Title: Information Security Policy

Summary: The objective of information security is to ensure the continuing of the Authority's business and to minimise disruption to our operations by preventing and reducing the impact of security incidents.

Further Information: Replaces previous version dated 17.10.2014, minor changes to reference Data Protection Act 2018

Contents

1 Policy Statement

- The Authority treats its information as a valuable asset and considers that it is essential that information must be protected, together with the systems, equipment and processes which support its use.
- The purpose of the policy is to protect these information assets from all threats, whether internal or external, deliberate or accidental.
- Information includes data stored on mobile computing devices (Laptops, Mobile Data Terminals, Tablets, phones etc.) and data transferred by removable media, as well as data transmitted electronically, printed on paper and the spoken word.

The Authority ensures that:

- Information is protected against unauthorised access.
- Confidentiality is assured and valuable or sensitive information is protected from unauthorised disclosure or intelligible interruption.
- Integrity of information is maintained, safeguarding the accuracy and completeness of information against unauthorised modification.
- Regulatory and legislative requirements for maintaining information are met.
- Business continuity plans are maintained and tested.
- Business requirements for the availability of information and information systems is identified and met.

- Appropriate information security training and advice is available to all staff.
- Breaches of information security, actual or suspected, will be reported to, and investigated by, the Head of ICT (HICT).

To ensure that good data management practices are followed and embedded within BFRS and that regulatory compliance such as the Data Protection Act 2018, which includes UK GDPR, are incorporated.

2 Organisational Responsibility

2.1	This document is intended for viewing by all Elected Members, officers, managers and employees, and where applicable, partners, volunteers and other agencies using the Service facilities. This policy applies to all who handle BFRS information and processing facilities away from the normal designated desk environment. All employees and third-party users must comply with this policy	All users
2.2	The CFO is accountable for data and system security	Principal Officer ...
2.3	The Assistant Chief Officer (ACO) is designated as the Senior Information Risk Owner (SIRO). The SIRO has responsibility for sponsoring and promoting information management and governance policy and ensuring compliance through the Corporate Management Team (CMT) meeting which will act as a governance board. Head of ICT (HICT) is responsible for system security, and the Data Protection Officer (outsourced to Bedfordshire Police) is responsible for data security.	ACO/HICT
2.4	The Information Security Officer is responsible for handling data breaches and notifying the Information Commissioners Office, where appropriate.	ISO
2.5	The Corporate Management Team (CMT) will ensure that staff are provided with education and training to support this policy.	Corporate Management Team
2.6	The ICT Shared Services Team will develop and maintain procedures to achieve compliance with this policy.	ICT Shared Services Team
2.7	All managers are responsible for implementing the policy within their areas of responsibility	All managers
2.8	All users provided with access to information processing tools, systems and facilities must comply with this policy	All users

3 Policy Text

3.1 Information Risk Strategy

The Authority follows a balanced information risk management strategy ensuring mitigation and controls are appropriate to the risk to ensure unacceptably high risks and unnecessarily bureaucratic or expensive controls are avoided.

The Authority maintains formal methods of risk management aligned to business impact assessment and associated business continuity plans.

3.2 Data Management

The objectives of Data Management & Protection are to ensure that:

- The handling of personal and sensitive data complies with Data Protection Act 2018 (DPA 2018) legislation throughout its lifecycle in the Service, from collection, transfer, processing and storage, through to disposal.
- Data captured on BFRS systems is accurate, consistent, comprehensive and timely, providing a solid foundation for data-driven decision making, and appropriate use of Service resources.
- Staff are trained in appropriate conduct regarding data handling and protection and are signed up to Acceptable Use Procedures in respect to transfer or exposure of personal and sensitive data via all communication channels, including email, instant messaging, social media, and chat rooms, both in and outside working hours. This includes data and images held on paper, electronic files on computers, in the cloud, or on storage media such as flash drives and CD/DVD.
- Prompt corrective action can be taken in the event of personal or sensitive data being improperly obtained, transferred, disclosed (data breach), stored and destroyed, whether deliberate or accidental, including:
- Rapid response to premises or system breach.
- Timely response to complaints.
- Investigation into the cause of improper handling or breach.
- Reporting to the Information Commissioners Office if deemed appropriate.
- Disciplinary action if harm is caused to others by improper handling or data breach by any member of BFRS staff.
- Data handling procedures are audited on a regular basis.

3.3 BFRS Personnel

All BFRS staff are required to:

- Co-operate with their employer to ensure the integrity of Information Security policies and procedures are maintained.
- To report Information Security events via ICT Service desk on the BFRS intranet (SharePoint) or telephone the Service Desk on 01954 714269

3.4 Policy Implementation

The Head of ICT is responsible for maintaining the Policy and providing advice and guidance on its implementation.

All managers are directly responsible for implementing this policy within their business areas and for adherence by their staff.

It is the responsibility of each employee to adhere to the policy.

4 People Impact Assessment

No People impact assessment required as this policy update only includes minor changes or consolidation of existing policy's which have not changed to add greater context

5 Review

5.1 This policy will be subject to review at 3 yearly intervals or following significant change to organisational structure, personnel, procedures or legislation etc.

Bedfordshire
Fire & Rescue Service

Service Information System

Polices and Procedures

Document Ref No: V01 07

Version: 2

Reference holder/Owner: Paul Hughes, Head of ICT

Author: Paul Hughes, Head of ICT

Reviewer: Paul Hughes, Head of ICT

Issue date: 25.04.2023

Review date: 01.05.2026

Approved by: HICT