South Kesteven District Council

CYBER SECURITY STRATEGY

SOUTH KESTEVEN DISTRICT COUNCIL

CONTENTS

FOREWORD

Cllr Richard Cleaver

Information and data are vital to every part of South Kesteven District 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 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 SKDC. We will strengthen and secure SKDC 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 protection 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 ICT 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.

INTRODUCTION

The South Kesteven priorities are:

- Connecting Communities
- Sustainable South Kesteven
- Enabling Economic Opportunity
- Housing
- Effective Council

This vision is set out in our Corporate Plan and our ICT strategy builds on that plan.

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

The Covid 19 pandemic impacted on all areas of public and private life. It led to more routine professional and personal interactions to move on-line and many of us now work from home.

This has presented new and lucrative opportunities to cyber criminals. The extent to which we exploit cyberspace and many of our working practice will not return to the pre-pandemic levels. 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 a crucial factor in combating cyber threats and reducing risk in a constantly changing online environment. Ongoing training and education programmes seek to raise awareness of digital security whilst improving and reinforcing the important of the human element of cyber defence.

This strategy is our cyber security commitment, both to the people we represent. It supports delivery of the ICT Strategy and the Council Corporate Plan by providing a framework for SKDC to securely harness the benefits of digital technology for the benefit of all.

PURPOSE AND SCOPE

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 seek to meet the requirements of the Cyber Assessment Framework (CAF) which is a framework provided by the National Cyber Security Centre (NCSC) to assess our resilience capability using 4 high-level objectives and 14 principles. Further detail can be found here Cyber Assessment Framework - NCSC.GOV.UK

The scope of this strategy includes all SKDC'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?

To deliver services, South Kesteven District Council collects, processes, transports and stores large amounts of personal and sensitive data. This data is transmitted internally and externally and is stored on both in-house and cloud-base servers.

A successful cyber-attack would disrupt the ability of the Council to deliver services, many of which are vital and support the most vulnerable residents within the district. The cost of a cyber incident can be significantly high as well as the cost to data integrity and damage to reputation.

A strong approach to cyber security enables us to protect information, the systems that are used to process and store it and ensure our services are kept secure and running. It is also vital in ensuring the public can trust the council with their information.

We have seen over the last couple of years that organisations like Councils, Academic and Health authorities that have suffered from a Cyber-attack had weeks of disruption and costs running into the hundreds of thousands of pounds to put system back into operation.

THE CHALLENGE WE FACE AS A COUNCIL

- The Council needs to keep pace with the ever-changing face of technology. New innovations such as AI, Process Automation and the Internet of Things mean we need to be ready to embrace these technologies but be assured we can do so safely and securely.

- 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. As well as providing a secure environment for these transactions we also need to ensure officers are educated in best-practices and be aware of indicators of a potential cyber-attack.

- 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.

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 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 .

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.

Terrorists

Some terrorist groups demonstrate intent to conduct cyber-attacks. Terrorist groups could obtain improved capability in several 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 AND RISK

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 unsupportable, 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 are the only solution to this challenge.

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.

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 user training** to help mitigate insider threats, understand supply chain risks and ensure all staff understand the issues and their responsibilities.

✓ **Cyber response planning and testing** to ensure we have clear plans to deal with an incident or suspected incident. These plans should be tested regularly within the IT team so that officers are familiar with the plans and that they are fit for purpose.

✓ **The Cyber Assessment Framework** is a collection of cyber security guidance created by the NCSC for organisations that play a vital role in the day-to-day life of the UK, with a focus on essential functions**.** This framework will be used to measure and monitor the effectiveness and validity of our strategy

IMPLEMENTING THE STRATEGY

Deter and Detect

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

Actions

✓ **Support enhanced governance** through the application of government's Cyber Awareness Framework .

✓ **Maintain secure configuration,** by following security baseline guidance and best practice from industry

✓ **Continue to strengthen identity security,** adopting modern authentication standards such as FIDO2

✓ **Maintain Defences at all Levels** by :

- » Keeping Anti-Virus and Malware prevention software is up to date.
- » Ensuring hardware and software version are kept up to date with latest firmware and patches

✓ **Removable media/device controls** .

✓ **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.

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**.

✓ **Provide training** for staff and elected members .

✓ **Continued development an incident response and management plan**, with clearly defined actions, roles and responsibilities.

✓ **Develop and maintain 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, SKDC have:

- A cyber-specific response plan which is regularly reviewed
- Set up playbooks to support test exercises on a regular basis; to ensure effective reaction to incidents when they occur.
- Setup monitoring tools provided by the NCSC to continually monitor the Council's systems.
- Engaged with NCSC to complete the Cyber Assessment Framework.
- Provide relevant cyber security training for staff and elected members.
- Complied with the applicable standards (PSN, PCI-DSS, etc).

CYBER SECURITY GOVERNANCE

ROLES AND RESPONSIBILITIES

Effective cyber security governance at South Kesteven is delivered through the following roles and functions

Senior Information Risk Owner (SIRO)
The Council's Senior Information Risk Owner (SIRO) will be a member of the Councils Senior Management Team. 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.

Corporate Information Governance Group (CIGG)
This group is made up of SKDC officers from multiple services and meets monthly. It aims to:

- Introduce new cyber information to analyse risk and inform on policy changes.
- Review any incidents or near misses to ensure lessons learnt are acted upon.

CYBER SECURITY GOVERNANCE

ROLES AND RESPONSIBILITIES

ICT Services
ICT services oversee the delivery of all IT systems for South Kesteven District Council.

Infrastructure Team
The infrastructure team is part of ICT services and manages the councils firewall and networking equipment as well as ensuring patch management is carried out to all South Kesteven equipment.

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

All South Kesteven Officers and Councillors
It is the responsibility of all officers to comply with the standards set out in this Cyber Security Strategy.

APPENDIX 1

STANDARDS

Currently SKDC must comply with the following standards:

✓ Bankers' Automated Clearing Services (BACS)

✓ Criminal Justice Secure Mail (CJSM)

✓ Payment Card Industry Data Security Standard (PCI DSS)

✓ Public Services Network (PSN)

In addition, SKDC should follow all relevant National Cyber Security Centre (NCSC) guidance

CONTACTS

Gyles Teasdale – Head of Property and ICT
Gyles.teasdale@southkesteven.gov.uk

Gary Andrew – ICT Manager
Gary.andrew@southkesteven.gov.uk