FIRE STANDARD

Title of Standard	Digital and Cyber Security
Business Area/Capability	Enabling
Sponsoring NFCC Committee or Lead	Digital, Data and Technology Committee

Desired Outcome

A fire and rescue service that delivers excellence to the public by using information and communications technology (ICT) safely, effectively and efficiently to deliver prevention, protection and response services. It uses ICT to provide appropriate access to information and facilitate vital communications when and where it is needed, contributing to the safety of communities.

A fire and rescue service whose approach to investment and development of ICT enables it both to meet its statutory obligations to its communities and take proactive steps to maintain sustainable technology and provision of service. That investment will be driven by a clear strategic approach to bring about necessary continuous improvement in using and evaluating technology.

A service which seeks opportunities to contribute to good practice in the sector and beyond, maximising the resources available to them. One that implements appropriate technology, which demonstrates value for money. It has proportionate security controls and enables and educates its employees to use the technology well. It maintains technology in line with good practice, planning for the replacement of assets and solutions before becoming end-of-life.

A service that supports its employees to achieve the level of digital skill necessary to carry out their roles effectively and safely, and to understand their obligations when using technology. Its leaders recognise how critical effective technology is and enables its workforce to fully engage with it.

One that governs and manages cyber security appropriately, balancing the protection of ICT services, assets and data, while making sure that those who need to use ICT have the correct authorisation and permission to do their work. It proactively monitors and mitigates against changing cyber threats and can continue to deliver its duties successfully in the event of a cyber incident. It encourages its people to remain vigilant with respect to such threats and to report any concerns without delay.

To Achieve the Fire Standard

A fire and rescue service **must**:

1. Maintain a continually evolving strategy for implementing and managing ICT to achieve its organisational objectives.
2. Know what its information and digital assets are and publish policies and procedures that protect those assets, including, but not limited to:
    a. Protection from and response to cyber security threats
    b. Lifecycle management for ICT services and assets, aligned to the Procurement and Commercial Fire Standard where appropriate
    c. Acceptable use expectations and obligations
    d. Major incident management and disaster recovery
    e. Procurement and supplier management, aligned to the Procurement and Commercial Management Fire Standard where appropriate
3. Understand its digital and cyber security related risks and put in place controls to manage them, demonstrating good practice in cyber security that meets or exceeds nationally accepted baselines.
4. Ensure that effective organisational security management is led at board level.
5. Align to a cyber security framework as directed by Government, following guidance and tools including relevant cyber security tools provided by the National Cyber Security Centre (NCSC).
6. Deploy and actively maintain security toolsets to safeguard sensitive data, prevent security incidents and ensure the integrity of production status technology, that include at a minimum:
    a. Endpoint detection and response
    b. Secure infrastructure, including firewalls, storage and networks
    c. Multi factor authentication
    d. Privileged identity management
    e. Encrypted transmission (information and communications) where necessary
    f. Assured security where third parties supply elements of ICT service, e.g. software/platform/infrastructure-as-a-service, outsourced infrastructure or desktop management
7. Identify and implement information and communications technologies which support and enhance emergency response capabilities.
8. Deploy mobilisation and incident management solutions that provide efficient co-ordination, communication and resource allocation during emergencies.
9. Provide solutions to connect employees to the information they require to effectively and efficiently undertake their roles, e.g. 4G/5G, wide area networks, local area networks.
10. Provide solutions to connect employees to each other, and to other agencies when required, for effective and efficient voice and data communications as part of their roles.

11. Continually assess security threats and controls to identify vulnerabilities, assess risks and control measures, and implement corrective measures when necessary to maintain or reinstate uncompromised ICT services.
12. Ensure the whole organisation is prepared to continue its essential operations in the event of ICT solution or service failures.
13. Effectively recover its use of ICT solutions or services in the aftermath of a failure, to agreed timescales appropriate to criticality, and periodically exercise such failures, thereafter applying lessons learnt.
14. Ensure all appropriate information assets are backed up and that backups are secure and encrypted.
15. Demonstrate continual development of digital skill to the standard determined necessary for people in their workforce to conduct their duties well.
16. Ensure sufficient ICT skills and roles are available to it, irrespective of governance and delivery model. These skills include but are not limited to:
    a. Technology strategy and ICT service design
    b. Information and infrastructure security
    c. Availability and service continuity management
    d. Fixed and mobile networks management
    e. ICT asset and device management
    f. Management of changes, problems, incidents and service requests
17. Deliver inclusive and accessible ICT solutions and toolsets, recognising that each workforce and community has different and diverse needs.
18. Engage across the organisation to ensure the ICT needs for the whole service are met.
19. Understand the reliance the service places on ICT in the delivery of its statutory duties and provide strategic investment that enables sustainable technology service provision.
20. Adopt the Data Management Fire Standard and Data Management Framework in conjunction with this Fire Standard, to establish clear data governance policies about the responsible and compliant handling of sensitive information held in the service's information and communication technologies.

A fire and rescue service **should**:

21. Adopt Government provided or advocated ICT and cyber security solutions when:
    a. Clear benefits for doing so can be articulated, and
    b. Existing solutions reach the end of their contracted period.
22. When appropriate, and likely to deliver better outcomes for communities and people, collaborate with stakeholders and similar organisations to deliver solutions.
23. Evaluate the ICT services it relies on to ensure the technological solutions and infrastructure remain fit for purpose, and that ICT practices are operated in line with service expectations.
24. Stay informed about emerging technologies and use cases, so that ICT strategy, solutions and processes evolve appropriately, and investment is forward planned.

25. Invest in research or innovation to deliver improved ICT solutions or to improve effectiveness and efficiency within existing ICT solutions.
26. In the interest of cost avoidance and to increase productivity, prevent the use of multiple solutions with duplicated functionality or outcomes, except where an alternative solution is provided to deliver specific requirements, such as enabling accessibility.

A fire and rescue service **may**:

27. Align its ICT services to ITIL®4 practices or similar recognised best practice frameworks, proportionately implemented in line with the needs of the service.
28. Maintain professional ICT delivery by investing in continued professional development through membership of relevant recognised professional bodies.
29. Work with accreditation bodies or agencies to raise the standards of its ICT delivery and that of its supply chain.

Expected benefits of the achieving the Fire Standard

1) Decreased risk of data breach or data loss
2) Enhanced professionalism and improved competence
3) Improved safety, health and wellbeing of communities
4) Improved quality of service provided to the public
5) Improved trust in and reputation of the service
6) Greater regional and national collaboration leading to increased consistency and reduced organisational risk
7) A more positive working culture generated

Legal Requirements or Mandatory Duties

This Fire Standard reflects legislation which is most pertinent to this topic.

We recognise that fire and rescue services must comply with a broader list of legislation (as amended from time to time) to undertake their duties, which would be applicable to all standards. View the key pieces of legislation which applies to ***all*** Fire Standards.

The Data Protection Act

Copyright, Designs and Patents Act

Computer Misuse Act

Online Safety Act

The Telecommunications (Security) Act

Linked qualifications, accreditations or Fire Standards

Fire Standards:

- Communications and Engagement
- Community Risk Management Planning
- Data Management
- Emergency, Preparedness and Resilience
- Fire Control
- Operational Learning
- Operational Preparedness
- Prevention
- Protection
- Safeguarding
- Procurement and Commercial (in draft)

Guidance and supporting information
National Protective Security Authority guidance: Security-Minded approach to Digital Engineering Open and Shared Data: Adopting a security-minded approach Triage Process - For Publication or Disclosure of Information Establishing information needs (Use Cases) Digitalisation Initiatives - Establishing High-Level Information Need And Management Requirements Developing a Security-Mindedness Approach https://www.security.gov.uk/guidance/secure-by-design/#about-the-secure-by-design-approach https://www.ncsc.gov.uk/ Cyber Essentials Active Cyber Defence (ACD) Cyber Assessment Framework (CAF) Supply Chain NFCC ICT glossary and terminology