STAFFORDSHIRE FIRE AND RESCUE SERVICE

INFORMATION SECURITY POLICY

CONTENTS

1. INTRODUCTION

This Policy forms part of the Information Security Management System (ISMS) and sets out the policy and procedures to be followed by Staffordshire Fire and Rescue Service (SFRS) staff in order to keep SFRS information assets secure.

2. PURPOSE

Staffordshire Fire and Rescue Service's core purpose is to:

- Respond: Put out fires and rescue people
- Prevent and Protect: Do sensible things to prevent fires and incidents occurring.

The Service can only fulfil its duties if its employees have timely access to accurate information and this information is adequately protected against damage, tampering, theft, destruction and other threats. Stakeholders rely on the Service keeping information secure.

3. DEFINITIONS

For the purposes of this policy, the following definitions apply:

Availability – the property of information being accessible and usable on demand by an authorised person.

Confidentiality – the property that information is not made available or disclosed to unauthorised individuals, organisations or processes.

Consequence – the outcome of an event affecting objectives.

IAO – Information Asset Owner, responsible for ensuring that specific information assets are handled and managed appropriately and that their value to the Service is not exploited.

Information security – the preservation of confidentiality, integrity and availability of information.

Integrity – an information asset's property of accuracy and completeness.

ITSO – IT Security Officer, responsible for applying technical controls to manage risk.

Likelihood – the chance of something happening.

Objective – a result to be achieved.

Policy – the intentions and direction of an organisation as formally expressed by its top management.

Risk – the effect of uncertainty on objectives.

Risk treatment – a process to modify risk.

SIRO – Senior Information Risk Owner, responsible for understanding how the strategic business goals of the organisation may be affected by failures in the secure use of the Service's information systems.

Stakeholder – a person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity.

Threat – the potential cause of an unwanted incident, which may result in harm to a system or organisation.

4. INFORMATION SECURITY OBJECTIVES

The Service's information security objectives are to:

- Continually strive to reduce the incidence of adverse information security incidents
- Increase the awareness of employees in relation to good practice and current information security threats
- Comply with relevant legislation, for example: Public Records Act 1967, Copyright, Designs and Patents Act 1988, Official Secrets Act 1911-1989, Computer Misuse Act 1990, Copyright (Computer Programs) Regulations 1992, Obscene Publications Act 1994, Data Protection Act 1998, Human Rights Act 1998, Freedom of Information Act 2000, Regulation of Investigatory Powers Act 2000, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, The Terrorism Act 2000, The Anti-Terrorism, Crime and Security Act 2001, Privacy and Electronic Communications Regulations 2003, Equality Act 2010, EU General Data Protection Regulation 2016
- Ensure the Confidentiality, Integrity and Availability of information is maintained in line with its classification.

These objectives will be met through the Service's Information Security Management System (ISMS) based on ISO/IEC 27001:2017. Performance of the ISMS will be monitored against these objectives.

5. INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Post	Role	Duties
Director of Finance, Assets and Resources	SIRO	Compliance with legislation and regulatory requirements.
Head of Property	IAO	Building security, waste disposal, utilities
Head of ICT	IAO	Security of IT hardware and software
Head of Personnel	IAO	Staff supply, vetting, training and discipline
Head of Emergency Response Team (ERT)	IAO	Business continuity, response and incident data
Head of Central Prevent and Protect (CPP)	IAO	Prevent and protect data
Financial Services Manager	IAO	All finance data, anti-fraud measures
Head of Marketing and Communications	IAO	Security of social media, web site and marketing data.
SDG Leads	IAO	Data held on stations, operational personnel and vehicles.
Secretary to the Fire Authority	IAO	All fire authority data
Information Security Manager		Staff awareness, policy creation and updating, advice and guidance
IT Integration Specialist	ITSO	Technical IT security controls

6. RISK ASSESSMENT AND ACCEPTANCE CRITERIA

The Service's Strategic Risk Management System grades all risks on a scale of 1-16 using a 4 x 4, Impact x Likelihood matrix and risks scoring 8 or less after treatment are deemed to be acceptable. If a risk is assessed to be greater than this level then suitable controls must be implemented so that the residual risk is within the accepted levels, ensuring that treatment of the risk does not adversely impact the ability of employees to fulfil their duties or the effectiveness of other risk controls.

This policy will be reviewed regularly to ensure that it continues to be aligned with the Service's business objectives and to enable any opportunities for improvements to be incorporated. These reviews will be carried out by the Protective Security Steering Group, who will also be responsible for making decisions on any deviations or exceptions from this policy.

7. INCIDENT REPORTING

All employees must report information security events, whether resulting in an actual information security incident or not, to their Line manager within 24 hours, so that they can be passed to a member of the Protective Security Steering Group. Incidents will be recorded so that progress can be monitored and improvements implemented from any lessons learned.

Consultation End Date: 19/07/2017	People Impact Assessed: 08/05/2017	Review Date: 20/07/2020
Personnel may share the information in this document with members of the public.	**YES**	NO

Date of Issue	Title of Document:	Job No.	Author:	Department:	Director/Manager Approval:	Additional Information:
20/07/2017	Information Security Policy	897	Andrea Jones	ICT	David Greensmith 20/07/2017	
21/07/2014	Information Security Policy	897	Tracey Merrington	ICT	David Greensmith 17/07/2014	
02/07/2014	Information Security Policy	897	Tracey Merrington	ICT		Consultation
27/05/2010	Information Security Policy	897	Sue Love	ICT		
23/04/2010	Information Security Policy	897	Sue Love	ICT		Consultation