PDS Cyber	Minor update following internal peer review	21/07/23

Approvals

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

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
NIST Cyber Security Framework	v1.1	04/2018

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 the National Policing Community Security Principles sets out National Policing requirements for the establishment, implementation, maintenance, and continual improvement of appropriate information security controls. The controls will continue to be improved and aligned to any changes in National Policing strategy, operating environment, risk profile, laws and regulations, and in response to incidents or emerging threats.

Introduction

This standard outlines requirements for any use of TikTok by the policing community.

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.

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 TikTok,
- Ensure that Policing mirrors Cabinet Office direction to government departments.

Audience

Anyone in the community who might have cause to use TikTok or has the ability to install it on policing technology.

Scope

This standard applies to the use of TikTok in national policing.

Requirements

The below statements outline the minimum requirements of this standard to minimise the risk of data loss through the unfettered use of TikTok and 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	TikTok must not be installed on police networked systems.	NIST CSF ID.BE.2 PR.IP.1 PR.PT.3	SyAP / TPAP to measure compliance
2	Where there is an operational necessity to use TikTok, it must be deployed in accordance with the NPCC/PDS Guidance Document 'Safe Deployment of TikTok'.	NIST CSF PR.DS.5	SyAP / TPAP to measure compliance
3	Where TikTok is used locally, in accordance with the NPCC/PDS guidance, the force SIRO must approve the reputational risk of doing so.	NIST CSF ID.RA.3 ID.RM.1	SyAP / TPAP to measure compliance
4	Local Acceptable Use Policies (AUPs) must reflect the requirements of this standard.	NIST CSF ID.GV.1	SyAP / TPAP to measure compliance

Reference	Minimum requirement	Control reference	Compliance Metric
5	The requirements of this standard will be communicated as necessary to ensure compliance.	NIST CSF ID.GV.1 PR.AT.1	SyAP / TPAP to measure compliance

Related Standards

National Community Security Policy Security Management Standard

Compliance / Performance measurement

Compliance to this standard will be measured via the Security Assessment for Policing (SyAP) or Third-Party Assurance for Policing (TPAP) process as appropriate.

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 Nation Cyber Policy & Standards Board (NCPSB) for review and approval.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

For external use (outside PDS), this standard should be distributed via Information Security Officers 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

PDS Audit Risk and Compliance Team will assess statements made by police forces or third parties in accordance with the established compliance measures for SyAP and TPAP.

Equality Impact Assessment

For organisations to conduct locally as appropriate.