



SERVICE INFORMATION SYSTEM (SIS)

INFORMATION SECURITY POLICY

SIS NO. : CS/FIN/11 Information Security Policy

SECTION : Finance and Governance

CONTACT MANAGER : Information Manager

DATE OF ORIGIN : December 2008

LAST REVIEWED : N/A

FUTURE REVIEW DATE : December 2010

OTHER REFERENCE DOCUMENTS :

Data Protection Act (1998)

ICT Acceptable Use Policy

Information Management Policy

Information Security Breach Investigation Policy

ISO 27001 Information Security

RISK ASSESSMENT NUMBERS :

POLICY STATEMENT

Cheshire Fire and Rescue Service will protect its information by adopting a range of measures to ensure an appropriate level of protection for information assets from possible threats, whether internal or external, deliberate or accidental. The implementation of this policy is important to maintain the integrity of our information, to meet information access legislation requirements, and to protect our reputation.

This policy must be applied in conjunction with the ICT Acceptable Use Policy, the Information Management Policy, Data Protection Policy and Freedom of Information Policy.

KEY INFORMATION

1. Purpose and Aims of the Policy	3
2. Scope	3
3. Security Requirements	3-4
4. Responsibilities	5
5. Monitoring	6
6. Sanctions	7

SUPPORTING INFORMATION

	Page
• Security considerations	7
a. Physical measures	
b. Technological measures	
• Additional security procedures for Blackberry's	8
• Encryption	
• Protective Marking Scheme	9
• Legislation	
• ISO Information Security	10
• Privacy Impact assessment	11
• Further guidance	12

KEY INFORMATION

1 Purpose and aims of the policy

1.1 The purpose of Information Security is to provide an appropriate level of protection for information assets from possible threats, whether internal or external, deliberate or accidental.

1.2 Cheshire Fire and Rescue Service is dependent on information and its availability. The Service holds and processes data which may be sensitive or be important information in supporting business processes and stakeholder services, in contributing to operational and strategic business decisions, and in conforming to legal and statutory requirements. The Data Protection Act requires information to be protected in line with individuals rights, and in consideration with individuals privacy.

1.3 The Service aims to identify risks to data security, in terms of loss of confidentiality, integrity and availability, (through a data privacy impact assessment conducted by the Information Manager where appropriate) and adopt appropriate measures to protect information from unauthorised or accidental modification, loss, or inappropriate release or use.

1.4 These measures will include a range of procedures and organisational and technological measures, to a level commensurate with the identifiable risks and the information's value to the Service. Details of physical and technological measures are included in the Supporting Information section of this policy.

2 Scope

2.1 The policy applies to all employees and staff including volunteers, contractors and temporary staff. All users of Service information are responsible for the information they use, create, process, access and transfer. All forms of data and information are included in this policy -

- Electronically held data, regardless of storage media and including information on servers and information in transit or on mobile devices;
- Paper based information;
- Information derived from any business process, regardless of the storage or presentation media;
- All Service and operational data; both internally produced or obtained from other bodies

KEY INFORMATION

3 Security requirements

3.1 Security is a requirement under the Data Protection Act, principle seven, and may additionally be contractually required by other organisations, particularly where data sharing operates.

3.2 Corporate actions are taken by ICT to ensure information security from a technology perspective by means of passwords, firewalls and back ups for example. The Information Manager provides guidance and monitoring for processes and standards. More specific guidance is listed in the Supporting Information section of this Policy.

3.3 Information users and Departmental Managers must follow all Corporate policies and guidance, and where necessary, in liaison with ICT and Information Manager, adopt any additional security commensurate with the nature, value and risk to the data. The Departmental Manager must establish this by completing a risk assessment, and where significant amounts of partner data are involved, also seek the advice of the Information Manager as regards a Privacy Impact Assessment.

3.4 The measures implemented must be an appropriate package of technology, process and organisational controls, and ensure the information is protected throughout the life cycle of the information from creation to processing, storage and disposal.

3.5 As a minimum, specific security measures must be applied which ensure that:-

- Information is valued, then the security of the information risk assessed, and appropriate controls implemented
- Unauthorized access is prevented
- Confidentiality is maintained.
- Unauthorised disclosure through deliberate or careless action is prevented.
- Integrity of information is assured by preventing unauthorized modification.
- Information is accessible to authorised users.
- Regulatory and legislative requirements are met.
- Business continuity plans for ensuring information availability are produced, maintained and tested as far as practicable.
- Information security guidance is available for staff.

KEY INFORMATION

- All suspected breaches of information security are reported to the Departmental Manager, Head of ICT and Information Manager and then investigated.
- All agreements relating to information and data sharing protocols must include a section detailing security requirements.

4. Responsibilities

The overarching responsibility for Information Security rests with the Deputy Chief Fire Officer - Corporate Services. Other employees have specific roles to deliver, including -

4.1 Head of ICT

The Head of ICT is responsible for ensuring that ICT:

- Implement appropriate technological measures to ensure the security of data capture, data integrity and data access on the servers and within their span of control.
- Advise and support Departmental Managers to implement any further technological measures for specific departmental systems, particularly in relation to data transfer, data sharing, disposal of equipment, and access to data. This may include encryption, and security of mobile devices.
- Monitor Service systems and report and escalate any potential security breaches.
- Comply to the relevant parts of ISO 27001 in adopting appropriate technological controls and ensuring the security of data.
- Respond to and assist in resolving any information security incidents.

4.2 Information Manager

The Information Manager will:

- Provide relevant guidance and support in implementing relevant organisational controls and processes to ensure information security.
- Monitor any areas of concern, and provide advice and guidance, and report and escalate any potential security breaches.
- Support managers to complete Privacy Impact Assessments where significant quantities of data\information are received or where new systems that will process personal data are implemented.
- Co-ordinate and advise on any data sharing protocols and related information security implications.
- Respond to and assist in resolving any information security incidents.

KEY INFORMATION

4.3 Internal Audit/Audit Quality and Assurance (AQA)

- The Deputy Chief Officer Corporate Services and the Head of Finance and Governance will instigate independent review by Audit into any areas of concern or high risk for data security.

4.4 Departmental Managers

Managers are responsible for:

- Ensuring the overall ethos and culture of security within their remit, including identification of information security risks, physical security, clear desk policy, training and awareness, local procedures, compliance to data sharing protocols, accountability, monitoring and investigating any security issues.
- Ensuring staff accessing data have the relevant skills and tools to ensure security, and that where applicable vetting is completed, and where relevant a confidentiality agreement is signed for key internal staff and for agency staff.
- Identifying and managing departmental information security risks.
- Reporting information security breaches to the Head of ICT and Information Manager.

4.5 Information Representatives

- Information Representatives are responsible for supporting managers and providing local expertise to departmental teams.

4.6 All employees

- All employees are required to comply with the information security guidelines, and procedures, and to play an active role in protecting Service information.
- Employees must not access or process information without authority.
- All employees must report security breaches or exposures coming to their attention to their line Manager. The Manager shall escalate such issues in accordance with this Policy.
- All employees must manage the risks to an acceptable level through the implementation and maintenance of a package of security measures including technology, organisational and process controls. (Support can be obtained from the Information Manager.)

5. Monitoring and review

5.1 Compliance to this policy will be monitored by ICT as part of the regular monitoring of the ICT Acceptable Use Policy, and by the Information Manager as part of monitoring of compliance with information legislation.

5.2 The Head of ICT, the Information Manager and Internal Audit will review this policy as a minimum every 2 years to ensure it remains appropriate for the Service's business needs.

KEY INFORMATION

6. Sanctions

Deliberate breach or circumvention of the principles of this policy, or of the other policies, standards, guidelines or procedures that implement it, may lead to the appropriate disciplinary action being taken.

SUPPORTING INFORMATION

Security considerations

People failing to implement existing technological and procedural controls cause the majority of security breaches. The overall management ethos must recognise this and ensure that security remains a high priority at all times.

In particular the operating environment must be appropriate to maintain security, including the Service premises, buildings and rooms, and externally, to include homes, other premises and data when in transit.

The systems employed (methods and procedures) must be designed to mitigate risks and ensure compliance to requirements.

Training must be provided for personnel who have access to data and information.

Contractual terms must be included for employees handling confidential data, including:

- Random checks and audits
- Adequate documentation and instruction
- Quick dissemination of changes in risks for information.
- Contractual terms and standards for any agency that operates on behalf of Cheshire Fire and Rescue Service as a data processor.

Other possible measures to ensure information security are –

Physical measures

- Access control to sites, installations and buildings
- Identity cards for personnel
- Secure locks on vulnerable areas and equipment, including filing cabinets and desks
- Good housekeeping of files, paper and data media
- Operating a clear desk policy
- Positioning PC screens so visitors can't view details

Technological measures

- The technology employed (hardware, software and telecommunications)
- Technical protection for networks (e.g. firewall), anti-virus software
- Maintenance of adequate backup information
- Password protection on PC's
- Use of adequate passwords, changed regularly.
- Use of network drives, not C drives (hard disks)
- Disposal of hardware and media devices

SUPPORTING INFORMATION

Additional security procedures for Blackberry devices

In order to assist with security specific procedures will be implemented on Blackberry devices.

This procedure will require entry of a password, minimum of 4 characters, in order to access Blackberries.

On first use of the Blackberry a prompt will ask for a new password, then entry of the password twice for confirmation, then the password is set.

After 2 minutes of no activity the Blackberry will lock, and when the Blackberry is placed into it's holder it will lock. It is necessary to enter the correct password to unlock it. After 10 attempts to enter the password the device automatically wipes itself and will have to be returned to ICT to be rebuilt.

Any queries should be directed to the Head of ICT.

Encryption

Data is at a higher level of risk if it is personal, confidential, sensitive or data which has a high value or could be used for crime. If this type of data is taken or sent off site, additional control measures must be applied to reduce the risk of the data being accessed by third parties. For example, additional control measures should be –

1. Any data that is classed as at higher risk for any of the reasons above, must be encrypted if stored on mobile devices (including CD's, memory sticks, USB drives).
2. Backup tapes must be encrypted where this is practical and where an assessment shows that there is a definite risk of access by external or unauthorised parties, who will be able to access the relevant specialist software and hold any relational data base.
3. Emails must be encrypted where higher risk data is sent externally.
4. Blackberries must be password protected.
5. Higher risk data must not be held on laptops or C drives. Where data has to be transported, arrangements to use encryption and USB key tokens must be made .

Support from ICT must be obtained .

SUPPORTING INFORMATION

Protective Marking scheme

Some documents and information need to be given a special level of protection to avoid breaching the confidentiality of victims, accused persons and witnesses and in more exceptional cases, to protect national security. The term document refers to all information formats, i.e. papers, drawings, photographs, disks and electronic data and records.

The Government Protective Marking Scheme is the nationally recognised common baseline for safeguarding information, particularly when it is shared by different organisations.

The scheme defines levels of protection according to the consequences of any compromise of the items. This dictates the steps to be taken to prevent any unauthorised disclosure or loss of the item.

The four levels of protective marking and recommended procedures that the service has adopted are:

1. Not Protectively marked (NPM)

Within the confines of 'need to know' may be freely shared amongst the participating organizations. Where compromised, would not cause undue distress or embarrassment. Anything valued above "NPM" should be treated as 'sensitive' and marked as one of the following levels -

2. Protect

Intermediate valuation between "NPM" and "Restricted". Classed as information that if compromised would undermine management of public sector, cause distress to individuals or breach undertakings on disclosure. May be transmitted over a public network (including by telephone) where impact of compromise is deemed to be outweighed by transmission and sharing advantages.

3. Restricted

Broadly as "Protect" but of a greater personal or corporate impact, requiring stronger controls. Staff handling/seeing the information need to be vetted and, where transmitted over a public network (e.g. dial-up or Internet), requires encryption.

4. Confidential

Impact of compromise would be considerable, including bad publicity, loss of public confidence, influence a criminal justice case or potentially cause undue personal distress or harm to staff or members of the public. May not be transmitted over a public network. Any transmission must be encrypted and separated from normal traffic. Endpoints (rooms, computers and users) must be pre-accredited before allowed access.

SUPPORTING INFORMATION

Each level of protective marking indicates the standard of protection which must be given to the item. The higher the level of protective marking the more extensive are the security measures which should be used to protect the item. One of the most effective ways of preventing the compromise of an item is to ensure that only those with a need to see it or handle it do so.

A protective marking may be supplemented by a descriptor, e.g. Restricted - Investigation. The descriptors serve two functions:

- to show the type of sensitive material which is being protected; and
- to help those handling the information to decide which people should have access to the material.

All employees must follow the appropriate procedures if they receive any item bearing a protective marking. Note that the schemes operation may vary between different organisations, and where a variance occurs it is normal to adopt the higher level of security in that instance. More details can be obtained from the Information Manager.

Relevant Legislation

There is currently no specific legislation relating to information security, but the following legislation has indirect requirements and may lead to penalties and enforcement action in the event of security breaches. Equally significant is the potential reputational damage and loss of partner and public confidence which would result from security issues.

Legislation including but not limited to -

The Data Protection Act 1998;

The Freedom of Information Act 2000, including the Lord Chancellors Code of Practice for Records Management.

Public Interest Disclosure Act 1998;

Defamation Act 1996;

Companies Act 1985;

Computer Misuse Act 1990;

Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992;

Electronic Communications Act 2000; Telecommunications Act 1984; The Regulation of Investigatory Powers Act 2000;

Obscene Publications Act 1959;

Protection of Children Act 1978; Criminal Justice Act 1988;

SUPPORTING INFORMATION

Protection from Harassment Act 1997; Sex Discrimination Act 1975; Race Relations Act 1976;
Human Rights Act 1998.

Privacy Impact Assessment

Projects that involve personal information or intrusive technologies inevitably give rise to privacy concerns. The cumulative effect of many such initiatives during recent decades has resulted in harm to public trust and to the reputations of corporations and government agencies alike.

Where the success of a project or work stream depends on people accepting, adopting and using a new system, process or programme, privacy concerns can be a significant risk factor that threatens the return on the organisation's investment. In order to address this risk, it is advisable to use a risk management technique commonly referred to as a Privacy Impact Assessment (PIA). The Information Manager can advise as to when it is appropriate to use a PIA.

See the Information Commissioners web site, at www.ico.gov.uk.

ISO 27001 Information Security and Audit

Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls comprising policies, practices, procedures, and includes people, processes and technology.

In 2007 Cheshire Fire & Rescue Service signed up to becoming demonstrably aligned to ISO 27001 as a result of our partnership agreement with the other members of the Cheshire Warrington and Halton Information Consortium CWHIC Information Sharing Toolkit, and because this standard is nationally and internationally recognised and seen as best practice.

The ISO standard considers the development of information technology, networks, communications and emphasises business involvement in and responsibility for information security. It includes a code of practice and requirements specification for establishing, implementing and maintaining the security of information management systems. It refers also to the physical environment, policies, processes, people and responsibilities in addition to technological systems.

Assessments against ISO 27001 provide indications of our information security risks and potential requirements. Information from the most recent audit report can be obtained from the Head of ICT, where required.

SUPPORTING INFORMATION

Further Guidance

Further guidance is available internally from the Information Manager and the Head of ICT, and through the information management pages on the intranet and the Information Representatives Group.

Useful web sites include –

Information Commissioner data security tips

http://www.ico.gov.uk/Home/for_organisations/topic_specific_guides/Data%20security%20tips.aspx

Information Commissioner Privacy Impact Assessment

http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/foreword.html

Department for Regulation and Reform

<http://www.berr.gov.uk/sectors/infosec/index.html>

Police Information Management Guidance

<http://www.npia.police.uk/en/8492.htm>

Health Information Management Guidance

<http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Informationsecurity/index.htm>