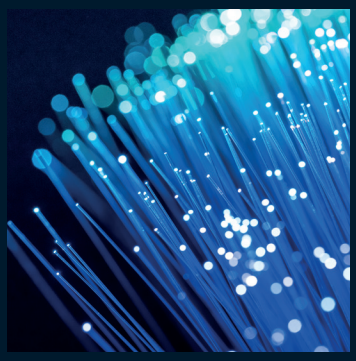
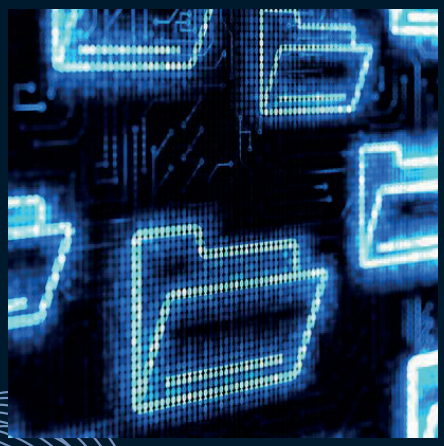
BRENT CYBER SECURITY STRATEGY

2019-2023





CONTENTS

FOREWORD

Information and data are vital to every part of Brent Council's business. As we continue with a digital programme that is transforming the way we work and how local people access information and services, we need increasingly robust security measures to protect against cyber threats.

Across the globe, cyber attacks are growing more frequent and sophisticated. When they succeed the damage can be life-altering; with severe personal, economic and social consequences.

This Cyber Security Strategy sets out our approach for protecting our information systems and the data they hold to ensure the services we provide are secure and our residents, businesses and stakeholders can safely transact with us. This includes achieving a balance of embracing digital opportunities, including making information more widely available and accessible, whilst ensuring that right levels of protection are in place.

This strategy demonstrates our commitment and the key actions we will take over the next four years to further establish a trusted digital environment for Brent. We will strengthen and secure Brent from cyber threats by investing in our systems and infrastructure, deterring our adversaries, and developing a wide range of responses; from basic cyber hygiene to the most sophisticated defences.

Cyber-attacks will continue to evolve, which is why we will continue to work at pace to stay ahead of all threats. We will deliver real-world outcomes and ground-breaking innovations to reduce the risks to our services and deter would-be attackers.

This Cyber Security Strategy underpins and enables the Brent Digital Strategy; which continues to ensure we harness the benefits of technology to improve the lives and life chances of all local people. The measures outlined in this strategy will safeguard trust and confidence in the way we operate and deliver our services, supporting Brent to remain at the forefront of the digital revolution.

Cllr Margaret McLennan
Deputy Leader, London Brent Council

INTRODUCTION

This document sets out Brent Council's application of information and cyber security standards to protect our information systems, the data held on them, and the services we provide, from unauthorised access, harm or misuse. It is our cyber security commitment both to the people we represent and the national interest; and emphasises the importance of cyber security in the role of all council staff.

WHAT IS CYBER SECURITY AND WHY IS IT IMPORTANT?

Cyber security is the practice of ensuring the confidentiality, integrity and availability (CIA) of information.

- **Attacks on Confidentiality –** stealing, or rather copying personal information.
- **Attacks on Integrity –** seeks to corrupt, damage or destroy information or systems and the people who rely on them.
- **Attacks on Availability –** denial of services, seen in the form of ransomware.

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

Cyber security is important because, in order to effectively deliver services, Brent council collects, processes, and stores large amounts of data on computers and other devices. A significant portion of this data is sensitive information, including financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.

Brent council transmits sensitive data across networks and to other devices in the course of providing services. Cyber security is the discipline dedicated to protecting this information and the systems used to process or store it.

Cyber security is crucial in ensuring our services are kept up and running. It is also vital in ensuring the public trusts the council with their information. A cyber-attack could have very serious consequences, both in terms of disrupting services – many of which serve our most vulnerable residents – and through damage to the council's reputation.

STRATEGIC CONTEXT

The overarching vision in the Brent Borough Plan (2019-2023) is "to make Brent a borough of **culture**, **empathy**, and **shared prosperity**". Achieving this vison will require innovation, continued and deeper partnerships, and careful planning based on sound evidence.

The Brent Digital Strategy (2019-2023) sets out Brent's ongoing digital transformation, including how technology will be used to progress each of the Borough Plan themes: strong foundations; every opportunity to succeed; a borough where we can all feel safe, secure, happy and healthy; a cleaner more considerate Brent; and a future build for everyone, an economy fit for all.

This Cyber Security Strategy supports delivery of the Borough Plan and Digital Strategy by providing a framework for Brent to securely harness the benefits of the digital revolution for the benefit of all stakeholders. It is essential to the efficient running and evolution of the council.

This Cyber Security Strategy sits alongside the Brent ICT Strategy and is supported by a suite of operational policies (Information Security Policy, Information Risk Policy and Access to Information Rule Book).

PURPOSE

The council seeks to deliver its digital strategy through transforming Brent into a digital place and a digital Council. The scale of transformation represents an unprecedented culture shift for the Council, residents, partners and businesses.

The Cyber Security Strategy is a new strategy, introduced in response to a number of successful and high profile cyber-attacks on public and private organisations. The purpose of the strategy is to give assurance to residents and other stakeholders of the council's commitment in delivering robust information security measures to protect resident and stakeholder data from misuse and cyber threats, and to safeguard their privacy through increasingly secure and modern information governance and data sharing arrangements - both internally and with partners.

Through delivery of this strategy we will comply with and embed the principles of 'Cyber Essentials'; a government-backed, industry-supported scheme to help organisations protect themselves against common online threats. We will also follow the "10 Steps to Cyber Security" framework published by the National Cyber Security Centre (included as Appendix 2).

SCOPE OF THE STRATEGY

This strategy is intended to cover all Brent Council information systems, the data held on them, and the services they help provide. It aims to increase cyber security for the benefit of all Brent residents, businesses, partners and stakeholders; helping to protect them from cyber threats and crime.

THE CHALLENGE WE FACE AS A COUNCIL

Brent Council is using an increasing range of technology, from apps and the cloud, to different devices and gadgets. Much of our business is online: corresponding with residents and local businesses, carrying out case work, and reviewing reports and papers for council meetings.

This direction of travel is expected to continue and accelerate; making effective cyber security ever more crucial in protecting against new types of threats, risks and vulnerabilities.

THREATS

A threat if left unchecked, could disrupt the day-to-day operations of the council, the delivery of local public services and ultimately has the potential to compromise national security.

TYPES OF THREATS

CYBERCRIMINALS AND CYBERCRIME

Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either selling illegally gained information to a third party, or using directly for criminal means.

Key tools and methods used by cybercriminals include:

- **Malware** – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals
- **Ransomware** – a kind of malware that locks victims out of their data or systems and only allows access once money is paid
- **Phishing** – emails purporting to come from a public agency to extract sensitive information from members of the public.

HACKTIVISM

Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause.

When targeted against local government websites and networks, these attacks can cause reputational damage locally. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services.

Hacktivist groups have successfully used distributed denial of service (DDoS – when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of a number of councils already.

INSIDERS

Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.

ZERO DAY THREATS

A zero day exploit is a cyber-attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator. It is an attack that exploits a previously unknown security vulnerability.

This poses a risk to any computer or system that has not had the relevant patch applied, or updated its antivirus software.

OTHER THREATS INCLUDE

PHYSICAL THREATS

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster natural or otherwise that impact upon council IT systems.

TERRORISTS

Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

ESPIONAGE

Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily.

VULNERABILITIES

Vulnerabilities are weaknesses or other conditions in an organisation that a threat actor; such as a hacker, nation-state, disgruntled employee, or other attacker, can exploit to adversely affect data security.

Cyber vulnerabilities typically include a subset of those weaknesses and focus on issues in the IT software, hardware, and systems an organisation uses.

- **System Maintenance –** IT systems should be updated and checked regularly and effectively. It is essential that the systems are fully updated and appropriate fixes are applied. Poor setup, mismanagement, or other issues in the way an organisation installs and maintains its IT hardware and software components is a threat.
- **Legacy Software –** To ensure that legacy systems have sufficient user and system authentication, data authenticity verification, or data integrity checking features that prevent uncontrolled access to systems.
- **Training and Skills –** It is fundamental that all employees have a fundamental awareness of cyber security and to support this.

RISKS

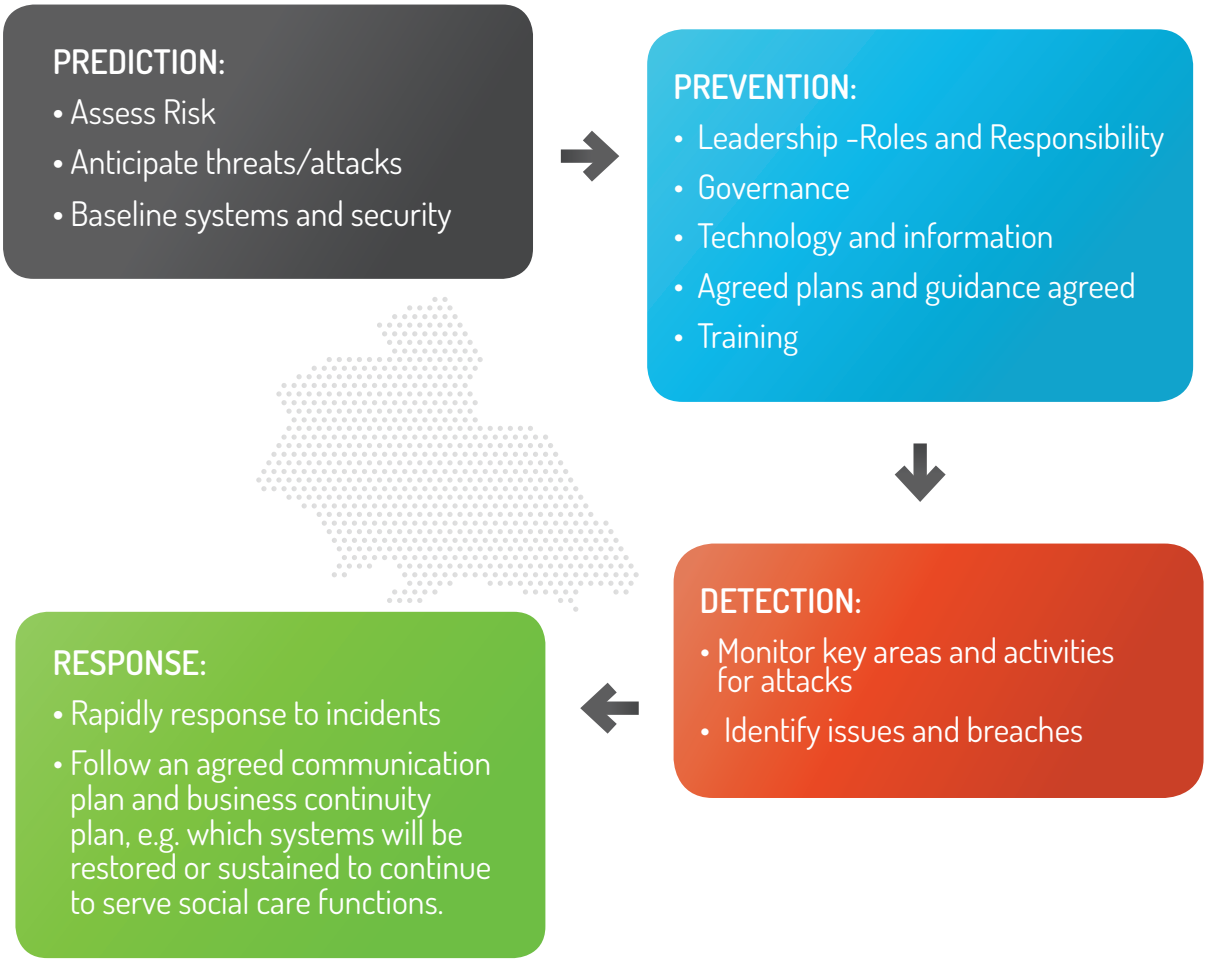
Cyber Risk Management is a fundamental part of the broader risk management to ensure cyber security challenges are fully identified across the council and appropriate action is carried out to mitigate the risk.

OUR APPROACH, PRINCIPLES AND PRIORITIES

To mitigate the multiple threats we face and safeguard our interests in cyberspace, we need a strategic approach that underpins our collective and individual actions in the digital domain over the next four years. This will include:

- **A council wide risk management framework to help build a risk aware culture within the council, ensuring staff understand how to identify and manage risks.**
- **Cyber Awareness training to help mitigate insider threats, understand supply chain risks and ensure all staff understand the issues and their responsibilities.**
- **Applying the Cyber Essentials scheme controls and complying with frameworks including ISO 27001 and CESG Information Assurance Standard 1 & 2 to ensure that the council will be able to identify, mitigate and protect against information security risks in a prioritised and resourceful fashion.**

The diagram below shows the key steps for protecting the council and its contractors for cyber attacks:



IMPLEMENTATION PLAN

To adapt to the changing landscape and achieve our vision we will align with the National Cyber Security Strategy's approach to defend Brent council and our residents' cyberspace, to deter our adversaries and to develop our capabilities.

DEFEND

The council will have the means to defend against evolving cyber threats, to respond effectively to incidents, and to ensure networks, data and systems are protected and resilient. It includes helping our residents, businesses and partners in gaining the knowledge and ability to defend themselves.

Actions:

- Implementing firewalls and scanning services
- Carrying out health checks, penetration test and cyber resilience exercises to test their systems and processes, e.g. Web Check – a website configuration and vulnerability scanning service, developed with a number of public sector organisations including councils. This is free to use and available to all public sector organisations
- Meeting compliance regimes, Code of Connection (CoCo) which require good cyber hygiene, to connect to government private networks, e.g. Public Sector Network (PSN) and the Health and Social Care Network
- Working with partners across the public sector through participation in Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting

DETER

The council will be a hard target for all forms of aggression in cyberspace. This will involve detecting, understanding, investigating and disrupting hostile action against us.

Actions:

- **Governance**
  - Applying government's cyber security guidance, e.g. 10 Steps to Cyber Security or Cyber Essentials
- **Technology and information**
  - Network Security

    Users with wide ranging or extensive system privilege shall not use their highly privileged accounts for high-risk functions, in particular reading email and web browsing

    → Multi-factor authentication shall be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi - factor authentication shall be used for access to enterprise level social media accounts

    → Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and shall not be easy to guess. Passwords which would on their own grant extensive system access, should have high complexity
  - Malware prevention
  - Removable media controls
  - Secure configuration
- **Agreed plans and guidance**
- **Training or educating users can help detect, deter and defend against the Cyber threats**

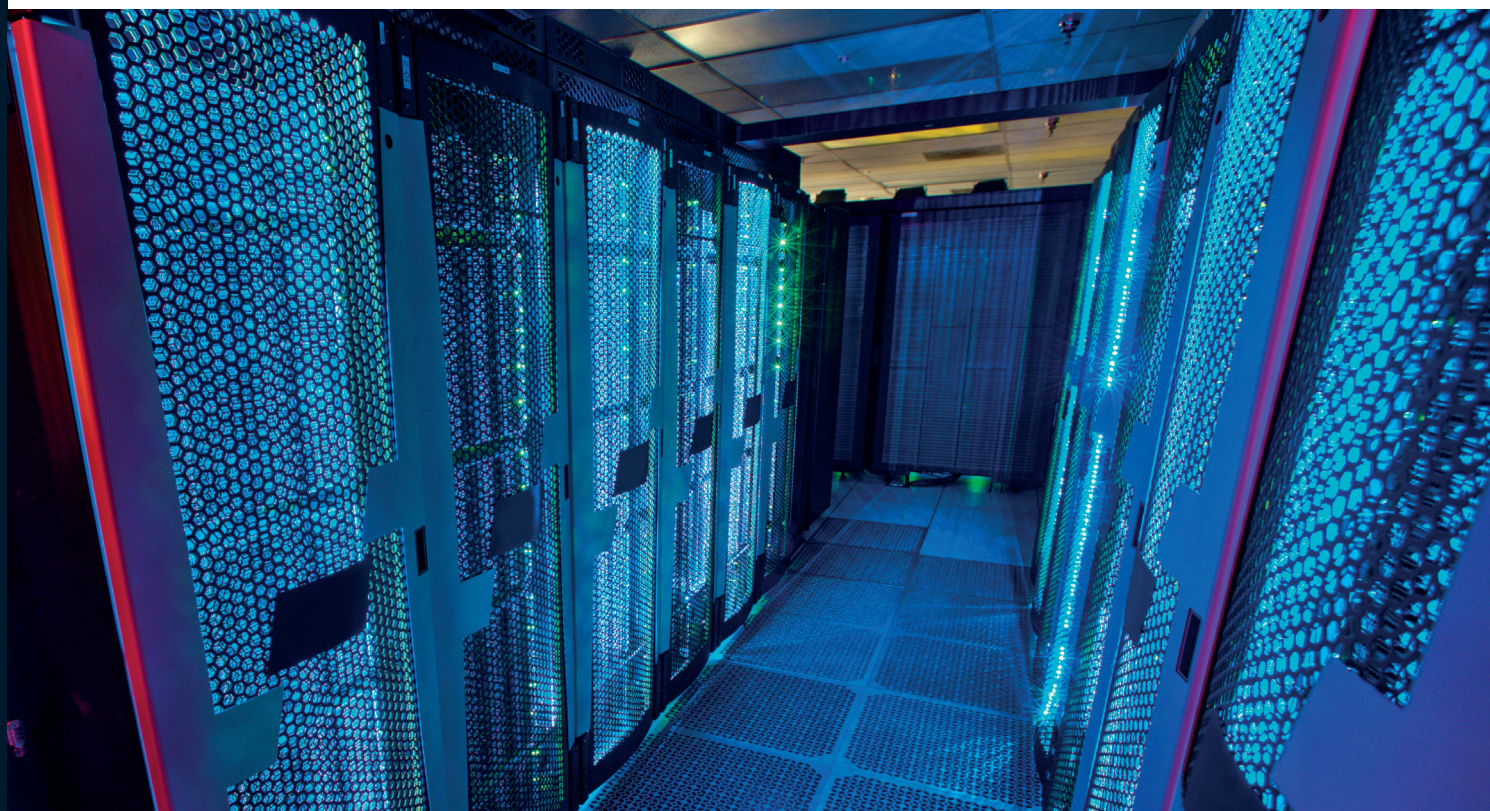
DEVELOP

The council will continually develop our innovative cyber security strategy to address the risks faced by our residents, businesses and community and voluntary sector.

This includes developing a co-ordinated and tailored approach to risks and threats that we may encounter and mitigate potential vulnerabilities.

Actions:

- Develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud
- Process, procedures and controls to manage changes in cyber threat level and vulnerabilities
- Managing vulnerabilities that may allow an attacker to gain access to critical systems
- Operation of the council's penetration testing programme; and Cyber-incident response
- Introducing training for staff and elected members
- Develop an incident response and management plan, with clearly defined actions, roles and responsibilities
- Develop a communication plan in the event of an incident which includes notifying (for example) the relevant supervisory body, senior accountable individuals, the Departmental press office, the National Cyber Security Centre (NCSC), Government Security Group (Cabinet Office), the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive)



CRITICAL SUCCESS FACTORS

Throughout this period of challenging transformation, the council has committed to delivering robust information security measures to protect residents and stakeholder data from misuse and cyber threats, and to safeguard their privacy through increasingly secure and modern information governance and data sharing arrangements both internally and with partners.

To continue to provide assurance on the effectiveness and robustness of the council's arrangements for IT security, the council will:

- Develop appropriate cyber security governance processes
- Develop a council wide Cyber Risk Management Framework
- Develop policies/procedures to review access on a regular basis
- Create a cyber-specific Business Continuity Management Plan and/or review Brent's Incident Plan to include emergency planning for cyber attack
- Develop an incident response and management plan, with clearly defined actions, roles and responsibilities. A copy of all incidents shall be recorded regardless of the need to report them
- Set up a Playbook to have test incidents on a regular basis; to ensure reaction to incidents where an incident is triggered
- Create standard test plans with security testing as a standard
- Reconcile current systems in place and last times these were reviewed (build into Enterprise Architecture)
- Review vendor management – process of assessments of third parties
- Explore Active Cyber Defence tools and new technologies to ensure Brent has best solutions to match to threats
- Apply the governments cyber security guidance – 10 Steps to Cyber Security
- Provide relevant cyber security training for staff and elected members
- Apply a regular schedule of cyber exercises, within the wider cycle of multi-agency incident response and recovery exercises
- Comply with the Governments Public Sector Network (PSN) Code of Connection and Payment Card Industry (PCI) standards; a minimum requirement for all systems used, audit trails, deletion of data etc.
- Protect enterprise technology by working with specialist partners to develop model architecture and review audit logs to reduce chances of threats

CYBER SECURITY GOVERNANCE ROLES AND RESPONSIBILITIES

Effective cyber security governance in Brent is delivered through the following roles and functions.

Senior Information Risk Owner (SIRO)

The Council's nominated Senior Information Risk Owner (SIRO), is the Director of Legal, HR, Audit and Investigations. The SIRO is responsible for the governance of cyber security and information risk within the Council. This includes ensuring that information governance risk is managed in accordance with GDPR.

However, whilst the SIRO is the nominated officer, responsibility for safeguarding information and information systems is shared across the organisation with all staff having a role to play.

The Cabinet

The Cabinet is made up of the Leader of the Council and other senior councillors (Cabinet members). Cabinet will agree and receive updates on implementation of the Cyber Security Strategy.

Council Management Team (CMT)

CMT sponsor the Cyber Security Strategy and oversee the strategic framework through which the council governs its information resources.

Information Governance Group (IGG)

The IGG is comprised of senior representatives from each service area. The group are responsible for overseeing the delivery of the Cyber Security Strategy and monitoring its effectiveness.

GDPR officer

The GDPR officer leads on the Readiness Programme. They monitor and report progress to the IGG and to all employees across the council; support services through a network of Information Champions; develop and maintain a corporate inventory of all processing activity across the council; review theses processing activities and seek legal assurance; and review contracts and ensure that GDPR changes are reflected.

Information Governance Team (IGT)

The IGT define the scope of the GDPR readiness strategy. They also design and oversee the work streams and liaise with services and specialist areas to ensure tasks are fully completed on time.

Technical Design Authority (TDA)

The Technical Design Authority (TDA) make decisions regarding technical implementations for projects. This includes ensuring that cyber security implications are properly considered.

Digital Board

The Digital Board oversees implementation of Brent's Digital Strategy. They ensure that risks, issues and dependencies are proactively managed and make decisions in relation to any risks and issues that have been escalated in relation to the digital programme.

Shared ICT Service

Shared ICT Services oversees the delivery of the Shared ICT Service for Brent, Lewisham and Southwark.

Information Asset Owners (IAO)

Information Asset Owners are responsible for all processing of personal data within their business area.

All Brent officers

It is the responsibility of all officers to comply with the standards set out in this Cyber Security Strategy

APPENDIX 1
STANDARDS

Information Security Management within Brent Council will comply with the British Standard: BS ISO/IEC 27001:2013

This standard specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the Council's overall business risks. It specifies requirements for the implementation of security controls customised to the needs of the Council.

ISO27032 and The Government's Cyber Essentials provide security standards for the Internet (referred to as "Cyberspace" or "Cyber")

Brent complies with PSN and PCI standards.

APPENDIX 2
NCSC: 10 STEPS TO CYBER SECURITY

Risk Management Regime

Embed an appropriate risk management regime following the ISO27k standards, across the organisation. This should be supported by an empowered governance structure, which is actively supported by the board and senior managers. Clearly communicate your approach to risk management with the development of applicable policies and practices. These should aim to ensure that all employees, contractors and suppliers are aware of the approach, how decisions are made, and any applicable risk boundaries.

Secure configuration

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

Network security

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites and the use of mobile or remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

Managing user privileges

If users are provided with unnecessary system privileges or data access rights, then the impact of misuse or compromise of that users account will be more severe than it need be. All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed. This principle is sometimes referred to as 'least privilege'.

User education and awareness

Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

Incident management

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact. You should identify recognised sources (internal or external) of specialist incident management expertise.

Malware prevention

Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by developing and implementing appropriate anti-malware policies as part of an overall 'defence in depth' approach.

Monitoring

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

Removable media controls

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

Home and mobile working

Mobile working and remote system access offers great benefits, but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers. Train users on the secure use of their mobile devices in the environments they are likely to be working in.