CYBER STANDARDS DOCUMENT

NCSP People Security Management

ABSTRACT:
This standard is intended to guide the reader through the process of securely managing personnel and embedding security at all stages of the employee lifecycle.

ISSUED	May 2024
PLANNED REVIEW DATE	April 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

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 for people security management.

Introduction

This People Security Management standard is intended to embed information security into each stage of the employment lifecycle (including personnel vetting, induction, employment contracts, ongoing management, and termination), assigning ownership of information (including responsibility for its protection) to capable individuals and obtaining confirmation of their understanding and acceptance. Enable individuals working in remote environments to protect critical and sensitive information they handle against loss, theft, and cyber-attack.

It seeks to help maintain a comprehensive, ongoing security education, training, and awareness programme (SETA), to promote and embed expected security behaviour in all individuals who have access to the organisation’s information and system.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this standard is to:

- ensure that employees are equipped with the skills, knowledge and tools to support the organisation's values, adhere to information security policies thereby protecting policing information and systems
- ensure security obligations are clearly communicated to all employees or external individuals and formally accepted, providing legal and contractual protection (e.g. in case of a dispute).
- achieve individual accountability for information and systems, provide a sound management structure for individuals running or using them and give their owners a vested interest in their protection.
- ensure that critical and sensitive information handled by individuals working in remote environments is protected against the full range of threats to that information.
- create a culture where expected security behaviour is embedded into regular day-to-day activities and where all relevant individuals make effective risk-based decisions and protect critical and sensitive information used throughout the organisation from being compromised.
- ensure individuals remain aware of the importance and need for information security on an ongoing basis and maintain a security-positive culture throughout the organisation.

Audience

This document applies to any member of the Policing Community of Trust as defined in the National Community Security Policy (herein referred to as a ‘member’).

This standard is aimed at:

- Any roles across policing who are responsible for personnel, sworn or unsworn at any stage of their employment lifecycle. This includes Human Resources directors, managers and teams.
- Supervisor, managers and senior leaders who are responsible for managing and developing their teams.
- Senior Information Risk Owners (SIROs), Information Asset Owners (IAOs) and supporting roles.
- Information & Cyber risk practitioners and managers.
- Any person handling or who has access to policing information assets, IT systems or services, buildings, property or operations.

- Suppliers acting as service providers or developing products or services for national policing.
- Those in compliance and assurance roles.

Scope

1. This standard applies to all information that is classified within the OFFICIAL tier including OFFICAL-SENSITIVE special handling caveat of the Government Security Classification Policy (GSCP). It should be considered to describe the baseline minimum requirements for higher classifications which will require additional controls to be implemented.
2. This standard applies to all roles (permanent and temporary) that are expected to access National Policing IT systems, Force IT systems, premises, and physical information assets (including documents and artefacts).
3. It applies to all member personnel who have a lawful business need to access National or Force IT systems, premises, or information assets. This includes temporary (contract), sworn and permanent personnel engaged in supporting policing activities.
4. It applies to third parties who have lawful business need to access National Policing IT systems, Force IT systems, premises, and physical information assets.
5. This standard does not affect access by individuals who are provided police information by the police in the course of their professional duties, solely for the purpose of performing those duties, such as regulatory audit and inspection bodies.

Requirements

These requirements are defined across the employee lifecycle and can be used to define a culture change programme or as continuous improvement objectives. Compliance metrics are provided as examples of evidence of implementation or maturity.

Ref	Minimum requirement	Control reference	Compliance Metric
1.	**Employment Lifecycle** Information security requirements must be embedded into each stage of the employment lifecycle. They must include those security actions that are required prior to, during, and on termination of employment.		
1.1.	All applicants for employment (including part-time employees, consultants, contractors and temporary staff) must be appropriately screened and vetted prior to starting work, in accordance with the Vetting Requirements for Policing. **See also:** - Vetting Requirements for Policing - College of Policing Authorised Professional Practice – Vetting APP on Vetting	**ISO/IEC 27002:2022:** 6.01 **NIST CSF:** PR.IP-11	*Published and up to date Vetting Policy* *Completed records demonstrating screening certification.*
1.2.	Induction training must be conducted for all employees and specifically include information security. It must ensure employees have the skills and knowledge to demonstrate expected security behaviour.	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT-1 **CIS Controls v8:** 14.1, 14.9	*Appropriate induction training content.* *Completed records of employees' induction training.*

Ref	Minimum requirement	Control reference	Compliance Metric
1.3.	Ensuring the security of policing information must be a responsibility of all employees. Methods to establish may include: a) compulsory participation in security awareness training b) signing code of conduct c) including security behaviour in individual's performance objectives d) addressing security-related behaviour that does not comply with policing standards. e) Notifying to managers and vetting teams of changes of individuals' circumstances or conflicts of interest as defined in the Vetting Authorised Professional Practice. f) Recognising and rewarding positive security behaviours or self-initiated improvements.	**ISO/IEC 27002:2022:** 5.02, 6.02 **NIST CSF:** ID.AM.3, PR.AT.4, PR.AT.5,	*Completed records of employees' security training.* *Signed Codes of Conduct.* *Employee objectives contain security related behaviours.* *Disciplinary Policy.*
1.4.	Employee performance management/appraisal must consider performance against security responsibilities, including the protection of policing information and systems.	**ISO/IEC 27002:2022:** 5.02, 5.04 **NIST CSF:** ID.AM.6	*Personal Development Reviews / Appraisals*
1.5.	Upon termination or change of employment, employees must be reminded that information security responsibilities remain valid as documented in the conditions of employment.	**ISO/IEC 27002:2022:** 5.04, 6.05 **NIST CSF:** PR.AT.5, PR.IP.11 **CIS Controls v8:**7.3.1	*Leavers' Checklist includes security reminders.* *Terms & Conditions includes post-employment security responsibilities.*

Ref	Minimum requirement	Control reference	Compliance Metric
1.6.	Upon impending termination or change of employment, employees must ensure that: a) business process documentation is up to date and accurate b) any security roles/responsibilities are transferred c) all copies of policing or organisational information are destroyed or returned. **<u>See also:</u>** - Information Management Standard	**ISO/IEC 27002:2022:** 5.04, 6.05 **NIST CSF:** PR.AT.5, PR.IP.11 **CIS Controls v8:** 7.3.1	*Movers'/Leavers' Checklist includes security reminders for Line Managers.* *Terms & Conditions includes post-employment security responsibilities.*
1.7.	Upon impending termination of employment, employees must return policing/organisational assets, including: a) documentation stored on removable media or in paper form b) equipment (e.g. laptops, tablets, smartphones, removable media and specialist equipment) c) software (including media, documentation and licensing information) d) authentication hardware (e.g. physical tokens, smartcards and biometric equipment). **<u>See also:</u>** - Information Management Standard	**ISO/IEC 27002:2022:** 5.04, 5.11, 6.05 **NIST CSF:** PR.AT.5, PR.IP.11, PR.AC-3 CIS 13.5	*Leavers' Checklist includes security reminders for Line Managers.* *Terms & Conditions includes post-employment security responsibilities.*
1.8.	Upon impending termination of employment the copying of critical or sensitive information by employees during their notice period should be risk assessed and restricted where appropriate. **<u>See also:</u>** - Identity and Access Management Standard	**ISO/IEC 27002:2022:** 6.05 **NIST CSF:** PR.IP-11 **CIS Controls v8:** 7.3.1	*Leavers' Checklist includes security reminders for Line Managers.* *Terms & Conditions includes post-employment security responsibilities.*

Ref	Minimum requirement	Control reference	Compliance Metric
2.	**Security Agreements** Security agreements (e.g. terms and conditions of employment or non-disclosure agreements) should be established with all individuals or third parties who access critical or sensitive information and systems.		
2.1.	Permanent employees must formally accept terms and conditions of employment. Non-permanent employees must sign nondisclosure/confidentiality agreements.	**ISO/IEC 27002:2022:** 5.02, 6.02, 6.06 **NIST CSF:** PR.AT-1, ID.SC-3	*Signed terms & conditions of employment.* *Signed NDA's.*
2.2.	Terms and conditions of employment and job descriptions must include information security responsibilities. Terms may include: a) information security responsibilities apply whether during or outside working hours b) information security responsibilities continue after termination of employment c) the employee has legal responsibilities (e.g. regarding intellectual property laws, data protection) d) adherence to the organisation's information security policy and supporting policies/guidelines is mandatory e) inclusion of a confidentiality clause (or separate non-disclosure agreement) f) stating the consequences of non-compliance with the information security policy.	**ISO/IEC 27002:2022:** 5.02, 6.02, 6.06 **NIST CSF:** PR.AT-1, ID.SC-3	*Terms & conditions of employment.* *Job descriptions.*
2.3.	All third parties who have access to critical systems or policing information must sign non-disclosure agreements.	**ISO/IEC 27002:2022:** 5.02, 6.02, 6.06 **NIST CSF:**	*Non-Disclosure Agreements* *Third Party Policy*

Ref	Minimum requirement	Control reference	Compliance Metric
		PR.AT-1, ID.SC-3	
2.4.	Non-disclosure agreements/confidentiality clauses should include the: a) classification of information b) conditions under which information may be used c) expected duration d) responsibilities of signatories.	**ISO/IEC 27002:2022:** 5.02, 6.02, 6.06 **NIST CSF:** PR.AT-1, ID.SC-3	*Non-Disclosure Agreements* *Third Party Policy*
2.5.	Non-disclosure agreements/confidentiality clauses should include processes for: a) reporting breach e.g. disclosure b) addressing non-compliance c) terminating an agreement d) responsibilities on termination of agreement.	**ISO/IEC 27002:2022:** 5.02, 6.02, 6.06 **NIST CSF:** PR.AT-1, ID.SC-3	*Non-Disclosure Agreements* *Third Party Policy*
2.6.	The conditions under which information may be used should be determined by: a) the classification of information to be handled b) compliance with appropriate legal and regulatory requirements.	**ISO/IEC 27002:2022:** 5.02, 6.02, 6.06 **NIST CSF:** PR.AT-1, ID.SC-3	*Non-Disclosure Agreements* *Third Party Policy*
3.	**Ownership and Responsibilities** Ownership of critical business environments, processes, applications (including supporting technical infrastructure) and information should be assigned to capable individuals, supported by responsibilities for protecting them that are clearly defined and accepted.		
3.1.	Ownership of critical business environments, processes, and applications (including supporting technical infrastructure) should be assigned to individuals (e.g. business managers), acknowledged and documented. **See also:** - Security Governance Standard	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2,	*Information Asset Register*

Ref	Minimum requirement	Control reference	Compliance Metric
	- Security Management Standard - Identity and Access Management Standard - Application Management Standard	PR.AT.3, PR.AT.4, PR.AT.5, PR.IP.11, RS.CO.1	
3.2.	A process should be established to: a) set approval levels for security-related activities b) determine the seniority/knowledge required for approval. **See also:** - Information Management Standard - National Police Information Security Risk Management Framework	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2, PR.AT.3, PR.AT.4, PR.AT.5, PR.IP.11, RS.CO.1	*Change Management Policy* *Risk Management Framework*
3.3.	Information Asset Owners (IAO's) should be informed of, and accept, responsibilities for protecting information and systems, which include: a) agreeing the systems under their responsibility b) understanding/identifying information risks c) determining and approving business requirements d) considering operational risk a) defining and modelling appropriate attitudes towards information security e) setting priorities and allocating resources	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2, PR.AT.3, PR.AT.4, PR.AT.5, PR.IP.11, RS.CO.1	*Risk Management Framework* *Role/Job descriptions* *IAO training*

Ref	Minimum requirement	Control reference	Compliance Metric
	b) ensuring information and systems are protected in line with their importance to the organisation. ***See also:*** - Security Governance Standard - Identity and Access Management Standard - Application Management Standard - National Police Information Security Risk Management Framework		
3.4.	IAO responsibilities should include: a) managing changes to associated information systems b) reviewing information transfer agreements c) agreeing service level agreements (SLAs) d) authorising new or significantly changed business applications, systems and networks e) approving resources to support information security arrangements f) supporting information risk assessment activities g) supporting information security reviews, assessments and audits h) determining and authorising access privileges i) ensuring individuals are aware of their security responsibilities j) ensuring individuals are able to fulfil their security responsibilities ***See also:*** - Security Management Standard	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2, PR.AT.3, PR.AT.4, PR.AT.5, PR.IP.11, RS.CO.1	*Role/Job descriptions* *IAO training* *Performance appraisal reflects IAO activities and objectives*

Ref	Minimum requirement	Control reference	Compliance Metric
	• National Police Information Security Risk Management Framework		
3.5.	A process should be established for: a) providing IAO’s with the necessary skills, tools, resources and authority to fulfil their responsibilities b) assigning responsibilities for protecting information and systems when owners are unavailable c) ensuring ownership is reassigned when IAO’s leave/change roles. ***See also:*** • Security Management Standard • National Police Information Security Risk Management Framework	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2, PR.AT.3, PR.AT.4, PR.AT.5, PR.IP.11, RS.CO.1	
3.6.	Individuals involved in implementing and maintaining systems should be: a) assigned clear responsibilities b) able to administer and use them correctly and deal with normal processing requirements c) competent to deal with error, exception and emergency conditions d) aware of information security principles and associated good practice e) sufficient in number to handle required normal and peak workloads at all times f) supported by documented, up-to-date operating procedures. **See also:** • System Development Standard • Application Management Standard	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2, PR.AT.3, PR.AT.4, PR.AT.5, PR.IP.11, RS.CO.1	

Ref	Minimum requirement	Control reference	Compliance Metric
3.7.	Individuals who maintain systems should be supported by approved methods of: a) administering users (e.g. adding new business users, updating access privileges and revoking user access privileges) b) monitoring key security-related events (e.g. system crashes, unsuccessful login attempts of authorised users and unsuccessful changes to access privileges) c) validating processes/data d) reviewing error/exception reports e) identifying potential security weaknesses/breaches (e.g. as a result of analysing user behaviour or patterns of network traffic). **<u>See also:</u>** - *System Development Standard* - *Application Management Standard* - *Vulnerability Management Standard* - *System Access Standard*	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2, PR.AT.3, PR.AT.4, PR.AT.5, PR.IP.11, RS.CO.1	
3.8.	The risk of individuals disrupting the running of business applications, systems and networks either in error or by malicious intent should be reduced by: a) segregating the duties of individuals a) minimising reliance on key individuals (e.g. ensuring supporting documentation is complete and accurate; and arranging alternative cover, job rotation and deputies for key positions) b) automating aspects of operation (where possible) to reduce the impact of human	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2, PR.AT.3, PR.AT.4, PR.AT.5,	

Ref	Minimum requirement	Control reference	Compliance Metric
	errors with appropriate oversight procedures established to enable human review c) using role-based access control (RBAC), taking care to ensure that users are not granted conflicting rights or privileges d) organising duties in such a way as to minimise the risk of theft, fraud, error and unauthorised changes to information (e.g. by supervising activities, prohibiting lone working and segregating duties). **See also:** - System Development Standard - Application Management Standard - System Access Standard - Identity and Access Management Standard	PR.IP.11, RS.CO.1	
3.9.	The types of activities that require segregation of duty should be defined and include: a) running business applications, systems and networks from the duties of those responsible for designing, developing and testing them b) using business applications and administering databases that support them c) designing, implementing and auditing security controls d) designing, reviewing and operating code and configurations e) access to development, testing and live environments	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2, PR.AT.3, PR.AT.4, PR.AT.5, PR.IP.11, RS.CO.1	

Ref	Minimum requirement	Control reference	Compliance Metric
	f) initiating (or changing) and approving critical or sensitive functions (e.g. payments, pricing and exchange rates) g) requesting, approving and provisioning access rights h) initiating, approving and implementing changes. **See also:** • System Development Standard • Security Management Standard • System Access Standard • Identity and Access Management Standard		
3.10.	The activities of individuals running business applications, systems and networks should be monitored (e.g. by providing supervision, recording activities and maintaining audit trails), particularly where segregation of duties is not practical.	**ISO/IEC 27002:2022:** 5.02, 5.03, 5.04, 5.37 **NIST CSF:** ID.AM.3, ID.AM.6, ID.GV.2, PR.AT.2, PR.AT.3, PR.AT.4, PR.AT.5, PR.IP.11, RS.CO.1	
4.	**Remote Working** Individuals working in remote environments (e.g. in locations other than the organisation's premises) should be subject to authorisation and provided with sufficient technical support to protect endpoint devices and the information they handle against loss, theft and cyber attack, especially when travelling to high-risk countries or regions.		

Ref	Minimum requirement	Control reference	Compliance Metric
4.1.	Documented standards/procedures should cover individuals working in remote environments (including from home) which cover: a. appropriate authorisation to work remotely b. the health and safety aspects of working in remote environments c. associated information security requirements d. physical protection against loss or theft of endpoint devices e. the requirements for individuals travelling to high-threat countries f. connecting securely to the organisation's network g. the right to perform audit and security monitoring h. revocation of authority and access rights, and the return of equipment when the remote working activities are terminated.	**ISO/IEC 27002:2022:** 6.07, 7.09, 7.10, 8.01 **NIST CSF:** PR.AC.3, PR.AT.5 **CIS Controls v8:** 12.7, 13.5	*Overseas Working Guidelines* *Remote Working Policies*
4.2.	Remote environments should be protected by: a) conducting risk assessments to understand vulnerabilities specific to remote working environments b) preventing the processing/storage of policing information on privately owned equipment via remote access solutions. **See also:** • Physical & Environmental security standard • *Overseas Access Guidelines*	**ISO/IEC 27002:2022:** 6.07, 7.09, 7.10, 8.01 **NIST CSF:** PR.AC.3, PR.AT.5 **CIS Controls v8:** 12.7, 13.5	*Overseas Working Guidelines* *Remote Working Policies*
4.3.	Employees working in remote environments should be:	**ISO/IEC 27002:2022:**	*Overseas Working Guidelines*

Ref	Minimum requirement	Control reference	Compliance Metric
	a) authorised to work only in specified locations. Unapproved locations for remote working (e.g. bars, public transportation and open spaces) should be listed. b) equipped with the necessary skills to perform required security tasks (e.g. restricting access, performing backups and encrypting sensitive files) c) notified of any additional risks associated with remote working (e.g. the increased likelihood of equipment theft, accidental disclosure of information) d) provided with adequate technical support (e.g. via a helpdesk, service desk or equivalent) e) in compliance with legal and regulatory requirements (e.g. health and safety laws and data privacy regulations) f) supported to securely store and destroy confidential printed information.	6.07, 7.09, 7.10, 8.01 **NIST CSF:** PR.AC.3, PR.AT.5 **CIS Controls v8:** 12.7, 13.5	*Remote Working Policies*
4.4.	Employees working in remote environments should be provided with: a) suitable secure storage to support remote working activities b) physical cable locks, anti-theft alarms or equivalent security devices for endpoint devices c) security screen filters **<u>See also:</u>** • Physical & Environmental security standard • Information Assurance standard	**ISO/IEC 27002:2022:** 6.07, 7.09, 7.10, 8.01 **NIST CSF:** PR.AC.3, PR.AT.5 **CIS Controls v8:** 12.7, 13.5	*Overseas Working Guidelines* *Remote Working Policies* *Asset Management Policy*

Ref	Minimum requirement	Control reference	Compliance Metric
4.5.	Endpoint devices that access corporate networks from untrusted environments should be configured to: a) establish a Virtual Private Network (VPN) between the device and the corporate network b) prevent access to untrusted networks while the device is connected to the corporate network (i.e. to avoid bypassing the VPN).	**ISO/IEC 27002:2022:** 6.07, 7.09, 7.10, 8.01 **NIST CSF:** PR.AC.3, PR.AT.5 **CIS Controls v8:** 12.7, 13.5	*Remote Working Policies* *Asset Management Policy*
4.6.	Individuals travelling to high-threat countries or regions should protect sensitive information from targeted attack in accordance with the Overseas Working Guidelines. **<u>See also:</u>** • Overseas working guideline	**ISO/IEC 27002:2022:** 6.07, 7.09, 7.10, 8.01 **NIST CSF:** PR.AC.3, PR.AT.5 **CIS Controls v8:** 12.7, 13.5	*Overseas Working Guidelines*
5.	**Security, Education, Training and Awareness (SETA)** Specific activities should be undertaken, such as a security, education, training and awareness (SETA) programme, to promote and embed expected security behaviour in all individuals who have access to the organisation's information and systems.		
5.1.	A security, education, training and awareness (SETA) programme should be established to promote and embed expected security behaviour throughout the organisation and establish a culture of security awareness. Maturity based approaches provide a target set of expected levels of behaviour which can help senior management to monitor and drive performance. **See Appendix 1.**	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme:* *Content* *Behavioural outcomes* *Performance metrics* *Frequency* *Uptake*

Ref	Minimum requirement	Control reference	Compliance Metric
5.2.	The SETA programme should have: a) endorsement at leadership level b) assigned responsibility to an individual, organisational unit, working group or committee c) a documented set of behavioural objectives d) focus on relevant information risks (e.g. new, increasing or high-level risks) e) regular and easily understood units which are tailored for specific functions and levels of the organisation f) appropriate change management disciplines g) up to date practices/requirements h) focus on behavioural change i) effectiveness measured	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme:* *Content – general and tailored packages* *Frequency* *Uptake* Metrics
5.3.	The SETA programme shall be tailored and targeted according to roles / functions and include as a minimum; • Senior Information Risk Owner • Information Asset Owner • Information Security Officer • ICT privileged user • All personnel **See also:** Security Management standard		
5.4.	A behavioural/cultural baseline should be established to identify minimum required security behaviours to include: a) collecting and reviewing evidence of positive security behaviour (e.g. alerts from tools such as Data Leakage Prevention (DLP), results of phishing	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme:* *User surveys* *Security tool outputs*

Ref	Minimum requirement	Control reference	Compliance Metric
	campaigns and feedback from awareness initiatives) b) identifying employees' existing attitude towards information security. A baseline should be conducted annually and following the delivery of a new programme of change. **See** NPSA SECURE tool on npsa.gov.uk		
5.5.	Objectives for the SETA programme should be specific, measurable, achievable, realistic and time-bound (SMART) objectives. Key areas to include are described in **Appendix 1**. The NPSA recommends a "5E's approach to embedding security behaviours": a) *Educating* people on what the security threats are today b) *Enabling* them to demonstrate security savvy actions c) Shaping the *Environment* to support people in being able to demonstrate these behaviours easily d) *Encouraging* people when they do things right e) *Evaluation* how well people are doing. For more information on the NPSA 5Es approach see NPSA.gov.uk	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme:* *Content* *Frequency* *Uptake*
5.6.	SETA programme content should be risk focussed, and include: a) identifying areas of human vulnerability	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:**	*SETA training programme:* *Content* *Frequency*

Ref	Minimum requirement	Control reference	Compliance Metric
	b) aligning to business requirements c) identifying groups of individuals segmented by different risk profiles d) assessing the information risks associated with groups of individuals e) considering types of inappropriate behaviour (e.g. malicious, negligent, accidental).	PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*Uptake*
5.7.	The SETA programme should be designed and delivered by competent professionals with assistance from: a) information security teams b) subject matter experts, including from i. communications and design ii. human resources / learning & development iii. Professional standards	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme: Content*
5.8.	The SETA programme should: a) test current employee awareness and understanding b) provide targeted information security education/training to reflect the needs of the role c) supply security awareness material on an ongoing basis d) use an approach appropriate and meaningful to each group of individuals e) provide tools and techniques to help embed behavioural change e.g. online tutorials, self-evaluation, behavioural insights etc.	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme: Content* *Performance appraisal and objective setting* *Reward & recognition scheme*

Ref	Minimum requirement	Control reference	Compliance Metric
	f) help managers to identify and reward positive security behaviours and recognise self-initiative which reduces risks.		
5.9.	Consider encouraging expected security behaviour by: a) defining expected security-related behaviour. Provide examples such as i. considering risks before acting ii. consulting others for help iii. protecting sensitive / classified information iv. maintaining a clear desk b) incorporating information security into regular day-to-day activities such as i. considering security requirements in planning decisions and budgeting activities ii. including information risk in decisions c) engage personal relevance by linking content to individuals' lives such as i. helping individuals protect their computers at home ii. highlighting how threats can impact individuals as well as the organisation iii. reducing exposure to fraud / cyber enabled crimes	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme: Content*

Ref	Minimum requirement	Control reference	Compliance Metric
	iv. emphasising how individuals can make a difference in managing information risk d) involving individuals in protecting important information e) delivering SETA content in an engaging manner f) reinforcing good security behaviours with acknowledgements or timely feedback. g) Recognise and reward positive security behaviours or self-initiated improvements that reduce risk. h) use approaches that make security awareness easy to understand, accessible, encouraging social engagement and timely.		
5.10.	As part of the SETA programme, employees should: a) have information security updates throughout the year, ideally utilising a range of communication methods b) annually confirm adherence to the information security policy c) be regularly tested on their knowledge of information security, no less than annually.	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme:* *Content* *Frequency* *Attendance*
5.11.	The effectiveness of the SETA programme should be monitored and evaluated by: a) developing and gathering metrics for each SETA initiative b) analysing the effectiveness of SETA initiatives c) reviewing the level of information security awareness on a regular basis (e.g. quarterly)	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme:* *Metrics* *Feedback*

Ref	Minimum requirement	Control reference	Compliance Metric
	d) assessing changes in security awareness and employee behaviour e) reviewing user feedback f) demonstrating business impact (return on investment) Consideration should be given to a maturity based approach to provide a target set of expected levels of behaviour. **See Appendix 1.**		
5.12.	The SETA programme should be evaluated annually to identify: a) the extent to which the objectives of the programme have been met b) opportunities to improve skills and behaviour of individuals c) recommendations for improving the security awareness programme. **See** NPSA SECURE tool on npsa.gov.uk	**ISO/IEC 27002:2022:** 6.03 **NIST CSF:** PR.AT.1, PR.IP.11 **CIS Controls v8:** 14.1, 14.9	*SETA training programme:* *Metrics* *Feedback*
6.	**Security Education/Training themes** **Appendix 1** describes the key messages and target behaviours to achieve a baseline of security culture.		

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.

For external use (outside PDS), this standard should be distributed with information security officers (ISOs) and Information Management teams 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.

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.)

Appendix 1 – Target Security Behaviours

Ref	**Key Target Behaviour**	**Maturity indicators**
Threat & Risk awareness		
1.	a) Is aware of negative activities associated with information including ; • Unauthorised disclosure • Unauthorised access • Interruption / unauthorised destruction • Corruption b) Is aware of the types of threat that wish to exploit or cause harm to policing information; • Hostile foreign states • Serious & Organised criminals including cyber-criminals • Hackers • Investigative journalists • Malicious insiders c) Is aware of the potential harm caused by failures in information security; • threats to life and wellbeing • financial loss (individual or organisation) • legal implications – fines, personal criminal charges • operational • reputational d) Is able to conduct a risk assessment; • Identifies information assets and their potential value or impact if compromised • Identifies potential threats to assets • Selects appropriate controls to protect against threats or reduce impact of compromise • Knows own level of risk responsibility and to whom to escalate to.	**Optimal** Current level of awareness of threats and risks. Able to discuss. Practices in place to actively identify risks and controls in place across all information assets.
		Improved General awareness of threats. Knows where to find latest threat information. Risks identified and some / generic controls in place. Information Asset register in place with IAOs identified.
		Improving Some awareness of threats. Generic risks identified and controls in place. Key / critical information assets identified.

Ref	Key Target Behaviour	Maturity indicators
General security behaviours		
2.	a) Understands the importance of information security in the context of own role b) Knows the leadership commitment to information security c) Understands why information security is needed d) Reads and applies local information security policies e) Knows key roles and responsibilities regarding information security f) Takes personal responsibility for information security g) Consults force / organisation information security roles for advice and guidance h) Applies information security across the lifecycle of the information they handle i) Applies and follows the government security classification scheme and follows handling instructions j) Recognises and reports potential security weaknesses and suspected breaches or near-misses. k) Promptly reports the loss of assets such as notebooks, files, laptops, mobile phones, Airwave handsets etc. l) Recognises and reports suspicious ICT activities such as phishing emails, sharing of passwords, malicious software. m) Knows how to create strong passphrases and keep them secret n) Complies with local physical / building security rules e.g. displaying ID, keeping areas secure, reporting malfunctions / damage. o) Handles information and ICT assets securely when outside of Force / organisational premises. p) Aware that all electronic communications are subject to lawful business monitoring. q) Disposes of information in accordance with local policies e.g. shredding r) Challenges poor behaviours. s) Promotes good security behaviours and suggests improvements to own areas of responsibility.	**Optimal** Incidents / mishaps are rare and low impact. Teams undertake self-checks. Individuals and teams proactively reduce risks. **Improved** Incidents / mishaps are detected and reported promptly. Managers include information security as part of regular team discussions. Few compliance issues identified. **Improving** Incidents / mishaps occur and are often reported. Managers rarely discuss information security with teams. Basic awareness of policies / practices amongst individuals. Frequency compliance issues identified.

Ref	Key Target Behaviour	Maturity indicators
PROHIBITED use of policing assets, systems, services and facilities		
3.	All personnel understand and agree that the following activities are PROHIBITED a) making obscene, discriminatory, harassing or other statements, which may be offensive or illegal b) posting personably identifiable information (PII) about another individual with malicious intent (i.e. doxing) c) downloading illegal content d) opening attachments from unknown or untrusted sources e) copying proprietary material f) interfering with or hiding suspected security vulnerabilities or incidents g) unauthorised use of the organisation's information or systems h) using information and systems for purposes that are not work-related i) using unauthorised information facilities or equipment (e.g. unauthorised external party software, removable media or modems) j) unauthorised copying of information or software k) disclosing sensitive information (e.g. command and control, intelligence, enterprise resource planning (ERP), case management, collaboration platforms or back office) to unauthorised individuals a) using weak / shared passwords/passphrases or disclosing passwords to others b) using personally identifiable information (i.e. information that can be used to identify an individual person) unless explicitly authorised c) moving information or equipment off-site without authorisation l) failing to protect endpoint devices when using them in remote environments (e.g. when travelling or working from home).	**Optimal** No prohibited use occurs. Personnel actively promote correct use.
		Improved Some rare prohibited use occurs. Managers regularly promote correct use. Personnel encouraged to flag where controls appear to hamper operational / delivery ability.
		Improving Prohibited use occurs. Managers follow up and address root causes. Basic awareness amongst personnel.

Ref	Key Target Behaviour	Maturity indicators
Specific areas to consider for targeted security awareness		
4.	**ICT Applications and services** a) Specific enhanced security awareness should be provided to those with privileged logical or physical access rights such as IT administrators, network managers, ICT server / equipment room engineers etc. b) Operational applications and services end users should only be provided access once they have completed training in the use and responsible data handling. This training should be repeated at intervals defined by the Information Asset Owner or System Owner. c) Users of specialist equipment such as forensic examination, body worn video, covert assets shall be subject to training before use in accordance with the requirements of the operational owner. d) All personnel should have access to basic end-users training for business applications and services (backoffice), this should focus on acceptable use and information handling requirements. e) Personnel acting as mobile / remote workers shall receive additional training and awareness to ensure that they apply mobile working security requirements.	**Optimal** Near-misses or data breaches are rare. Systems are maintained and operated efficiently with minimal errors. Information Asset Owners are confident that all users are trained and confident. **Improved** Accidental near-misses are infrequent. Data quality improvements. Losses of assets are rare. **Improving** Near-misses and data breaches occur. Information handling errors are frequent. Assets lost or unaccounted for.

Ref	Key Target Behaviour	Maturity indicators
5.	**Information Handling** Education/training given to business users should include guidance on how to protect information, and cover: a) Information Asset Registers (IARs) and Information Asset Owners. b) Data retention and disclosure rules such as Management of Police Information, the Freedom of Information and the Data Protection Acts. c) The information lifecycle and security requirements across each stage. d) Creating and protecting digital files using the appropriate tools. e) Classifying and labelling information using the Government Classification Scheme (GCS.) f) Information storage / filing requirements. g) Removing unnecessary metadata from electronic documents. h) Information sharing using approved secure methods according to classification and recipients. i) Ensuring that only the minimum necessary information is shared. j) Only using approved information exchange methods such as file sharing, cloud storage etc. k) Mobile / remote working. l) Identifying and reporting potential or actual information breaches. m) Deleting / disposing unwanted information once no longer required. n) Local archiving requirements. **See also:** Information management standard	**Optimal** Data breaches do not occur. Handling processes are proactively monitored and improved by personnel.
		Improved Data breaches are rare. Near misses are reported quickly and root cause identified.
		Improving Data breaches and mis-sharing of information frequently occur. Oversharing of information is the norm. Limited self-reporting – most issues are detected by monitoring or victim reporting.

Ref	Key Target Behaviour	Maturity indicators
6.	**ICT system / application / service development** Education/training should be given to provide IT and system development specialists with the knowledge and skills they need to: a) implement solutions following the Secure By Design methodology such as described in the NCSP System Development standard. b) design systems and develop security controls in a disciplined manner (e.g. using an approved system development lifecycle (SDLC).) c) implement information security controls and security technology in accordance with local and national requirements. d) configure and maintain systems, storage systems and networks correctly, throughout the complete information lifecycle (including backup, archive and restoration.) e) write and review secure application source code. f) design user interfaces and workflows to support expected security behaviour (e.g. making secure configurations a default, and requiring access privileges to be assigned individually rather than in groups.) g) maintain required security controls effectively (e.g. preventing unauthorised or incorrect updates). **<u>See also:</u>** System development, system management, application management and technical security management standards	**Optimal** Information security requirements are considered from the outset and controls are validated at key project stages and before delivery. Risks above appetite are remediated before delivery.
		Improved Information security expertise is engaged during key stages. Some vulnerabilities / issues are identified at or after delivery. These are recorded as risks and escalated to the SIRO. In-service incidents are rare.
		Improving Systems or applications are introduced with poor security controls. Sensitive / classified information is exposed to unauthorised access or disclosure.

Ref	Key Target Behaviour	Maturity indicators
7.	**Use of social media services and applications** Education/training should cover practical recommendations about safe and secure use of social networking, which includes: a) Adhering to the organisation's policy on social networking. b) Understanding the terms and conditions when signing up to social networking websites. c) Awareness of threats and risks associated with social media services and applications. d) Withholding the elements of the user's personal life that don't need to be made public. e) Taking control of personal information (e.g. by resisting the urge to make a blog entry when tired or upset and avoiding publication of work-related information on websites) f) Being sceptical (e.g. questioning or doubting unusual messages to help detect social engineering attacks). g) Avoiding platforms described as high risk, e.g. Tik Tok.	
8.	**Video conferencing** a) Use the right service for the classification being discussed. b) Validate attendees before conducting sensitive or classified meetings. c) Be aware of the environment when joining calls with the camera on. d) Use headphones to protect the privacy of the meeting. e) Warn attendees before recording meetings.	

Ref	Key Target Behaviour	Maturity indicators
9.	**Building and Office security practices** a) Clear or cover whiteboards, including electronic versions, or any other type of display when no longer needed. b) Lock away sensitive media and sensitive / classified documentation when not in use (i.e. complying with a clear desk policy) using appropriate lockable containers. c) Collect sensitive printed material from printer output trays in a timely manner. d) Ensure that material marked for destruction is secured until destroyed / collected for destruction. e) Ensure that secure areas are kept secure, e.g. code locked doors are kept shut, access codes are kept private etc. f) Log off or lock systems when leaving an endpoint device unattended (e.g. during a meeting, lunch break or overnight) g) Ensure that visitors are escorted and that sensitive assets or information is not visible to them. h) Ensure all sensitive information is securely stored before leaving a location (e.g. meeting room). i) Conduct end of shift / day checks to ensure facilities are clear of sensitive / classified assets and are locked. j) Reporting weaknesses or failed physical / office security measures. **<u>See also</u>** Physical and Environmental security management standard.	

People Security Management
Standard

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	Cyber PDS	Initial version	15/03/24
0.2	Cyber PDS	Internal peer review	19/03/24

Approvals

Version	Name	Role	Date
1.0	NCPSB	National Cyber Policy & Standards Board	23/05/24

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
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
Vetting Requirements for Policing	V1.0	10/23
College of Policing Authorised Professional Practice – Vetting APP on Vetting	2021	08/23
NPSA 5Es of embedding security culture	Web page	01/22