AVON FIRE & RESCUE

www.avonfire.gov.uk

Information Security Policy

This document is uncontrolled when printed. All users are responsible for checking to confirm that this is the current version before use.

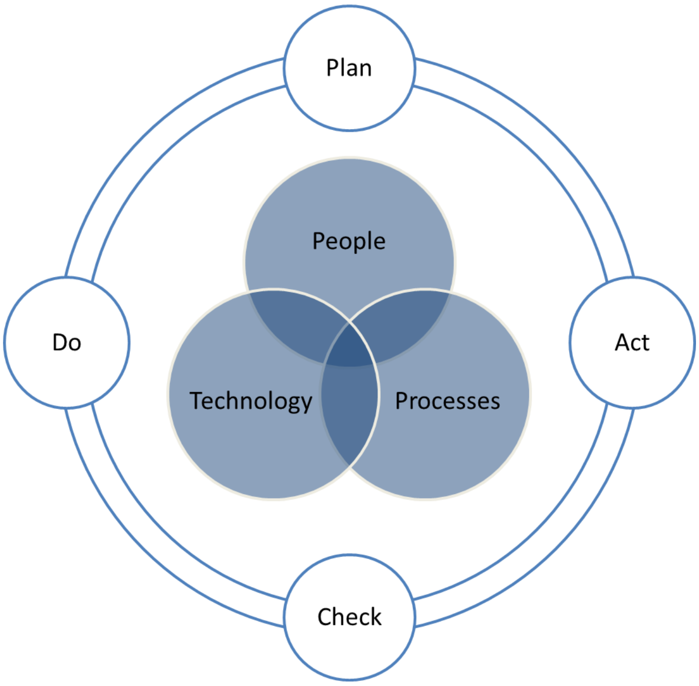
Contents

1 Purpose 4
2 Scope 5
3 Responsibility 5
4 Definitions 6
5 Risk management 7
6 Applicable documentation 8
7 Managing information security within AF&RS 9
8 Information Asset Management 9
9 Personnel security 9
10 Physical and environment security 10
10.1 Documents in Transit 11
10.2 Confidential Waste 11
11 IT security 12
11.1 Procedures and change management 12
11.2 Third parties 12
11.3 System planning and acceptance 13
11.4 Protection against malicious software 13
11.5 Back-up 13
11.6 Network security 13
11.7 Handling Removable Media 14
11.8 Exchanging information 15
11.9 Publishing information and sharing information with the public 16
11.10 Monitoring and logging 16
11.11 Disposal of IT equipment 17
12 Access control 17
12.1 Policy and management 17
12.2 Passwords 18
12.3 Unattended equipment and clear desk / locked screen policy 18
12.4 Network access control 19

12.5 Application access control 19
12.6 Operating system access control 20
12.7 Mobile working 20
13 Systems acquisition, development and maintenance 20
13.1 Security of Information Systems 20
13.2 Security of applications processing 20
13.3 Cryptographic controls 21
13.4 Security of system files 21
13.5 Security in development and support processes 21
13.6 Technical vulnerability management 21
14 Security incident management 22
15 Business continuity 22
16 Compliance with legal requirements 23

1 Purpose

Avon Fire & Rescue Service (AF&RS) is committed to protecting the information with which it has been entrusted, whether this is information relating to staff or to the local community. To this end, AF&RS has an Information Security Management System (ISMS) which consists of a set of policies and procedures for systematically managing our data in order to minimise risk and ensure business continuity by pro-actively limiting the impact of a security breach. The ISMS includes people, processes and technology and provides organisational direction and management confidence that AF&RS's critical information assets are appropriately protected. It also incorporates how AF&RS 'Plan, Act, Check and Do' to ensure a cycle of continuous improvement for our ISMS.



The purpose of this Policy is to ensure that AF&RS staff are aware of the controls that have been implemented and understand their own responsibilities.

This Policy is reviewed regularly in line with Service protocols and/or following an investigation into any major data breach, to ensure that it remains appropriate to the needs of the organisation and we learn from any information security incidents.

2 Scope

This Policy applies to all AF&RS staff, our suppliers, contractors, Avon Fire Authority (AFA) Members and anyone acting on behalf of the organisation. It applies to all AF&RS sites and at all points of interaction with our local community and partner organisations.

3 Responsibility

Overall responsibility for the AF&RS ISMS resides with the Chief Fire Officer/Chief Executive (CFO/CE). The CFO/CE will ensure that suitable resource is allocated to the security of the organisation and that staff are trained as appropriate.

A member of Service Leadership Board (SLB) or appropriate senior level delegate carries the role of Senior Information Risk Owner (SIRO). The SIRO ensures that the CFO/CE and the SLB are fully aware of the status of information risk. The SIRO provides sign off for any Data Protection Impact Assessments (DPIAs) and risk assessments relating to information security where the residual risk is medium or high.

SLB members ensure that appropriate mitigating actions are implemented across the Service. The Duty Principal Officer would take responsibility for the SIRO role in their absence.

The Strategic Asset Management Board (SAMB) provides corporate assurance that the risks surrounding information, data and associated systems are managed appropriately and that the Service's ISMS is aligned with the Service's Mission, Vision and Values, whilst meeting legislative and HMG requirements (where appropriate). The group will also provide advice and recommendations to ensure that appropriate, risk-based, cost-effective controls and measures are implemented to adequately protect the Service's information assets. This will be done by taking into account results of any DPIAs, risk assessments, audits, incidents, log reports, organisational change and any feedback from interested parties. Where the SAMB are unable to determine an appropriate course of action, the matter will be escalated to the SLB by the SIRO.

The IT Contractor is responsible for receiving alerts and warnings, implementing technical controls, advising on technical solutions and monitoring for vulnerabilities and risks relating to IT security. The IT Contractor is also responsible for meeting the requirements of the Cyber Essentials Plus certification and ensuring this certification is renewed annually alongside network security penetration testing. The IT Contractor produces and maintains IT Policies and provides regular reports to management including key information security updates such as backup success and failures, anti-virus status, key changes, information security incidents and patch updates.

The Corporate Assurance Team is responsible for ensuring compliance with security policies, controls and standards. This role is sometimes referred to as the 'Accreditor'.

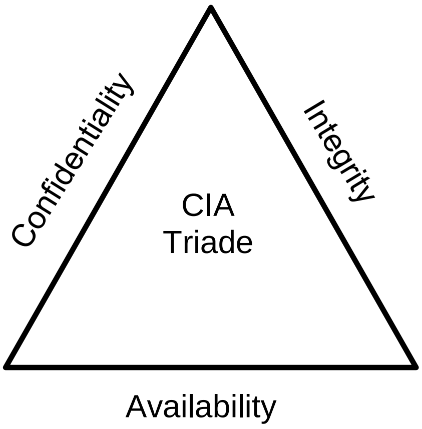
Information Asset Owners (IAOs) are responsible for ensuring that assets under their control are logged on the Critical Information Asset Register and the Record of Processing Activity and that identified risks are dealt with according to the risk management process. All assets must have appropriate security and control measures and be fully documented to ensure that there is a record of the 'life cycle' of that information.

All members of staff, AFA Members, as well as any third party contractors or consultants working on behalf of AF&RS, are responsible for adhering to the requirements of this Policy. Wherever this Policy refers to 'staff', the term also applies to third party contractors or consultants and Members.

4 Definitions

Information Security

The 'CIA Triade' is a useful way to explain the principles of Information Security.



Confidentiality	Ensuring that access to sensitive data is restricted to those who need access and not accessible to those who do not need access.
Integrity	Ensuring that the information we hold is accurate, preventing unauthorised or unintentional changes or deletions.
Availability	Ensuring that the information we hold is available to those who need it, when they need it.

Data Protection Legislation
A range of legislation exists to protect personal data, this will be referred to throughout this Policy as 'Data Protection Legislation'. The most relevant are listed here:

The EU **General Data Protection Regulation** (the GDPR) ensures fundamental data protection rights and freedoms for individuals, particularly the right to privacy. It places obligations on organisations to be accountable and transparent in the way that they use individuals' data. It aims to achieve consistency across all EU Member States and reflects the changes in technology in a more digital world. The GDPR will still apply when the UK leaves the EU.

The **Data Protection Act 2018** (DPA) should be read alongside the GDPR for organisations to understand the full legislative framework that applies to them. It sets out rules which are specific to the UK, ensuring that GDPR works in harmony with domestic law. It includes specific provisions for law enforcement and processing special categories of personal data.

Personal data means any information relating to a living individual who can be identified, directly or indirectly. This could be a name, address, contact details, location data, and online identifiers. Examples of personal data that the Service hold include HR data, finance and pensions data relating to staff and Health, Safety & Welfare data. Personal data also extends to data we collect while delivering our services, such as data collected at incidents, community safety engagements and safeguarding information.

Special categories of personal data (or sensitive personal data) are afforded a higher level of protection under the Data Protection Legislation. This includes data about things like racial or ethnic origin, religious or philosophical beliefs, trade union membership, and data concerning a persons health or their sex life or orientation.

Staff should also be aware that data which is classed as 'non personal data', which may still be sensitive or confidential information and must be handled with care. Examples of **sensitive non-personal data** may include; Fire investigation reports; Coroner reports; Operational planning for major incidents; Commercially sensitive contract information including tender documents; Security incidents; Operational intelligence and procedures which could affect our resilience to respond to an incident in the wrong hands.

5 Risk management

AF&RS will adopt an approach to risk management that:

- identifies critical information assets and ownership of these assets;
- analyses and evaluates the risk to these assets;
- identifies and evaluates options for treatment of the identified risks;
- selects appropriate controls for managing risks; and
- obtains management approval for actions and overall management of risks.

An 'information asset' is defined as any information that has value to AF&RS. A 'critical information asset' meets one or all of the following criteria:

- A breach of an asset's confidentiality, integrity (that is, accuracy or reliability) or availability will seriously impact on AF&RS's ability to deliver services; on AF&RS's reputation; on the rights or freedoms of an individual; or on AF&RS's ability to meet its legal and regulatory obligations.
- Should an asset be lost, it is not easily replaced without cost, skill, time, resources or a combination of these.
- Any other reason for which the Information Asset Owner considers the asset to be 'critical'.

Risk assessments are undertaken as required and should be signed off by the SIRO to confirm any mitigating actions are acceptable and any residual risks are accepted. Where residual risks are identified and the SIRO wishes to accept the risk, this will be signed off using a 'Residual Risk Statement'.

6 Applicable documentation

This Policy is part of a suite of AF&RS Corporate Policies, which contribute to the Information Security Management System (ISMS).The following Policies may be read in conjunction for a fuller context about how we manage information and keep it safe.

- Data Protection Policy*
- Freedom of Information Policy*
- Security Incident Management Policy
- IT Systems Acceptable Use Policy
- Laptop and Mobile Device Security Policy
- Anti-virus Policy
- Information Classification Policy

All policies are available to staff via the staff intranet. The documents marked with a * are also available to members of the public via the website.

Applicable documentation also includes output of risk assessments and minutes of management meetings and other IT, HR and Operational policies and operating procedures.

The ISMS and this Information Security Policy are based on best practice, using the requirements of the HMG Security Policy Framework and the IEC/ISO 27000 Series (in particular ISO 27001) for guidance which are International Information Security Standards.

7 Managing information security within AF&RS

In addition to the responsibilities identified above, processes shall be in place to authorise and manage the implementation of all new IT systems and any facilities / systems involved in processing information. The SLT will authorise Business Cases and requests impacting on budget. The Strategic Asset Management Board should be consulted prior to implementing any new IT system or making major changes or additions to existing systems. DPIAs must also be completed when planning changes, new processes, systems, and initiatives or projects that impact on personal data, data protection or privacy.

Appropriate controls shall also be put in place to maintain the security of AF&RS systems and facilities that are accessed by third parties, including contractors, suppliers and members of the public. Any third party agreements shall also include requirements for managing security of critical assets and data sharing and/ or non-disclosure agreements where necessary.

8 Information Asset Management

Critical information assets are identified in the AF&RS Critical Asset Register. Information Asset Owners (IAO) are identified and are responsible for maintaining the integrity and accuracy of this register. The Critical Information Asset Register is a live document which should be reviewed regularly and updated when changes occur. The Data Protection Team will facilitate a review of the register at least annually.

IAOs are also responsible for ensuring that protective controls are implemented in line with the asset's risk rating and aligned with organisational objectives.

9 Personnel security

In order to ensure the protection of AF&RS critical information assets and of the community within which we work, AF&RS is committed to ensuring that staff meet the appropriate security requirements of their roles. This involves appropriate screening prior to employment and incorporating security responsibilities within job descriptions and terms & conditions of employment. Reviews of security clearance will also be conducted, as appropriate, during employment.

Staff have the right to challenge National Security Vetting decisions and should seek advice from HR should they wish to do so.

Acceptable use of AF&RS systems and information assets is defined in the AF&RS IT Systems Acceptable Use Policy. All staff are required to read this as part of the induction process. In addition every time staff enter the AF&RS IT system they should read and accept the terms stated.

During employment, staff receive training (normally via e-learning) and as appropriate to their role. This includes the completion of a Data Protection and Information Security e-learning course which is mandatory for all staff (temporary, permanent and agency workers) to be completed within the first two weeks of employment and subsequently every 2 years.

Policies as outlined in Section 6 and guidance documents provide further guidance. A breach of any of the Service's policies will be dealt with in line with the disciplinary procedures.

On termination of employment, staff must return any of the Service's assets (including information assets, IT equipment, ID cards, access fobs and key cards) in their possession. Managers, HR and IT are responsible for ensuring that access rights are removed promptly when a member of staff leaves the Service.

10 Physical and environment security

Appropriate physical entry controls and security perimeters are in place to ensure that only authorised personnel can gain access to AF&RS critical assets and for the overall physical protection of buildings, appliances and staff. Regular security risk assessments must be conducted for all sites and appropriate physical security controls put in place. Security controls are also checked via the H7 Quality Assurance Audit and Workplace Inspections.

Protection measures are also in place to safeguard against damage from fire, flood, explosion, civil unrest and other forms of natural or man-made disaster. Where appropriate, procedures shall be put in place to provide guidance for working in secure areas.

Areas where the public or unauthorised persons may enter AF&RS premises should be controlled. Any non-AF&RS personnel should ensure that a member of AF&RS staff is aware they are on site, sign in and out, and where possible, be accompanied on the premises. Their access should be restricted only to those areas where they have a need to go.

Staff who work at the joint AF&RS and Avon & Somerset Constabulary Headquarters will be subject to the Police's own security vetting process. Any member of staff or site visitor who has not been granted security clearance is required to sign in to the HQ site as a visitor and must be accompanied whilst on site.

Thought must be given to siting equipment (including IT equipment) in areas that will reduce the risk from threats / hazards and opportunity for unauthorised access. This includes ensuring appropriate protection from power failures or damage to cabling and ensuring that equipment is correctly serviced / maintained.

Equal care should be taken of any equipment that is taken off site. No equipment shall be removed from site without prior authorisation. The Laptop and Mobile Device Security Policy provides guidance for users of laptops and mobile devices.

10.1 Documents in Transit

Documents and folders containing personal and sensitive data should not be removed from AF&RS premises without a genuine business need. Should documents need to be transferred from one site to another, care should be taken to ensure that they are secure whilst in transit, the following measures should be considered:

- Ensure loose documents are placed in a sealed folder or envelope
- If folders are boxed, tape them up securely
- Label boxes, envelopes or folders as Private and Confidential
- If transported in a car, ensure it is locked when unattended and documents are out of sight
- Do not leave in a car overnight.
- Where appropriate, keep an inventory of documents that are moved off site and log them in and out to maintain an audit trail.
- If documents are lost or compromised, refer to Section 14 of this policy.

10.2 Confidential Waste

Staff must ensure that any documents that are no longer required or meet their document retention period are securely disposed of either via shredding, or the use of confidential sacks/bins. Confidential waste will include any personal data or operationally sensitive data, including documents which bare any Government Security Classification. Confidential waste contractors are subject to the relevant industry checks, including accreditations and guarantees for information security. These contracts are facilitated by the Procurement and Supplies Department.

At end of life, equipment must be disposed of according to procedures, including checking that any information has been removed or securely overwritten prior to disposal. See section 11.11, Disposal of IT Equipment.

11 IT security

11.1 Procedures and change management

In order to ensure secure operation of AF&RS IT systems and facilities, the IT Contractor is responsible for ensuring that appropriate IT policies and procedures are documented and maintained. In particular, procedures shall be put in place to control changes so that unauthorised changes cannot be made, and that systems can be restored to their former state should there be a problem as a result. To ensure that there is no conflict of interest, duties and areas of responsibility shall be appropriately segregated in order to reduce opportunity for unintentional modification or misuse of AF&RS assets. Similarly, development, test and operational facilities shall be separated to reduce risks of unauthorised access or changes to the operational systems.

All changes to AF&RS IT systems or communications systems must be authorised by the Director of Corporate Services in conjunction with the IT Manager (Contractor) or the Group Manager (GM) for Fire Control and Communications.

11.2 Third parties

Security controls must be included in Contracts, Information Sharing Agreements and Service Level Agreements with third parties. Regular reviews should be carried out, as appropriate, to ensure that agreements are being met.

Any work on AF&RS premises or equipment that may require the use of, or could impact on, AF&RS IT networks, equipment, or Control and Communication equipment, must be carried out in liaison with the appropriate department, such as the IT Contractors or Control and Communications.

This is to ensure that as a Service, we consider any such alterations or access, and how this may impact on our systems. We need to ensure that our systems are not compromised, that we maintain IT and Communications security and we continue to adhere to this and other Service policies, such as the Remote Access Policy.

Third parties are not permitted to install or connect non-AF&RS approved devices to the network without written authorisation from the Director of Corporate Services in conjunction with IT Manager (Contractor) or GM for Fire Control and Communications. Any changes to the provision of service from third parties must be appropriately authorised and managed, taking account of the criticality of business systems and processes.

11.3 System planning and acceptance

In order to minimise the risk of systems failure, IT will monitor capacity demands and make projections of future capacity requirements to ensure that adequate processing power and storage are available.

Software acceptance criteria for new information systems, upgrades and new versions must be applied and suitable tests of the new system carried out prior to acceptance.

11.4 Protection against malicious software

Detection, prevention and recovery controls in the form of anti-virus software, audit and monitoring software, web monitoring software, firewalls, patching processes and appropriate server configurations have been implemented to ensure AF&RS is protected against malicious software (such as viruses, worms, Trojans and spyware). All computers attached to the Avon Fire and Rescue Service network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date. Computers directly connected to the network are automatically updated. Laptop users must ensure that their anti-virus software is regularly updated, and all users must adhere to the IT Systems Acceptable Use Policy and the Anti-virus Policy to ensure that malicious software is not introduced accidentally to AF&RS systems.

Where the use of mobile code is authorised (for example, use of JavaScript and ActiveX controls), the configuration must ensure that unauthorised mobile code is prevented from executing.

11.5 Back-up

Back-up copies of information and software must be taken regularly by the IT Contractors in accordance with back-up policy and procedures. Staff should be aware that information on C: drives (that is, on the hard disc of a laptop or desktop computer) is not subject to back-up.

11.6 Network security

Controls shall be implemented to ensure the security of information as it passes over AF&RS networks. This includes:

- Establishing responsibilities and procedures for managing remote equipment.
- Establishing controls where data passes over public or wireless networks.
- Where appropriate, implementing logging and monitoring tools to record actions.
- Ensuring controls are applied consistently across the organisation.

- Identifying security features, service levels and management requirements of all network services, including any network services agreements, whether these services are provided in-house or outsourced.

11.7 Handling Removable Media

Removable media refers to all types of computer storage which are not physically fixed inside a computer and includes the following:

- Memory cards (like those used in cameras);
- USB pen drives etc;
- Removable or external hard disk drives;
- Newer Solid State (SSD) drives
- Mobile devices (iPod, iPhone, iPad, MP3 player);
- Optical disks i.e. DVD and CD;
- Floppy disks;
- Backup Tapes.

The use of removable media is not prohibited within Avon Fire & Rescue Service; it is an essential part of everyday business. However, we must ensure that personal and sensitive information is protected from unauthorised access, disclosure or misuse.

Removable media devices must only be used to save and transport personal data, special categories of personal data or operationally sensitive data if you have a genuine business need and, you must seek approval from Senior Information Risk Officer (SIRO) or a member of Senior Leadership Team.

Group policies are configured to enforce BitLocker 256-Bit AES encryption on all removable media before data can be successfully written. This Policy is managed by the IT Contractors.

The Service has implemented a DLP (Data Loss Prevention) solution that records activity relating to data being copied onto removable media. Individuals who are identified as downloading data that is flagged by the system as a concern (such as personal or sensitive information), will be contacted to provide an explanation of the activity to ensure that it conforms to Service policies.

Staff must comply with the following requirements:

- If you are unclear what constitutes personal data, special categories of personal data or operationally sensitive data, please seek guidance from the Data Protection Team, to ensure the level of security is appropriate.
- Only removable media devices obtained from AF&RS should be used.

- Ensure that regularly updated Anti-Virus software is present on all machines from which the data is to be used. All AF&RS devices have anti-virus software.
- Any removable media device used to transport data must be encrypted to a recommended encryption standard using BitLocker before use. This is enforced by Group Policy. Instructions for encryption can be found on the staff intranet.
- Any sensitive or highly sensitive data transferred to a removable media device must remain encrypted and must not be transferred to any external system in an unencrypted form.
- Data stored on removable media is the responsibility of the individual who operates the devices.
- All data must be kept backed-up securely in a central location; the removable device must not be used to keep data that is not backed up.
- The user must note and accept that a lost password may render the data un-recoverable.
- Removable media should be physically protected against loss, damage, abuse or misuse when in use, storage and transit.
- Any mobile devices and/or removable media that have become damaged should be handed back to the IT Contractors to ensure they are disposed of securely to avoid data leakage.
- All leavers must return all devices to the IT Contractors for secure destruction and/or redistribution. Line Managers are responsible for ensuring all devices are returned on or before the post-holder’s last day at work.
- The use of removable media by sub-contractors and temporary workers of AF&RS is equally subject to these policies. Supervising officers should ensure that all sub-contractors comply.
- When the business purpose has been satisfied, the contents of the removable media should be removed from the media through a destruction method that makes recovery of the data impossible, for example, re-format the device. Alternatively the removable media and its data should be destroyed and disposed of beyond its potential reuse.

11.8 Exchanging information

AF&RS exchanges and shares information regularly, both within the organisation and with partner organisations. Information should only be exchanged where the recipient has a ‘need to know’. An Information Sharing Agreement must be drawn up and agreed prior to systematic information sharing with external partners or suppliers. Staff are reminded of the following:

- All data exchange and sharing must be compliant with current Data Protection Legislation. The Data Protection Team is available to provide compliance advice.

- When using e-mail to exchange or communicate information including special categories of personal data, secure email must be used or the information should be put in a password protected document attached to the email. Passwords should be communicated via a different method (eg text or phone call) or sent by a separate e-mail to a **different** email address.
- If removable media is used to exchange information, the guidelines above must be followed (11.7 Handling Removable Media).
- If hard copy documents are provided to third parties containing information including special categories of (sensitive) personal data, use a reliable courier or tracked and recorded Royal Mail service to provide evidence that the documents have been received.
- Take care when discussing information ensuring that others with no 'need to know' cannot overhear what is being said and when necessary, verify they authenticity of the person you are speaking to.

11.9 Publishing information and sharing information with the public

Care must be taken when publishing information to ensure that publication will not breach current Data Protection Legislation.

External requests for information, such as Freedom of Information or requests made under current Data Protection Legislation are dealt with by Data Protection Team. Guidance is available to staff so that they can recognise when such a request is received and forward to the team so it can be dealt with accordingly.

11.10 Monitoring and logging

AF&RS IT systems are monitored and audit logs recorded centrally. Logs and audit reports will be reviewed at regular intervals. Action will be taken in relation to security events or to unauthorised use of AF&RS systems in accordance with the IT Systems Acceptable Use Policy.

System logs are protected to ensure that data cannot be modified by unauthorised personnel.

Audit logs capture information from multiple sources including (but not limited to):

- Authentication activity
- File system and SharePoint access (opening, saving, modification of permissions)
- Internet browsing
- Web server access
- DHCP, NPS, DNS, Firewall activity

11.11 Disposal of IT equipment

IT and other electrical equipment (including removable media) that has reached the end of its useful life must be disposed of correctly and securely, to ensure that any confidential or personal data is appropriately disposed of. Disposal of AF&RS owned IT equipment is approved by the IT Contractors and facilitated by the Procurement and Supplies Department.

The Procurement and Supplies Department arrange for the decommissioning of the equipment and for the any information to be securely saved/ transferred or securely deleted (including the destruction of computer hard drives). Contractors employed by the Service to dispose of IT equipment will be subject to the relevant checks and guarantees to ensure that they meet current Information Security requirements, such as Waste Electrical and Electronic Equipment (WEEE) Regulations 2013, ISO, BSI and other quality accreditations, in addition to the relevant environmental standards. The IT Contractor is responsible for updating the Service’s Asset Management System to reflect the changes.

Similarly, the AF&RS Fire Control and Communication Department is responsible for the decommissioning and disposal of any command and control communication equipment, facilitated by the Procurement and Supplies Department.

The Procurement and Supplies Department facilitates the Service’s photocopier contract and the disposal of any other printing, imaging and fax equipment, and therefore the above considerations will also apply.

12 Access control

12.1 Policy and management

All staff are responsible for keeping themselves up to date with Service policies and for any new starters, the reading of key policies will form part of their induction process.

The Data Protection Policy is a key policy for ensuring that staff are aware of their duties under the Data Protection legislation.

As already noted, staff should ensure that they are familiar with the AF&RS Access Control Policy. On or before their first day, all new staff must read and sign the IT Systems Acceptable Use Policy prior to being granted access to any AF&RS system. Staff should be given the opportunity to discuss the Policy with their line manager prior to signing to ensure that they understand the content. Access is granted to systems on a least privilege basis, and these accesses will be revoked / changed whenever a user changes role or when they leave the organisation. It is the line manager’s responsibility to inform HR of any changes to staffing or staff responsibilities. The IT Contractors will be informed of staff movement and changes as well as ‘starters and leavers’ and will make changes to system accesses accordingly.

Access rights will be reviewed at regular intervals to ensure the integrity of access to AF&RS systems.

The Service will issue regular staff communications and information security and data protection guidance is available via the staff intranet and various policies/documents.

12.2 Passwords

All passwords must be kept confidential and never shared. Good security practice will be employed by staff and users in the selection and use of passwords, in particular:

- to avoid keeping a record of passwords, unless this can be stored securely;
- to change passwords regularly (at least every 90 days) and as prompted by AF&RS systems;
- if there is reason to believe that a password may have been compromised, this must be changed immediately and the suspected breach recorded on the Health Safety & Welfare recording system ‘Oshens’ (Wellworker);
- to select passwords that are:
    - easy to remember;
    - not based on something that is easy to guess (e.g. names, telephone numbers, dates of birth);
    - not identical letters or numbers and not consecutive all-numeric or all-alphabetic characters;
    - composed of a combination of letters, numbers and characters, both upper and lower case.
- not to use the same password for a number of applications and not to use the same password for work and non-work use.

12.3 Unattended equipment and clear desk / locked screen policy

Staff should practice a ‘clear desk’ and locked screen policy.

To ensure that no-one can gain access to systems via a username / password that is not their own, staff must always lock screen when leaving a device unattended and log off if it is a shared computer. At the end of a working day, staff should shut down and switch off systems.

Laptop and tablet computers must be locked away out of sight when unattended and at the end of the working day. This is particularly relevant to staff who work in open plan offices, on station and other remote working, such as at home.

Staff should not leave sensitive or protectively marked documents unattended on a printer or fax. The ‘secure print’ function should be used as best practice where available, in particular where personal or sensitive information is being printed. This requires a password or key fob to activate a print job.

To further safeguard sensitive or protectively marked paper documents and removable media, staff should always ensure that such documents are removed from desks and locked away when not required, when the office is left unattended and at the end of the working day.

12.4 Network access control

Users will only be provided with access to services that they have been authorised to use and appropriate authentication methods (such as two factor authentication) will be used to control access to remote users. Where appropriate, segregation of users /services/systems will be implemented to maintain integrity and confidentiality.

Physical and logical access controls will be implemented to protect access to diagnostic and configuration ports. Access will only be granted by permission of the IT Manager (Contractor) or appointed deputy.

Visitors to AF&RS sites will not be able to access the AF&RS network unless prior authorisation and access has been granted by the IT Manager (Contractor).

Where appropriate, network routing controls will be implemented to ensure that controls around access to specific business applications are not breached.

12.5 Application access control

Access to applications is typically role based, with managers determining who should have access and the extent of that access. Managers in control of granting access to applications must ensure that there is no conflict of interest when defining roles and the scope of access granted to individuals.

Unapproved software is blocked from execution and installation by AppLocker. Written requests must be submitted to the IT Helpdesk for approval of software installation.

Access control must be in line with the AF&RS Access Control Policy.

12.6 Operating system access control

Access to operating systems shall be controlled through secure log-on; unique user IDs; quality passwords; control of utility programmes; shut down of inactive sessions after a defined period of inactivity; and, where an application is deemed to be 'high-risk', a restriction on connection time may be implemented.

12.7 Mobile working

Users must always be aware of the increased risk to sensitive information where such information is being carried or accessed when away from AF&RS locations. As such, users operating away from the office must ensure that they are familiar with the AF&RS Laptop and Mobile Device Security Policy.

13 Systems acquisition, development and maintenance

13.1 Security of Information Systems

To ensure that security is built into information systems, a security requirements analysis shall be performed and the requirements specified prior to acquisition of new systems or enhancements to existing systems. Security requirements are also inbuilt in the projects process. The business requirements for new systems or enhancements to existing systems shall specify the requirements for controls.

13.2 Security of applications processing

To prevent errors, loss, unauthorised modification or misuse of information during applications processing, the information shall be checked (validated) at both the input and output stages. This may take the form of randomised checking, or a more robust technical solution. However, the method of validation shall be determined for each application.

A system of validations checks shall also be implemented to detect any corruption that could arise as errors during the internal processing of the information or as a result of a deliberate act.

Where appropriate, message authentication shall be used for applications where there is a security requirement to protect the integrity of the message content.

13.3 Cryptographic controls

Wherever appropriate, information of a sensitive nature shall always be stored and/or transmitted in encrypted form using approved cryptographic standards. A key management system shall be used to support the use of cryptographic techniques.

13.4 Security of system files

To ensure the security of system files, the implementation of software on operational systems shall be performed solely by an authorised agent of the IT Contractor or by the software supplier in conjunction with the authorised agent of the IT Contractor.

Test data should never be live data, and should be carefully selected, protected and controlled against access by unauthorised persons.

Where program source libraries are supplied, strict control shall be maintained over access to those libraries.

13.5 Security in development and support processes

To maintain the security of application system software and information, and to minimise the risk of corruption, changes shall be controlled by the IT Contractors in line with the governance arrangements set out in Section 7 'Managing information security within AF&RS' above.

Similarly, any changes to operating systems will also involve a review of business critical applications to ensure that there is no adverse impact on performance as a result of the change.

Modifications to software packages are discouraged. If essential, changes shall be strictly controlled, with particular emphasis on maintaining the integrity / confidentiality of existing data and ensuring there is no breach to access control policies.

AF&RS do not typically carry out outsourced software development. However, should there be a requirement; any such development must be carried out strictly in accordance with AF&RS policy, to include adequate due diligence and a DPIA to assess risk.

13.6 Technical vulnerability management

Technical vulnerabilities are identified from time to time by third party organisations, and these vulnerabilities are published. IT will be informed of these vulnerabilities and will ensure that risk to AF&RS systems is mitigated by employing a patch management / vulnerability management process in line with the IT Patching Policy.

The AF&RS network is regularly assessed against known vulnerability databases using a range of security assessment tools.

14 Security incident management

All staff are responsible for reporting security incidents, losses, thefts or potential security breaches without delay to a Manager, the IT Contractor and/or Control. This includes but is not limited to mobile devices, removable media such as USBs, building access fobs or cards, two factor authentication fobs, data and paper based information.

All security breaches must be reported on Oshens (Wellworker). The Security Incident Management Policy provides further information about reporting or responding to security incidents involving AF&RS information and/or information technology resources. Incidents are allocated to an appropriate person for investigation. The IT Contractors will assist in investigating and remedying any IT security incidents or breaches.

Reported incidents will be reviewed by the Strategic Asset Management Board. They will make recommendations to the Service Leadership Team (SLT) or Service Leadership Board (SLB), where further improvement action is considered necessary.

The SIRO and/or Data Protection Officer (DPO) will determine whether any notification should be made to the Information Commissioner’s Office (ICO), HMG or other bodies / committees following the reporting of a security incident. In some cases it will be mandatory to report a breach to the ICO within 72 hours. Should the DPO and/or SIRO not be available, the Duty Principal Officer will be the decision maker.

15 Business continuity

To ensure that critical services delivered by AF&RS can continue to be delivered in the event of a major failure of information systems or a disaster, all directorates are responsible for developing Business Continuity plans that identify risks, actions to be taken should a risk be realised, and responsibilities for ensuring that critical services can be maintained. These plans will include timelines for resolution.

All plans shall be tested and updated regularly to ensure their effectiveness.

All plans should also take into account contingency plans and additional security controls should there be a rise in the Government Response Level.

AF&RS has developed a single framework of business continuity plans that aligns to the ISO standard 23001, to ensure that all plans are consistent and risks are prioritised.

An IT Disaster Recovery plan is in place. It shall be tested regularly to ensure that critical information systems can be recovered and continue to run in the case of a major Information System failure. The IT Manager (Contractor) is responsible for the IT Disaster Recovery Plan and for a schedule of testing.

16 Compliance with legal requirements

To avoid breaches of any law, statutory, regulatory or contractual obligation, and of any security requirements, all staff (and anyone acting on behalf of AF&RS) are responsible for complying with relevant legislation. This legislation is identified within training courses and via policies and operating procedures.

Managers are responsible for keeping up to date with policy changes and for ensuring that their staff are aware of their responsibilities and have completed appropriate training.

Document Control Information:

Policy title:	Information Security Policy
Policy owner: (role)	Business Planning and Assurance Officer
Authoriser: (role)	SIRO
Issue status:	Published
Protective marking:	-
Issue date:	18/12/2017
Next review due:	05/10/2020
Audience:	For external publication
Version Number:	5

Document History:

Review Date	Version No	Summary of Changes	Equality Impact Assessed (Y/N)
24/10/2012	1.1	Initial draft for consultation	Y
29/11/2012	1.2	Draft incorporating Director comments	
14/02/2013	1.3	Change from IT Security Acceptable Usage Policy to IT Systems Acceptable Use Policy	
07/05/2013	2.0	Final document	
20/05/2015	2.1	Minor changes to reflect changes to HMG requirements for Protective Marking	
27/11/2017	3.17	Minor changes as review of whole policy	
14/12/2017	4.0	Final changes following consultation	
18/12/2017	4.0	Published	
15/01/2019	4.01	Minor changes as review of whole policy. Brought the Removable Media Policy into this policy to help reduce overall number of policies	
14/03/2019	4.02	Further changes following consultation with DPO and SIRO	
05/04/2019	5.0	Published	

Distribution History:

Date	Version No	Distributed to: (role(s) or group)
24/10/2012	1.1	Directors
15/03/2013	2.0	Negotiating Committee and Joint Consultation Committee
08/05/2013	2.0	Published – Distributed to all staff intranet
24/07/2014	2.0	Circulated to all staff by new intranet pages
22/05/2015	3.0	Published – Distributed to all staff intranet
04/08/2015	3.0	Published on website
27/11/2017	3.17	Circulated to Unit Heads and Union Reps for consultation
14/12/2017	4.0	SIRO for sign off
18/12/2017	4.0	Published – Distributed to all staff intranet and Website
15/01/2019	4.01	IT Manager, SIRO, DPO
19/03/2019	4.02	Unison Representatives for comment
04/04/2019	4.03	FBU Representatives for comment
05/04/2019	5.0	Published – Distributed to all staff intranet and Website