Caerphilly County Borough Council

Cyber Security Strategy 2022-2025

Protecting and Securing Our Digital Future

CONTENTS

1 Foreword

Information and data are vital to every part of Caerphilly CBC's ('the Council') 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 in frequency and becoming more sophisticated. The increased use of the internet caused by Covid 19 pandemic means that cyber criminals have become more active, and our exposure has increased. When cyber-attacks succeed the damage can be significant; with personal, economic and social consequences.

This Cyber Security Strategy ('Strategy') sets out our approach for protecting our information systems and the data we 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 established.

This Strategy demonstrates our commitment and the key actions we will take to further establish a trusted digital environment for the Council. We will strengthen and secure the Council from cyber threats by increasing Security awareness throughout our workforce, 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 learn and to work at pace in an attempt to stay ahead of all threats.

The Council strives to be an innovative, forward looking local authority that is committed to modernising and perfecting our approach to Cyber Security. We will be bold in our approach, we will explore innovation and, if necessary, we will learn from our mistakes to ensure continuous improvement in delivering a secure and advanced Cyber Security Strategy.

This Strategy underpins and enables the Council's Customer and 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 the Council to remain at the forefront of the digital revolution.

Cllr Sean Morgan
Leader of Council

Christina Harrhy
Chief Executive

2 INTRODUCTION

This document sets out the 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?

Cyber Security is the practice of ensuring the confidentiality, integrity and availability of information using the technologies, processes, and people behaviour practices designed to protect the IT infrastructure, applications and data from attack, damage, or unauthorised access that we use in our everyday lives.

Attacks on Confidentiality – stealing or 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.

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

Cyber Security is important because, in order to effectively deliver services, the 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 unauthorised access or exposure could have negative consequences.

The 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.

The Covid 19 pandemic has impacted on all areas of public and private life. Amongst other things it has it has forced a great deal more of our routine professional and personal interactions on-line and many more of us now work predominantly from home. This has presented new and lucrative opportunities to cyber criminals. Whilst much will return to normal in due course, the extent to which we exploit cyberspace and many of our working practice will not return to the pre-pandemic norm. Cyber Security has become, and will remain, a key responsibility for all of us, collectively and as individuals.

This Strategy is supported by a suite of operational policies and procedures.

3 PURPOSE & SCOPE OF STRATEGY

The Council seeks to deliver its digital strategy through transforming Caerphilly 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 Council are dedicated to ensuring that all digital strategies are cohesive and have the same aim in mind, to be compliant, secure, and cutting-edge to ensure the Council are prepared for any obstacles or cyber-attacks in the digital world. A key area of focus is improving information assurance, risk management and care of personal data.

This Strategy has been produced in response to the increasing threat from cyber criminals and 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 our partners.

The Council will continue its vision for developing and managing its interface with customers and its digital environment. Pursuing this vision against an increasingly complex public service landscape as we face substantial social, economic, and political challenges.

This Strategy supports that key area of focus and includes protecting an ever-increasing agile workforce, growth in the uptake of technologies such as cloud-based systems, internet-enabled services, mobile devices, high-speed broadband and together with the digital agenda on utilising/sharing more data of all forms to develop public services means that Cyber Security will be increasingly tested.

The Strategy is designed to further enhance and strengthen the Council's Security position. The Council has already built a model to ensure that it has a healthy and systematic Security posture that protects against most types of threats. The Model follows industry best practices such as the National Cyber Security Centre (NCSC), National Institute of Standards and Technology (NIST) & Warning, Advice and Reporting Point (WARP) a community-based service where members can receive and share up-to-date advice on information Security threats, incidents, and solutions.

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

This Strategy will evolve so that it continues to support national strategies and legislation such as:

1. Digital Vision for Wales https://gov.wales/digital-strategy-wales-html
2. Digital Inclusion Digital Inclusion Forward Look: towards a digitally confident Wales [HTML] | GOV.WALES
3. The Future Generations Act Well-being of Future Generations (Wales) Act 2015 – The Future Generations Commissioner for Wales
4. Cymraeg 2050 strategy Cymraeg 2050: our plan for 2021 to 2026 [HTML] | GOV.WALES
5. NCSC Cyber Strategy National Cyber Strategy 2022 (HTML) - GOV.UK (www.gov.uk)

4 THE CHALLENGE WE FACE AS A COUNCIL

The Council is using an increasing range of technology, from apps and the cloud to different devices and gadgets. Much of our business is done online such as 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

Types of Threats

Cybercriminals and Cyber Crime - 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 several 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 often 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 types of Threat

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 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 crucial that all employees have a fundamental awareness of cyber Security and to support this.

Risks

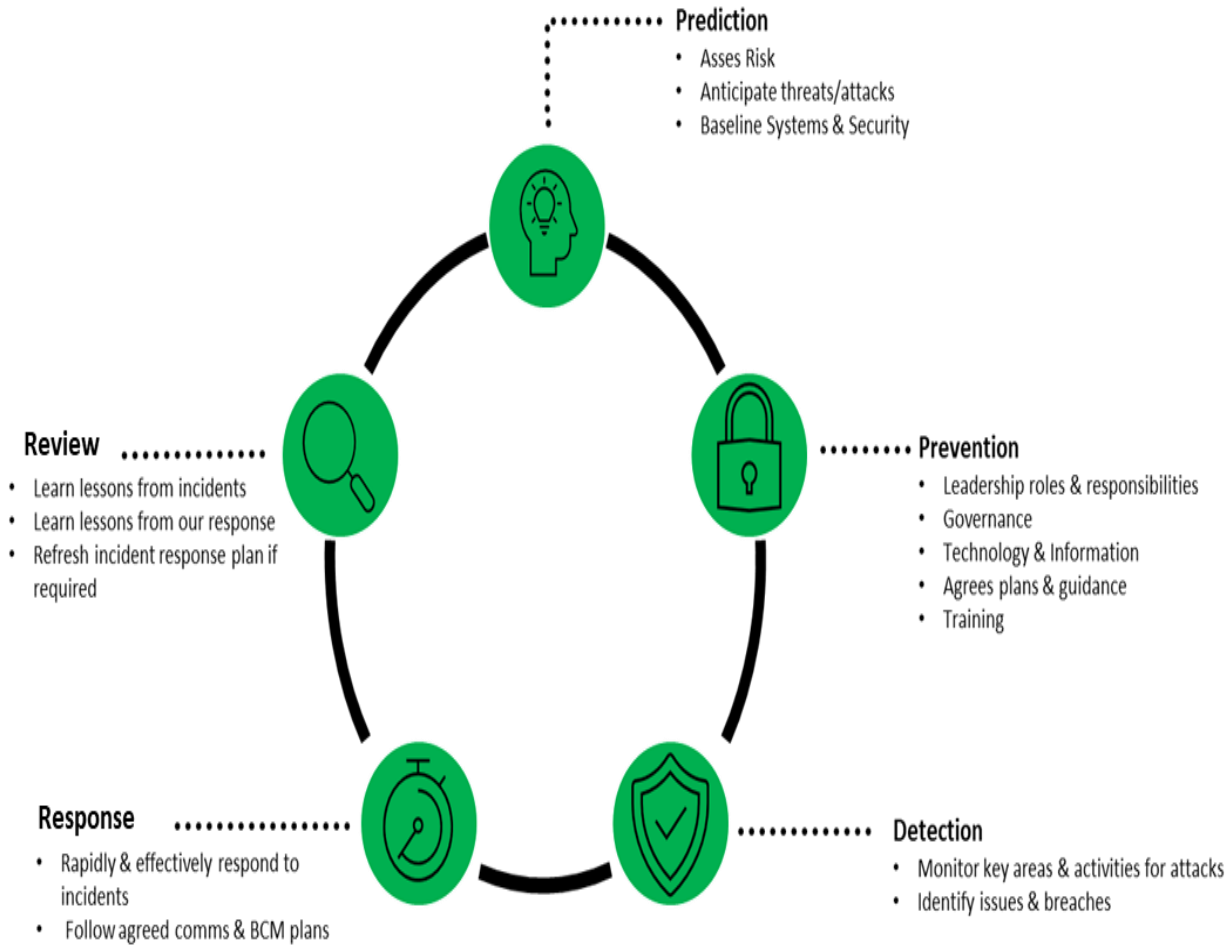
Cyber Risk Management is a fundamental part of the broader risk management to ensure cyber Security challenges are fully identified across the council and appropriate action is carried out to mitigate the risk.

5 OUR APPROACH, PRINCIPLES & 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. 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 conforming to appropriate frameworks to ensure that the council will be able to identify, mitigate and protect against information Security risks in a prioritised and resourceful fashion.

The Council will adopt the following approach shown in the diagram below:



6 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 the 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:

- Implement firewalls and scanning services.
- Carry out health checks penetration test and cyber resilience exercises to test systems and processes.
- Meet compliance regimes, which require good cyber hygiene, to connect to government private networks, e.g. Public Sector Network (PSN).

- Work with partners across the public sector through participation in the Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting Point (WARP) and other networks.

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.

Governance - Applying Cyber Security guidance, e.g. 10 Steps to Cyber Security and Cyber Essentials Plus

Technology 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 and education so that all users can help detect, deter and defend against 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.
- Put in place processes, 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.
- Continuation of 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 Council's Communications Unit, Local Resilience Forum (LRF), Welsh Government Cyber Resilience Team, the National Cyber Security Centre (NCSC), Government Security

Group (Cabinet Office), the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive).

7 CRITICAL SUCCESS FACTORS

The Council is 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.
- Adopt a council wide Cyber Risk Management Framework (Cyber Essentials Plus).
- Develop policies/procedures to review access on a regular basis.
- Create a cyber-specific Business Continuity Management Plan and review the Council's Incident Plan to include emergency planning for a cyber-attack.
- Maintain, rehearse and regularly review 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 playbooks to support test exercises on a regular basis; to ensure effective reaction to incidents when an incident occurs.
- Create 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 the Council has best solutions to match to threats.
- Apply the Cyber Security guidance – 10 Steps to Cyber Security.
- Continue to 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 Public Sector Network (PSN) requirements and the Payment Card Industry Data Security Standard (PCI DSS); 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.

8 CYBER SECURITY GOVERNANCE ROLES AND RESPONSIBILITIES

Senior Information Risk Owner (SIRO)

The Council's nominated Senior Information Risk Owner (SIRO) is the Head of Customer and Digital Services. The SIRO is accountable for the governance of Cyber Security and information risk within the Council. This includes ensuring that information governance risk is controlled 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.

Corporate Management Team (CMT)

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

Digital Leadership Group (DLG)

The DLG provides strategic direction and decision making on the Council's digital strategy, Security, information governance, projects, initiatives, skills and policy.

Digital Solutions Board (DSB)

The DSB ensures all new ICT requirements for the Council are in line with the emergent ICT Strategy and Strategic Principles such as but not limited to Security standards.

Corporate Information Governance Unit (CIGU)

The group are responsible for overseeing the delivery of the Cyber Security Strategy and monitoring its effectiveness.

Data Protection Officer (DPO)

The DPO complements the activity of and supports the Digital Specialist Security and Compliance, leading on non-technical aspects of data protection and providing assurance.

Information Asset Owners (IAO)

Information Asset Owners are established across the Council and are responsible for all processing of personal data within their business area.

All Elected Members and Council Officers

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

9 STANDARDS

Public Services Network (PSN) Compliance

The purpose of PSN compliance

The PSN uses a 'walled garden' approach, which enables access to Internet content and shared services to be controlled. This is because the Security of any one user connected to the PSN affects both the Security of all other users and the network itself.

The PSN compliance process exists to provide the PSN community with:

- Confidence the services they use over the network will work without problems assurance that their data is
- Protected in accordance with suppliers' commitments the promise that if things do go wrong, they can be quickly put right.
- Holding a valid PSN compliance certificate gives you our permission to interact with the PSN in a specific, pre-agreed ways.

Cyber Essentials Certification

What is Cyber Essentials?

Cyber Essentials is a simple but effective, Government backed scheme that will help protect the Council against a whole range of the most common cyber-attacks.

Cyber-attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals. They're the digital equivalent of a thief trying your front door to see if it's unlocked. Our advice is designed to prevent these attacks.

10 NCSC: 10 STEPS TO CYBER SECURITY

The Council will follow the ***"10 Steps to Cyber Security" framework published by the National Cyber Security Centre (NCSC)*** to ensure that technology, systems and information within the Council are protected appropriately against the majority of cyber attacks and enable the Council to best deliver its business objectives. The ***"10 Steps to Cyber Security"*** are as follows:

1. Risk management Regime - Embed an appropriate risk management regime following the corporate standard 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.

2. 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.

3. 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.

4. 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'.

5. 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.

6. 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.

7. 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.

8. Monitoring - 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.

9. 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.

10. Home and Mobile Working - Mobile working and remote system access have become the norm since Covid 19, but they expose 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.