POLICY

Title: INFORMATION SECURITY AND INFORMATION SECURITY MANAGEMENT

Policy owners	Head of Information Security (Suffolk) and Head of Professional Standards (Norfolk)
Policy holder	Information Security Manager (Suffolk) and Information Security and Vetting Manager (Norfolk)
Author	Information Security Manager (Suffolk)

Policy No.	152

Approved by

Legal Services	√
Policy owner	√

Publication date	30.03.12.
Review date	30.03.14.

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

Legal Basis

(Please list below the relevant legislation which is the legal basis for this policy). You must update this list with changes in legislation that are relevant to this policy and hyperlink directly to the legislation.

Legislation specific to the subject of this policy document

Act (title and year)
Data Protection Act 1998
Computer Misuse Act 1990
RIPA 2000
Human Rights Act 1998
Freedom of Information Act 2000
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Copyright, Designs and Patents Act 1988
Obscene Publications Act 1959
Telecommunications Act 1984 (computer transmission of obscene or indecent images via public telecommunications system)
Protection of Children Act 1978 (re possession/distribution of indecent photos of children)
Criminal Justice Act 1988 (re possession/distribution of indecent photos of children)
Official Secrets Act 1989

Other related Documents:

ACPO Community Security Policy	Information Technology Standard 17799:2005
ACPO Vetting Policy	ISO 27001 – Information Security Management
MOPI	Home Office Police Buildings Design Guide
Cabinet Office HMG Security Policy Framework	Home Office Custody Design Guide
HMG Infosec Standards	Secured by Design and Standards LPS1175 and BSPAS24
CESG Memorandum (Passwords)	Anti-Virus Incident Response
Clear Desk and Screen Policy	Electronic Information Security Policy
Government Protective Marking Scheme Policy	Information Security and Management Policy
Management and Reporting of Security Incidents Policy	Physical and Personal Security Policy
Secure Management of Confidential Information Systems Policy	Email, Internet and Intranet Use Policy
Data Protection Policy	UNIRAS Policy

NORFOLK	SUFFOLK
INFORMATION SECURITY SINGLE POINT OF CONTACT	
Jim McIntyre MCINTYREJR@NORFOLK.PNN.POLICE.UK 01953 425699 Ext 2809	Lee Scott LEE.SCOTT@SUFFOLK.PNN.POLICE.UK 01473 613815
ICT SINGLE POINT OF CONTACT	
Joint ICT Service Desk ICTSERVICEDESK@NORFOLK.PNN.POLICE.UK 01953 424747 (1)	

1 Purpose of this Policy and Associated Policies

1.1 The purpose of the Information Security Policy (ISP) and its associated policies is to ensure that:

- the Constabularies seek to, and does, maintain a high security standard;
- staff read and understand the parts of the ISP relevant to them and are aware of their personal responsibilities and that managers read and understand the ISP to ensure the correct application of security procedures in their responsibility areas, and annually review this against the ISP (see section 6);
- the Constabularies have in place an appropriate Information Security policy with a suitable supporting rationale, strategy and management structure;
- information and equipment is sufficiently protected from unauthorised access, disclosure, modification, loss or damage (accidental or deliberate);
- information is accurate and reliable;
- secure information sharing is facilitated with our partners;
- potential risks are identified, assessed, recorded and managed;
- audit records are created and maintained;
- security incidents are recorded and lessons learned;

- sufficient and adequate safeguards/countermeasures are in place as outlined in the above to ensure the availability, integrity and confidentiality of assets;
- all information security breaches are identified and addressed;
- appropriate protection is in place to protect staff, premises, information and other assets from harm;
- the Constabularies supply third parties (e.g. Council Workers, Volunteers, staff from other Police Forces, Contractors, etc) accessing Constabulary information with the ISP and the relevant associated policies and uphold Constabularies security standards;
- Information Security staff are in place to implement the above.

1.2 For additional information, refer to the HMG Security Policy Framework (SPF), ACPO CSP, other relevant Policy/Procedure and Government standards.

2 Introduction and Rationale

2.1 The Constabularies have become more dependent upon the use of information systems for the delivery of services as well as strategic and administrative functions. For the continuing successful operation of services and assurance of Confidentiality, Integrity and Availability of information, there is a need for a high standard and consistent approach to information security across the entire organisation.

2.2 The Information Security Policy (ISP) communicates to everyone in the organisations the principle that information is a valuable asset to the Constabularies and that everyone is responsible and accountable for protecting it. This outlines security considerations, requirements, priorities, assumptions and responsibilities. It strikes a compromise between the business requirements and security needs.

2.3 The policy encompasses all electronic and manual information. The lifeblood of the Constabularies is their information – customer data, business records, and sensitive and personal information. If any such information is corrupted, lost or destroyed, whether accidentally or maliciously, then policing services are likely to suffer.

2.4 Information can be protected. For this protection to be complete and to support the operations of the Constabularies, the protections employed must be derived from an analysis of the threats facing the information. This analysis results in requirements for protecting the information that are appropriate for the types of information the Constabularies use, the way in which the information is used and nature of the threats facing the information. These requirements are stated as clearly defined rules of behaviour for using the corporate information resources.

2.5 There are three basic components of information security:

Confidentiality – Ensuring that information is accessible only to those authorised to have access;

Integrity – Safeguarding the accuracy and completeness of information and processing methods;

Availability – Ensuring that authorised users have access to information when required.

2.6 Information Security covers all information and related policies, procedures and processes. Implementing Information Security improves performance by preventing:

Information leakage – Staff must have a 'need to know' and authorisation to access information. This protects staff and improves the likelihood of operational success;

Data corruption – Prevents information systems from processing incorrect/damaged data to allow speedy, accurate decisions with confidence;

Downtime – Maintain system availability and disaster recovery.

2.7 The Information Security Policy describes what information must be protected, who must protect it and how it must be protected. It states requirements for conduct and responsibilities and the consequences for misuse of information resources.

3 Obligation

3.1 The Constabularies accept all obligations in respect of information security and the protection of information in its control by implementing recognised best practices that will achieve a balance between cost and risk.

4 Who and What are Covered by the Policy

4.1 The Policy applies to all information whether recorded voice, written, filmed, photographed, printed, otherwise copied or computer-based, which is owned, held in the custody of or is used by the Constabularies. The Policy also applies to all resources used in creating, processing, transmitting, storing, using or controlling that information.

4.2 The Information Security Policy (ISP) is mandatory and applies to employees of the Constabularies, Police Authorities as well as third parties, partnership agencies and contract employees involved in contracts operated on behalf of the Constabularies.

5 Implementation

5.1 The requirements of the Policy are to be implemented by the whole of the Constabularies. In some cases where formal procedures are required, existing practice will need to be reviewed for adequacy. If a department needs additional explanation of how a policy should be applied to the particular circumstances pertaining to that department, then additional explanatory advice may be published.

5.2 The Policy must remain inviolate and implemented to the same standard in ALL departments unless there are circumstances specifically covered by other approved security policies.

6 Associated Policy Portfolio

6.1 As a minimum, staff should read the following associated policies:

- Information Security Incidents;
- Electronic Information Security;
- Physical and Personal Security;
- Government Protective Marking Scheme;
- Clear Desk and Clear Screen.

6.2 Specialist staff (e.g. ICT, line managers, managers of CONFIDENTIAL information systems) must reference the below to ensure they have read all job role relevant policies. This is especially important for Information Asset/System Owners and Department Heads/Commanders as shared security responsibilities exist. They are personally accountable and chiefly responsible, with the support of Information Security, for implementing the ISP upon information and systems they own and/or are used by their staff. The policies are entitled:

- Secure Information Systems Development, Configuration and Management
- Secure Management of Confidential Information Systems
- Secure Disposal of Digital Storage Media (Electronic Information Security – Appendix C)
- Cryptographic Controls and their Management (Electronic Information Security – Appendix D)
- Network Management (Electronic Information Security – Appendix E)

6.3 Additionally all staff must read the following policies and procedures:

- Data Protection Policy/Procedure
- Email, Internet and Intranet Use Policy
- Disclosure of Information Policy/Procedure

7 Information Security Strategy

7.1 The purpose of the Information Security Strategy is to:

- reduce the risk of security breaches to the Constabularies;
- minimise the impact of security controls on operational activity;
- ensure the security of staff, premises and information;
- ensure security relevant decisions are made at an appropriate level;
- provide practical and suitable solutions to security issues;
- build security into Information Systems before deployment;
- incorporate Information Security into the Constabularies culture.

8 Information Security Management

8.1 A management framework will be established to initiate and control the implementation and ongoing management of information security.

8.2 Quarterly meetings of the Information Management Programme Board (IMPB) ensure appropriate management of the implementation of Information Security.

8.3 Ultimate responsibility for Information Security rests with the IMPB chair or designated deputy, who is also the Senior Information Risk Owner (SIRO). IMPB attendees include Information Communications Technology (ICT), a Commander, Professional Standards and Information Security, with additional attendees (e.g. HR, Procurement) selected based on the content of the agenda.

8.4 IMPB discusses, considers and decides action relating to security issues. The IMPB Chair's secretary accepts security related papers for IMPB consultation and decision and can supply the terms of reference on request.

8.5 The Constabularies have a dedicated Information Security handling security issues. Information Security is the single point of contact (SPoC) for security issues, advice and guidance within the Constabulary.

8.6 As required, Information Security enlists the help of external experts such as NPIA (National Policing Improvement Agency), CESG (Communications Electronics Security Group) and HMIC (Her Majesty's Inspectorate of Constabulary).

9 Roles and Responsibilities (Partly defined by ISO 27001)

9.1 Key responsibilities and duties within the information security infrastructure are identified as the following – further details can be found within the Information Management Strategy.

Role	Responsibilities
IMPB Chair, SIRO	Overall responsibility for Information security
IMPB	Oversees the strategic implementation of security Provides consultation and decision forum as required
Information Security	Oversees practical implementation of Information Security Implements some aspects of security at a practical level Develops and maintain policies and procedures Investigates security breaches Provides advice and guidance as required Accredits Information Systems before operating on the Constabularies networks Audits the Constabulary for CSP compliance

Information Asset Owners & designated deputies All information should be assigned an Information Asset Owner	Overall responsibility for their assigned Information Assets / system/s Development of policy and procedure for the assigned system/s / Information Assets Ensuring Risk Management & Accredited Document Sets (RMADS) compliance Ensuring training of appropriate staff as crypto custodians and the management & security of Cryptographic assets Ensuring staff handling the information are suitably vetted Assigning the information a security classification and labelling as per the GPMS Defining and agreeing who is authorised to access that information Ensuring that equipment and information is only used for the Constabularies business and authorised private purposes Ensuring that information is authentic, correct, complete and auditable Authorising the Review, Retention & Disposal of information and data in accordance with Constabularies, MOPI and any legal requirements.
System Security Managers	Responsible for the systems routine operation and security Ensuring compliance with the System Security Policy (SSP) Audits systems logs for security issues Ensures the management & security of Cryptographic assets
Director of ICT / ICT	Assisting Information Security in fulfilling their responsibilities Ensures the security of the network and information systems Ensuring appropriate staff are trained as crypto custodians Ensuring staff involved with encryption are suitably vetted Ensures the management and security of Cryptographic assets
Crypto-custodian	Ensuring they understand and fulfil their Crypto responsibilities Inform Crypto community of Cryptographic Material compromise Ensuring appropriate staff are trained as crypto custodians Ensuring staff involved with encryption are suitably vetted Ensures the management and security of Cryptographic assets
Force Solicitor	Assisting Information Security in fulfilling their responsibilities Provide assurance / legal advice of digital signature usage
Force Employees	Assist in maintaining the security of information and premises Informing Information Security of any Information Security incidents Must complete a Computer Based Training Modules for Data Protection: Freedom of Information, Information Security and Government Protective Marking Scheme

9.2 Information Security, with ICT assistance, allocates critical information systems to responsible Information Asset Owners.

The basis for deciding which systems are 'Critical' are the Constabularies daily operational reliance on the system and its financial value in the event it is destroyed or compromised. Systems may up and down grade from 'Critical' status as required.

10 Compliance

Internal and External Compliance Review

10.1 Information Security will review CSP compliance based upon an IMPB approved Strategic Information Security Plan. External agencies (e.g. HMIC and NPIA) also review ACPO CSP and other relevant policy or legislation compliance.

Retention of Information

10.2 All information will be reviewed, retained and disposed of as per the ACPO CSP and MOPI COP.

Compliance with the Security Policy

10.3 External and Internal Audit is required to ensure compliance with both the Information Security policy and standards (CSP) and should include audits of all areas within the Constabularies.

10.4 Internal Audit should comment on the existence and implementation of security policies and procedures and highlight where a lack of security measures may pose a material risk to the Constabularies. If an audit concludes that Force Information is or has been at Medium or High risk, the relevant findings will be shared with the SIRO.

Legal Obligations and Data Protection

10.5 The Data Protection Act 1998 requires that appropriate security measures should be taken against unauthorised access, disclosure or destruction of personal data and against accidental loss or destruction of personal data. Constabularies must ensure the Act (and subsequent amendments) has full compliance.

11 Recruitment Screening, Job Descriptions, Confidentiality

11.1 All police officers, police staff, volunteers, partnership agencies and contractors/consultants will require security vetting before accessing the Constabularies premises and/or information. This will be carried out in accordance with the ACPO National Vetting and Force Vetting Policy.

11.2 Job descriptions will include clear definition of any Information Security roles and responsibilities.

11.3 All staff will be required to sign the Official Secrets Act at recruitment.

12 Information as a Shared Resource

12.1 The Constabularies will ensure information is accurate, reliable and up-to-date, and available to any other police Force as specified in the MOPI COP (Code of Practice) requiring information for police purposes provided that the Chief Officer responsible for the record is satisfied that the police Force seeking access to the information applies the principles set out in the MOPI COP.

12.2 The Force has in place appropriate protocols for sharing information.

12.3 Special procedures will be applied to a request for access to information recorded for police purposes, in particular, where it is necessary to protect the source of sensitive information or the procedures used to obtain it.

12.4 Managers must ensure that information exchange with external organisations (whether Local Authorities, Healthcare, Central

Government or commercial) does not compromise the confidentiality of sensitive information; nor does it increase the risk of data corruption.

12.5 The exchange of information between external organisations and the Constabulary must take place within formal Information Sharing Agreements (ISAs), which reflect MOPI, Data Protection and legal requirements for the sharing of information. Information Sharing Agreements will be based on:

- duty to share information lawfully;
- the right information for the right person at the right time;
- protection of sensitive information and sources; and
- obligations of those receiving Information.

13 Working with External Systems, Agencies, Organisations, Suppliers and Contractors

External Suppliers and Contractors – risks and conditions

13.1 Suppliers of services to the Constabularies must guarantee compliance with the Force Information Security Policy and a formal agreement confirming the guarantee must be signed between the Constabularies and the third party.

A COPY OF ANY SUCH AGREEMENT IS TO BE FORWARDED TO INFORMATION SECURITY

13.2 Where externally supplied goods or services are used to process Constabulary information, documentary evidence of the supplier's security control procedures to a specified and appropriate level may be required e.g. ISO 27001 or BS7799.

13.3 Procedures must be in place to ensure the protection of the Constabularies information assets. These will include equipment security, media handling and virus control.

13.4 Where a third party (contractor, supplier, partnership agency) are required to process personal information on their premises and/or equipment, third parties will be required to sign a Data Processing Agreement and undergo a security assessment and personnel vetting checks.

13.5 Where suppliers of ICT services have access to Constabulary information, they must comply with the ISP and ensure that access control including user ID and password procedures are implemented to at least an equivalent standard as those used by the Constabularies.

13.6 The information asset owner must maintain logs of all such individuals authorised to access Constabularies systems. Where such access is required with a network account, refer to ICT for the appropriate forms and procedure to create the account.

13.7 Third parties must sign a code of connection form before accessing the Constabularies networks. The form and procedures are found in Appendix E: Network Management of the Electronic Information Security Policy.

13.8 Suppliers must have Employer's Liability insurance plus Public Indemnity and Third Party insurance, or provide suitable guarantees to financially protect the Constabularies against losses caused by the conduct of the supplier's own and any subcontracted employees.

13.9 The ownership of title and copyright to any information and software developed for the Constabularies and any authorised partners must be agreed and a copy of any source code lodged with the Constabularies or a suitable third party (such as an escrow agent) if appropriate.

13.10 Contracts with suppliers must clearly state or identify:

- a description of the ICT services to be made available;
- times and dates when the services are to be available;
- contingency arrangements where appropriate;
- responsibilities with respect of adherence to any relevant UK legislation;
- the right of the Constabularies to monitor (and revoke) user activity;
- procedures for handling Constabulary information;
- responsibilities regarding hardware and software installation and maintenance including the use of formal change control procedures;
- the right to audit contractual responsibilities;
- the right to inspect, both physically and electronically, third party sites and equipment used on behalf of the Constabularies;
- measures to ensure the return or verified destruction of information and other assets at the end of the contract;
- any required physical protection measures;
- mechanisms to ensure security measures are followed;
- user training in methods, procedures and security (where appropriate);
- measures to ensure protection against the spread of computer viruses or other such malicious software;
- an authorisation process for user access;
- physical access requirements to IT sites or other office buildings;
- arrangements for reporting and investigating security incidents;
- acceptance and responsibility for any breaches resulting from remote access maintenance.

13.11 An assessment may be required of the quality and integrity of a company's internal controls. The requirement for an assessment will be based on the sensitivity of the contracted role and the information to which contracted employees will have access. The assessment may

include a Police Approved Secure Facility audit conducted on the Contactor's site.

Public Sector Partner Organisations

13.12 Partner organisations such as District Councils, Victim Support etc will formally accept and abide by the Force Information Security Policy or reassurances must be given, and demonstrated, that the partner's security policy is of at least equivalent standard as that of the Constabularies.

13.13 Access controls will be implemented accordingly. Conversely precautions will be implemented by the Constabularies to protect any partner's information or assets, particularly where there are gateway connections between organisations.

14 Policy Approval, Publication and Review

14.1 This policy and its associated policy portfolio is biennially reviewed 'living' portfolio, updated as required, and all such policies are subject to approval by the Chief Constable.

14.2 Information Security will consult about updates upon their implementation and will review the policies periodically to ensure that they continue to meet the requirements of the Constabularies, legislation, ACPO CSP and ISO 27001. (See Appendix B for further information on key legislation and standards.)

14.3 Staff developing policy affecting this policy and any associated policy should inform Information Security, who will check cross-references when updating other policies.

14.4 The policy will be reviewed at least every 2 years or following a serious security incident or in light of any major changes in policy or business processes. Any review of the ISP will be progressed through the Policy Unit to ensure a full consultation and equality impact assessment is conducted.

Appendix A: Glossary

Term	Explanation
CJX	Criminal Justice Extranet – Secure Police domain
CSP	ACPO/ACPOS Community Security Policy
Confidentiality Agreement	A formal agreement drawn up between the associated parties explaining the needs for confidentiality and the penalties of breaching such agreements.
Encryption	The translation of data into a secure code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a private key or password that enables you to decrypt it.
Escrow	An agreement between a software provider, the Constabularies and an agent to ensure that ownership of application source code remains with the Constabularies in the case of the software provider becoming bankrupt.
Firewall	A system designed to prevent unauthorised access to or from a private network. Firewalls are frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
ISDN	Integrated Services Digital Network. An international communications standard for sending voice, video and data over digital telephone lines or normal telephone wires.
MOPI COP	Management of Police Information Code of Practice
Novate	The ability to pass ownership of a contract from one party to another. For example 'novate the contract from Dell and supplier x to the Constabularies and supplier x'.
OI	Office Infrastructure; Norfolk Constabulary Network.
PolWaRP	Police Warning and Reporting Point. NPIA central reporting point for security incidents.

Appendix B: Key Legislation and Standards

B.1 Data Protection Act 1998

B.1.1 See Data Protection FPD.

B.2 Computer Misuse Act 1990

B.2.1 This Act legislates against unauthorised or malicious use of any computer system.

B.2.2 It is the law used to prosecute 'hackers' and those who write and distribute computer viruses deliberately.

B.2.3 It is a criminal offence to access or attempt to access any computer system which you are not authorised to access.

B.2.4 This law protects the organisation against users and members of the public who deliberately cause damage to systems or data.

B.3 Human Rights Act 1998

B.3.1 The Constabularies will comply and abide by the Human Rights Act 1998. This Act implements Article 8(I) of the European Convention on Human Rights, which declares that everyone has a right to respect for their private and family life, their home and correspondence, and that there shall be no interference to that right, apart from exceptional circumstances such as national security, public safety, prevention of disorder or crime, protection of health or morals, and protection of the rights and freedoms of others.

B.4 Regulation of Investigatory Powers Act 2000

B.4.1 Part I of the Regulation of Investigatory Powers Act 2000 (RIP Act) makes it unlawful for employers and others to intercept communications in the course of their transmission on a private telecommunications system unless certain conditions are met. The RIP Act only restricts access to the contents of a communication.

B.4.2 Interception is allowed where:

- the parties to the call, email or other communication have both consented to the interception;
- the interception is of communications taking place in the course of carrying out the Constabularies business and is authorised under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

B.5 Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

B.5.1 The Lawful Business Practice Regulations authorise certain interceptions of telecommunications, which would otherwise be prohibited by section I of the RIP Act 2000. The interception has to be by or with the consent of a person carrying on a business (which includes the activities of government departments, public authorities

and others exercising statutory functions) for purposes relevant to that person's business and using that business's own telecommunication system.

B.5.2 Interceptions are authorised:

- for monitoring or recording communications;
- to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures, or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training);
- in the interests of national security (in which case only certain specified public Officials may make the interceptions);
- to prevent or detect crime;
- to investigate or detect unauthorised use of telecommunication systems;
- to ensure effective system operation;
- monitoring received communications to determine whether they are business or personal communications;
- monitoring communications made to anonymous telephone help lines.

B.6 Copyright, Designs and Patents Act 1988

B.6.1 The Constabularies will ensure that the software, which is being used on its premises and by its employees, is subject to an authorised and appropriate licence agreement.

B.6.2 Any illegal copying of software or other infringement of the licence agreement will be dealt with in an appropriate way by senior management.

B.6.3 Copyright law applies equally to the Internet. The Constabularies general restriction on the downloading of information from the net reinforces these requirements.

B.7 Obscene Publications Act 1959

B.7.1 All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.

B.7.2 A computer disk, including the principal hard disk of the computer, can constitute an obscene article for the purposes of this Act if it contains or embodies matter that meets the test of obscenity. 'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act.

B.8 Telecommunications Act 1984

B.8.1 The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

B.9 Protection of Children Act 1978; Criminal Justice Act 1988

B.9.1 These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under sixteen that are indecent.

B.10 Information Security Management ISO 27001

B.10.1 The International Standard for Information Security Management ISO 27001 provides a well-proven framework to initiate, implement, maintain and document information security within an organisation. The standard is a business-led approach to best practice on information security management.