Overseas IT Access Guideline

ABSTRACT

This guidance describes best practice risk management controls for accessing Policing ICT resources whilst abroad. It also describes the circumstances when forces can make a local decision or when referral to NSIRO is required when use abroad is required.

ISSUED:	February 2026
PLANNED REVIEW DATE:	February 2027
DOCUMENT OWNER:	National Chief Information Security Officer
DISTRIBUTION:	Members of the Policing Community of Trust
COPYRIGHT:	All content – copyright Police Digital Service
DOCUMENT HANDLING:	OFFICIAL – FOR PUBLIC RELEASE

POLICY VALIDITY STATEMENT

This guideline is due for review on the date shown above. After this date, policy and process documents may become invalid.

Readers 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

Individuals working in overseas environments (i.e., locations outside the United Kingdom) should be subject to authorisation and provided with technical support to protect ICT assets and the information they handle against loss, theft and cyber-attack, especially when travelling to high threat countries or regions.

Consult Counter Terrorism Security Advisors (CTSA's) for the latest information on high threat regions.

Suspicious occurrences such as unusual approaches or behaviour should be reported to UK National Security Vetting (UKNSV) via local vetting teams.

This guidance document includes controls to minimise the risk to policing information whilst individuals are working overseas.

Purpose

The purpose of this standard is to:

Ensure that risks to policing information handled by individuals working in overseas environments is minimised, by protecting against threats to that information.

Audience

Force / organisational Senior Information Risk Owners (SIROs), Information Security Officers (ISOs), information security practitioners, Information Asset Owners (IAOs), all individuals travelling overseas and accessing/processing policing information.

Scope

This guidance applies to any member of the Policing Community of Trust travelling / deployed overseas and accessing / processing policing information. This guidance is focussed for temporary travelling overseas to support operational requirements. For longer-term overseas working, such as living abroad, the requirements of this guidance should also be considered alongside wider implications such as employee regulations and HMRC requirements.

Guidance

REQUIREMENTS

Reference	Minimum requirement	Control reference	Compliance Metric
1.0	**General**		
1.1	An Authority for Travel process should be in place to ensure the requirements of this guideline are adopted and relevant parties are engaged before travel outside the UK with Force or National Policing ICT assets [**ICT Assets**] occurs.	ISO/IEC 27002:2022 5.9, 5.10	Documented, published process. Targeted awareness initiatives to supervisors, managers and personnel. Records of adoption.
1.2	ICT Assets include any device that either stores policing data or can access policing data, for example laptops, mobile phones, tablets. **See NCSP Asset Management standard**	ISO/IEC 27002:2022 5.9, 5.10	Documented asset management processes.
2.0	**Risk Assessment** A full risk assessment **must** be documented. **See National Information Risk Management Framework**		
2.1	Evaluating vulnerabilities specific to overseas working environments (e.g. weak or unknown physical security, single-factor authentication mechanisms for remote access or use of collaboration platforms).	ISO/IEC 27002:2022 6.7, 7.5, 7.7, 8.8	Documented local current assessment of risk of overseas use of ICT assets.
2.2	Physical protection against loss, theft or tampering of ICT assets (e.g. cable locks, indelible marking, tamper-evident seals etc.) **See NCSP Asset Management standard**	ISO/IEC 27002:2022 6.7, 7.5, 7.7	Physical controls in place on ICT assets
2.3	The health and safety aspects of working in overseas environments, including insurance. **Refer to HMG country-specific guidance** (*see Related Documents for link*)	Local health & safety policy	Local insurance cover in place. Tailored health & safety advice.

Reference	Minimum requirement	Control reference	Compliance Metric
2.4	The requirements for individuals travelling to high threat regions. *(see Section 9.0 – High Threat Regions)*	ISO/IEC 27002:2022 6.7	Tailored briefings / advice to individuals based upon trusted sources such as Foreign & Commonwealth Office.
2.5	Connecting securely to the organisation's network (e.g. through a Virtual Private Network [VPN] or secure web-browser session).	ISO/IEC 27002:2022 6.7	VPN in place and verified secure by security testing check (ITHC)
2.6	A Business Impact Assessment for each information asset accessed.	ISO/IEC 27002:2022 5.33, 5.34	Business Impact Assessments conducted and kept up to date.
2.7	Consideration of local laws around encryption. Government agencies overseas may require you to hand over ICT Assets for an indefinite period, or to decrypt your ICT Assets or files upon entry to or exit from their territories. The risk assessment must consider the consequences of such disclosure.	ISO/IEC 27002:2022 5.31, 8.24	Risk assessment conducted and reflected in briefings / advice to travellers.
2.8	A Risk Balance Case **must** be completed for each instance of overseas working and authorisation obtained by the appropriate risk owner.	ISO/IEC 27002:2022 6.7	Risk Balance Case process in place. Risk Balance Cases for travel.
2.9	The process for revocation of authority and access rights, and the return of equipment when the remote working activities are terminated, should be included within the Risk Balance Case.	ISO/IEC 27002:2022 6.7, 8.2	Process in place with supported records of implementation.

Reference	Minimum requirement	Control reference	Compliance Metric
3.0	**Authorisation**		
3.1	Authorisation **must** be obtained by appropriate line management for individuals to access or process policing information overseas. This must include a definition of: • the work permitted and • the duration of the visit An approved Risk Balance Case must be obtained before overseas information access is granted.	ISO/IEC 27002:2022 5.9, 5.10, 6.7	Overseas travel process in place with proper authorisations, including information asset owners and Senior Information Risk Owner. Business trigger points in place to ensure process is applied to all business / operational travel where IT / information assets taken. Approved Risk Balance Case.
4.0	**Risk Owners** The Risk Owner(s) will depend on the information available to access from overseas, as defined within the National Policing Information Risk Appetite and Authorised Professional Practice on Information Assurance. In summary:		
4.1	If access to National Systems is required, the Risk Owners will be the Force SIRO and each System's Information Asset Owner. Where there is no Information Asset Owner, the Risk Owner will be the National SIRO.	NIST CSF ID.RM-3	Asset register details information asset owners and whether local / National system.
4.2	If the risk is identified as above the force risk appetite, the Risk Owners will be the Force SIRO and the National SIRO.	NIST CSF ID.RM-3	Local risk escalation procedure.
4.3	If access to National Systems is not required and the risk is identified as within the force risk appetite, the Risk Owner will be the Force SIRO.	NIST CSF ID.RM-3	Local risk escalation procedure.
5.0	**Overseas environment** Activities in overseas environments should be protected in line with the risk assessment including:		
5.1	Implementing controls described in the Risk Balance Case to remediate identified vulnerabilities to within the risk appetite.	NIST CSF ID.RA-1 ID.RA-5	Vulnerability management in place validated security testing (ITHCs) & continuous assurance.

Reference	Minimum requirement	Control reference	Compliance Metric
5.2	Implementing secure remote access solutions. Consider HMG advice for appropriate/approved VPNs (*see country-specific guidance in Related Documents*)	NIST CSF PR.AC-3	Secure remote access solution which is assured by IT health-checks.
6.0	**Individual assurance**		
6.1	Travel with the minimum necessary equipment and ICT assets to perform the objectives of the role.	NIST CSF PR.PT.3	Targeted awareness initiatives to supervisors, managers and personnel. Records of adoption.
6.2	Work only in appropriate locations (e.g. do not work in bars, on public transportation or in open spaces). Information above OFFICIAL should not be discussed over public telephony (mobile or fixed.)	NIST CSF PR.IP-5	Documented, published process. Targeted awareness initiatives to supervisors, managers and personnel. Pre-travel briefs. Records of adoption.
6.3	Have the necessary skills and knowledge to perform required security tasks (e.g. restricting physical access, performing backups and encrypting sensitive files).	NIST CSF PR.AT-1	Targeted awareness initiatives to supervisors, managers and personnel. Pre-travel briefs. Records of adoption.
6.4	Be aware of the additional risks associated with overseas working. Consider risk to personal devices as well as corporate devices. This includes wearable tech (smart watches, rings etc.) Assume any tech device can and will be compromised.	NIST CSF PR.IP-5 PR.AT-1	Tailored briefings / advice to individuals based upon trusted sources such as Foreign & Commonwealth Office. Pre-travel briefs. Records of adoption.
6.5	Be provided with technical support (e.g. via a helpdesk, service desk or equivalent).		Documented, published process.

Reference	Minimum requirement	Control reference	Compliance Metric
6.6	Act in compliance with all local and UK legal and regulatory requirements (e.g. health and safety laws and data privacy regulations). Suspicious occurrences such as unusual approaches or behaviour should be reported to UK National Security Vetting (UKNSV) via local vetting teams.	NIST CSF PR.IP-5	Tailored briefings / advice to individuals based upon trusted sources such as Foreign & Commonwealth Office. Pre-travel briefs.
6.7	Securely store and destroy sensitive printed information, where printed documentation is unavoidable (e.g. lockable fireproof storage areas and cross-cut shredders).	NIST CSF PR.AC-2	Documented, published process. Targeted awareness. Pre-travel briefs.
7.0	**Equipment** Individuals who work in overseas environments should be provided with security equipment such as:		
7.1	Secure storage.	NIST CSF PR.AC-2	Evidence of equipment provided. Targeted awareness. Pre-travel briefs.
7.2	Physical cable locks, anti-theft alarms or equivalent security devices for ICT assets. Anti or tamper-evident measures.	NIST CSF PR.AC-2	
7.3	Security screen filters (often referred to as privacy filters) to help protect against the threat of shoulder surfing.	NIST CSF PR.AC-2	
7.4	Access to technical support (e.g. via a helpdesk, service desk or equivalent).	NIST CSF RS.CO-2	
7.5	By all practicable means avoid leaving equipment or ICT Assets unattended and in plain sight.	NIST CSF PR.AC-2	
7.6	Non-attributable (burner) phone/device	NIST CSF ID.AM-1 PR.AC-2 PR.DS-3	
8.0	**ICT Asset configuration** ICT Assets that access corporate networks from untrusted environments should be configured to:		
8.1	Block overseas access to corporate network without an approved Risk Balance Case.	NIST CSF PR.DS-1	Use of 'geo fencing' or conditional access technical controls. Validated by security testing (ITHCs) and configuration reviews.

Reference	Minimum requirement	Control reference	Compliance Metric
8.2	Ensure that the use of a Virtual Private Network (VPN) is legal in the country being travelled to and is in place between the ICT Asset and information systems accessed. (*see also 5.2*)	NIST CSF PR.AC-3	Validated by security testing (ITHCs) and configuration reviews.
8.3	Prevent access to untrusted networks while the ICT Asset is connected to the corporate network (i.e. to avoid bypassing the VPN).	NIST CSF PR.DS-5	Validated by security testing (ITHCs) and configuration reviews.
8.4	Configure appropriate Office 365 security controls e.g. Multi-Factor Authentication, device compliance.	NIST CSF PR.AC-7	Validated by security testing (ITHCs) and configuration reviews.
8.5	Configure Conditional Access Policies to allow for easier monitoring of login attempts from overseas.	NIST CSF DE.CM-1	
8.6	Appropriately isolate information systems to ensure only necessary access to information.	NIST CSF PR.DS-1	
8.7	Revocation of authority and access rights, and the return of ICT Assets should be carried out promptly when the remote working activities are terminated, or when the approved period ends – whichever is soonest.	NIST CSF PR.AC-1	Documented, published process. Evidence of compliance.
9.0	**High threat regions** High threat regions may be identified via external sources such as the FCDO website or Forces' own sources. The UK Government Security Awareness in Fragile Environments (SAFE) guide should be consulted – link on UK Government Security site (registration required) along with HMG Country-specific guidance - link Consult with Counter Terrorism Security Advisors (CTSA). Note that certain countries prohibit satellite communication devices including handheld GPS units and satellite phones. Individuals travelling to high threat regions should protect sensitive information from targeted attack by:		
9.1	Using temporary or loan ICT Assets (including laptops, tablets and smartphones).	NIST CSF PR.AC-2	Documented, published process. Configuration / build for ICT assets to high threat regions.
9.2	Limiting the amount of information stored on ICT Assets (e.g. by using a new build or securely deleting all information previously stored before travelling).	NIST CSF PR.PT-3	

Reference	Minimum requirement	Control reference	Compliance Metric
9.3	Storing sensitive information, where permitted by local law, on approved, encrypted removable media, which is kept with the individual (to help ensure the information is protected when the ICT Asset is unattended).	NIST CSF PR.PT-2	Secure cleansing process for ICT Assets returning from high threat regions. Secure method for importing data from ICT Assets that have been to high threat regions.
9.4	Avoiding the use of unknown ICT Assets for communicating or processing sensitive information (e.g. provided by unknown individuals or available in internet cafes).	NIST CSF PR.AC-5	Documented, published process.
9.5	Limiting the number and duration of discussions that involve sensitive information.	ISO/IEC 27002:2022 7.7, 7.9	Targeted awareness. Pre-travel briefs.
9.6	Ensuring that all ICT Assets used within high threat regions are safely decommissioned by a competent authority (e.g. force IT team) immediately on return to UK. *This should be actioned prior to the device reconnecting to the organisation's corporate network, or any other network / system that can access law enforcement data.*	ISO/IEC 27002:2022 5.9, 6.7	Secure cleansing process for ICT Assets returning from high threat regions.

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.

Document Compliance Requirements

(Adapt according to local policy needs.)

Equality Impact Assessment

(Adapt according to local policy needs.)

Review

This document 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 policy continues to meet the objectives and strategies of the police service.

Related documents

DOCUMENT NAME	VERSION AND DATE
NPCC National Policing Digital Strategy 2025-2030	2025
NPCC National Policing Cyber Security Strategy	2024
ISF - Standard of Good Practice (for Information Security)	2024
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	02/2022
CIS Controls	V8.1 06/2024
NIST Cyber Security Framework v2.0	V2.0 02/2024
CSA Cloud Controls Matrix v4.0	V4.0 08/05/2025
NCSC Cyber Assessment Framework v4.0	V4.0 2025
National Police Chiefs' Council (NPCC) Covenant for Using Artificial Intelligence (AI) in Policing	V1.1
Authorised Professional Practice on Information Assurance	June 2020
Security Awareness in Fragile Environments (SAFE) – UK Government Security - link	HMG online resource
Country-specific guidance - link	HMG online resource

Document Information

Document Location:

National Policing Policies & Standards Platform - https://knowledgehub.group/web/national-standards

Version History

VERSION	AUTHOR	REVISION	DATE
0.1	PDS Cyber	Initial version	10/01/23
0.2	PDS Cyber	Rebrand to NPCC PDS template, tabulated requirements and inc comments from NCPSWG.	02/02/23
1.1	PDS Cyber	Annual review and rebrand	05/02/24
1.2	PDS Cyber	Annual Review and new guidance template transposition	19/02/2025
1.3	PDS Cyber	Annual Review and new guidance template transposition	19/12/2025

Approvals

VERSION	AUTHOR	NATIONAL CYBER POLICY & STANDARDS GOVERNANCE	DATE
1.0	NCPSWG	NCSPWG	01/03/23
1.1	NCPSWG	NCPSWG	01/05/24
1.2	NCPSWG	NCPSWG	05/03/25
1.3	NCPSWG	NCPSWG	04/02/26