



Durham County Council

CYBER SECURITY STRATEGY 2022-2025



CONTENTS



Foreword	3
Introduction	4
Purpose and scope	5
Cyber security – what is it?	6
Why is Cyber security important?	7
The challenge we face as a council	8
Threats	9
Vulnerabilities	11
Risks	12
Our approach, principles and priorities	13
Implementing the strategy	14
Critical success factors	16
Cyber security governance / roles and responsibilities	17
Appendices:	
Appendix 1 Standards	19
Appendix 2 NCSC: 10 Steps to Cyber Security	20
Contacts	22

FOREWORD

Cllr Susan McDonnell



Information and data are vital to every part of Durham County Council's business. As we continue to deliver 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 2022-2025** 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 are in place.

This strategy demonstrates our commitment and the key actions we will take to further establish a trusted digital environment for DCC. We will strengthen and secure DCC 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 to work at pace to stay ahead of all threats. The Cyber Security Strategy underpins and enables the DCC Digital Strategy, which continues to ensure we will place the customer at the heart of everything we do in a changing technological landscape. The measures outlined in this strategy will safeguard trust and confidence in the way we operate and deliver our services, supporting DCC to remain at the forefront of digital leadership.

INTRODUCTION



We want Durham to be a county where:

- ✓ **There are more and better jobs.**
- ✓ **People live long and independent lives.**
- ✓ **Our communities are well connected and supportive.**

This vision is set out in our corporate plan and our digital strategy builds on that plan.

The Council's Digital Strategy sets out how technology is used to support the delivery of services to the residents, businesses and visitors in County Durham. Our digital ambitions are fundamental to delivering quality services to our communities.

The Covid 19 pandemic has impacted on all areas of public and private life. Amongst other things it has led to more routine professional and personal interactions to be conducted on-line and many more of us now work 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.

The prevalence of digital services and the dependence on their availability and integrity means that a robust and comprehensive cyber security strategy and framework are vital to ensure that appropriate measures are in place.

Staff training is also an important factor in combating cyber threats and reducing risk in a constantly changing online environment. Ongoing programmes seek to raise awareness of digital security and to strengthen the human element of cyber defence.

This strategy is our cyber security commitment, both to the people we represent and the national interest; and supports delivery of the Digital Strategy and the Council Plan by providing a framework for DCC to securely harness the benefits of digital technology for the benefit of all.

PURPOSE AND SCOPE



The council seeks to deliver its digital strategy through transforming Durham 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 the increasing threat from cyber criminals and several 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 Plus**'; 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.



**10 Steps to
Cyber Security**

The scope of this strategy includes all DCC's information systems, the data held on them, and the services they help provide. It aims to increase cyber security for the benefit of all residents, businesses, partners and stakeholders; helping to protect them from cyber threats and crime.

CYBER SECURITY – WHAT IS IT?



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



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.



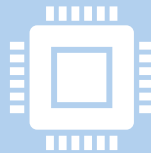
Attacks on Availability

– denial of services.

WHY IS CYBER SECURITY IMPORTANT?



In order to deliver services, Durham County Council collects, processes, transmits and stores large amounts of personal and sensitive data and transmits sensitive data across networks to other devices.



A successful cyber-attack would considerably interrupt DCC's ability to deliver services – many of which serve our most vulnerable residents – as well as incurring large recovery costs and significant damage to our reputation.



A successful cyber security approach enables us to protect information the systems that are used to process or store it, ensures our services are kept up and running, and is vital in ensuring the public trusts the council with their information.

THE CHALLENGE WE FACE AS A COUNCIL



The council continues to use an increasing range of technology, from apps and the cloud, to different devices.



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



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

Types of threat:

Cyber criminals and cyber crime

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

Key tools and methods used by cyber criminals 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 overwhelmed by an electronic attack, and 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.

THREATS



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.

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. Mistakes are constantly discovered and fixed in all deployed systems. If systems are not quickly patched, then anyone who wishes to attack a system has a much better chance of success.



Legacy Software. Software that is in use but out of support, or unsupported, cannot be patched. Therefore, the likelihood of it being successfully compromised grows over time and cannot be addressed.



People. 'Social engineering' seeks to trick people into allowing access to systems or handing over their passwords. Training and support is the only solution to this challenge.

RISKS



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

The management of cyber security is, in large part, the management of risk. DCC has robust processes in place to manage risk at various levels within the organisation.



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.

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.



IMPLEMENTING THE STRATEGY



Deter and Detect

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:

- ✓ **Support enhanced governance** through the application of government's cyber security guidance, e.g. 10 Steps to Cyber Security or Cyber Essentials.
- ✓ **Support network security** through:
 - » The use of multi-factor authentication, where technically possible.
 - » Application of complex password protocols – Passwords which would on their own grant extensive system access, will have high complexity.
- ✓ **Raise defences** through malware prevention.
- ✓ **Review removable media/device controls.**
- ✓ **Maintain secure configuration.**
- ✓ **Deliver agreed plans and guidance.**
- ✓ **Training and educating users** to help detect, deter and defend against the Cyber threats.
- ✓ In line with the **Counter Terrorism and Security Act 2015**, the council has a duty to ensure that those vulnerable to radicalisation have appropriate safeguards and support. Measures are in place to block access to online resources where recruitment, radicalisation and dissemination can take place. Daily reports are sent to a cross-service Moderation Group and summarised and reported to management teams regularly.

IMPLEMENTING THE STRATEGY



Defend and 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 coordinated and tailored approach to risks and threats that we may encounter and mitigation of potential vulnerabilities.














Actions:

- ✓ **Develop and maintain risk management framework**, internal control and governance for the prevention and detection of irregularities and fraud.
- ✓ **Implement process, procedures and controls** to manage changes in cyber threat level and vulnerabilities.
- ✓ **Manage vulnerabilities** that may allow an attacker to gain access to critical systems.
- ✓ **Operate the council's penetration testing programme and cyber-incident response.**
- ✓ **Introduce 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



In continuing to provide assurance, DCC will:

-  Develop appropriate cyber security governance processes and a security framework with policies/procedures reviewed on a regular basis.
-  Create a cyber-specific Business Continuity Management Plan and review DCC's Incident Plan to include emergency planning for 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 they occur.
-  Create test plans with security testing as a standard.
-  Reconcile current systems in place and previous review points (build into Enterprise Architecture).
-  Review vendor management – process of assessments of third parties.
-  Explore Active Cyber Defence tools and new technologies to ensure DCC has best solutions to match with threats.
-  Apply the government's 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 applicable standards (PSN, PCI-DSS, etc).
-  Protect enterprise technology by working with DCC's supply chain to develop model architecture and review audit logs to reduce chances of threats.

CYBER SECURITY GOVERNANCE

ROLES AND RESPONSIBILITIES



Effective cyber security governance in Durham 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 Resources. 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.

Corporate Management Team (CMT)

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

Safer Cyber Working Group

This stakeholder group is made up of DCC and partner organisations, including police, probation service, education, community/voluntary sector, CCG, fire and rescue, PCC, victim support and business. It aims to:

- Raise awareness of the general population about staying safe online
- Reduce risk to the most vulnerable groups
- Build resilience of local businesses to the threat of cyber crime

Cyber Security Steering Group (CSSG)

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

CYBER SECURITY GOVERNANCE

ROLES AND RESPONSIBILITIES



Digital Security Team

The Digital Security Team lead the cyber security programme. They monitor and report progress to the CSSG 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 these processing activities and seek legal assurance; and review contracts and ensure that GDPR changes are reflected.

Digital Programme Board

The Digital Programme Board oversees implementation of DCC's Digital Programme. 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.

Digital Services

DCS oversees the delivery of the ICT Service for Durham County Council.

Information Asset Owners (IAO)

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

All DCC officers

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

APPENDIX 1

STANDARDS



Currently DCC must comply with the following standards:

- ✓ Bankers' Automated Clearing Services (BACS)
- ✓ Cyber Essentials (for a subset of traded services)
- ✓ Criminal Justice Secure Mail (CJSM)
- ✓ NHS Data Security and Protection Toolkit (DSPT)
- ✓ Payment Card Industry Data Security Standard (PCI DSS)
- ✓ Public Services Network (PSN)

In addition, DCC should follow all relevant National Cyber Security Centre (NCSC) guidance and Center for Internet Security (CIS) benchmarks.



APPENDIX 2

NCSC: 10 STEPS TO CYBER SECURITY



- 1. Risk management** – Taking risks is a natural part of doing business. Risk management informs decisions so that the right balance of threats and opportunities can be achieved to best deliver business objectives. Risk management in the cyber security domain helps ensure that the technology, systems and information in an organisation are protected in the most appropriate way, and that resources are focused on the things that matter most to the business. A good risk management approach will be embedded throughout the organisation and complement the way that other business risks are managed.
- 2. Engagement and training** – People should be at the heart of any cyber security strategy. Good security takes into account the way people work in practice and doesn't get in the way of people getting their jobs done. People can also be one of the most effective resources in preventing incidents (or detecting when one has occurred), provided they are properly engaged and there is a positive cyber security culture which encourages them to speak up. Supporting staff to obtain the skills and knowledge required to work securely is often done through awareness raising or training. This not only helps protect your organisation, but also demonstrates that staff are valued, and that their importance to the business is recognised.
- 3. Asset management** – Asset management encompasses the way that the required knowledge of your assets can be established and maintained. Over time, systems generally grow organically, and it can be difficult to maintain an understanding of all the associated assets. Incidents can occur as the result of not fully understanding an environment, whether it is an unpatched service, an exposed cloud storage account or a mis-classified document. Ensuring that all of these assets are known about is a fundamental precursor to being able to understand and address the resulting risks. Understanding when systems will no longer be supported can help to better plan for upgrades and replacements and help to avoid operating vulnerable legacy systems.
- 4. Architecture and configuration** – The technology and cyber security landscape is constantly evolving. To address this, organisations need to ensure that good cyber security is baked into their systems and services from the outset, and that those systems and services can be maintained and updated to adapt effectively to emerging threats and risks.
- 5. Vulnerability management** – The majority of cyber security incidents are the result of attackers exploiting publicly disclosed vulnerabilities to gain access to systems and networks. Attackers will, often indiscriminately seek to exploit vulnerabilities as soon as they have been disclosed. Therefore, it is important (and essential for any systems that are exploitable from the Internet) to install security updates as soon as possible to protect the organisation. Some vulnerabilities may be harder to fix, and a good vulnerability management process will help to prioritise remedial actions.

APPENDIX 2

NCSC: 10 STEPS TO CYBER SECURITY



6. **Identity and access management** – Access to data, systems and services need to be protected. Understanding who or what needs access, and under what conditions, is just as important as knowing who needs to be kept out. Appropriate methods must be chosen to establish and prove the identity of users, devices, or systems, with enough confidence to make access control decisions. A good approach to identity and access management will make it difficult for attackers to pretend they are legitimate, whilst keeping it as simple as possible for legitimate users to access what they need.
7. **Data security** – Data needs to be protected from unauthorised access, modification, or deletion. This involves ensuring data is protected in transit, at rest, and at end of life (that is, effectively sanitising or destroying storage media after use). In many cases, data will be outside your direct control, so it important to consider the protections that can be applied, as well as the assurances that may be needed from third parties. With the rise in increasingly tailored ransomware attacks preventing organisations from accessing their systems and data stored on them, other relevant security measures should include maintaining up-to-date, isolated, offline backup copies of all important data.
8. **Logging and monitoring** – Collecting logs is essential to understand how systems are being used and is the foundation of security (or protective) monitoring. In the event of a concern or potential security incident, good logging practices will allow a retrospective view of what has happened and understand the impact of the incident. Security monitoring takes this further and involves the active analysis of logging information to look for signs of known attacks or unusual system behaviour, enabling organisations to detect events that could be deemed as a security incident, and respond accordingly in order to minimise the impact.
9. **Incident management** – Incidents can have a huge impact on an organisation in terms of cost, productivity and reputation. However, good incident management will reduce the impact when they do happen. Being able to detect and quickly respond to incidents will help to prevent further damage, reducing the financial and operational impact. Managing the incident whilst in the media spotlight will reduce the reputational impact. Finally, applying what has been learned in the aftermath of an incident will better prepare the organisation for any future incidents.
10. **Supply chain security** – Most organisations rely upon suppliers to deliver products, systems, and services. An attack on suppliers can be just as damaging as one that directly targets the organisation directly. Supply chains are often large and complex, and effectively securing the supply chain can be difficult due to inherent vulnerabilities, introduced or exploited at any point within the chain. The first step is to understand the supply chain, including commodity suppliers, such cloud service providers and those suppliers of bespoke contracts. Exercising influence where possible, and encouraging continuous improvement, will help to improve security across the supply chain.

CONTACTS



Victoria Murray – Head of Digital Services

Victoria.Murray@durham.gov.uk

Steve Hodgson – ICT Technical Services Manager

Steve.Hodgson@durham.gov.uk

Matt Manning – Hosting and Security Manager

Matt.Manning@durham.gov.uk

Please ask us if you would like this document summarised in another language or format:



Braille,



Audio,



Large print.

Email: digitalsupport@durham.gov.uk