Security Framework Policy (Surrey and Sussex) (1192/2025)

Abstract

This policy and procedure outline the Forces' approach to protective security including physical, personnel and information security.

Policy

1. Introduction

1.1 This policy and procedure outline the Surrey Police and Sussex Polices' (hereafter referred to as the Forces) approach to protective security.

2. Scope

2.1 This policy and procedure covers protective security, including physical, personnel and information security.

3. Policy Statement

3.1 Protective Security, including physical, personnel and information security, is an essential enabler to making the Forces work better and is vital to maintaining public confidence. Security risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.

3.2 The accompanying procedure details the Forces' approach to control and prevention.

Procedure

1. The Threats

1.1 The Forces are responsible for activities that include the prevention and detection of crime, with substantial resources being engaged in combating serious and organised criminality. As a consequence, the Forces' activities and assets are under threat from those who seek to undermine or disrupt effectiveness in these areas, as well as the threat posed by terrorism, or the consequences of negligence or corruption by staff or others connected with the organisations. Each of these is likely to result in damage to the reputation of the Forces and result in poor operational effectiveness.

1.2 Security is broken down into three main business areas:

Physical – the security of our buildings, estate, vehicles and equipment

Personnel – the vetting, identification and ongoing suitability of staff, delivery partners and visitors

Information – the security and protection of all information including IT systems and services, paper based records, storage, transport, access and disposal

And each of these areas is underpinned by processes defining how the Forces' activities, roles and documentation are used to mitigate risks.

2. Objectives

2.1 To set out a broad security agenda to reduce risks and protect the organisations staff, assets and the interests of those connected with the Forces including victims, witnesses and offenders.

2.2 To underpin the need for a combination of protective measures to be embraced within everyday activity by the engagement of all staff to ensure that security issues are identified and receive necessary, appropriate, proportionate and timely attention.

2.3 To define the key principles of security risk management, and the roles and responsibilities of the managers and teams involved.

2.4 This framework is the source document for a range of security related material and will be accompanied by specific procedures and guidance that set out the security standards to be adopted throughout both Forces.

3. Scope

3.1 These security requirements will apply to all officers, Special Constables (SCs), police staff, volunteers and any other individual or organisation that is granted access to our premises, information, or equipment.

4. Key Guiding Principles

4.1 All officers, SCs, police staff, volunteers and contractors must take personal responsibility for security and be prepared to identify, challenge, and report security breaches and non-compliance.

4.2 Operational Commands and individual departments, via their Senior Leadership Teams, must identify and manage their security risks within the parameters set out within this strategy and its associated policies and guidance.

4.3 Information assets must be safely and securely stored, processed, transmitted and disposed of whether managed within the Forces or by delivery partners and third party suppliers.

4.4 Only staff (and contractors) in whom the Forces' can have confidence and whose identities are assured will be employed.

4.5 The Forces' operations and business must have resilience in the face of major disruptive events, with plans in place to minimise damage and rapidly recover capability.

5. National Standards

5.1 In setting the standards the Forces will, as far as is reasonably practicable, to comply with recognised national guidance with relevance to the Police service, including

• His Majesty's Government (HMG) Security Policy framework

• National Police Chiefs' Council (NPCC) Community Security Policy

• Government Security Classification scheme

• NPCC National Vetting Standards

• UK Data Protection Legislation

• College of Policing Code of Practice for the Management of Information

• NPCC Corruption Prevention Strategy

6. Governance

6.1 All Security and Information Assurance matters are overseen by the Security and Information Management Board (SIMB) under the Chair of the Force Senior Information Risk Officer (SIRO), the Chief Operating Officer.

7. Roles and Responsibilities

7.1 Senior Information Risk Officer (SIRO)

Responsibility for understanding how the strategic aims of the Forces, may be affected by failures in the secure use of the organisations' information assets. The SIRO has ultimate responsibility for deciding the proportionality of security measures against vulnerabilities to mitigate risk.

7.2 Chief Security Officer

Responsible for co-ordinating all aspects of security and providing advice required to necessitate the established information security and physical security standards necessary to safeguard the Forces' assets. Additionally responsible for the investigation of security incidents and providing security advice and guidance throughout the Forces'.

7.3 Security and Information Assurance Advisor

Ensures information systems and architecture meets legislative, statutory and mandatory requirements. Provide security assurance expertise and ensure effective liaison and co-ordination of information security matters throughout the life of an information asset.

7.4 Security and Information Assurance Co-ordinators

Responsible for conducting physical security reviews of police owned and police occupied premises and for tracking and monitoring security incident trends.

7.5 Information Governance Teams

Under the direction and guidance of each Force's Data Protection Officer (DPO), Information Governance Teams will identify and introduce better ways to record and manage information, influencing what to record, improving data quality, reducing bureaucracy and risks.

7.6 Information Asset Owners

Their role is to understand the information management processes within their area of responsibility, what information is added and what is removed or destroyed, how information is moved / archived and who has access and why. Through this understanding, with advice from the Information Management and Security and Information Assurance teams, they will provide assurance to the SIRO that the appropriate security measures are in place to protect their assets and that their staff have the appropriate information assurance training required for their roles. All new information systems should be subject to a Data Protection Impact Assessment to ensure risks are identified and mitigated.

7.7 Joint Force Vetting Manager (JFVM)

The JFVM is the delegated authority of the Chief Officers to grant, decline or withdraw vetting clearances. They must deliver the expectations set out in the College of Policing Vetting Code of Practice and comply with the standards set out in the Authorised Professional Practice for Vetting.

7.8 Data Protection Officers (DPO)

Responsible for ensuring Forces' use of data is compliant with legislation, providing information and guidance on the processing of all personal data, and handling requests from data subjects in exercising their rights to access data and the rectification of any concerns. The DPO is responsible for breach notification to the Information Commissioner's Office (ICO).

7.9 Head of Procurement

Ensures that suppliers understand their responsibility to provide appropriate protection for contract information and contracted products and services and the implications of failing to do so.

7.10 Service Director Estates and Facilities

Responsible for implementing and maintaining physical security standards in line with policy across all police premises.

7.11 All Managers

Responsible for ensuring processes are followed to protect the physical environment where information is processed or stored. They are also responsible for ensuring that their permanent, temporary staff, and contractors are aware of the information security policies and procedures applicable in their work areas, their personal responsibilities for information security, and how to access advice on information security matters and that all staff know how to report a security breach.

7.12 All Police and Non-Police Personnel working for the Forces'

Adherence to the security standards; taking personal precautions to protect the Forces' assets which they have either possession of or to which they have access.

8. Physical

8.1 Strategic aim: The Forces' assets must be safeguarded against a range of physical threats, including crime, natural hazards, and national security threats.

We will determine an appropriate security posture for the estate and put in place effective and proportionate security controls to reduce the risks to our assets to an acceptable level. This includes ensuring that assets held or managed by delivery partners and third party suppliers are properly protected.

8.2 Business Lead: Security and Information Assurance Team in conjunction with the Estates and Facilities Team.

8.3 Physical security involves the proper layout and design of facilities and the use of measures to delay and prevent unauthorised access to the Forces' assets. The creation of appropriate standards will be the responsibility of the Chief Security Officer who will ensure policies and guidance are in place to cover;

• Physical security protection for all police and shared premises, storage facilities (including cloud storage) and cabling infrastructure.

• Protection of information (including cloud-hosted), equipment, storage devices and media away from police premises.

• Secure disposal and/or re-use of equipment.

9. Personnel

9.1 Strategic aim: To build a trust environment where staff and visitors feel secure and confident. This should include corporate photo identification displayed at all times whilst on Police premises and a timely process for validating staff access to buildings and systems. Such security should not increase bureaucracy but should promote opportunities for the adoption of role-based privileges to cover both premises access and systems access.

9.2 Business Lead: Security and Information Assurance Team in conjunction with the Estates and Facilities Team and Professional Standards Department.

9.3 It is vital that the Forces have confidence in the identity and integrity of its staff and visitors to ensure only appropriate personnel can gain access to assets. It is also important that personnel are aware of their individual responsibilities in relation to security. Ongoing security awareness is essential for all staff, not just on appointment but throughout their service.

9.4 The Joint Force Vetting Manager will ensure policies and guidance are in place to cover:

Verification of identity of police officers, police staff, volunteers and contractors on appointment

Appropriate vetting for all personnel based upon their role within the Forces’

An aftercare regime to ensure continued suitability

9.5 The Chief Security Officer will ensure policies and guidance are in place to cover:

Ongoing security awareness training and communications for police officers and police staff

Corporate identification of police officers, police staff, volunteers and contractors whilst on premises

Role based access to premises and information systems

Secure audit and disposal of uniforms, equipment, and identity badges

Mechanisms to allow for the independent and anonymous reporting of security incidents

10. Information

10.1 Strategic aim: To ensure information owned and managed by the Forces is held securely, appropriately accessed and used as necessary for the policing purpose for which it was created.

10.2 Business Lead: Security and Information Assurance Team in conjunction with the Digital, Data and Technology Division.

10.3 The use of the Forces' information, either electronic or on paper, must meet public expectations with regard to confidentiality and comply with the UK Data Protection Legislation. Information should be handled so as to preserve the integrity of core Police business whilst maintaining availability for operational purposes; and this must happen throughout the delivery chain.

10.4 The Chief Security Officer will ensure policies and guidance are in place to cover:

Security classification and protective control of information assets

Assurance of all business systems that handle, store and process the Forces' information

A range of technical controls for IT systems proportionate to the value, importance and sensitivity of the information held e.g. patching, boundary protection, protective monitoring, lockdown to restrict unnecessary services, and user and privileged account management.

A range of procedural controls for handling information to prevent unauthorised access, modification, or misuse e.g. authentication controls, transferring information protocols, mobile and remote working procedures, clear processes for reporting, managing and resolving security breaches

Assessment of any security risks associated with outsourcing or commissioning of delivery partners or third party suppliers to manage our information or services

10.5 A tested business continuity programme to respond to, investigate and recover from security incidents or other disruptions to core business must be in place.

11. Monitoring

11.1 Compliance Measurement: The following tools will be used to measure the effectiveness of this framework and its associated policies:

The HMG Security Policy Framework

NPCC Community Security Policy, including compliance against the Security Assessment for Policing

11.2 Reports will be produced annually to the relevant governance authority together with exception reports relating to identified best practice, security incidents and national and emerging risks.

It is the role of the Operational Commands and individual departments, via their Senior Leadership Teams, to monitor compliance, identify future risks and any other related security issues within their sphere of responsibility.

11.3 In addition, pro-active security checks and audits will be undertaken by the Security and Information Assurance Team to ensure compliance with the Forces' security and information assurance standards.

12. Critical Success Factors

12.1 Security procedures, guidance and activities which reflect business objectives.

12.2 Consistent approach to implementing, maintaining, monitoring and improving security that meet the Forces requirements.

12.3 Visible support and commitment from all levels of management.

12.4 Security risk management is part of day to day business and is the responsibility of every staff member, including contractors and delivery partners.

12.5 Distribution of guidance on security policies and standards to all managers, officers, SCs, police staff, volunteers and other parties.

12.6 Provision of an ongoing and continuous security awareness, training and education programme.

13. Supporting Policies:

13.1

Surrey Police and Sussex Police Information Security Policy (722)

Joint Force Vetting Policy (Surrey and Sussex) (592)

Data Protection Policy (Surrey and Sussex) (780)

Data Protection Breach Policy (Surrey and Sussex) (1180)

Identification Passes and Access to Police Premises Policy (Surrey and Sussex) (1135)

Physical Security Standards Policy (Surrey and Sussex) (1208)

Information Asset Owners Policy (Surrey and Sussex) (1236)

Team: Security and Information Assurance