LONDON FIRE BRIGADE

Report title

Cyber security policy

Report to	Date
Corporate Services Board Commissioner's Board London Fire Commissioner	30 March 2021 7 April 2021

Report by	Report number
Chief Information Officer	LFC 0514x

Protective marking: **OFFICIAL - Sensitive**
Publication status: Published with redactions
If redacting, give reason: Security

I agree the recommended decision below.

Andy Roe
London Fire Commissioner

Date This decision was remotely signed on 26 May 2021

Executive Summary

The report seeks approval for a new Cyber Security Policy (CSP) which defines objectives and guidelines in relation to cyber security for the Brigade. The policy, designed largely for ICT staff, is designed to provide a basis on which the Brigade provides and maintains a secure environment for its information assets across its ICT estate. This will encompass personnel, physical, procedural and technical controls as needed, and expectation is (e.g. from internal audit) that it is signed off at corporate level.

Recommended decision

For the London Fire Commissioner

That the London Fire Commissioner approves the cyber security policy (attached as an appendix to this paper).

Introduction and background

1. An ever-increasing number of public and private sector organisations are being targeted by cyber-attacks. Successful attacks are often reported widely in the media but many attacks are not reported and therefore the extent of the issue facing all organisations is often not recognised.

2. A successful cyber-attack can have a devastating impact upon an organisation; in some cases, meaning that the organisation is unable to continue to deliver their normal business operations. Depending on the type of organisation, the impacts can range from financial loss, to the inability to discharge their statutory responsibilities.

3. Defences against cyber-attacks, range from dedicated cyber defence systems such as the Brigade's Darktrace Immune System product, to training/awareness initiatives to support 'safe' behaviours by users of all Brigade computer systems.

4. The Brigade has worked with specialist in the cyber-security field to produce a specific policy which outlines the steps it will take to defend the Brigade's ICT infrastructure from cyber-attack.

The cyber security policy

5. The new cyber security policy – which should be read in conjunction with the existing Information Security Strategy (published as policy 443) – s designed largely for ICT staff and the expectation is (i.e. from internal audit) that it is signed off at corporate level. This policy is based on the guidance issued through the National Cyber Security Centre's (NCSC) cyber essentials scheme and "10 steps to cyber security" along with applicable industry best practice.

6. The policy sets out our objectives and approach in relation to cyber defence and covers the following main areas:

    - Information risk management regime
    - Secure configuration of computer systems
    - Management of security and other patches to systems
    - Network security
    - User access control / education and awareness
    - Security Incident management
    - Virus / malware prevention and protection
    - Monitoring the environment
    - Removable media controls (for example, USB)
    - Home and mobile working

7. The new policy has been discussed with the ICT management team and the ICT Security Manager. In addition, the new policy was an agenda item at the inaugural meeting of the ICT Security Forum on 5 March 2021. The policy was circulated to board members for comment/ feedback, and any comments received have been included in the policy.

Objectives and expected outcomes

8. The objective is to put in place a policy that sets out how ICT will implement and manage personnel, physical, procedural and technical controls to ensure that the Brigade mitigates the risk from a potential cyber-attack.

9. Once in place, ICT staff will have access to a defined statement of how they are expected to maintain a secure environment for ICT assets across the estate. In addition, the policy contains a set of policy statements which taken together provide an overarching approach to ensuring that users are kept informed of their responsibilities by ICT staff. This will be via the introduction of

security awareness training, leading to an enhanced security-conscious culture running through the organisation

Impacts

Equality impact

10. The London Fire Commissioner and decision takers are required to have due regard to the Public Sector Equality Duty (s149 of the Equality Act 2010) when taking decisions. This in broad terms involves understanding the potential impact of policy and decisions on different people, taking this into account and then evidencing how decisions were reached.

11. It is important to note that consideration of the Public Sector Equality Duty is not a one-off task. The duty must be fulfilled before taking a decision, at the time of taking a decision, and after the decision has been taken.

12. The protected characteristics are: Age, Disability, Gender reassignment, Pregnancy and maternity, Marriage and civil partnership (but only in respect of the requirements to have due regard to the need to eliminate discrimination), Race (ethnic or national origins, colour or nationality), Religion or belief (including lack of belief), Sex, Sexual orientation.

13. The Public Sector Equality Duty requires us, in the exercise of all our functions (i.e. everything we do), to have due regard to the need to:

    a) Eliminate discrimination, harassment and victimisation and other prohibited conduct.
    b) Advance equality of opportunity between people who share a relevant protected characteristic and persons who do not share it.
    c) Foster good relations between people who share a relevant protected characteristic and persons who do not share it.

14. Having due regard to the need to advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it involves having due regard to the need to:

    a) remove or minimise disadvantages suffered by persons who share a relevant protected characteristic where those disadvantages are connected to that characteristic;
    b) take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it;
    c) encourage persons who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such persons is disproportionately low.

15. The steps involved in meeting the needs of disabled persons that are different from the needs of persons who are not disabled include, in particular, steps to take account of disabled persons' disabilities.

16. Having due regard to the need to foster good relations between persons who share a relevant protected characteristic and persons who do not share it involves having due regard to the need to—

    a) tackle prejudice, and
    b) promote understanding.

17. An EIA has been conducted for the proposed new cyber security policy as this is about the approach to managing cyber security risk at the Brigade which involves interaction with mainly ICT staff. Overall, this EIA has identified a low impact on equality. It did identify a potential impact for those with a learning disability, such as dyslexia or neurodiversity conditions, as the policy is largely text based. The planned mitigation is that the implementation of the policy and the actions required of ICT staff is a collective experience facilitated through conversations, meetings, training, awareness raising and feedback. Naturally, this will include those ICT staff with a learning disability, and they will be engaged with so that the actions that the policy requires are accessible and known to them. We are also exploring alternative ways of conveying policy objectives and actions through different visual presentation methods.

Procurement and sustainability

18. There are no procurement or sustainability implications

Strategic Drivers

19. A healthy cyber security culture is essential for the Brigade as ICT systems and information underpin all Brigade activities and operate in the context of the wider "digitally connected" world.

20. Safeguarding our information and systems from hostile external actors will ensure that the Brigade continues to operate its core systems and will ensure that the Brigade can continue to be *"trusted to serve and protect London"*;

21. The new cyber security policy supports the TDP pillar "**delivering excellence**" by ensuring that all reasonable steps have been taken to defend against cyber threats, protecting Brigade systems from disruption.

Workforce impact

22. The new cyber policy will not have any impact upon the workforce. It is predominantly aimed at ICT staff.

Finance comments

23. This report recommends that the London Fire Commissioner approves the new Cyber Security Policy. The Cyber Security policy does not have any financial implications at this stage, however, should implementation of the policy result in additional costs these should be contained within the current resources.

Legal comments

24. Section 1 of the Fire Services and Rescue Act 2004 ('the Act') provides that the London Fire Commissioner is the fire and rescue authority for Greater London. Under section 5A of the Act, the Commissioner as a relevant fire and rescue authority, may do anything he considers appropriate including anything incidental or indirectly incidental for the purpose of carrying out his functions.

25. The recommendation to approve a new policy is within the powers of the Commissioner.

26. The LFC Scheme of Governance (May 2020) gives delegated authority to the Head of Service to approve ongoing changes to policies and procedures of which they are the designated custodian.

27. This report is presented to the Commissioner following a recommendation from Internal Audit that this matter receive such this level of oversight.

List of Appendices

Appendix	Title	Protective Marking
1.	Cyber Security Policy	Official Sensitive - Security

LONDON FIRE BRIGADE

LFB cyber security

Issue date:	4 February 2021
Reviewed as current:	
Owner:	Chief Information Officer
Responsible work team:	ICT Security Manager

Contents

Summary **8**

Scope and review **8**

Policy scope 8

Other reference documents 8

Policy **8**

Introduction 8

Information risk management regime 9

Secure configuration 10

Patch management 11

Network security, boundary firewalls and internet gateways 11

Managing user privileges and user access control 11

User education and awareness 12

Incident management 12

Malware prevention and protection 13

Monitoring 13

Removable media controls 14

Home and mobile working 14

[redacted]

Assessments **22**

Audit trail **22**

Subject list **22**

Freedom of Information Act exemptions **22**

Summary

This policy document defines the policy objectives and guidelines for London Fire Brigade (LFB) for cyber security. It aims to a provide basis on which LFB provides and maintains a secure environment for its information assets across its ICT estate. This will encompass personnel, physical, procedural and technical controls as needed.

This policy is based on the guidance issued through the National Cyber Security Centre's (NCSC) cyber essentials[1] scheme and "10 steps to cyber security"[2] along with applicable industry best practice.

Scope and review

Policy scope

1. This policy is applicable to all LFB information, information systems, infrastructure and cloud services.

2. This policy applies to services provided by external third-party suppliers.

3. This policy is part of the suite of policies that falls under the information security strategy/policy (Policy number 443 – Information security strategy - and Policy number 442 – Information security policy).

Other reference documents

4. This document references and relies upon several other documents and systems, including:

   (a) LFB information governance arrangements.

   (b) LFB Information Security Management System (ISMS).

   (c) LFB Information Security policy suite including:

      i. LFB ICT AUP (Policy number 485 – ICT acceptable use policy).
      ii. NCSC cyber essentials scheme.
      iii. NCSC 10 steps to cyber security.
      iv. ISO 27001, 27002 and 27017.

Policy

Introduction

5. This policy establishes the objectives for the operation, control and protection of LFB's ICT against cyber security threats. It makes statements to provide adequate governance arrangements, risk management processes and information assurance policies and processes to meets its business needs, in order to defend its business from cyber security threats.

6. In line with NCSC's cyber essentials scheme, LFB will implement controls aligned with the cyber essentials (CES) scheme and the "10 steps to cyber security" (10 steps):

   (a) Information risk management regime (10 steps).

[1] NCSC Cyber Security Essentials available here
[2] NCSC 10 Steps to Cyber Security available here

(b) Secure configuration (CES and 10 steps).

(c) Patch management (CES and 10 steps).

(d) Network security (10 steps) and boundary firewalls and internet gateways (CES).

(e) Managing user privileges and user access control (CES and 10 steps).

(f) User education and awareness (10 steps).

(g) Incident management (10 steps).

(h) Malware protection (CES and 10 steps).

(i) Monitoring (10 steps).

(j) Removable media controls (10 steps).

(k) Home and mobile working (10 steps).

7. These are detailed in the following policy statements.

Information risk management regime

Introduction

8. In order to support the business of the London Fire Brigade, the organisation needs access to quality information. Risks to that information that could compromise it are to be mitigated to a proportionate level.

9. This section establishes policy statements for an effective information risk management regime which are in line with industry good practice and which aim to minimise the potential impact of a breach of information and ICT security on operational and support services.

Policy

10. LFB will operate an effective information governance regime across the organisation, complemented by an Information Systems Management System and an appropriately detailed and well-communicated suite of information assurance policies. Risk assessments will be made as appropriate and risk treatment steps made to mitigate the risks.

11. The LFB senior management will be committed to, and demonstrate, effective support of the governance arrangements.

12. LFB's Chief Information Officer (CIO) will make sure that the information governance arrangements are communicated to all LFB staff and contractors and that compliance measures are put in place to ensure their effectiveness.

13. All information assets will, in the future, be assigned an Information Asset Owner (IAO) at Head of Service (HoS) level, responsible for ensuring the risks to the asset are effectively managed. IAO roles will be developed accordingly. Digital Information Assets will be jointly owned by the HoS and the CIO.

14. All information assets will be documented in an Information Asset Register (IAR) maintained by the CIO.

15. The state and configuration of all LFB IT systems will be documented in a system configuration management database.

16. This system configuration management database will be maintained and updated in line with any changes to IT system configuration anywhere in the LFB ICT estate.

External standards and accreditation

17. LFB is due to replace its current mobilising system by 2024, with contingency to run until 2026 . LFB will ensure that the replacement mobilising system is compliant with its standards for cyber security and shall specify that the full scope of the solution must be Cyber Essentials Plus and ISO27001 certified.

18. For its other information systems, LFB is committed to monitoring the replacement of its remaining legacy business applications and progress of actions to fully comply with the Cyber Essentials standard. LFB aims to achieve Cyber Essentials Plus certification when compliant against the standard.

19. LFB's Information Security Policy follows the ISO 27001 standard. LFB is currently focused on achieving Cyber Essentials and Cyber Essentials Plus compliance and certification. Once this is achieved, LFB will consider and assess the actions to achieve ISO27001 compliance for its information systems and will consider certification, subject to budget and resource considerations.

Secure configuration

Introduction

20. By identifying baseline technology builds and following configuration management processes LFB will be able to ensure that any ICT deployed by the organisation is suitably protected from security threats. Disabling or removing unnecessary functionality and following processes to quickly fix known vulnerabilities form a core part of secure configuration and help to minimise the risk of compromise of LFB systems and information. This section includes a set of policy statements providing the overarching policy to be followed when developing processes for configuration of LFB ICT equipment.

Policy

21. All LFB-managed ICT is configured in a secure manner suitable for the needs of the organisation. Contracts with third parties, including Software as a Service (SaaS) and outsource suppliers stipulate appropriate controls for any systems or services processing LFB's information and/or interfacing with LFB systems and that those systems and services must be maintained in a secure configuration.

22. LFB's Microsoft 365 services are configured in accordance with good practice guidance published by Microsoft and NCSC.

23. LFB's ICT (and outsourced ICT) will be developed such that unnecessary functionality is removed or disabled. An approach will be developed to identify baseline technology builds and best practice configuration management processes followed.

24. Known and emerging vulnerabilities are fixed quickly to bring systems back into a secure configuration resistant to security vulnerabilities.

25. The CIO will establish, document, implement and review a set of operating procedures for all information processing and communication systems.

Patch management

Introduction

26. Any software programme can contain weaknesses or flaws referred to as technical vulnerabilities which can be exploited by threat actors to attack the system on which the software is installed. Vendors typically attempt to provide fixes for identified vulnerabilities for any software they provide (assuming the software is still being supported) and release them as soon as possible to their customers as software patches. By patching any software in use across the LFB ICT estate the threat posed by those looking to exploit software vulnerabilities can be minimised. The following section contains policy statements that will be used to govern the overarching approach taken by LFB in managing the patching of systems across the LFB ICT estate.

27. Supported versions of software are used and that these are kept up to date with necessary patches as supplied by the vendor.

28. Where unsupported or legacy systems and/or software need to be operated for essential business purposes a risk assessment will be made and other mitigating controls will be applied to protect the system and its utility to LFB.

Network security, boundary firewalls and internet gateways

Introduction

29. The connections between LFB networks and the internet or other external networks provide great opportunities for data exchange, but also open avenues by which threats can access LFB systems. To reduce the likelihood of such threats successfully compromising any system managed by or for the LFB a series of policies and architectural and technical responses should be utilised. This section includes a set of policy statements describing the high-level controls required to ensure that LFB networks are sufficiently secure.

Policy

30. LFB's network and cloud infrastructure is designed to have a robust security architectural framework based on best practice and NCSC guidance.

31. LFB's networks and cloud services are well configured and boundary firewalls and internet gateways are used across the LFB ICT estate. LFB will approach network security in a holistic manner ensuring appropriate controls are applied both at boundaries between systems and within LFB networks. LFB networks will be segregated from the internet via control barriers (firewalls, malware detection, DMZs etc.) as needed with no direct routing between internal systems and external networks.

Managing user privileges and user access control

Introduction

32. By ensuring that users are provided with appropriate system privileges and data access rights the impact of potential misuse or account compromise can be minimised while still allowing users access to the services they require. Regularly reviewing access rights across all LFB managed systems and cloud services will help the organisation to minimise the risk of attack by a threat actor using credentials that need not have been active. This section contains a set of policy statements designed to provide an overarching approach to managing user access privileges that provide an appropriate balance between accessibility and security for LFB.

Policy

33. Users are only given access to systems as required by their role and the level of access to these systems given to users is appropriate.

34. Privileged access permissions are periodically reviewed and amended as needed.

35. Staff who leave, have their accounts disabled. Any leaver must return all LFB assets to LFB.

User education and awareness

Introduction

36. To ensure that LFB ICT is used in a secure manner it is imperative that users are kept informed of their responsibilities. This can be achieved through the delivery of awareness training supported by a security-conscious culture running through the organisation. This section contains a set of policy statements designed to provide LFB with an overarching approach to delivering security awareness training to users.

Policy

37. All users are given regular (annual) cyber security awareness training.

38. Policy number 485 – ICT acceptable use policy describes the acceptable use of LFB's systems. Primary use of LFB's ICT is to carry out the business of LFB, although personal use is allowed as stated in the ICT acceptable use policy.

39. Security related roles (such as system administrators, and incident management team members) are provided with appropriate specialist training.

Incident management

Introduction

40. In the event of a security incident, it is important for the LFB to have structured procedures in place that can be followed to mitigate any potential impact on LFB operations. Without such procedures, the likelihood of a major breach in confidentiality or significant system downtime increases considerably. The following section contains a set of policies designed to ensure that LFB security incident management processes improve the resilience of the organisation to potential security incidents.

Policy

41. Security incident management procedures are implemented to supplement the incident management procedures in use by the LFB Service Desk. These procedures will aim to:

    (a) Minimise business harm.

    (b) Ensure that the root cause of an incident is identified and addressed.

    (c) Reduce the risk of a breach of legal and regulatory reporting requirements.

42. An incident response and disaster recovery capability is established that addresses the full range of incidents that can occur. All incident management plans (including disaster recovery and business continuity) will be regularly tested on a two-year rolling programme.

43. The incident response team receives specialist training as needed across the range of technical and non-technical areas required to support LFB business.

44. Any Cyber-crimes that significantly impact LFB operations are reported to the relevant law enforcement agency (Metropolitan Police, GLA, NCSC) to help the UK build a clear view of the national threat and deliver an appropriate response.

Malware prevention and protection

Introduction

45. Malware (malicious software) is an umbrella term describing any code or content that may have a malicious undesirable impact on a system causing anything from localised data loss to significant network downtime. It is important for the organisation to protect its ICT infrastructure using anti-malware measures. The following section contains a set of policy statements describing a high-level, pragmatic approach to protecting LFB ICT infrastructure from malware intrusion and the associated damage such intrusion can cause. It is LFB policy that it will protect all of its ICT assets from malware using reputable and effective solutions. The CIO will ensure that virus and malware protection is installed across the ICT estate and is kept up to date.

Policy

46. Boundaries to the Internet are protected, in particular, from malware attacks. All information supplied to or from LFB will be scanned for malicious content.

47. Staff are well educated to detect and takes steps to control social media malware attacks, phishing emails and the like.

48. Scanning for malware occurs across the organisation and protects all host and client machines with antivirus solutions that will actively scan for malware.

49. Malware protection logs are reviewed to detect trends and changes in threat profiles and make appropriate adjustments and improvements as needed.

Monitoring

Introduction

50. System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. By gathering data on system events and compiling it using a performance monitoring tool common patterns of network activity can be determined and deviations from these patterns flagged for further consideration. Any major issues can more quickly be identified, and incident management processes invoked. This helps to minimise the risk of data loss and allows regulatory compliance to be ensured. The following section contains a set of policy statements describing the principles that should be behind the LFB Protective Monitoring Policy which will sit below this Cyber Security Policy.

Policy

51. Darktrace is used to monitor the LFB network with alerts set in place via various thresholds. The tool is appropriately configured and regularly adjusted. Darktrace's SOC team is available 24/7. Security reports are provided on a periodic basis to LFB.

52. The CIO will evaluate the establishment of an estate wide Security Incident and Event Management system (SIEM.

53. The use of LFB ICT equipment and networks will be monitored to detect any actual or attempted attack on LFB systems and ensure that LFB systems are operated in line with organisation policy.

54. Protective monitoring controls will be based on NCSC guidance such as:

    https://www.ncsc.gov.uk/collection/cyber-security-design-principles/making-compromise-detection-easier. The exact specification and mechanisms will be described in other supporting policies and will take into account any previous security incidents and attacks. LFB will ensure that it continuously monitors inbound and outbound network traffic to identify unusual activity or trends that could indicate attacks and the compromise of data. LFB will monitor all ICT systems using Network and Host Intrusion Detection Systems (NIDS/HIDS) and Prevention Systems (NIPS/HIDS).

Removable media controls

Introduction

55. In addition to connections to third party networks, removable media presents another avenue through which LFB ICT infrastructure could be infected/LFB data compromised. While the use of removable media is likely to be required for some organisational functions applying appropriate security controls to its use can significantly reduce the risk presented by such media to LFB ICT infrastructure. The following section contains a set of policy statements designed to provide high-level controls to the use of removable media within the LFB.

Policy

56. Removable media will only be allowed using approved devices. Access to media ports is disabled by default and only enabled for authorised use.

57. Removable media must be issued by LFB, data stored on the removable media must be encrypted and the removable media returned when no longer required.

58. Where information exchange is required for business purposes this will be controlled:

    (a) Using LFB media.

    (b) Using encryption to protect the business information on the media.

    (c) By scanning for malware on export and/or import to LFB.

    (d) Where backup tapes are used, they will be subject to strong physical controls and transported and stored by a reputable storage management company.

Home and mobile working

Introduction

59. Home and mobile working expose the data of LFB to risks and risk vectors in addition to those associated with working at an LFB site. As such these risks must be managed and mitigated to minimise the likelihood of an accidental breach in confidentiality. The following section contains a set of policy statements that describe high-level controls to be implemented by LFB for home and mobile working.

Policy

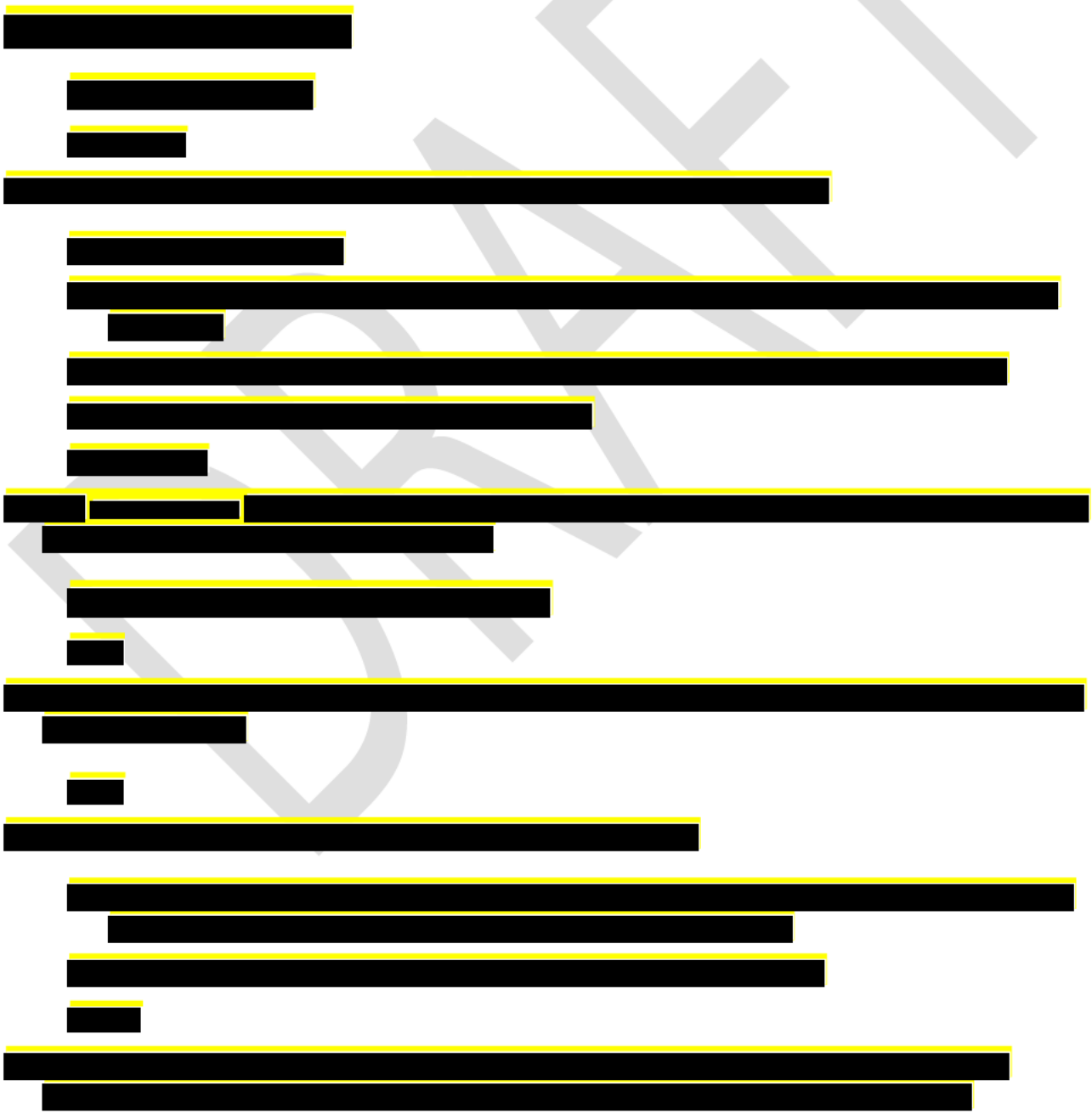
60. Home and mobile working will be facilitated by LFB in support of its business needs.

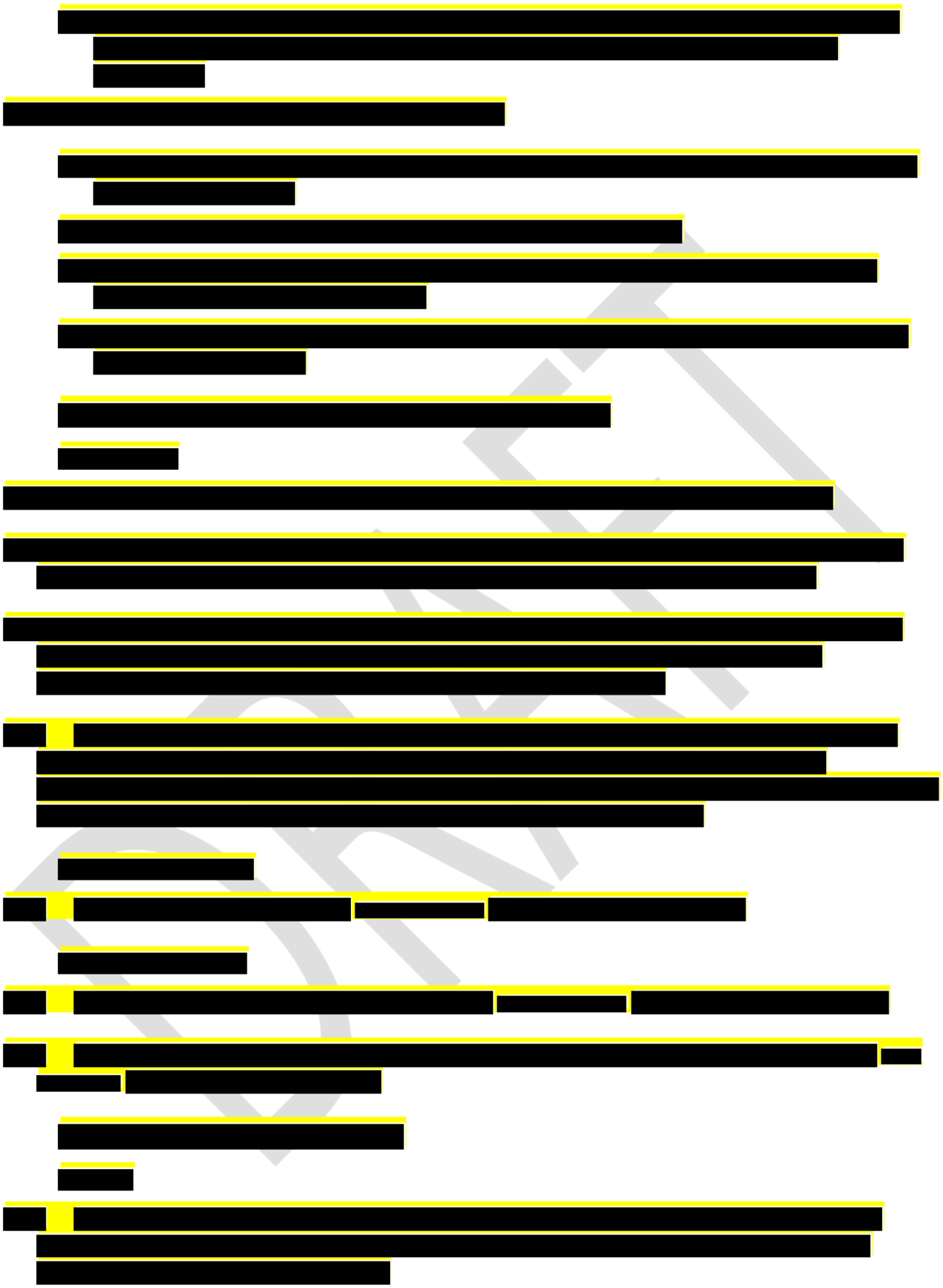
    The risks to all types of home and mobile working, including remote access to the LFB network, cloud computing and Bring Your Own Device (BYOD) are assessed and appropriate policies developed. Risks introduced through home and mobile working are managed in a pragmatic and appropriate manner.

61. Cloud and mobile platforms will be designed so that it is straightforward for users to adopt secure operating practices.

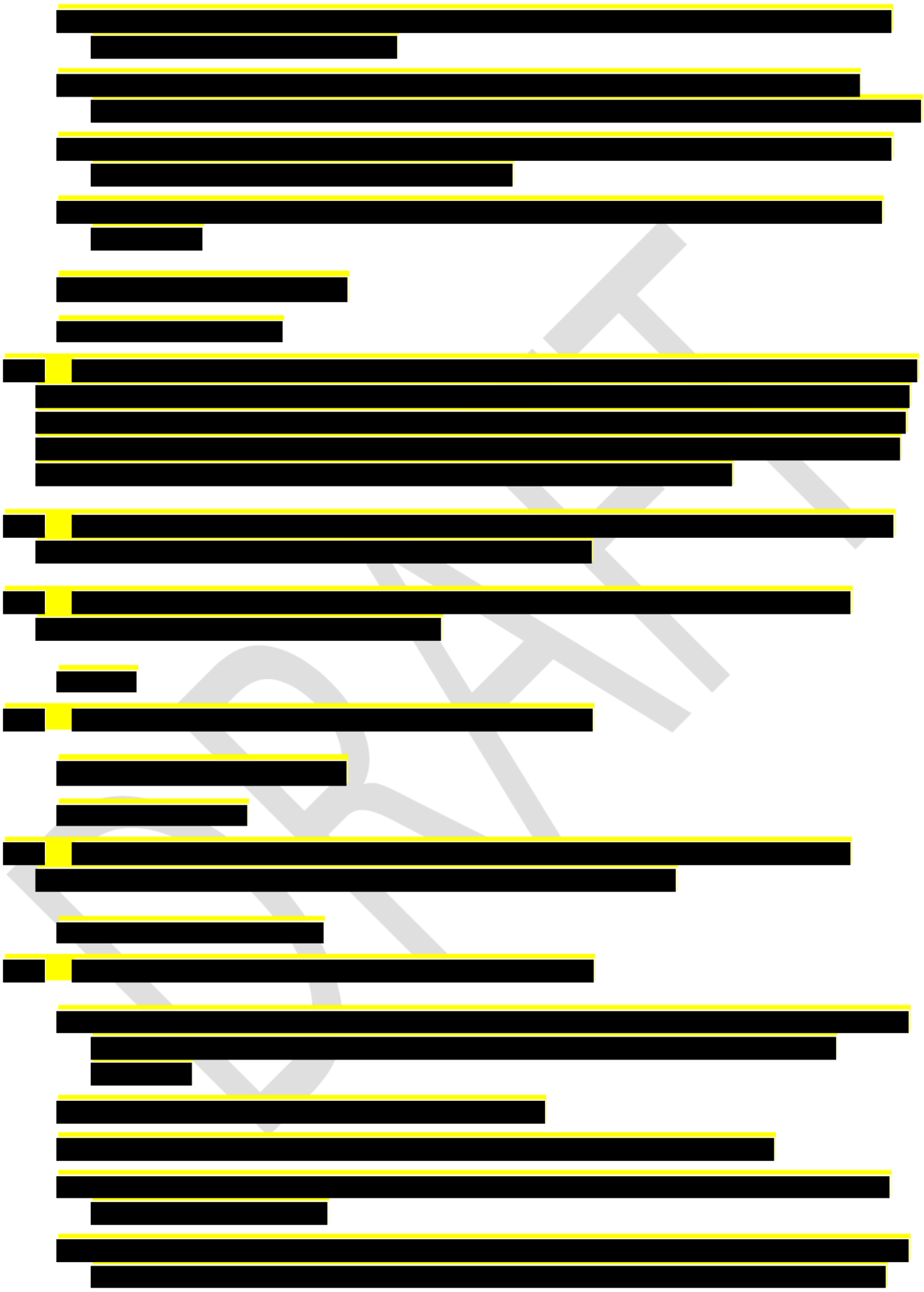
62. Secure baseline builds will be applied to all types of mobile device issued.

63. Data-at-rest will be protected using encryption and data-in-transit will be protected using a securely configured Virtual Private Network (VPN) or other robust encryption method as appropriate to the requirement.





[redacted]



Document history

Assessments

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

EIA		SDIA		HSWIA		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

Subject list

You can find this policy under the following subjects.

Freedom of Information Act exemptions

This policy/procedure has been securely marked due to:

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