



South Yorkshire Fire & Rescue

WORKING FOR A SAFER
SOUTH YORKSHIRE

Security Policy

INFORMATION TECHNOLOGY 1
INFORMATION SYSTEMS SECURITY POLICY

<u>SECTION</u>	<u>CONTENTS</u>	<u>PAGE</u>
	Preface	
1	Introduction	1
2	Objectives	1
3	Definitions	1
4	Responsibilities	2
5	General Policy – Statement of Intent	3
6	Network Security Policy	4
7	Physical Security Policy	4
8	Media Security and Backup Policy	5
9	Data Security Policy	5
10	Acceptable Use Policy	6
<u>APPENDIX A</u>	Incident Reporting Incident Report Form	
<u>APPENDIX B</u>	Malicious Software (Virus)	
<u>APPENDIX C</u>	Malicious Software – Do's and Don'ts	
<u>APPENDIX D</u>	Software Code of Conduct	

SOUTH YORKSHIRE FIRE AND RESCUE

BRIGADE ORDERS

INFORMATION TECHNOLOGY 1

INFORMATION SYSTEMS SECURITY POLICY

PREFACE

South Yorkshire Fire and Rescue relies on the Information System resources to handle vast amounts of information. Because the data can vary widely in type and in degree of sensitivity, employees need to be able to exercise flexibility in handling and protecting it.

A formal Information Systems Security Policy helps establish standards for the Information Systems resource protection by assigning management responsibilities and providing basic rules, guidelines and definitions for everyone in the organisation. It will help prevent inconsistencies that can introduce risks, whilst serving as a basis for the enforcement of more detailed rules and procedures.

This Policy document will be accepted and followed throughout the organisation, however, it is flexible enough to accommodate a wide range of data activities and resources and will be reviewed on a regular basis.

INFORMATION TECHNOLOGY 1

INFORMATION SYSTEMS SECURITY POLICY

1. INTRODUCTION

- 1.1 The British Standard BS 7799 on Information Security Management has been used as a basis from which to formulate the Information Security Policy of South Yorkshire Fire and Rescue (SYFR).
- 1.2 The following document mandates the security requirements for any IT system used by SYFR.
- 1.3 A copy of this document can be found on SYFR's Intranet at
http://command-apps3/SYFRS/Web/Site/PoliciesProcedures/Asset_Management/ICT.asp

2. OBJECTIVES

- (i) To ensure that authorised people have efficient access to South Yorkshire Fire and Rescue's Information Resources.
- (ii) To maintain the security, confidentiality and integrity of South Yorkshire Fire and Rescue's Information Resources.
- (iii) To maximise the availability of Information Resources without sacrificing security.
- (iv) Enhance the availability and quality of information to support management and operational decision making.
- (v) To maintain the security and availability of all hardware platforms both network and stand-alone.

3. DEFINITIONS

3.1 Confidential

- (i) Confidential items include matters regarding Personnel Policy, Personnel Files, Employee information and any other item designated as Confidential by the Chief Fire Officer.

3.2 Information Resources

- (i) Hardware: includes computers (network servers workstations, laptops, handheld devices, etc.), storage devices (disk drives, tape drives, optical devices, etc.) input devices (keyboards, scanners, etc.), output devices (monitors, printers, etc.), communications devices (modems, switches routers, etc.), communication lines (cables, phone lines, digital lines, etc.), the component parts of any of these resources, and inventory.
- (ii) Software: includes methods, instruction sets, source programs, applications, utilities, diagnostic programs, operating systems, communication programs and licences.

- (iii) Data: includes information stored in any form, in transit over any media, being executed on any device, and any copies of such information for purposes of backup, auditing, or transport.
- (iv) Users: people who use or manage Information Resources.
- (v) Documentation: description manuals, instructions, or procedures related to Information Resources.
- (vi) Supplies: including paper, forms, labels, ribbons, storage media (disks, tapes, cartridges, paper, etc.), and inventory.
- (vii) Access Tools: including keys, user names, passwords, certificates, and any other tools used to authenticate identity or otherwise indicate permission to use Information Resources.

4. RESPONSIBILITIES

4.1 In order to comply with the policy and the law regarding personal data, software copyright and the use of both personal and network computers, the following shall apply:

4.2 Senior Management and Section Heads

- (i) Declare who has access to what.
- (ii) Ensure that all employees are aware of the Security Policy Document at the time of their orientation.
- (iii) Notify the Information and Communications Technology (ICT) Section in writing of any new employee who needs a network account(s), passwords, or access to other Information Resources.
- (iv) Notify the ICT Section in writing when employee accounts should be terminated.
- (v) Inform the ICT Officer, prior to purchase, installation or use of any Information Resource which the ICT Section is expected to support.

4.3 ICT Support Staff

- (i) Develop SYFR's Security Policy and associated Procedures
- (ii) Monitor the use of Information Resources
- (iii) Update the Security Policy and Procedures as necessary
- (iv) Develop and execute prevention strategies to protect Information Resources from loss, destruction, tampering and unauthorised access, modification or use.
- (v) Develop and execute recovery plans in the event that prevention strategies fail.
- (vi) Maintain the Security Policy during the purchase, implementation and use of new Information Systems and Hardware.
- (vii) Create and remove user accounts at the request of Senior Management and Section Heads.

4.4 Individual Members of Staff

- (i) Each user is responsible for the protection of his/her password and other access tools.
- (ii) Each user is responsible for the backup and security of information not stored on network drives. This includes information stored on hard disk or USB stick.
- (iii) Each user is responsible for reporting security breaches and potential problems to Information Systems. Breaches include, but are not limited to virus infections, lost disks or other storage media, and unauthorised use of the Systems.

5. GENERAL POLICY

5.1 Statement of Intent

South Yorkshire Fire and Rescue has a duty to protect its information assets and thus to ensure business continuity and minimise the adverse effects of security incidents.

The Organisation recognises the need to ensure full compliance with all the relevant legislation including the Data Protection Act 1998, the Computer Misuse Act 1990 and the Copyright Designs and Patents Act 1988.

The Organisation's policy is to ensure that ICT Systems, including computer systems, network components and electronic data, are adequately protected from identified threats. The policy covers all aspects of the environment: systems, administration systems, environmental controls, hardware, software, data and networks. It will apply to all stages of the system lifecycle and is independent of whether the system is developed in-house or purchased externally. It is the responsibility of all Managers to ensure that the policy is observed, by themselves and members of their staff.

Security measures will be reviewed regularly to ensure they remain appropriate.

Any major change to ICT systems or surrounding environment should be accompanied by a review. Security measures should be formally documented, the document being updated whenever significant changes take place.

The Security Policy is applicable to all existing and proposed systems and is effective from the date of issue.

5.2 Summary

South Yorkshire Fire and Rescue shall:

- (i) Implement at least the minimum security requirements as identified in this policy, to protect SYFR's resources and information which is processed, stored or transmitted by any employee of the organisation.
- (ii) Safeguard information against unauthorised disclosure, modification, access, use or destruction.
- (iii) Not connect to any other system or network (which is not under SYFR's authority), unless formally approved by an appropriate Senior Officer.
- (iv) Ensure that all persons who use, manage, operate, maintain, or develop SYFR's applications or data comply with these policies.
- (v) SYFR will put in place a reporting structure to deal with breaches of security and ensure that all such breaches are fully investigated and those responsible dealt with via Disciplinary and/or Criminal proceedings.

6. NETWORK SECURITY

6.1 Policy Statement

South Yorkshire Fire and Rescue recognises the additional security hazards posed by network systems and will endeavour to reduce these threats wherever possible. The policy restricts the transfer of confidential information over unprotected communication links, whether within the organisation's private local area network or via the wide area network.

Sufficient safeguards will be implemented to prevent unauthorised persons from accessing its information resources.

6.2 Summary

South Yorkshire Fire and Rescue shall:

- (i) Develop and observe standards and procedures to maintain an acceptable level of security on all networks.
- (ii) Develop and observe standards and procedures for connecting internal networks to external information resources including the Internet.
- (iii) Ensure that the software security features of the networks it manages are installed and functioning correctly.
- (iv) Monitor network security on a regular basis. Adequate information concerning network traffic and activity will be logged to ensure that breaches in network security can be detected.
- (v) Implement and maintain procedures to protect the network against intrusion and interference.
- (vi) Ensure passwords and other access tools to networks are protected.

7. PHYSICAL SECURITY

7.1 Policy Statement

South Yorkshire Fire and Rescue will observe standards and procedures required to ensure security of the physical premises and computing equipment.

Only authorised personnel will have access to sensitive areas and confidential material should be held in secure cabinets, even within ICT secure areas, and be available only to authorised people.

7.2 Summary

- (i) Ensure Network servers are protected by adequate battery backup and UPS (uninterrupted power supplies).
- (ii) Security for information resources is the responsibility of the group or person to which the resource is assigned.
- (iii) Equipment may be borrowed according to procedure by authorised people to conduct South Yorkshire Fire and Rescue business for pre-set lengths of time.
- (iv) Any equipment borrowed for off-site use must first be signed out. Any equipment removed from the premises which is not properly authorised will be considered stolen.
- (v) Users of computers in open areas must log off from all networks when leaving the computer unattended.
- (vi) Computers should not be left unattended and "logged on" or otherwise available for use by unauthorised persons.

- (vii) The risk of the unauthorised viewing of screens should be minimised by careful planning of office layouts; for example the screen should not be visible through a window or by people entering the Section.
- (viii) For sensitive applications equipment should be located in a secure area which is itself subject to access control.
- (ix) All manuals, books, letters and other material relating to Brigade computers should be treated as confidential and not revealed to unauthorised persons.
- (x) Faulty equipment should be treated with the same level of security as that applicable when it is fully operation.
- (xi) Strict security should be exercised over printouts and access should be denied to unauthorised persons. Careless handling of printouts can easily lead to unauthorised disclosure.

8. MEDIA SECURITY AND POLICY BACKUP

8.1 Policy Statement

South Yorkshire Fire and Rescue is committed to the use of authorised software only within its computer systems. It is expressly forbidden for individuals to load or operate software gained from computer bulletin boards, magazine gifts or any other sources.

It is the personal responsibility of all users to ensure that they do not introduce viruses into computer systems.

Corporate Information Systems will be backed up on a regular basis and this information will be locked securely away in a safe environment, separate to the server/computer which stores the prime copy.

8.2 **Summary:**

South Yorkshire Fire and Rescue shall:

- (i) Develop and observe standards and procedures to ensure security of storage media
- (ii) Develop and implement backup and recovery routines for all Network Server storage media.
- (iii) Ensure users are aware of the procedures for the proper backup and security of all data not stored on a Network. This includes all non Network storage media including disks and local hard drives.
- (iv) Removable disks/tapes must be stored in secure drawers/cabinets when not in use.

9. DATA PROTECTION

9.1 Policy Statement

South Yorkshire Fire and Rescue's policies and procedures are compliant with all of the data protection principles set out in the Data Protection Act insofar as they apply. The Organisation will regularly monitor its policies and procedures for such compliance.

9.2 **Summary**

South Yorkshire Fire and Rescue shall:

- (i) Develop and observe standards and procedures to ensure the security of data.

- (ii) Implement data encryption techniques when confidential information is transmitted.
- (iii) Ensure security precautions are retained when data is moved or copied to another system.
- (iv) Use confidential passwords, which are known only to authorised personnel.

10. ACCEPTABLE USE

10.1 Policy Statement

South Yorkshire Fire and Rescue will make available its information resources to facilitate workflow and communication throughout the Organisation. In so doing, the Organisation shall make regular checks to ascertain the appropriateness of both internal and external communications.

10.2 Summary

South Yorkshire Fire and Rescue shall:

- (i) Forbid all attempts to obtain unauthorised use of any internal or external network or computer.
- (ii) Forbid the use of its network(s) in such a way that it disrupts another user's use of the network(s).
- (iii) Forbid activities which are prohibited under the Data Protection Act 1998.
- (iv) Not tolerate the presence of sexist, pornographic, racist or ageism materials on the Organisation's property.
- (v) Limit the use of its electronic mail system to general office communication. Sensitive data shall be submitted through the normal channels.

Chief Fire Officer

Command Headquarters

Wellington Street

SHEFFIELD

S1 3FG

OPS/Z17/LG

1st July 2007

INCIDENT REPORTING

1. The introduction of a system of incident reporting will enable the ICT Section to maintain a day-to-day overview of any breaches of security, deliberate or accidental, thus enabling resources or counter measure to be targeted effectively.
2. Incident reporting should be encouraged for any breach of security of whatsoever nature, actual or suspected, and such report should be acted upon as described below. It is preferable to have to deal with a number of false alarms than have a problem develop through lack of awareness.
3. The incidents that must be reported are shown below:
 - (i) Breach or suspected breach of passwords;
 - (ii) Interference or suspected interference with the hardware or software;
 - (iii) Unexpected responses from the hardware or software (may indicate the presence of a virus);
 - (iv) Loss of data;
 - (v) Back-up difficulties;
 - (vi) Damage to hardware or storage mediums.
4. A form for incident reporting has been designed (copy attached) and this form should be used for all reports of IT security matters together with any other supporting documentation.
5. The originator of the report must ensure that it is submitted as soon as possible to their line manager, who should ensure that the report is passed, suitably endorsed, to the ICT Officer.
6. Where the report reveals a deliberate breach of security that contravenes the ICT Security Policy or Brigade Orders, an investigation will be instigated as envisaged by the statement of intent contained within the ICT Security Policy.
7. The form endorsed as to what action is needed should then be passed to a member of the ICT Section for their attention.
8. When the appropriate corrective action has been taken the form should be returned to the ICT Officer for filing and retention.
9. South Yorkshire Fire and Rescue has implemented this ICT Security Incident Reporting Scheme to collect evidence of computer abuse and disasters. Based on this scheme, reports will be produced periodically to help target security measures more effectively.

SOUTH YORKSHIRE FIRE AND RESCUE
ICT SECURITY INCIDENT REPORT

This form is to be used to report ANY incident or suspected incident concerned with ICT Security.

Name of person making initial report:

System on which fault occurred:

P.C. Number (if applicable):

Nature of Incident:

.....
.....
.....

(Continue on separate sheet if necessary) Supporting paperwork attached: **YES/NO**

Line Manager/Supervisor's Comments:

.....
.....

TO BE COMPLETED BY THE ICT OFFICER

Action to be taken:

.....
.....

TO BE COMPLETED BY THE ICT SECTION

Final Resolution:

.....

MALICIOUS SOFTWARE (VIRUS)

1. There are many different definitions of the term malicious software. For the purpose of the ICT Security Policy of South Yorkshire Fire and Rescue, the definition that seems most appropriate is:

“Unofficial code, concealed with the intent that it be introduced surreptitiously to ICT Systems”

2. Such code is always concealed in some way, because it acts in ways which the user does not desire, if its purpose or presence was clear, the user would not run it.
3. The purpose is invariably to disrupt normal system operation, or destroy or gain access to computer held data or program files. Malicious software is not always intended to cause damage, sometimes it starts life as a “joke” but whether damage is intended or not, any unauthorised code introduced to a system runs the risk of damaging that system and/or the information it holds and renders the perpetrator liable to prosecution under the Computer Misuse Act 1990.
4. Computer “experts” use many different, often conflicting, methods of categorising malicious software but the general consensus is that there are four main types. It may be helpful to explain each briefly so that the various effects can be more easily understood.

TROJAN HORSE

This term is generally used to describe malignant code hidden in or added to an existing program; usually a utility or a game that causes the program to perform some extra function(s) it was not designed to do. If the programme is attractive to use, for instance a game, then it has a high chance of being copied and transferred onto another system by an unknowing user.

LOGIC BOMB

This refers to malignant code which is activated when certain criteria is met. Once introduced into a system a logic bomb lies dormant until triggered by a pre-defined condition like time/date or the presence or absence of certain data. Famous well documented examples include the Friday the 13th code which was activated by the date and included an instruction to corrupt certain vital files and another when the programmer’s name failed to appear on the company’s payroll the program triggered enormous damage to the system.

VIRUS

This refers to malignant code which attaches itself either to what is known as the “boot Block” of a disk or to an existing program file on the disk. Viruses have the ability to copy themselves to other files, disks or, via the disks, to other computers. The term “virus” is a reflection of the fact that they can “infect” systems in the same way as a flu virus may “infect” humans.

WORM

The worm attack is more usual on multi-user machines or networks it continually replicates itself until it destroys the original. It will reproduce ad infinitum until it has taken all the available disk space or all memory has been used which would, of course, bring the system to a halt.

MACRO VIRUS

This virus is usually hidden within Word documents and is activated once loaded onto the system. To prevent the introduction of a macro virus, no documents obtained from a third party source should be loaded onto a PC unless the disk has been virus checked.

The above list is not exhaustive but does give a feel for the consequences of any sort of virus being introduced to a South Yorkshire Fire and Rescue System.

5. It is essential that NO unauthorised software of any description is applied to a SYFR system without first being approved for use by the ICT Section and checked with the latest anti-virus software.

6. Anti Virus Software

Before any floppy disk that has been used on a P.C. outside SYFR environment is used on a corporate resource **IT MUST BE CHECKED FOR VIRUSES** by submission to the ICT Section or if available by use of anti-virus software on your own desktop.

7. Sources of Malicious Software

The main sources of malicious software introduced to P.C.'s are:

- (i) Free "applications" from magazines
 - (ii) Maintenance engineers diagnostic disks
 - (iii) Salesmen's demonstration disks
 - (iv) Commercial games and utility software, particularly "pirate" copies
 - (v) Public domain (shareware, freeware, etc) games and utilities
8. Despite there being no complete solution there are a number of measures, some very basic, which can help minimise the risk.
 9. All users need to be aware of both the danger posed by malicious software and of the ways in which it may be prevented from affecting "their" system.
 10. The following precautions are necessary, as a minimum, to try and protect South Yorkshire Fire and Rescue systems from a virus attack.
 - (i) Never use other than officially provided software on an officially provided machine unless:
 - (a) You have authority to do so;
 - (b) You are certain it has been checked by anti-virus software;
 - (c) Take regular backups of data;
 - (d) Never let an unauthorised user have access to an officially provided machine;

- (e) Never let anyone other than ICT staff, or a person authorised by them, install new software or amend existing software on your machine;
- (f) Use the incident reporting system to alert the ICT Officer to anything that may indicate the presence of a virus;

MALICIOUS SOFTWARE – DO'S AND DON'T'S

DO	Make sure you are aware, and make others aware, of the dangers of malicious software.
DO	Ensure you stick to established procedures
DO	Report any faults, suspicious or unexpected activity, on the part of the computer or any person using the computer immediately.
DO	Ensure that only officially provided software is loaded onto your computer.
DO	Ensure that any disk from an unofficial source is sent via the ICT Section for virus checking.
DO NOT	Load any software that is from an unofficial source unless you have been authorised to do so.
DO NOT	Attempt to put a problem right, unless you are trained to do so, this could lead to further damage.
DO NOT	Attempt to boot up (start) a PC that has a hard disk, or is connected to a network, from a floppy disk unless authorised to do so.
DO NOT	Allow any unauthorised person to use your machine.
DO NOT	Experiment with the system or attempt to write or modify programs for it unless you are authorised to do so and do not allow anyone else to do so.

SOFTWARE CODE OF CONDUCT

1. All staff must adhere to the following code of conduct to ensure that SYFR is not subjected to legal action for the use of unauthorised/unlicensed software.
 - (i) All software must be procured through the ICT Section.
 - (ii) The ICT Section will be required to maintain a central register of all proprietary software and computer hardware owned/used by SYFR.
 - (iii) A programme of checking P.C.'s for software used and licences held will be undertaken by the ICT Officer on an adhoc basis.
 - (iv) Any unlicensed software will be deleted