P133/02
ESSEX POLICE INFORMATION SECURITY POLICY

1. TITLE

The Essex Police (Force) Information Security Policy (FISP).

2. ABOUT THIS POLICY

2.1 Introduction

The Essex Police (Force) Information Security Policy (FISP) commits us to compliance with the ACPO/ACPOS Community Security Policy (CSP). A compliance work project has been formulated and will be overseen by an Information Security Board (ISB) chaired by the Deputy Chief Constable. The FISP for Essex Police is to be supported by other guiding documents to provide a cascading set of detail for distribution to different audiences.

Essex Police is fully committed to recording and processing information securely in accordance with UK governing legislation and Government guidelines.

2.2 Statement of Intent

We will take measures to:

- Adopt all aspects of the ACPO/ACPOS CSP which is aligned to HMG's Manual of Protective Security as well as the British Standard on Information Security Management BS7799.
- Implement and monitor information security policies and practices to control **Confidentiality, Integrity, Availability and Non-Repudiation** of sensitive information received, processed or stored by Essex Police.
- Guard against unauthorised and inappropriate recording and processing of data and against deliberate or accidental loss, destruction or damage.
- Control physical security.
- Audit information and systems use and hold accountable individuals who breach the rules.
- Establish a business continuity plan.
- Continually assess risks to our premises and systems.
- Control access to information.
- Develop Officers, Support Staff and Information Sharing Partner Agencies on Police security systems and procedures.
- Detect and investigate breaches of security when they occur.

Our adoption of the CSP, and associated baseline measures will be documented and monitored through a continual programme of risk assessments, education and training events and systems audits.

In the application of this policy, Essex Police will not discriminate against any person regardless of sex, race, colour, language, religion, political, or other opinion, national or social origin, association with national minority, property, birth or status as defined in Article 14, European Convention on Human Rights (ECHR).

The Force Information Security Officer (ISO) will retain overall responsibility for maintenance of the FISP documentation set and supporting guidelines. The ISO will also fulfil the role of Project Manager and will advise, guide and co-ordinate all aspects of information security management across the Force.

2.3 Introducing the Information Security Issue

Information exists in many forms and can be printed or written on paper, stored electronically, transmitted by post or electronic means, shown on films or spoken in conversation.

For many years police information files, systems and processes have been rigorously managed and monitored both by internal supervision and external inspection. However, much of the focus has been based upon performance review and continued drive for economy, efficiency, effectiveness and quality.

The rapid changes in both electronic service support and delivery presents new and growing threats, vulnerabilities and risks to information systems on an almost daily basis. To remain effective within this new information society, policing services must develop their information systems and processes in order to ensure they are protected from abuse and misuse. This is widely recognised both nationally and internationally, especially so where there is a requirement for high levels of confidence and trust between customers and suppliers. This also applies between forces, criminal justice agencies and crime and disorder partners.

Increasingly the Police Service and other organisations are faced with security threats to its information resources from a wide range of sources, including computer assisted fraud and sabotage as well as the more usual threats of wilful and accidental damage, human error, carelessness and ignorance.

2.4 Information Security Management - Guidance and Certification

To assist in moving information security management forward, in 1995 the British Standards Institution published 'BS7799 A guide to Information Security Management', and amended it in 1999. Other

legislative developments (such as the Data Protection Act 1998, Human Rights Act 1998, Freedom of Information Act 2000, Copyright Designs and Patents Act etc. 1988) and Central Government directives (Manual of Protective Security etc.) have been drawn up to support this important standard. Collectively, their demands create an significant impact on resources (both financial and human) and growing difficulties when trying to balance information sensitivity with the practical sharing of knowledge to deal with policing objectives and priorities including:

- Call Handling and Management.
- Crime Management.
- Traffic Management.
- Public Reassurance and Public Order Maintenance.
- Community Relations and Community Problem Solving.

The Police Service nationally (through ACPO) has identified and responded to these problems by producing the ***ACPO/ACPOS Community Security Policy (CSP).*** This policy requires all forces and their 'community partners' (CPS, PNC, NCS, NCIS, etc.) to work closely together on the practical implementation issues. It requires us to adopt BS7799 and HMG's Manual of Protective Security as a baseline security standard from which we can all demonstrate confidence and trust in the collection, storage, dissemination and exchange of information - *especially as much of it is sensitive and personal* - about police officers, police support staff, criminals, witnesses, victims, suspects, prisoners and volunteers. Stronger protection measures may also be needed for police systems in specialist areas (e.g., intelligence, witness protection, child abuse etc.).

The National Strategy for Police Information Systems (NSPIS) also requires confidence and trust between the police and suppliers to ensure that individual NSPIS applications as well as their interfaces and integrated modules are secure from misuse and abuse. This is also true of other national infrastructure systems and developments – including Police National Network (PNN/PNN2), PNC, HOLMES, Valiant and the Public Safety Radio Network (PSRN - Airwave).

It is vital to recognise that information security is not limited to computing. Information processes typically span large areas of both manual and computerised procedures and activities. Both the ACPO CSP and BS7799 apply to the whole information process. The rules and guidance contained in this FISP are similarly applicable, even where an information process is entirely manual.

2.5 Information Value and Sensitivity

A fundamental aspect of information security is to examine the nature of the information used in the context of its attractiveness as a valuable asset. The concept of protective marking and the principle of need-to-know have existed within Central Government for many years to

indicate the level of sensitivity of information - but these principles are less well practised within the Police Service at local force level.

The Data Protection Act 1998 recognises personal information as sensitive and requires specific controls over its collection and use. Data protection registration and notification of information categories, purposes, sources and disclosures is widely practised by Essex Police yet many of our public and private sector community partners appear not to apply the same level of protection and inspection. The cumulative effect is that our sensitive information is becoming increasingly more attractive (valuable) and under increasing threat of misuse or theft - more so from within our community than outside of it.

There are significant potential benefits to be realised from maintaining an holistic approach to security over the Force's assets, which can be summarised into four categories:

- physical assets (buildings, vehicles, equipment);
- personnel;
- money; and
- information.

In this model, information has no lesser or greater intrinsic worth than other assets. However, compared to many types of business, it must be recognised that much of the Police Service's stock in trade is information of a confidential character, disclosure of which has potential risks to both public safety and the effectiveness of the criminal justice system. Protection of this asset should be appropriate to the risks it carries.

Overview of Strategy, Aims, Objectives and Methods

2.6 Security Strategy

The information security strategy of the Force is to maintain the confidentiality, integrity, availability and non-repudiation of all information and information processes throughout the Force. This will require the Force to comply with the following:

All legal, statutory and contractual requirements relating to all information and information processes.

The British Standard on Information Security Management (BS7799), and HMG Manual of Protective Security, wherever practical.

The ACPO/ACPOS CSP 1999 and all other ACPO guidance and standards for Data Protection.

2.7 Security Objectives

Key objectives and components necessary to protect all information assets and meet the above aims include a number of essential detailed requirements as follows:

- Security policy management direction, commitment and review.
- Security management organisational structures to initiate and control information security work – especially System Security Policies for discrete systems, and the Systems Operating Procedures, together with the work structure for the ISB and ISO.
- Identification of, accountability for and classification of information assets by way of Protective Marking.
- Personnel security and vetting procedures.
- Processes for physical and environmental security of Force premises, vehicles and other workplaces where information may be deployed.
- Management of communications systems.
- Access control procedures and processes.
- Systems development and support structures.
- Business continuity management and planning.
- Processes for compliance with legal, statutory and contractual requirements.

The above requirements are not exhaustive. Further details of each of the above areas are described in BS7799.

2.8 Security Controls

In order to meet the information strategy aims and objectives, a range of technical and non-technical control measures will be assessed and implemented appropriately. The controls will cover sites, buildings, rooms, equipment, people and procedural security. An existing set of baseline measures has already been derived from formal CRAMM risk assessment techniques, coupled with BS7799 review, and covers Force policy and procedure in the following areas:

♦ Identification and Authentication	♦ Software Maintenance Controls
♦ Logical Access Control	♦ User Control
♦ Accounting	♦ Application Input/Output Controls
♦ Audit	♦ Hardcopy Output Controls
♦ Object Re-use	♦ Recovery Option for Hosts
♦ System Testing	♦ Recovery Options for Network Interfaces
♦ Software Integrity	
♦ Protection Against Malicious Software	♦ Recovery Options for Network Services
♦ Software Change Controls	♦ Business Continuity Planning
♦ Software Distribution	♦ Back-up of Data
♦ System Input/Output Controls	♦ Capacity Planning
	♦ Equipment Failure Protection

♦ Network Security Management ♦ Data Confidentiality Over Networks ♦ Network Access Controls ♦ Physical Network Protection ♦ Message Security ♦ Data Integrity over Networks ♦ Operations Controls ♦ System Administration Controls ♦ Application Development Controls ♦ Application Programmer Controls	♦ Power Protection ♦ Site/Building Physical Security ♦ Room/Zone Physical Security ♦ Personnel (vetting, confidentiality & discipline) ♦ Security Education and Training ♦ Security Policy ♦ Security Infrastructure ♦ Incident Handling ♦ Compliance Checks

2.9 Responsibilities

All major Force information systems will be allocated to responsible System Owners – who will be primarily responsible, with the ISO's support, for implementing this policy in respect of information and systems under their control.

Information security is a shared responsibility. However, Heads of Department / Division have a personal accountability and responsibility to oversee the implementation of the FISP in respect of information holdings and systems under their control and/or used by their staff.

2.10 Training and Development

All staff are developed in use of information and information systems and, where necessary, assessed for competence of use before being allowed access. Development will be commensurate with an individual's functional role and access needed to do their job.

2.11 Security Incident Reporting/Management

As defined in the original CSP, a security incident is any suspected failure in information security, namely:

- accidental or deliberate unauthorised destruction of information;
- accidental or deliberate unauthorised modification of information;
- accidental or deliberate unauthorised disclosure of information;
- deliberate and unauthorised unavailability of the system;
- unauthorised access to the system;
- misuse of data;
- theft of assets;
- any other event which affects data security.

All managers as well as staff allocated a security role are required to undertake the monitoring, reporting and resolution of security related

incidents. Serious information security breaches (including those involving more sensitive levels of information, deliberate unauthorised actions or where policies/practices need to be amended) will be reported to the ISB, via the ISO. Where necessary the matter will also be forwarded to the Professional Standards Department for the appropriate action and potentially formal criminal investigation.

2.12 Audit of System/Data Use

Policy is to adopt a cyclical programme of system security audits, managed by the ISO and aligned to Data Protection reviews and where appropriate Force/HMIC inspections. Outcomes of audits must be reported to the ISB. Specific audits outside the normal programme may also be required where a security breach is identified or where a significant change in system/service provision or use is planned.

2.13 System Developments and Projects

All Heads of Departments and Divisional Commanders responsible for the development of new information systems must, at the time of the development, undertake an information security risk assessment, producing a system security policy and system operating procedures (as required by the CSP). This includes all local projects where information is collected, processed or stored. The outcome must be reported to the ISB via the ISO.

2.14 System Upgrades and Service Pack Releases

All IT systems must be regularly upgraded to the highest level of service pack/release available and operable. This will ensure that security holes in a previous release (version) of a product are patched as soon as possible. The use of upgrades and patches will be fully documented to ensure actions can be reviewed and audited.

2.15 Legislative Changes, Government, Home Office and PITO Directives

Policy is to ensure compliance with all relevant legislation. A list relevant legislation, directives and other guidelines, which are collectively encompassed in the FISP overall, can be accessed from the hyperlink in the electronic version of this 'Policy Guideline'.

2.16 External Network Connections

The Force already has many computer and communication connections with organisations such as DVLA, Magistrates' Courts, Local Councils, Internet etc. The ACPO CSP specifically states that these connections must be risk assessed. It further states that firewalls will be installed at the point of connection to the Force network and that

the firewall product will be certified to level EAL4 under the Common Criteria as approved by CESG.

Our policy is to comply fully with this requirement, although formal certification against the Common Criteria will be through documentary evidence rather than formal CESG testing. Where risk assessments suggest the need specific penetration testing will be considered and the outcome reported to the ISB. Any manager contemplating connecting any system to the outside world must contact the ISO to review the necessary protection strategy prior to action.

2.17 Personnel Security

Policy requires all staff to be vetted to the appropriate level appropriate to the role they perform and the sensitivity of information they have access to. This will be within the bounds of Human Rights legislation and taking into account risks, costs and benefits. Awareness training must continually emphasise a stronger culture of vigilance and challenge to unidentified and unescorted visitors and contractors. Each staff member is responsible for accompanying any visitor in their care until such time as either the visitor is handed over to another staff member or they leave the building. All managers should ensure that the proper vetting of prospective staff and contractors is followed in conjunction with the Personnel & Training Department, Vetting Unit and Special Branch as appropriate. As a general rule where staff or contractors will be deployed in a continually supervised capacity, a basic PNC and Local Intelligence check will suffice. Where there is regular unsupervised deployment then a higher level of checking must be considered.

2.18 Inventory Management

Policy is to ensure that all information assets are identified and valued and recorded on a central inventory. Those allocated a security role will be expected to support on this matter and to work closely with the ISO to establish a Force wide inventory of information assets.

2.19 Virus Control and Checking

A significant risk to computerised information systems is from malicious software (e.g., viruses). This policy requires that all relevant systems be protected from malicious software through use of the most up-to-date anti-virus tools. Virus checking databases must be updated regularly and checking should be automated on file access (wherever practical) so that checking occurs on file access.

2.20 Criminal Justice Process

Processing information through the criminal justice system is complex and prone to errors and duplications in producing and tracking files

between the Police, Courts and CPS. Problems are often compounded by weaknesses with the storage and accessibility of manual files and in processing timely and accurate result updates from Court hearings. Force policy is to review, challenge and revise the manual filing and transfer mechanisms between the Force and other Departments and agencies. Wherever possible review and risk assessment of the processes themselves should be undertaken.

2.21 Backup and Recovery

Fundamental controls for computer systems must include backup and recovery. Arrangements can range for simple daily file copies to full-scale disaster recovery services. Specific requirements for each system must be determined following risk assessment and audit of information value, sensitivity and criticality of availability to the wider business processes. Force policy requires that a disaster recovery plan for centrally managed systems will be formulated and maintained by named system owners in conjunction with appropriate representatives of the IT Department or IT contractor. The Head of IT will maintain a disaster recovery plan for the computer rooms and Force network.

2.22 Intelligence Information

The categorisation of intelligence information across the Police Service has recently undergone a substantial change, from a current 4 x 4 grading to a new 5 x 5 x 5 grading structure. Full details are contained within separate ACPO guidance, which includes specific sections on IT systems, including security. Outcomes of criminal intelligence, as well as other, data audits should be fed via the ISO to consider whether this FISP needs to be updated and to ensure that appropriate security controls are assessed and implemented.

Our policy focus is therefore to use the above and also the BS7799 checklist to assess risk and monitor our current position and to indicate to us the gap to formal compliance.

2.23 Implementation

To assist staff with the local implementation of the FISP the following appendices are provided by way of hyperlink from the electronic version of this 'Policy Guideline':

APPENDIX A the latest version of the ACPO Community Security Policy.

APPENDIX B a high level summary of the British Standards Institute (BSI) BS7799 Information Security Management controls recommended as baseline measures by the ACPO CSP. BS7799 controls have been derived through many years of

work by a group of public and private organisations. These must be applied where relevant.

APPENDIX C System Owner – Definition of role, for those who will be responsible for ensuring the use and functionality of a particular information system or facility is continuously aligned with business and legislative requirements. (Current list of systems and owners included).

APPENDIX D lists a range of legislation, directives and other guidelines, which are collectively encompassed within the overall FISP.

APPENDIX E provides an initial overall allocation of security roles, responsibilities and accountabilities. These may change as the project progresses move forward.

APPENDIX F a list of essential DO and DON'T actions for distribution to all staff and users of IT systems.

3. CERTIFICATION OF HUMAN RIGHTS COMPLIANCE

This policy has been drafted in accordance with the principle of Human Rights legislation.

4. DISCLOSURE STATEMENT

This policy is suitable for public disclosure.

5. GUIDANCE/PROCEDURES/TACTICS

Not applicable.

6. HUMAN RIGHTS CONSIDERATIONS

This policy deals with Information Security and, as such, may engage the following Articles of the Human Rights Act 1998:

- Article 8 Right to respect for private and family life.
- Article 10Freedom of expression.
- Article 11Freedom of assembly and association.

6.1 Legal Basis

The legal basis for the actions directed within this policy can be accessed from the hyperlink in the electronic version of this 'Policy Guideline'.

6.2 Legitimate Aim

The legitimate aims in respect of this policy, for the potential interference with an individual's rights have been identified and considered necessary for the following reasons:

- Articles 8 and 11: In the interests of national security, public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others.
- Article 10: In the interests of national security, public safety, for the prevention of disorder or crime, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

6.3 Proportionality

When applying this policy you must consider a fair balance between the protection of individual rights and the interests of the community at large. You must be able to demonstrate that the actions taken were proportionate to the threat or problem that you are seeking to prevent.

Key questions you must ask yourself are:

- Is the intended action arbitrary or unfair?
- Is the intended action limited to what is required to achieve the aim (of information security)?
- Is the intended action necessary in a democratic society?
- Does the intended action balance the rights of the individual against those of society in general?

6.4 Decision Making and Recording

You must be aware of the need to follow a clearly defined decision making process in considering all information and deciding on your course of action. You should refer to the aide memoire 'Stop, Think and Record'. This will guide you in applying this policy in compliance with the Human Rights Act. If you do not have a copy, contact your Divisional Administration Manager.

It is not enough to apply a decision making process when implementing a policy. The process must be recorded. When decisions are made which may impact on an individual's rights, the decision may subsequently be examined in detail to discover whether it was one which was reasonable in the circumstances.

You must document the outcomes of your actions. Include what options you considered, why you chose to take the action you did. You must be able to justify your actions and show they were proportionate in seeking to achieve the aim (i.e., they must be the least intrusive and damaging option).

E.g., in the event of an applicant for a post in Essex Police is excluded through the vetting process, a record must be made recording the decision and the relevant decision making factor.

This 'Policy Guideline' (P133/02) will be included as a new paragraph 32 (page 120) in Section 7 of the hard copy version of the General Policy & Guidelines Manual which should be cross-referenced accordingly. The Intranet version of the General Policy & Guidelines Manual will be updated in due course.