LONDON FIRE BRIGADE

Information security policy

Policy number:	**442**
Old instruction number:	**MAN:F005:a1**
Issue date:	**24 August 2006**
Reviewed as current:	**26 February 2020**
Owner:	**Chief Information Officer**
Responsible work team:	**ICT Security**

Contents

Key point summary

- This information security policy provides a framework for the protection of information and ICT resources used to hold and process information.
- The Brigade is committed to ensuring that information, including that relating to its clients, partners and staff, along with the ICT systems and environments used to process, store, display or transmit this information, are appropriately protected against malicious or accidental loss, damage or abuse, commensurate with the risks.
- This policy sets out the mandatory requirements that all employees, contractors including third parties, and managers must follow to make sure the Brigade's information assets are kept appropriately secure. It is essential that all staff familiarise themselves with this policy along with Policy Number 485 - ICT Acceptable Use Policy – and understand responsibilities relevant to their role within the organisation.
- This policy is intended to support and enable the Brigade's existing and evolving ICT including Cloud and digital solutions, as well as mobile and agile methods of working.
- The information security policy has been approved and mandated by the Brigade's Chief Information Officer (CIO) following consultation with heads of service and the Senior Information Risk Owner (Assistant Director, Strategy and Risk) and applies consistently across all parts of the Brigade.
- The CIO owns the information security policy. All queries relating to policy implementation or compliance should be directed to the ICT Security Manager.

1 Introduction

1.1 This document defines the Brigade's information security policy. It provides an agreed framework for the management of the security of the Brigade's information assets and technology environments.

Definition

1.2 The policy is based on ISO/IEC 27001, the British Standard for Information Security Management, and reflects industry good practice.

1.3 It aims to implement and enforce the Brigade's Information Security Strategy.

1.4 The scope of this document is currently limited to ICT-based information security. Policies relating to controls for paper-based records are documented in the Records Management Strategy (policy number 605) and supporting policies and Protective Security Policy (policy number 851).

Purpose

1.5 The information security policy applies to all parts of the Brigade and covers:

- Information.
- Information systems.
- Networks.
- Physical and cloud environments.
- Computers and devices, including laptops, tablets and Corporately-Owned, Personally-Enabled ("COPE") devices.
- As well as staff and manager responsibilities, third party access and access to the Brigade's information beyond the Brigade's environments.

1.6 It defines the Brigade's policy for the protection of its information assets including hardware, software, information/data, information systems, networks, applications, cloud services and shared and managed services.

1.7 This policy – with supporting documents and processes – will ensure that:

- Confidentiality of information is appropriately maintained.
- Integrity of information can be relied upon.
- Availability of information is ensured where and when required.
- The reputation of the Brigade is maintained.
- All applicable laws, regulations and contractual obligations are met.
- The information security responsibilities are established.
- Individual users of the Brigade's ICT resources and third parties, who process information relevant to our business, will be identifiable and accountable for their use of ICT resources .
- Access to the Brigade's ICT resources and information is permitted based on the principle of the "need to know" (or by knowing could reap benefits that are positive for the Brigade).
- The Brigade's Users will be granted the minimum access to ICT applications, systems and services required to fulfil their job function.
- All access to information and ICT resources must be properly authorised.
- The requirements for information security compliance are defined, understood and fully implemented.

2 Objective, position and scope of the information security policy

Information security policy objectives

2.1 The objective of this policy is to ensure that the security applied to the Brigade's information and information systems adequately safeguards and protects those assets, supports our control requirements and maintains our reputation.

2.2 The information security policy reflects the scope, objectives and approach defined in the Information Security Strategy. The CIO approves the Information Security Strategy and Policy.

Compliance

2.3 A fundamental aim of the Brigade's Information Security Strategy is to comply with the latest ISO/IEC 27001 standard for information security in proportion with the risks to its information assets. This is an internationally recognised standard and represents "best practice" within the security industry.

The aim of the Brigade is to comply with the standard and not necessarily to gain accreditation.

2.4 The Brigade will implement security controls following ISO/IEC 27002 Code of Practice for Information Security Controls, as appropriate to the risks.

2.5 The Brigade will assess ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services, and apply controls as appropriate to the risks.

2.6 In response to evolving cyber threats, the Brigade will develop a separate Cyber Security Policy based on good practice advice issued by the National Cyber Security Centre.

2.7 The Cyber Security Policy will be a sub-policy to this Information Security Policy which will establish the objectives for protecting the Brigade against cyber security threats.

2.8 The Brigade will comply with mandatory security standards required to enable connection to external networks in order to meet business objectives.

Scope of information security policy

2.9 The CIO has approved the policy for implementation across the Brigade, and has responsibility for the ownership and communication of the policy.

2.10 The CIO will put in place arrangements to monitor policy implementation, verify the level of compliance and will ensure that heads of service respond promptly to any security incident or audit report that highlights a risk to the security of information or information systems, to ensure that remedial action is taken.

2.11 The information security policy addresses the following areas:

- Responsibilities and accountabilities.
- Laws and regulations.
- Information security incident management.
- Access and authorisation.
- System design.
- Development environment.
- Production systems and networks (on-premise and Cloud).
- Mobile devices and remote working.
- Asset management.
- Third party access.

- Business continuity management.
- Education, training and awareness.
- Technology.

2.12 The policy has been derived from:

- Brigade business requirements.
- Legal and regulatory requirements.
- ISO/IEC 27001 British Standard for Information Security Management.
- Brigade ICT security documentation and practices.

2.13 The following controls will be implemented:

- Specific policies will be developed to address particular issues relating to legal, regulatory or technology requirements that have an impact on information security within the Brigade.
- A formal process of risk management will be employed to ensure that information assets are protected in a manner appropriate to their sensitivity, value, and criticality.
- A business continuity management process will provide protection to the availability of Brigade business critical activity.
- Staff will be provided with information security education and awareness training and supporting awareness material to enable them to effectively protect and manage Brigade information assets; be vigilant to threats that exploit the human factor; and prevent security incidents.
- An information security incident reporting procedure will enable all staff to report security incidents, software malfunctions, viruses, faults, weaknesses or threats observed or suspected that pose a risk to systems or services.
- A security incident management process will ensure preparedness for incidents as well as a timely and effective response to and recovery from incidents and learning from incidents to implement security improvements.
- Information security policy and supporting documentation (procedures and principles) exist to ensure that, in conjunction with the process of risk management, appropriate controls are implemented to enable information assets and information systems to be adequately protected.
- Policy number 485 - ICT Acceptable use policy – sets out the rules for the use of the Brigade's ICT resources.

Cyber Security

2.14 LFB must be prepared to prevent, detect, respond to and recover from cyber attacks. The CIO shall develop the Cyber Security Policy that defines objectives and guidelines for LFB's cyber security based on existing and emerging standards and guidelines published by the National Cyber Security Centre (NCSC). The scope of the Cyber Security Policy shall include:

- Secure configuration.
- Network security.
- Malware prevention.
- Cyber incident management.
- Monitoring.
- Removable media controls.
- Home and mobile working.

3 Policy compliance, measurement, dispensation and risk management

Responsibility for compliance

3.1 Directors and heads of service (including assistant directors and assistant commissioners) are responsible for ensuring the implementation of, and compliance with, the information security policy. In order to achieve compliance, heads of service must ensure that the appropriate knowledge, skills, resources and expertise are available to enable staff to meet the security requirements of the Brigade.

3.2 Compliance with the information security policy is an ongoing process incorporating:

- Implementation.
- Dispensation.
- Measuring compliance.
- Reporting.

Implementation

3.3 Implementation is ongoing, with compliance to the information security policy being mandatory for all staff, contractors, third parties and suppliers

Dispensation

3.4 Non-compliance with this policy is permitted only where approved by the CIO, in consultation with the SIRO if appropriate. Dispensations are temporary and must be viewed in terms of impact, risk and duration. The CIO may only approve them if they are considered acceptable and appropriate. Dispensations will be reviewed as part of the ongoing compliance measurement process.

Measuring compliance

3.5 The Brigade's internal audit service (currently provided by the Mayor's Office for Policing and Crime) will audit compliance on a periodic basis. This process will also be overseen by the Director of Corporate Services, the Chief Information Officer the Assistant Director, Finance and the SIRO if appropriate.

3.6 Any non-compliance with policy, highlighted by compliance reviews, dispensations, audit findings or security incidents, will be reviewed by the CIO and shared with the SIRO as appropriate.

3.7 Where appropriate, non-compliance with the information security policy will be assessed by the SIRO to ensure that the risks to Brigade information and ICT resources are known, understood and formally accepted.

3.8 The SIRO will maintain a record of Brigade information security risks.

Risk management

3.9 The CIO will carry out security risk assessment(s) in relation to the business process covered by this policy, as is deemed necessary. These risk assessments will cover all information systems, applications and networks/cloud environments that are used to support those business processes. The risk assessment will identify proportionate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

Type of risk assessment

3.10 Risk assessments will be conducted using an appropriate risk assessment methodology.

Policy statements

4 Responsibilities and accountabilities

Information security roles

Chief Information Officer (CIO)

4.1 The CIO is responsible for the following information security matters:

- The effective implementation of a Brigade-wide framework for managing information security.
- Ownership, development, maintenance and communication of the information security policy.
- The development of Brigade-wide information security strategy and architecture in line with Brigade business requirements.
- Providing an interface between Brigade and external regulatory and industry bodies in relation to all aspects of information security.
- Reviewing and challenging any non-compliance with the information security policy as highlighted by compliance reports, dispensations, audit findings or the incident management processes.
- Overseeing the implementation of Information Security and risk management strategy/policy.
- Maintaining the IT business continuity plan and IT disaster recovery plan.
- Approving system security policies for the infrastructure and common services.
- Approving tested systems and agreeing rollout plans.
- Reporting to the SIRO on matters relating to information risk as appropriate.
- Representing the Brigade on matters relating to information security.

ICT security manager

4.2 The ICT security manager is responsible for:

- Assisting the CIO in the functional management of information security and compliance with this policy.
- Building and maintaining the information security management system.
- Providing support, advice and guidance to facilitate the implementation of the information security policy, this will include:
  - Policy compliance.
  - Security alerts and incident investigation.
  - Information security education, awareness and training.
  - Security of external service provision.
- Information security input into the IT business continuity plan and IT disaster recovery plan.
- Participating in and reporting to the CIO on matters relating to information security.
- Representing the Brigade on matters relating to information security.
- Ensuring that risks to information systems are reduced to an acceptable level by applying proportionate security countermeasures identified through risk assessments.
- Ensuring that access to the organisation's assets is limited to those who have the necessary authority.

Data Protection Officer

4.3 The Brigade's Data Protection Officer is responsible for:

- Ensuring that the Brigade's data protection law notification is maintained.
- Dealing with enquires in relation to UK GDPR and the data protection law, including handling subject access requests.
- Advising users of information systems, applications and networks on their responsibilities under the data protection law, including subject access and ensuring the a data protection impact assessment is carried out for projects and system changes.
- Advising the Commissioner, as appropriate, on breaches of data protection law and the recommended actions.
- Monitoring and checking compliance with UK GDPR and the data protection law.
- Liaising with external organisations on data protection matters.
- Promoting awareness and providing guidance and advice on UK GDPR and the data protection law as it applies within the Brigade.

The SIRO

4.4 The SIRO is responsible for:

- Information risk across the Brigade, supported by the CIO and heads of service.
- The escalation of any significant risk or non-compliance to the Commissioner's Board.
- In conjunction with the Assistant Director, Strategy and Risk and the CIO ensuring that Business Contingency Plans (BCP) and IT Disaster Recovery (IT DR) plans respectively are developed implemented and tested to protect all critical information, information systems and functions of the Brigade.
- Maintaining the Brigade's corporate risk register

Internal audit service (currently provided by the Mayor's Office for Policing and Crime)

4.5 The Brigade's internal audit service (currently provided by the Mayor's Office for Policing and Crime) is responsible for Monitoring the level of compliance with the information security policy.

Information governance group

4.6 An information governance group, made up of heads of service or their nominees, shall have oversight of this information security strategy.

Business owner

4.7 The business owner is responsible for:

- The protection and use of the data.
- Safeguarding the confidentiality, integrity and availability of the data.
- Ensuring that due care is taken to protect the data from any negligent acts that result in the corruption or disclosure of the data.
- Creating data and allowing access to it.
- Deciding the security classification of the data.
- Managing a particular individual or end-to-end system, network and/or service.
- Referring business requirements for Internet-based applications and services (Software as a Service (SaaS)) to the Head of ICT Business Engagement.

IT end user

4.8 Staff, contractors and third parties (for example, suppliers) who are users of Brigade ICT resources and information are responsible for:

- The security of the Brigade's ICT resources and information.
- Operating only within the scope of their job function.
- Only accessing the systems they are authorised to use.
- Safeguarding the hardware, software and information in their care.
- Following policy requirements and guidance issued relating to security, including the ICT Acceptable Use Policy (policy number 485).
- Preventing the introduction of malicious software on the organisation's Information systems.
- Reporting any security incident or suspected breach of the information security policy.
- Ensuring that they are aware of their information security responsibilities, relevant to their job function.

Heads of service (assistant directors and assistant commissioners)

4.9 In addition to their individual security responsibilities, heads of service are responsible for:

- Ensuring that the security of the organisation's assets, information, hardware and software used by staff and, where appropriate, by third parties is consistent with legal and management requirements and obligations.
- Implementing the information security policy within their area of responsibility.
- Ensuring that their staff are aware of their information security responsibilities.
- Developing a security risk aware culture within the Brigade that embraces security.
- Ensuring that all business systems and services have a nominated business owner.
- Ensuring that a risk assessment is performed for all new business systems and services, and for major changes to existing business systems and services, to ensure that they comply with the information security policy.
- Reporting to the SIRO on matters relating to information risk as appropriate.
- Informing the CIO of all new developments to ensure the correct implementation and use of information security mechanisms and procedures.
- Ensuring that their staff have the appropriate skills, expertise and training to enable them to perform their security responsibilities.
- Reporting any security incident or breach of the information security policy that presents a risk to the security of information or systems.

Assistant Director, Finance

4.10 The Brigade's internal audit function, currently provided by the Mayor's Office for Policing and Crime, in agreement with the CIO, is responsible for:

- Undertaking a programme of audits designed to verify the Brigade's compliance with:
  - Legal and regulatory controls in respect of information security.
  - Information security policy.
  - Best practice guidelines.
- Reporting findings and recommendations to senior management.

Ownership and accountability

4.11 All information assets shall have a nominated business owner.

4.12 The business owner is accountable for ensuring that the information assets they are responsible for comply with the information security policy, in particular:

- The confidentiality, integrity and availability of the information processed, stored, displayed or transmitted, is maintained commensurate to its sensitivity and criticality as established via the risk assessment process.
- ICT service providers (both internal and external), are aware of the business specific security and control requirements, and that these are agreed and formally signed off by the CIO.
- ICT systems and services meet the requirements of the business, as defined within an appropriately documented set of requirements and/or service agreements.
- The security measures and controls surrounding a business system and its associated information are suitable and effective.
- Accountability for any associated security risk is accepted and signed off.
- A documented agreement exists in order to control and manage the activities of internal or external service providers in accordance with the information security policy.

Business requirements for cloud-based applications and services (Software as a Service (SaaS)) must be referred by the business owner to the Head of ICT Business Engagement in the first instance. Potential SaaS solutions will be subject to a detailed security and governance review prior to product evaluations taking place.

5 Laws and regulations

Legal and regulatory compliance

5.1 All information systems used to process, store, display or transmit Brigade information shall always operate in accordance with applicable laws and regulations.

5.2 The CIO will ensure the development and review of specific information security policies to address issues that may have a legal or regulatory impact on the Brigade.

5.3 The Brigade's General Counsel will formally review and approve all such policies.

5.4 The legislation relevant to the Brigade includes and is not limited to:

Act	URL Links
General Data Protection Regulation (EU)	https://gdpr-info.eu/
Data Protection Act, 2018	http://www.legislation.gov.uk/ukpga/2018/12/contents
Copyright Designs and Patents Act. 1988	http://www.legislation.gov.uk/ukpga/1988/48/contents
Computer Misuse Act, 1990	http://www.legislation.gov.uk/ukpga/1990/18/contents
Police and Criminal Evidence Act, 1984	http://www.legislation.gov.uk/ukpga/1984/60/contents
Terrorism Act 2000, Terrorism Act 2006	http://www.legislation.gov.uk/ukpga/2000/11/contents http://www.legislation.gov.uk/ukpga/2006/11/contents
Communications Act 2003	http://www.legislation.gov.uk/ukpga/2003/21/contents
Malicious Communications Act 1988	http://www.legislation.gov.uk/ukpga/1988/27/contents
Human Rights Act, 1998	http://www.legislation.gov.uk/ukpga/1998/42/contents
Freedom of Information Act, 2000	http://www.legislation.gov.uk/ukpga/2000/36/contents
Regulation of Investigatory Powers Act, 2000	http://www.legislation.gov.uk/ukpga/2000/23/contents
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000	http://www.legislation.gov.uk/uksi/2000/2699/contents/made
Defamation Act 1996	http://www.legislation.gov.uk/ukpga/1996/31/contents
Obscene Publications Act 1959 Obscene Publications Act 1964	http://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents http://www.legislation.gov.uk/ukpga/1964/74/contents
Protection of Children Act 1978	http://www.legislation.gov.uk/ukpga/1978/37/contents

6 Information security incident management

Preparing for information security incidents

6.1 The CIO will ensure that policies and procedures are in place in preparedness for information security incidents in order to minimise adverse impact on the Brigade's business operations.

6.2 A structured approach exists to detect, report and assess information security incidents.

6.3 In the event of a security incident occurring, tested procedures are in place that will facilitate prompt response and recovery, in conjunction with business continuity processes where appropriate.

6.4 Response and recovery processes will be reviewed, developed and tested, as appropriate, in response to emerging threats.

6.5 Security incident response plans shall enable the reporting of incidents to the authorities and data subjects within statutory timescales.

Responding to information security incidents

6.6 Operating procedures exist to assist specialist staff in responding to an incident and recovery activities.

6.7 Staff involved in investigation into security incidents, recovery procedures and collection of evidence are appropriately trained.

6.8 Evidence gathered in responding to an incident is reliable and legally admissible.

6.9 Crisis activities are instigated for incidents that can not be quickly contained or controlled.

Post-incident

6.10 The costs arising from an incident are reported, including the cost of both responding to the incident and the damage caused by its impacts.

6.11 Lessons are learnt and improvements implemented where appropriate, cost-effective and proportionate, with the aim of preventing recurrence.

7 Access and authorisation

Logical access

7.1 Brigade Policy 869 - ICT Access Control – sets out policies that ensure logical access to information and systems is protected and controlled commensurate with associated risks to ensure that information and information processing facilities are available where and when required by those authorised to have access.

Physical access to ICT resources

7.2 The CIO in conjunction with the heads of service will ensure that all ICT resources used to process, store, display or transmit Brigade information shall be physically protected by suitable mechanisms or methods in order to minimise the risk of malicious damage, tampering and unauthorised use. The Assistant Director, Technical and Commercial has responsibility for building security.

7.3 The level and stringency of security facilities used to achieve this shall be determined by risk assessment.

7.4 Appropriate assurances relating to physical security shall be obtained in respect of Cloud providers processing the Brigade's sensitive data.

8 System design

8.1 The business owner with the CIO will ensure that systems have been appropriately designed to incorporate the controls necessary to meet Brigade information security requirements. The level and stringency of these controls must be commensurate with the sensitivity, criticality or value of the business process and associated data.

8.2 Systems, which are unable to meet Brigade information security requirements, shall not be approved for use and will therefore be required to either:

- Be redesigned and amended so that they comply with the requirements of the information security policy.
- Meet the conditions of the dispensation process outlined in section 3 - policy compliance, measurement, dispensation and risk management.

8.3 Information systems must incorporate the controls necessary to meet the information security requirements of the Brigade. To facilitate this, the following areas of control must be formally considered during system design:

- Technical security architecture.
- Risk assessment outcomes.
- Access and authorisation.
- Protection of data in transit and at rest.
- Input and output processing controls.
- Monitoring and audit logging.
- Contingency.
- Production of appropriate documentation, e.g. security profile, operational procedures, security standards.
- Connectivity controls.
- Current and emerging security standards and legal, regulatory, compliance and contractual requirements.
- Design and configuration guidance published by the National Cyber Security Centre.
- Cloud solutions shall be designed with consideration to the Cloud Security Principles.

8.4 When designing a new system or enhancing an existing one, the business owner must assess the impact that this development or enhancement will have on the overall business process, system design and interfaces. Appropriate data protection and privacy controls must be integrated at the design stage and throughout the development life cycle, in compliance with UK GDPR and data protection law principles and requirements.

8.5 The CIO may require checks on, or an audit of, actual implementations based on the information security policy.

9 Development environment

9.1 The CIO will manage and control the ICT technical environment, in which systems are developed, established, tested, enhanced or maintained, to ensure that products incorporate appropriate security controls and function as required by the business owner.

9.2 The level and stringency of these controls must be commensurate with the sensitivity, criticality or value of the relevant business process and associated data, which the system supports.

9.3 Development environments and associated processes, whether in-house or managed by a third party, must incorporate appropriate controls to ensure the security of the systems throughout their development lifecycle.

9.4 This policy applies to the use of all development tools, methodologies and techniques as well as manual procedures surrounding the preparation of all new systems or changes for production implementation. The following areas of control must be formally considered to ensure the security of the development environment:

- Access and authorisation.
- Separation of production, test and development environments.
- Segregation of duties.
- Testing controls.
- Depersonalisation of live data used in test environments.
- Version controls.
- Monitoring and audit.
- Contingency.
- Connectivity controls.
- Specific development methodologies.

10 Production systems and networks

10.1 The CIO will ensure that the security of the Brigade's on-premise and Cloud production systems, networks and associated data is maintained and that:

- All production systems and networks comply with appropriate, documented security and control acceptance criteria for the production environment in which they function, which shall be based on approved risk management recommendations.
- Adequate operating procedures, which detail how the system and network environments are managed, are documented and maintained.
- Change management and version control procedures are implemented to maintain the integrity of the production systems and networks environment.
- A physical and/or logical segregation between the production and non-production systems (e.g. test), is established.
- An appropriate segregation of duties exists to reduce the risk of accidental or deliberate system misuse.
- An effective and timely response procedure for the management of incidents exists in line with the other risk type policies on incident management.
- Capacity planning and IT continuity facilities and processes, ensuring the ongoing, optimum level of system or network performance, are documented and maintained.
- All connections between Brigade networks and externally owned or managed ICT resources or cloud services are documented and formally agreed by the business owner.
- Appropriate administration and monitoring processes to provide assurance as to the security of the operational environment are documented and maintained.
- Appropriate environmental controls exist to support the requirements of the ICT resources.

11 Third party access

11.1 When the management, operation or supply of Brigade information, ICT functions, systems, services or development services are to be undertaken by a third party, in order to manage

associated risks the CIO, with the Assistant Director, Technical and Commercial, must ensure that:

- The risks associated with the third party access and supply chain security are assessed and understood.
- Security considerations are built into third party procurement processes.
- Security requirements to protect information, systems and services are consistent with the information security policy, and are agreed with the third party and incorporated into the contract or service agreement.
- Personal data stored or processed by third parties shall be protected in accordance with data protection law and any guidance issued by the Information Commissioner's Office and the Brigade's policy number 351.
- Third parties providing Cloud-based services to the Brigade should be required to define how security requirements meet each of the National Cyber Security Centre's Cloud Security Principles as appropriate.
- Third party connections must be approved, documented and appropriately secured.
- Third party suppliers are required to provide assurance that agreed security controls are in place and transited through their supply chain where applicable. Third party access to the Brigade's network is approved in accordance with Policy number 824 Third Party Network Access Policy and the third party enters into an agreement that sets out the Brigade's security standards, including compliance with the ICT acceptable use policy.
- Brigade information and assets are protected via an appropriate contract which should include a non-disclosure agreement (subject to the requirements of the freedom of information act).
- Appropriate business continuity plans are developed, tested and approved.
- Security compliance processes are established.
- Due diligence checks are performed to ensure compliance with the information security policy.
- The right to audit compliance against agreed security targets is agreed contractually.
- Penetration testing against agreed security targets is conducted where appropriate.
- Responsibilities and procedures for immediate reporting of and managing security incidents are established between the Brigade and the third party.
- Third party contracts shall set out requirements for deleting the Brigade's data and returning assets, where applicable, when contracts expire or transfer.
- Third party user access is revoked promptly when no longer required.

11.2 Cloud services must be evaluated for compliance with the Brigade's security standards commensurate with the risks presented.

11.3 Where the Brigade enters into shared service arrangements requiring access by the shared services partner to the Brigade's network, policies applicable to third party access shall apply.

11.4 Third party/outsourcing proposals that are unable to meet the appropriate Brigade security requirements shall not be approved.

11.7 A risk assessment must be used to ascertain the level of risk associated with outsourcing a system or service, and to ensure that the appropriate level of security controls are implemented to safeguard the Brigade information / information system.

11.8 Based upon the outcome of the risk assessment the approval to outsource must then be obtained from the relevant head of service, in conjunction with the CIO and the Assistant Director, Technical and Commercial.

11.9 Security requirements for outsourced systems and services must be clearly specified and agreed with the supplier.

12 Business continuity management

Business continuity management

12.1 The Assistant Director, Strategy and Risk has a responsibility to ensure that there is an effective enterprise-wide business continuity plan (BCP) in place for the Brigade.

12.2 This will incorporate an ICT Business Continuity Plan (ICT BCP) and ICT Disaster Recovery (ICT DR) Plan (for which the CIO has responsibility).

12.3 These plans should ensure:

- That the strategy for business continuity and IT disaster recovery are clearly documented and understood.
- The continuity of critical business functions and provides rapid recovery to reduce the overall disruption of a disaster or a disruption.
- That ICT DR provides procedures for emergency response, extended backup operations, and post disaster recovery.
- That a process of risk management is used to produce a formal business impact analysis.
- That a programme of BCP and ICT DR education, training and awareness is implemented to communicate its requirements and procedures to staff.
- BCP and ICT DR plans are tested and updated on a regular basis, with a minimum requirement being an annual test.

13 Information security education, training and awareness

Education, training and awareness

13.1 The CIO will maintain an information security education, training and awareness programme.

13.2 The programme will deliver appropriate and cost effective methods for delivering the necessary awareness and training to all levels of staff.

13.3 Heads of service are responsible for ensuring that their staff receive information security training to an appropriate level for their job role and for making sure that all staff are aware of their responsibilities for information security, and the actions that they need to undertake in order to discharge those responsibilities.

13.4 Each member of staff should understand the importance of information security to the Brigade and be made aware of their responsibilities and the consequences of non-compliance with the information security policy which could lead to disciplinary action being taken under the Brigade's disciplinary procedures, which could result in action up to and including dismissal.

14 Use of technology

Technology

14.1 Technology solutions used to process, store, and display or transmit Brigade information, whether internally or externally sourced, must be appropriately controlled and users of those systems must understand what is acceptable and proper behaviour.

14.2 The CIO will ensure the development and review of specific policies governing the use of technology; in order to provide continued protection of ICT resources and data, against threats associated with the changing use of current technologies and the emergence of new technologies.

14.3 In particular these policies will cover:

- General computer use.
- Protecting personal data and other sensitive data, including the use of security classifications in documents (refer to policy number 619 LFB Security Classifications System).
- Use of electronic communication, including email.
- Use of the Internet and Cloud services.
- Use of digital services.
- Acceptable standards of behaviour when using ICT equipment and systems.
- Policies relating to personally owned equipment.
- Use of mobile devices and supporting security controls to protect LFB data.
- Use of Corporately-Owned, Personally-Enabled ("COPE") devices.
- Remote working.
- Use of encryption to protect sensitive information when stored or in transit, or to authenticate users, devices or other system resources.

14.4 The Brigade's acceptable use policies are defined in Policy number 485 - ICT Acceptable Use Policy.

14.5 The CIO will formally review and approve all such policies following consultation with heads of service and the SIRO.

Appendix 1 – Glossary of terms

Term	Definition
Acceptable use	Describes the ways in which ICT resources can and cannot be used.
Dispensation	A temporary exemption from compliance with the information security policy granted by the CIO.
Cloud computing or Cloud	Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand.
Compliance	The security controls meet the requirements defined in the information security policy.
Cyber attack	Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks, devices or information, often via the internet.
Cyber incident	A breach of the security rules for a system or service - most commonly: • Attempts to gain unauthorised access to a system and/or to data. • Unauthorised use of systems for the processing or storing of data. • Changes to a system's firmware, software or hardware without the system owners' consent. • Malicious disruption and/or denial of service.
Cyber security	The protection of devices, services and networks, and the information processed by them, from theft or damage.
Denial of Service	When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.
Formally consider	To "consider formally" embraces the use of risk assessment techniques to ascertain the appropriate level of security control to be applied.
ICT resources	'ICT resources' refers to all technical ICT components that store, process, display or transmit Brigade information. This includes; networks, servers, workstations, software, monitors, backup media, telephony, faxes, video conferencing, printer's etc.
Least privilege	A process has the minimum level of privilege required to perform its functions.
Need to know	A principle by which information is only provided to those with a legitimate need for that information.
Non compliance	Failure to adhere to the minimum security controls defined in the Information Security Policy.
On-premise	Installed on computers on our premises.
Policy	The mandatory rules as defined by the CIO that govern the management of Brigade information and information systems. The Brigade's information security policy defines the minimum security controls that must be adhered to.

Term	Definition
Practices	Practices support adherence to the policies, by providing a detailed framework of security and control techniques and guidance that should be used to help the business and project management to design appropriate security and control facilities.
Procedures	These provide prescriptive guidelines for specific system, service and component implementations. They will be used by ICT operational and support areas and end users to support and operate the implemented controls.
Risk assessment	Risk assessment is a formal method of identifying and assessing the possible damage that could be caused in order to justify security safeguards. The cost of the safeguards should not be greater than the value of the asset it's protecting.
Risk management	A management process used to identify, assess and reduce the level of risk to an acceptable level and to implementing the appropriate controls to maintain that level of risk. Risk assessment is used as part of the risk management process to determine the level of risk associated with systems, services or processes. Standards, practices, procedures and the Technical Security Architecture are then used to defining the detailed controls necessary to mitigate the identified level of risk.
Software as a Service (SaaS)	Software that is deployed over the Internet.
Staff	Refers to all Brigade staff and individuals whether permanent, temporary, contract, 3rd party or outsourced.
Standards	Standards detail the minimum level of security control required to secure a particular ICT resource, component, or environment commensurate with the sensitivity, value and criticality of the information which it processes. Adherence to these standards should ensure compliance to information security policy.
Statement of applicability	Describes how an organisation has interpreted and applied the ISO/IEC 27001 Standard. It maps the ISO/IEC 27001 controls to the results of the risk assessment and provides the basis for the compliance project.
Systems	All ICT resources and ICT applications involved in the storage, processing, display and transmission of information.
Third parties	External companies with whom the Brigade has entered into contractual agreements.
Technical Security Architecture	The technical framework, (e.g. infrastructure), through which the information security policies are implemented.
UK GDPR	The EU General Data Protection Regulation as amended by Schedule 6 of the Data Protection Act 2018 (also known as "The Applied GDPR").

Document history

Assessments

An equality, sustainability or health, safety and welfare impact assessment and/or a risk assessment was last completed on:

EIA	09/12/2019	SDIA	04/09/2019	HSWIA	05/09/2019	RA	

Audit trail

Listed below is a brief audit trail, detailing amendments made to this policy/procedure.

Page/para nos.	Brief description of change	Date
Throughout	Review of policy	20/08/2009
Throughout	All references to Assistant Commissioner Risk replaced by Head of Strategy and Performance. Policy number 485 added to all 'CoPUC' references.	16/11/2009
Throughout	Department names updated in line with the Top Management Review.	25/10/2011
Throughout	Minor changes have been made to this policy throughout.	18/01/2013
Throughout	Policy reviewed as current, minor changes throughout. Protective marking scheme now replaced with security classifications system.	11/07/2014
Section 4	Amendments made through out to replace the incorrect references to L&DS with S&P where appropriate.	01/10/2014
Page 24	SDIA updated.	16/10/2014
Throughout	Reviewed as current with minor changes made throughout.	26/02/2020
Throughout	'GDPR' updated to 'UK GDPR', to correct for the Brexit impacts.	24/06/2021

Subject list

You can find this policy under the following subjects.

Information Technology	Security

Freedom of Information Act exemptions

This policy/procedure has been securely marked due to:

Considered by: (responsible work team)	**FOIA exemption**	**Security marking classification**