West Yorkshire
Fire & Rescue Service

Information Security Policy

Overarching framework for Information Security controls across the Authority

OFFICIAL
Ownership: Information Governance Group
Date Issued: 18/04/2018
Version: 10.0 Status: Final

Making West Yorkshire Safer
www.westyorksfire.gov.uk

Revision and Signoff Sheet

Change Record

Date	Author	Version	Comments
19/01/2015	Allan Darby	6.1	Minor changes throughout to reflect changes to posts and document titles
06/01/2016	Allan Darby	7.1	Minor changes including Org Structure terminology at section 2.5 to reflect new reporting.
16/03/2017	Allan Darby	8.1	Expansion of section 12.2
23/05/2018	Chris Gray	10.0	Minor changes - added the need for Information Sharing Agreement and Privacy Impact Assessment. 79.1, 9

Reviewers

Name	Version Approved	Organisation	Date
Information Governance Group	7.0	WYFRS	19/01/2015
Information Governance Group	8.0	WYFRS	14/01/2016
Information Governance and Security Group	9.0	WYFRS	11/01/2017
Information Governance and Security Group	10.0	WYFRS	18/04/2018

Distribution

Name	Position	Organisation
	All Staff and Authority Members	WYFRS/WYFRA

Document Properties

Item	Details

Document Title	Information Security Policy
Author	Administrator
Creation Date	19 January 2015
Last Updated	18 April 2018

Contents

1 Introduction

West Yorkshire Fire and Rescue Authority uses information, and is often dependent on it. Various risks may affect the security - confidentiality, integrity and availability - of this information. Information security is founded on risk management because total security is unaffordable and probably unachievable. Information security is not an 'IT problem', it is a business issue. Risks are managed by reducing their likelihood and or mitigating their business consequences.

The purpose of this Information Security Policy is to help establish and maintain the Authority's Information Security Management System (ISMS). An ISMS is appropriate to the Authority's 'business', information assets, the risks to them, any specific statutory or policy requirements and the Authority's risk exposure.

This Information Security Policy is based upon the International Standard ISO 27001:2013 the Code of Practice for Information Security Management, which is the de facto standard for the development of information security strategy world-wide.

Storage of West Yorkshire Fire and Rescue Authority data on computers and transfer across the network eases use and expands our functionality. Commensurate with that expansion is the need for the appropriate security measures. Security is not distinct from the functionality.

2 Policy

2.1 Requirements for the Policy

Managing risk is the basis for managing information security. Security management should be part of the Authority's overall risk management. Information security is one aspect of security.

Information security is a cyclical management process called an Information Security Management System (ISMS). Within this process risks are continuously managed by applying appropriate safeguards to reduce the likelihood and or mitigate the consequences of unacceptable risks.

It is the Authority's policy that the information it manages shall be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

This Information Security Policy provides management direction and support for information security across the Authority. Specific, subsidiary information security policies shall be considered part of this information security policy and shall have equal standing.

2.2 Policy Structure

This document forms the Authority's Information Security Policy. Its purpose is to provide an overarching framework (a commitment of undertaking) to apply information security controls throughout the Authority.

Supporting policies containing detailed information security requirements will be developed in support of this policy. Dependent upon the subject matter, supporting policies will apply either holistically or to specific groups or individuals within the Authority. Employees of the Authority, who have access to the Authority's computers, information systems and key information, and all other parties who have been granted such access, are responsible for complying with supporting policies that are applicable to them.

The Authority will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the Authority's data, network and system resources.

Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

Reference to supporting policies is made in bold italic text throughout the remainder of the document.

2.3 Purpose and scope

By information security we mean protection of the Authority's data, applications, networks, and computer systems from unauthorised access, alteration, or destruction.

The purpose of the information security policy is:

- To establish an Authority-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of Authority data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of the Authority and allow the Authority to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

The Information Security Policy is designed to provide protection from internal and external security threats, whether deliberate or accidental by:

- Defining the Authority's policy for the protection of the Confidentiality, Integrity and Availability of its' key data and information;
- Establishing responsibilities for information security;
- Providing reference to documentation that comprises the Information Security Management System (ISMS).

2.4 Objective

Information Security controls are designed to protect employees and members of the Authority and the Authority's reputation through the preservation of:

- *Confidentiality* - knowing that key data and information can be accessed only by those authorised to do so;
- *Integrity* - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,
- *Availability* - knowing that the key data and information can always be accessed.

The Authority is committed to protect both its employees and members and its key data and information and to deploy controls that minimise the impact of any *Security Incidents*.

2.5 Applicability

This policy has been ratified by the Authority and forms part of the policies and procedures of its Information Security Management System. It is applicable to and will be communicated to staff, Members, contractors and other relevant parties.

Principal Officers are ultimately responsible for ensuring that the Information Security Policy is implemented within their respective Directorate or Department and for overseeing compliance by individuals under their direction, control or supervision.

It is the personal responsibility of each person to whom the Information Security Policy applies to adhere with its requirements.

3 Organisation of information security

Information security governance has been implemented to ensure effective controls are in place throughout the Authority.

3.1 Information security infrastructure

An *Information Security Infrastructure* has been developed to support the Information Security Policy

3.1.1 Ownership and maintenance of the Information Security Policy

The Authority's *Information Governance Group* (IGG) will maintain the Information Security Policy. The IGG will include representatives from both operational and non-operational departments, utilising specialist input where contents or topics warrant this.

The group will ensure that there is clear direction and visible management support for security initiatives.

3.1.2 Independent review

An independent review of the implementation of the Information Security Policy, its effectiveness and the degree of compliance with it will be carried out periodically by bodies that have appropriate experience of workings within the Emergency Services.

3.2 Security of external parties

Access to the Authority's information processing facilities by *third parties* will be controlled and periodically reviewed where appropriate.

3.2.1 Identification of risks from third party access

Third parties who require access to the Authority's IT/IS infrastructure will be bound by a contract that defines Authority security requirements. Prior to being granted any network connectivity they will be required to sign an undertaking to adhere to the requirements of the ***Third Party Access Policy (IS-POL006.1)*** and where key data is involved, they will be required to sign a non-disclosure agreement.

4 Information asset management and classification

Information assets will be categorised and recorded to enable appropriate management and control.

4.1 Inventory of assets

An inventory will be maintained of all the Authority's major information assets and the ownership of each asset will be clearly stated. This inventory will be developed and maintained in accordance with the ***Information Asset Management Policy (IS-POL007.1).***

4.2 Information classification

Key data and information will be classified, protectively marked and handled and managed in accordance with the ***Information Classifications Policy (IS-POL007.6).***

5 Human resources security

Controls will be deployed to reduce the risks of human error, theft, fraud, nuisance or malicious misuse of facilities.

5.1 Security in job descriptions

Security roles and responsibilities will be included in job descriptions where appropriate. These will include any specific responsibilities for the protection of particular assets, or the execution of particular processes or activities such as data protection.

5.2 Personnel screening policy

New employee references must be verified appropriately and steps must be taken in accordance with the Baseline Personnel Security Standard to minimise the likelihood of personnel, who pose a security risk, being employed in posts involving key data and information, such as those concerned with financial or personnel related data.

5.2.1 Confidentiality undertaking

All employees have a duty to protect confidential information both during and after their employment with the Authority, in accordance with the Authority's standard terms and conditions of employment.

5.2.2 Employee responsibilities

All employees must comply with the Authority's information security policies. Any information security incidents resulting from non-compliance will result in appropriate disciplinary action.

Employees will be informed of their information security responsibilities during induction training and these will be reiterated on the Authority intranet in accordance with the Information Security Management System (ISMS)**.**

5.3 Training and awareness

All staff are to be provided with *Information security awareness* training and / or instruction. The Training and Development Framework will identify where such training is mandatory.

An appropriate summary of the information security policies must be formally delivered to Members and other users, such as visitors and other third parties. They may be made aware of their responsibilities through various information security awareness documents and publications.

6 Physical and environmental security

The procedures for the operation and administration of the organisation's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.

Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to, information assets.

6.1 Physical security

Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff with authorisation to enter such areas are to be provided with information on the potential security risks and the measures used to control them. These security controls will be in accordance with the ***Physical Security Procedures and Guidance (IS-POL009.1)*****.**

Server rooms, data centres, offices and other locations either housing critical information processing facilities or from where such facilities might be accessed must have good physical security. Equipment that supports critical business activities must be physically protected from security threats and environmental hazards and must be sited, or protected, to reduce the risks of damage, interference and unauthorised access.

6.2 Environmental security

Whether offices or computer rooms, physical security protection should be based on defined perimeters with security enforced at an appropriate level for each one. As far as practicable, only authorised persons should be admitted to such areas and appropriate entry controls should be implemented to achieve this. All Authority employees are required to wear visible identification and should be encouraged to challenge strangers.

Visitors to secure areas should only be granted access for specific, authorised purposes and should be supervised. As security could be compromised by allowing members of the public temporary access for enquiry or delivery purposes, separate enquiry, delivery or loading areas should be provided outside secure areas.

Key Information will be protected in accordance with the ***Information Classifications Policy (IS-POL007.6)***.

Laptop computers and mobile equipment will be protected in accordance with the ***Mobile Computing and Communications Policy (IS-POL011.3)***.

7 Communications and operations management

Controls will be implemented to enable the correct and secure operation of information processing facilities.

7.1 Documented operating procedures

The procedures for the operation and administration of the Authority's business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.

Sensitive documentation will be held securely and access restricted to staff on a need to know basis.

7.2 Segregation of duties

Duties and areas of responsibility shall be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the Authority.

The segregation of duties acts as a primary internal control to prevent, or reduce the risk of, errors, irregularities, or unauthorised modification of information. Likewise, dual control is a simple means of ensuring that colleagues perform critical activities as a team and is particularly relevant where the validation of information is critical.

Sensitive operations will be identified and action taken to implement split functional controls where appropriate.

7.3 Systems planning and acceptance

Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within the Authority must follow a formalised development process.

The security risks to the information assets of all system development projects shall be assessed and access to those assets shall be controlled.

7.3.1 Capacity planning

Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity to be made available.

7.3.2 System changes

Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

All changes to live critical systems will follow a pre-defined change management process, to ensure that activities are undertaken in accordance with stringent change control processes.

7.4 Controls against malicious software

External software or files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

7.5 Virus protection

A ***Malicious Code Policy and Procedure (IS-POL010.11)*** has been implemented to prevent the introduction and transmission of computer viruses both within and from outside the Authority. This extends to managing and containing viruses should preventative measures fail.

7.6 Backup and archiving

7.6.1 Backup

Information Asset Owners must ensure that appropriate backup and system recovery procedures are in place.

Backup of the Authority's information assets and the ability to recover them is an important priority. Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.

Data on critical systems will be managed in accordance with the ***Backup Procedure (IS-PRO010.13)***.

7.6.2 Archiving

The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, with liaison between technical and business staff, and in keeping with the organisation's ***Retention of Records Procedure (CS-POL008)***.

7.7 Network management

The Authority's network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity in collaboration with individual system owners. All network management staff shall be given relevant training in information security issues.

The network is designed and configured to deliver high performance and reliability to meet the Authority's needs whilst providing a high degree of access control and a range of privilege restrictions.

Controls are implemented in accordance with the ***Network Management Procedure (IS-PRO010.14)*** and the ***Account and Password Management Policy (IS-POL011.2)***.

7.8 Media handling and security

7.8.1 Handling and storage

Removal off site of the Authority's sensitive information assets, either printed or held on computer storage media, should be properly authorised by the Information Asset Owner or a member of Management Team. Prior to authorisation, a risk assessment based on the criticality of the information asset should be carried out.

Media containing key data will be marked and handled in accordance with the ***Information Classifications Policy (IS-POL007.6)*** and the ***Mobile Computing and Communications Policy (IS-POL011.3)***.

7.8.2 Disposal

When permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site using procedures authorised by the Information Governance Manager.

Damaged storage devices containing sensitive data will undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the Authority and only be removed from site with the permission of the information asset owner.

Where custody of equipment containing key data is to be relinquished, procedures will be implemented in accordance with the ***Information Classifications Policy (IS-POL007.6)*** to securely delete such data first.

Redundant computer equipment will be disposed of in accordance with the ***Secure Disposal of Removable Storage Media Procedure (IS-PRO009.11)*** and the Waste Electrical and Electronic (WEEE) Regulations through secure and auditable means.

7.9 Information exchanges

7.9.1 Information sharing

Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must also be seen to continue to assure the confidentiality and integrity of the information. Such exchanges should be controlled by appropriate Information Sharing Protocols agreed by all parties and by strict adherence to the ***Data Protection Policy (CS-POL008)***.

Sensitive data or information, may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured throughout the transfer.

Routine exchanges of personal data with third parties require an Information Sharing Agreement supported by a Privacy Impact Assessment. The Information Sharing agreement and Privacy impact Assessment needs to be reviewed annually or at the event of any confidentiality breach.

7.9.2 Email exchanges

Email should only be used for business purposes in accordance with the ***Rules for Email Usage (IS-POL007.3)*** and in a way which is consistent with other forms of business communication. The attachment of data files to an email is only permitted after confirming the classification of the information being sent and then having scanned and verified the file for the possibility of a virus or other malicious code.

Information received via email must be treated with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code.

8 Access control

8.1 Authority requirements for systems access

The control of access to information is fundamental to information security. This area deals with the controls that need to be in place and is a major component of the ISMS.

8.1.1 Access management and administration

Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users' access rights match their authorisations. These procedures shall be implemented only by suitably trained and authorised staff in accordance with the ***Account and Password Management Policy (IS-POL011.2)***.

Access control standards must be established for all information systems, at an appropriate level for each system, which minimises information security risks yet allows the organisation's business activities to be carried out without undue hindrance. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.

8.1.2 Remote access

Controls will be implemented to manage and control remote access to the Authority's IT systems and data in accordance with the ***Mobile Computing and Communications Policy (IS-POL011.3)***.

8.1.3 Privilege Management

Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need; staff change their role or leave the Authority. Users' access rights will be reviewed at regular intervals.

8.1.4 Password management

Password management procedures shall be put into place to ensure the implementation of the requirements of the information security policies and to assist staff in complying with best practice guidelines.

The allocation and management of passwords shall be controlled in accordance with the ***Account and Password Management Policy (IS-POL011.2)***.

8.1.5 Passwords

All users shall have a unique identifier (user ID) for their personal and sole use for access to all the organisation's information services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason. The selection of passwords, their use and management must adhere to best practice guidelines.

8.2 User responsibilities

All staff who use the Authority's computer systems and/or networks must do so in accordance with the ***Acceptable Use Policy (IS-POL007.2)***.

8.2.1 Unattended user equipment

The Authority advocates a ***Clear Desk and Clear Screen Policy (IS-PRO011.4)*** particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons.

All users of Authority computing systems are responsible for safeguarding key data by ensuring that desktop machines are not left logged-on when unattended, and password protected screensavers should be utilised to prevent unauthorised access.

Portable equipment should be used and safeguarded in accordance with the ***Mobile Computing and Communications Policy (IS-POL011.3)***.

8.3 Network access control

The use of *networked services*, connectivity to the Authority network and the use of *information systems* connected to the Authority network will be in accordance with the ***Network Management Procedure (IS-PRO010.14)***.

8.4 Monitoring system access and use

Access to operating system commands is to be restricted to those persons who are authorised to perform systems administration or management functions. Use of such commands should be logged and monitored in accordance with the ***Network Management Procedure (IS-PRO010.14)***.

9 Information systems acquisition, development and maintenance

New information systems, or enhancements to existing systems, must be authorised jointly by the manager(s) responsible for the information and the ICT Manager and the Information Governance Manager. The business requirements of all authorised systems must specify requirements for security controls.

A Privacy Impact Assessment will need to be conducted to ensure Privacy by Design and reviewed throughout the implementation of the new Information System or enhancement. This will ensure that all the data protection principles have been considered from the very outset rather than a costly after thought.

Equipment supporting business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

9.1 Security requirements within projects

The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the ***Information Classifications Policy (IS-POL007.6)***, and a risk assessment undertaken to identify the probability and impact of security failure.

9.2 Use of cryptography

A policy on cryptographic controls will be developed with procedures to provide appropriate levels of protection to sensitive information whilst ensuring compliance with statutory, regulatory and contractual requirements.

Confidential information shall only be taken for use away from the organisation in an encrypted form unless its confidentiality can otherwise be assured.

The confidentiality of information being transferred on portable media or across networks must be protected by use of appropriate encryption techniques in accordance with the ***Mobile Computing and Communications Policy (IS-POL011.3)***.

The use of all cryptographic controls will be in accordance with the ***Encryption Usage Policy (IS-POL012.1)***.

9.3 Security in test and development processes

Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the Authority's information security policies, access control standards and requirements for ongoing information security management.

10 Information security incident management

Procedures and controls will be put in place to report and learn from security incidents and weaknesses and to escalate action on dealing with these.

All employees, Authority Members, contractors and third party users will be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of the Authority's assets.

10.1 Responding to security incidents and suspected security weaknesses

Users of information systems must be encouraged to note and report, to the IT Help Desk, any software or system that appears not to be functioning correctly, i.e. not as expected or according to specification.

Users must not, without authority, attempt to prove a suspected weakness; their action in testing the weakness might be interpreted as a potential misuse of the system. All investigations of weaknesses must follow approved procedures.

10.2 Reporting security incidents

Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the organisation's business operations and information processing systems. Mechanisms shall be in place to monitor and learn from those incidents.

All security incidents need to be reported at the earliest convenience to ensure the Authority can meet its obligations to report incidents to the ICO within 72hrs

All actual and suspected security incidents are to be reported in accordance with the ***Information Security Incident Management Policy and Procedure (IS-POL013.1)***.

10.3 Security incident management

Controls will be put in place to ensure a consistent and effective approach is applied to the management of information security incidents.

All 'security incidents' will be controlled and managed through a process of investigation and review with appropriate corrective action taken to prevent recurrence.

11 Business continuity management

Business continuity plans protect critical business processes from major failures or disasters affecting information systems. These plans (which include elements of disaster recovery) must be developed and maintained across the Authority.

The Authority has developed a project to assess business continuity requirements and to identify appropriate areas for further action. A formal risk assessment exercise has been conducted to classify all systems according to their level of criticality to the Authority and to determine where business continuity planning is needed.

11.1 Data backup and storage

Critically important and sensitive data should ideally be stored on systems that are permanently connected to the Authority's network so that the data is routinely backed up. Where such data has to be stored remotely then sufficient regular and frequent backups shall be made in accordance with the ***Mobile Computing and Communications Policy (IS-POL011.3)*** and the ***Backup Procedure (IS-PRO010.13)***.

11.2 Fallback and recovery procedures

Procedures will be put in place to describe the actions to be taken to move essential business activities or services to temporary locations following a major incident that may jeopardise Authority operations. These procedures should include details regarding the handling, transportation, storage and retrieval of backup media containing key data.

Further procedures will be adopted describing the action to be taken to return the Authority to normal full operational status.

11.3 Business Continuity and Risk Management Strategy

A *Business Continuity and Risk Management* Strategy has been developed, *exercised* and maintained to ensure the availability of services in the event of unexpected disruption in accordance with the ***Business Continuity and Risk Management Strategy (CS-STR003)***.

12 Compliance

The Authority aims to ensure both compliance with legal obligations and compliance with its own information security standards. The Information Security Policy sets out the processes for identifying any legal obligations which may bind the Authority, defines measures to avoid any breaches of those obligations, and describes the controls necessary to ensure that the standards in the corporate security policy are met.

12.1 Compliance with legal requirements

The Authority will only process personal data in accordance with the requirements of the data protection legislation. Personal or confidential information will only be disclosed or shared where an employee has been authorised to do so and will be in accordance with the ***Data Protection Policy (CS-POL008)***.

12.2 Review of the Information Security Policy

This Policy will initially be reviewed and updated annually to ensure that it remains appropriate in the light of any relevant changes to the law, corporate policies or contractual obligations or any changes in regards to technical updates or as a result of information security incidents.

12.3 Compliance with the Information Security Policy

Compliance with the Information Security Policy is mandatory. Failure to comply with policy requirements will be viewed as a breach of security. Any such event may be the subject of investigation and possible further action in accordance with Authority procedures.

Principal Officers shall ensure that the security policy is adhered to within their Directorate/Area of Responsibility. All parts of the Authority will be subject to review to ensure compliance with the Information Security Policy.