**Cyber Security Strategy Blueprint**

Introduction

This blueprint has been developed by the Local Government Association (LGA). It aims to assist councils in England with managing, detecting, defending against and minimising the impact of cyber incidents in line with the National Cyber Security Centre’s (NCSC) [Cyber Assessment Framework](https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework).

It is not possible to completely eliminate the risk of a cyber incident. However, councils should take steps to maximise defences and minimise vulnerabilities in a way that is proportionate to the risks faced by the authority across all its services and departments. Developing a cyber security strategy is an important step in doing this.

This blueprint outlines the key things to consider when writing or updating a cyber security strategy. It sets out an approach to protecting services and assets which enable councils to continue delivering critical services for the benefit of local communities.

It is recommended that the blueprint is read in conjunction with our [Cyber 360 Framework](https://www.local.gov.uk/publications/lga-cyber-360-framework#introduction). This is a resource which supports councils to develop their security and resilience capabilities and knowledge in line with existing good practice, advice, and standards.

**Disclaimer**: This blueprint is meant to provide general guidelines and should be used as a reference. It may not take into account all relevant local and national considerations and is not a legal document. The LGA will not assume any legal liability that may arise from the use of this document.

# **User Guide**

## **Why develop a cyber security strategy?**

A cyber security strategy is an organisation’s strategic plan for building cyber resilience. It sets out a vision for managing cyber risks, mitigating vulnerabilities, and ensuring the confidentiality, integrity, and availability of an organisation’s digital resources. It does this by setting out an organisation’s approach to protecting its information systems, networks, data, and digital assets from potential threats, attacks, and unauthorised access.

This is important in ensuring that councils can provide critical services to local communities. Councils across the country continue to pursue new, emerging, and innovative ways to deliver improvement to services through digital, data and technology. From tech enabled care to machine learning and implementing cloud solutions, there are wide ranging opportunities for local government to streamline the delivery of services, save costs and create better outcomes for residents. However, councils also need to consider and mitigate associated security risks.

As a custodian of large datasets and a service provider to some of the most vulnerable in society, it is also essential that councils take steps to protect personal data.

A cyber security strategy therefore acts as a key enabler for the council’s wider corporate plan, digital transformation ambitions and ICT modernisation strategy by setting out an approach to minimise existing and emerging cyber risks.

There are also a number of other benefits to having a strategy in place:

* The NCSC’s [Cyber Security Toolkit for Board Members](https://www.ncsc.gov.uk/collection/board-toolkit/embedding-cyber-security-into-your-organisation) recommends creating a strategy to reduce risk, financial impact and reputational damage to an organisation.
* It can be helpful in demonstrating the organisation’s cyber security vision which can be useful for external suppliers, partners and auditors when considering an organisation’s cyber security maturity.
* It can also be used to mobilise resources and bring together existing policies, processes, sub policies and standards - for example an Information Security Policy and ISO/IEC27001 standard - into one overarching strategy.
* It can foster a multi-disciplinary approach to managing cyber risk by promoting council wide awareness of managing cyber risk.

## Who should use this Blueprint?

In a council, depending on its size, its Director of IT/ Head of IT or Senior Information Risk Owner (SIRO) will typically ‘own’ its cyber security strategy. The ‘owner’ should have sufficient accountability, authority, and responsibility to help secure resources and support for the delivery of the strategy. Crucially their involvement can also help foster a multi-disciplinary approach across the council and facilitate a culture which sees cyber security as a small part of everyone’s job.

This helps to maintain a strong cyber security posture across the council and protect its assets from external threats. It is an ongoing effort and collaboration among various council departments promotes a shared responsibility and a holistic understanding of cyber security risks and mitigation strategies. This is also important in ensuring that a cyber security strategy reflects an organisation’s unique requirements and addresses potential vulnerabilities effectively.

We therefore outline the roles of multiple stakeholders in developing and maintaining a cyber security strategy.

How to use this Blueprint

This blueprint has been designed as a starting point to support councils in England develop an effective and comprehensive cyber security strategy. It uses the NCSC’s Cyber Assessment Framework as a good practice framework.

There are three main purposes for the blueprint:

* To assist councils in considering how to write, update or review their cyber security strategy.
* To assist in starting conversations with key stakeholders who will be involved in implementing the strategy.
* To assist councils in collecting the information needed to support the development of an effective strategy through a series of prompt questions.

Note: We recognise councils will operate within different structures and financial constraints and some might have existing cyber security action plans or policies in place. This blueprint has been developed to assist councils in writing a visionary strategic document which brings existing plans together and is aligned to the corporate plan, wider digital transformation programmes and ICT modernisation strategies. If intending to share the document publicly, councils should take care to ensure sensitive or classified information is not disclosed.

Here’s a suggested approach to using this template effectively:

**Figure 1: How to use this blueprint?**

Review the blueprint: Familiarise yourself with the template and its sections. Understand the overall structure and the purpose of each section.

Gather organisation-specific information: Identify the specific details and information that are unique to your council. This may include the governance structure, existing policies and procedures, risk assessment results, regulatory requirements, and any other relevant information.

Customise the blueprint: Fill in each section with the appropriate details based on the council’s requirements, resources, and risk profile. Address the questions and provide relevant details, policies, and procedures that align with your council’s needs and resources. Once the information is completed, customise with the council’s corporate template ready for publication.

**Please note:** The boxes contained in this blueprint are for guidance only. All boxes and highlighting should be deleted prior to publishing the strategy and appropriate document classification should be added.

## How to mobilise, develop and report on the strategy

### Figure 2: Seven steps to mobilising, developing and reporting on a strategy

**Step 1. Engage stakeholders:** Engaging stakeholders from the outset is an important first step to secure buy in and to ensure that representatives from different services have an opportunity to feed into the process. It can also establish the council’s baseline systems, assets, risk management approach and security policies and processes. Depending on who is initiating the development of the strategy, conversations should be sought with a senior level officer with sufficient authority, accountability and responsibility to champion the strategy. The specific individuals to be involved will depend on the size and structure of the council, but Table 1 outlines some key stakeholders.

**Step 2. Establish a timeline.** Securing buy in and cooperation from stakeholders will take time. You should give yourself plenty of time to develop the strategy in conversation with stakeholders and to secure senior and political support. The exact timeline will be dependant on the council’s maturity levels and wider cultural awareness of cyber risk. You should also consider what period of time the strategy will cover, for example 2024 – 2027.

Step 3. Seek expert advice if needed: If you don’t have in-house expertise in cyber security, consider engaging external consultants or experts to provide guidance and assistance in developing the strategy. They can help ensure that the strategy aligns with industry best practices and addresses any specific challenges or requirements. But note that the scope and parameters of the strategy will ultimately need to be determined by the council in close discussion with any consultant you may commission. The [National Cyber Security Centre](https://www.ncsc.gov.uk/) is the preeminent organisation in the UK for the provision of advice, support and guidance on cyber security and it is useful to review the resources on their webpage for assistance.

Step 4. Develop, review, and refine: Once the initial draft is completed, review the entire strategy document to ensure coherence, consistency, and completeness. Seek feedback from relevant stakeholders and make necessary adjustments.

Step 5. Obtain approval: Present the finalised strategy to appropriate personnel within the council for review and approval. This may involve obtaining approvals from senior management, elected members, the IT department, legal department, and other relevant decision-makers.

Step 6. Communicate and implement: Once the strategy is approved, develop a plan for communicating the strategy to all relevant employees and stakeholders. Ensure that everyone understands their roles and responsibilities and the importance of adhering to the strategy. Implement the necessary measures and controls outlined in the strategy.

Step 7. Monitor, evaluate, and update: A cyber security strategy should be treated as a living document that evolves with the changing threat landscape and organisational needs. Continuously monitor the effectiveness of the strategy, assess emerging risks, and evaluate the organisation’s cyber security posture. Regularly review and update the strategy to address new threats, technologies, and regulatory requirements.

**Table 1: Stakeholder insights and actions**

|  |  |  |
| --- | --- | --- |
| **Who**  | **Mobilising role** | **Ongoing role** |
| Executive Leadership * Chief executive officer Chief information officer
* Chief technology officer
* Senior Information Risk Owner
* Chief Information Security Officer
 | Input of vision, strategic direction, risk appetite, resources and active involvement in development of the cyber security strategy. | Reviewing and discussing cyber security measures at board level, receiving updates on cyber risks, releasing resources to support cyber security improvement, championing cyber security across council. |
| Elected Members * Cabinet/Committee
* Portfolio holder for cyber security policies and procedures and their governance or equivalent
 | Input of strategic direction and political buy in, signing off on budget and strategy. | Accountability for cyber strategy, scrutinising functions in place to review policies, practices and procedures relating to cyber security, championing cyber security as part of broader corporate risk management. |
| IT Department * IT managers
* IT Security Manager
* Network administrators
* System administrators
* Security Operations Centre (if relevant)
* Other IT staff members
 | Input of technical knowledge and insights, including policies and processes for protecting IT systems, networks and servers and security monitoring. | Implementing cyber security measures and ensuring the protection of digital infrastructure. |
| Information Security Officer or equivalent | Input of expertise and experience in cyber security including risk assessment, compliance, incident response, and security governance. | Overseeing and managing information security. |
| Data protection officer or equivalent | Input on correct processes and procedures regarding council’s data protection obligations under GDPR.  | Overseeing and monitoring the council’s compliance with data protection legislation. |
| Information Governance Officer or equivalent | Insight into prioritisation and risk planning to protect your council’s IT estate, data, and other digital assets. | Overseeing compliance with relevant data protection, freedom of information, and other information governance policies. |
| Information Asset Owners | Insight into existing assets and existing security controls, policies, and process. | Managing and protecting the assets under their control, including managing joiners, leavers process, reviewing access controls etc. |
| Audit officer | Independent review and testing of security controls, mitigations and risk management processes that are in place. | Assurance on defences and resilience plans which comply with a relevant information security management framework. |
| Business Continuity, and/or Emergency Planning teams | Inputs to ensure there is a robust business continuity plan in place that incorporates cyber incident planning which is sufficiently exercised. | Sufficient exercising of strategy to ensure disruption to business services are mitigated. |
| Legal and Compliance Team | Insights to ensure that the cyber security strategy aligns with legal requirements and regulations. | Assessment of legal risks including securing contracts and legal documents, identification of privacy concerns, and compliance with relevant data protection laws and regulations. |
| Human Resources, and Learning and Development teams | Insights into developing staff awareness training programme and processes to embed a cyber security culture across whole council. | Development of policies and procedures related to employee training, awareness programs, and defining acceptable use of technology resources |
| Communications and Public Relations | Insights into concerns about cyber security incidents and public trust and organisational reputation. | Creating effective communication plans, managing public relations during incidents, and ensuring consistent messaging to stakeholders. |
| Departmental Representatives Finance, public safety, planning, social care, revenues and benefits, housing and other relevant departments | Insights from different departments to aid understanding of the specific cyber security needs and challenges faced by each department.  | Ongoing monitoring of cyber security risks within service risk register/ Business-as-usual services as well as in new and planned projects as well as in supply chain. |
| External ExpertsExternal cyber security consultants, auditors, or advisors to supplement internal expertise | Provision of specialist knowledge and expertise, conducting risk assessments, and making recommendations based on industry best practices. | Periodic review and audit of the effectiveness of the cyber security strategy, risk management and security policies and processes.  |

# The Local Government Association – Cyber Security Strategy Template

Date: April 2024

Date of next review: July 2024

# [Insert your Council’s name] Cyber Security Strategy

Version: [Enter version reference]

Date: [Enter Date]

Period: [Enter the period the strategy will cover. It should give your organisation enough time to deliver against the strategy, but not too much time that it becomes obsolete due to changes in direction or other factors.]

## Table of Contents

1. [Foreword](#_Foreword_1)
2. [Summary](#_Summary)
3. [Introduction](#_Introduction)
	1. [Background, Scope and Purpose](#_Background,_scope,_and)
	2. [Technology and industry trends](#_3.2_Technology_and)
	3. [Objectives](#_Objectives_1)
	4. [Vision](#_Vision_1)
4. [Managing Security Risk](#_Governance_and_Leadership)
	1. [Cyber security governance framework](#_Cyber_security_governance_1)
	2. [Risk Assessment Framework](#_Cyber_Security_Governance)
	3. [Risk Treatment Framework](#_Risk_Treatment)
	4. [Embedding cyber security and resilience in supply chains](#_Embedding_cyber_security)
5. [Protecting against cyber attack](#_Security_Controls)
	1. [Policies and processes](#_Policies_and_processes)
	2. [Identity and Access Control](#_Identity_and_access)
	3. [Data Security and Privacy](#_Data_security_and)
	4. [System and Software Security](#_System_and_Software_1)
	5. [Resilient networks and systems](#_Resilient_networks_and)
	6. [Training, Communication, and Awareness](#_Training,_communication_and)
6. [Detecting cyber security events](#_Detecting_cyber_security)
	1. [Security Monitoring](#_Security_Monitoring)
	2. [Proactive Incident Detection](#_Proactive_Incident_Detection)
7. [Minimising the impact of cyber security incidents](#_Compliance_and_Legal)
	1. [Incident Response Approach](#_Incident_Response_Approach)
	2. [Business Continuity and Disaster Recovery Approach](#_Business_Continuity_and)
	3. [Lessons Learned](#_Lessons_Learned_1)
8. [Compliance, constraints, interdependencies, and obligations](#_Compliance,_constraints,_interdepen)
	1. [Data protection](#_Data_Protection)
	2. [Compliance](#_Legal_and_Contractual)
	3. [Constraints and interdependencies](#_Constraints_and_interdependencies)
	4. [Legal and contractual obligations](#_Legal_and_Contractual_1)
9. [Managing progress and delivery of strategy](#_Managing_progress_and)
	1. [Security Metrics and Key Performance Indicators (KPIs)](#_Training_and_Awareness)
10. [Conclusion](#_Conclusion)

|  |
| --- |
| This blueprint has been funded by the UK Government and is made available under the [Open Government License V3](https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/). Councils are free to copy, publish, distribute, transmit, combine and/or adapt the Information in this strategy for local use. This box should be deleted prior to publishing your strategy. |

## Licensing notice

## Foreword

|  |
| --- |
| The cyber security strategy should be introduced by the relevant portfolio holder or member of the Executive Leadership team within a council outlining ownership and/or political buy in. They should champion the commitments set out in the strategy thereby providing a governance link to the implementation of the strategy. The foreword should provide an overview of why it is important, how it fits in with wider council strategies and how it can create better outcomes for local communities through the protection of key council assets. |

## Summary

|  |
| --- |
| The summary should provide a high-level overview of the cyber security strategy, including the vision and key objectives. It should summarise the council’s commitment to protecting information assets, ensuring the confidentiality, integrity, and availability of systems and data, and safeguarding against cyber threats. You should consider how this can underpin and enable the council’s corporate plan, digital transformation programme as well as other relevant strategies such as ICT Modernisation programmes. It should explain how protecting and maintaining systems, and other digital assets can enable the council to empower communities by being able to continue to deliver critical services. You should also consider the role that councils play in safeguarding residents by protecting data and how this can contribute to maintaining trust and confidence between the council and communities. |

## Introduction

###  Background, scope, and purpose

|  |
| --- |
| State the purpose of the cyber security strategy, outlining why it is important for the council to have a comprehensive and robust approach to cyber security considering the current threat landscape and why councils are at risk. Define the scope of the strategy, including the systems, networks, and data covered by the strategy.Consider:Background* What is the wider national context that affects councils? For example, Government strategies, policies, and roadmaps e.g. ([National Cyber Strategy](https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022), [Roadmap for Digital and Data, 2022 – 2025](https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025))
* What are the potential risks and threats that the council faces in the realm of cyber security particularly in proportion to its vulnerabilities?
	+ Include the evolving nature of cyber threats and the importance of keeping pace with emerging technologies.
	+ Include the impact of known vulnerabilities on your council services
* What are the relevant regulatory requirements and standards that the council must comply with?
* How can this strategy enable the council to comply with, monitor and report on these requirements and standards?

Scope* At a high level, have you considered what systems, networks, and data as well as other key assets will be covered by this strategy? (Consider if this is a public document, what information you would release into the public domain?)

Purpose* How does a comprehensive and robust cyber security strategy help protect sensitive data, information, and systems and prevent disruption to services within the council?
	+ Include compliance with relevant data protection and privacy regulations and other legal frameworks.
* How does an effective cyber security strategy contribute to maintaining public trust and confidence in the council’s ability to handle sensitive information securely?
* What are the potential financial and reputational consequences for the council if it does not have a comprehensive and robust cyber security approach in place?
* How does the cyber security strategy facilitate collaboration and information sharing with other councils, government agencies, commissioned services, and health and social care agencies to strengthen overall resilience against cyber threats?
* How does the cyber security strategy address emerging technologies such as Machine Learning and Artificial Intelligence in the cyber landscape?
* How does this strategy align with your council’s overarching corporate strategy and deliver better outcomes for residents by preserving critical services?
* How does it link with wider relevant strategies such as your IT Strategy, Risk Management Strategy, Digital Transformation Strategy, HR Strategy, Data Protection and Privacy Strategy, and the wider organisational strategy.
 |

### 3.2 Technology and Industry Trends

|  |
| --- |
| Explain how the council will stay abreast of emerging cyber security technologies, threats, and industry best practices, ensuring that the strategy remains up-to-date and effective.Consider:* External forums that share best practice, advice, guidance and alerts on cyber threats for example the [Warning Alerts and Response Points (WARPs)](https://socitm.net/about/warps/) forums.
* Signing up to free alert services e.g. [NCSC’s Early Warning Service](https://www.ncsc.gov.uk/information/early-warning-service)
* Who will be responsible for horizon scanning?
 |

### Objectives

|  |
| --- |
| This template sets out four overarching objectives **from sections 4 to 7** which are linked to the NCSC’s Cyber Assessment Framework. Councils can use these objectives as a baseline and consider how these align with the overall goals of the council and address any unique challenges or requirements. Include reference to wider policies and compliance obligations e.g. Data Protection Act (DPA), and Data Security and Protection Toolkit (DSPT) (where appropriate). |

### Vision

|  |
| --- |
| Outline the desired end state that you are hoping to achieve by developing this cyber security strategy considering how developing a strong cyber security strategy can support the efficient and high-quality delivery of important council services and to maximise productivity by enabling staff to deliver their work with minimal disruption. Consider how it can maintain trust and integrity in council services by local communities by ensuring data and other assets are safeguarded and protected.Consider using sections 4 to 7 to describe the journey from current state to desired end state. **N.B.** You should consider the sensitive nature of information captured and whether this information can be shared publicly or whether there are elements you wish to retain in an internal classified document. |

## Managing security risk

### Cyber security governance framework

|  |
| --- |
| Describe the improved governance framework that will guide cyber security risk management and improvement initiatives and how this will be integrated into organisational risk management and decision making. This may include policies, procedures, and standards for cyber security.Consider:Leadership and direction* Is there a senior champion involved who can secure and release resources, and promote the vision across the council?
* Consider the appropriate board or committee that will oversee and champion the delivery of the strategy.
* Is there a portfolio holder?
* Are there sufficient senior officers on this committee?
* Is there a change management board or technical design authority (TDA) who will need to be involved in its oversight?

Assurance* Consider how the council will seek assurance in its cyber security, through audits, penetration checks, IT health checks, compliance regimes and accreditations.

Roles and responsibilities* Consider what roles and responsibilities need to be delegated and where accountability lies for implementing the strategy as well as the escalation routes. In particular, consider the responsibilities and accountabilities of the following roles:
* Senior management team, including Chief Executive, Senior Information Risk Owner, Chief Technology Officer, Senior Information Security Officer
* Elected Members
* IT manager
* IT Security Manager
* Network Administrator
* Security Analyst
* Incident Response Lead
* Business Continuity/Emergency Planning Lead
* Data Protection Officer
* Information Security Officer
* Information Governance Officer
* Audit Officer
* Information Asset Owners
* Learning and Development Lead
* HR Lead
* Legal and compliance
* Communications team
* Shared services teams (if relevant)
* Heads of Service
* Managers
* Whole workforce
* Security Operations Centre (if relevant)
 |

### Risk assessment framework

|  |
| --- |
| Describe how you will manage cyber security risks throughout the lifecycle of the strategy. Consider how the organisation works together as part of its corporate risk management approach to own and mitigate new and existing risks related to the council’s assets e.g., systems, hardware and data. Consider:* Assets
	+ How will assets be identified and managed?
* Threats x Vulnerabilities = Risk
	+ How will threats be identified?
	+ How will vulnerabilities be assessed?
* Mitigations and treatments
	+ How will mitigations be identified, prioritised, and funded?
	+ How will existing controls be built upon?
* Monitoring and reporting
	+ How will risks be escalated and prioritised?
	+ How will risks be monitored and reviewed?
	+ How will you ensure consistency so risks are comparable across the organisation?
* The known and unknown risks in complex supply chains. How will these be identified and managed? Who will be responsible?
* The roles and responsibilities of service leads, asset owners, IT and third-party suppliers and providers.
 |

### Risk treatment framework

|  |
| --- |
| Outline the measures and controls that will be implemented to mitigate identified risks and how you will prioritise addressing vulnerabilities to reduce the impact of potential cyber threats.Consider:* The appropriateness of background checks on certain employees and contractors to ensure trustworthiness.
* Incident reporting and response: What existing procedures do you have in place for identifying incidents both at an organisational and individual level? Do you have proactive security monitoring capabilities? Is there a no blame culture which encourages reporting?
* Security policies and procedures: What policies and procedures are in place which describe security measures, acceptable use guidelines, incident response protocols, and regular security assessments.
* Change management: Do you have a process for managing and documenting changes to systems, software, and configurations to prevent unauthorised modifications?
* Network security measures: What is your approach to securing the network? Do you have firewalls, intrusion detection systems, and/or intrusion prevention systems in place to monitor and protect the network from unauthorised access and malicious activities?
* Secure configurations: How will you monitor and implement industry best practices for secure configurations of operating systems, applications, and network devices to minimise vulnerabilities?
* Encryption and secure data transmission: How will you use encryption technologies to protect sensitive data during transmission and ensure secure communication channels?
* Regular patching and updates: How will you maintain up-to-date software and firmware by applying security patches and updates to address known vulnerabilities?
 |

### Embedding cyber security and resilience in supply chains

|  |
| --- |
| Outline how vulnerabilities in supply chains, that could have an impact on key systems or compromise sensitive datasets, will be managed. This should include maintaining appropriate obligations in contracts with suppliers and ensuring these are covered for sub-contractors as well. Consider:* The processes you have in place for engaging with suppliers about security requirements at the procurement stage. How are these managed during the lifecycle of the product/service?
* The systems and registers your council utilises to manage and monitor contracts.
* Do you know what key systems are reliant on suppliers. If not, how will you identify these? What contractual obligations are in place for the supplier to ensure adequate protections are in place to protect these systems?
* How is ownership of risk shared between IT teams and service leads/officers?
* What policies and processes does the supplier have in place to manage cyber risk and ensure data is protected in rest and in transit?
* What collaborative arrangements are in place with suppliers to maintain awareness of evolving threats and maintain and improve arrangements to respond to these threats?
 |

## Protecting against cyber attack

### Policies and processes

|  |
| --- |
| Outline the improved policies and processes that will direct the council’s overall approach to securing systems and data that support the operation of essential functions*.*Consider the relevance of the following policies and plans. Are they relevant/up to date and are there any others to consider?* Information Security Policy
* Acceptable Use Policy
* Access Control Policy
* Data Classification and Handling Policy
* Incident Response Plan
* Disaster Recovery Plan
* Business Continuity Plans
* Patch Management Policy
* Data Backup and Recovery Policy
* Risk Management Policy
* Awareness and Training Policy
* Clear Desk and Clear Screen Policy
* Remote Working Policy
* Change Management Policy
* Supply Chain Security Policy
* Working from Abroad Policy
 |

### Identity and access controls

|  |
| --- |
| Outline how access control mechanisms and identity management practices will be used to ensure only authorised individuals have access to systems and data.Consider:* The roles and responsibilities of HR, IT, Managers, Asset Owners.
* Privileged user management. Are full privileges absolutely necessary and are these regularly reviewed?
* The policies and processes for identity verification, multi factor authentication (for privileged accounts and consider for all accounts) and authorisation.
* Password policy – does it balance usability and security?
* The policies and processes for ensuring only trusted devices have access to the council’s networks and systems. Has Multi-Factor Authentication been set up on these devices?
 |

### Data security and privacy

|  |
| --- |
| Explain how the council will protect sensitive data, including personal information, through encryption, data classification, access controls, and data lifecycle management.Consider:* Do you know what types of sensitive data, including personal information, the council handles and how it is currently classified? How will you identify these and ensure adequate controls and encryption mechanisms are in place?
* Do you have access controls to restrict unauthorised access to sensitive data? If not, how will you develop these?
* What data lifecycle management practices are followed to ensure secure handling of sensitive data from creation to disposal?
* Who are the data controllers and data processors and what are your compliance responsibilities under data protection legislation?
* Who does the Data Protection Officer report to and what processes are in place to ensure the advice and guidance provided is applied to ensure you are following the correct data protection regulations?
* How does the information security officer create, maintain, and communicate security risks and issues to other teams and departments and implement mitigation strategies to manage these?
* How are employees trained and educated about their responsibilities for protecting sensitive data, including data security best practices and privacy principles?
 |

### System and Software Security

|  |
| --- |
| Explain which measures will be implemented to ensure the security of systems and software used by the council, including secure configuration, patch management, and vulnerability scanning.Consider:* Do you know what current system and software security vulnerabilities the council has? If not, how will you identify these?
* What policies are in place which document vulnerability management and patch management?
* Who is responsible for managing and monitoring system vulnerabilities and risks? Is this in house, outsourced, or both?
* How will you identify and protect from the potential threats and attack vectors that could exploit the council’s systems and software?
* What are the existing security controls and measures in place? How will you continuously review these to ensure they remain effective?
* What are the legal and regulatory requirements related to system and software security that the council must comply with?
* What are the best practices and industry standards for system and software security that the council should follow?
* What policies and processes do you have in place to protect physical assets, such as servers, data centres, and other critical infrastructure? Who is responsible for implementing these?
 |

### Resilient networks and systems

|  |
| --- |
| Outline the measures and policies that will be implemented to increase the resilience of networks to attacks, and what back-ups and recovery plans are in place to mitigate disruption to systems.Consider:* What processes do you have for maintaining backups of priority datasets that can be recovered in the event of an attack? Are there offline as well as cloud-based back-ups?
* Are there alternative routes or standby systems which can provide access to your systems?
* How do you identify what the essential operational systems are? Do you know if they are segmented from other business systems to prevent lateral movement in networks?
* How do you identify the attack surfaces vulnerable to attack and do you have a policy in place for regularly updating these, and removing default configurations that aren’t required (e.g. user accounts, passwords, demo capabilities)?
 |

### Training, communication and awareness

|  |
| --- |
| Explain how the council will promote an improved culture of cyber security awareness and ensure effective communication channels are established to disseminate information and guidance to all staff. Describe the training programmes that will raise awareness of individual responsibility in reducing cyber-attacks.Consider:* Is there training in place and what is the scope of the training?
* What training will be offered to the whole workforce? What about role-based training both for non-technical and technical staff?
* How often will refresher training need to be done (e.g. annually)? How long after joining will staff need to complete certain training?)
* What policies and guidelines will be created to ensure there is a clear protocol for dealing with cyber threats? Is this owned and developed by the organisation’s CISO?
* Which channels can staff use to report suspicious emails or potential cyber threats? Are staff aware of how to access these and report these incidents?
* Are there any campaigns in place to raise awareness of cyber threats through your council’s internal staff communication channels?
* Who is responsible for monitoring emerging threats and working with other teams, training providers, comms to update learning resources and policies?
 |

## Detecting cyber security events

### Security Monitoring

|  |
| --- |
| Outline the security monitoring policies and processes that you will put in place to collect, analyse and store logs to ensure they can be utilised in the event of a cyber incident.Consider:* What policies and processes do you have in place for collecting logs? How will you ensure it is proportionate to the levels of threat your systems and networks face and is balanced against available resources?
* How will you classify the types and sources of data you need and are able to collect? For example, website traffic, email traffic, IP connection, host-based activity etc
* What processes do you have in place to analyse your logs? How will you ensure they are retained for an appropriate timeframe? Is there a process for storing them based on the sensitivity of the data/systems?
* What encryption and security policies are in place to protect logs? Are they accessible and encrypted e.g. in a centralised location and in transit?
* Where is the skillset/expertise in your council to be able to detect incidents and analyse logs? Are they in house or outsourced?
 |

### Proactive Incident Detection

|  |
| --- |
| Outline how your council will proactively detect and respond to cyber security incidents. This may include establishing an intrusion detection system or security information and event management (SIEM) solution. You may also consider a Security Operation Centres (SOC) (subject to budget) or outsourcing to a Managed Security Service Provider (MSSP). Consider:* What systems are in place to monitor user access and activity to identify abnormal activities? Are system abnormalities from past attacks used to enrich monitoring solutions?
* Are there specialist monitoring tools in place such as SIEM, SOC or MSSP to identify security incidents and generate alerts? If not, would you consider introducing them subject to budget and proportionate to the threat the council faces?
* Have you used your understanding of logs to create detection alerts based on the expected threats?
* Are you signed up to any relevant forums and networks which share intel on latest threat information and indicators of compromise, e.g. [Cyber Security Information Partnership (CiSP)](https://www.ncsc.gov.uk/cisp/home) forum?
* Are you utilising free tools to assist with detection such as the [NCSC’s Early Warning Service](https://www.ncsc.gov.uk/information/early-warning-service)?
 |

## Minimising the impact of cyber security incidents

### Incident Response Approach

|  |
| --- |
| Outline how you will prepare and respond to incidents, taking into account the role of an incident response team and the implementation of incident response playbooks. Refer to incident response procedures, including how communication and reporting channels will be maintained and escalation processes established. Consider:* Is there an incident response team in place in the case of a cyber incident?
* Who are the key contacts in the event of an incident? What are the roles of various departments e.g. IT team, Senior Management, Legal, PR, HR, Insurance?
* Has a communications plan been developed and approved by the Executive Leadership team?
* Does the plan include details of external organisations that can/should be contacted in line with the severity of the breach, for example, NCSC, Information Commissioner’s Office, Government Security Group?
* Is there a process for categorising the severity of an incident? What is the escalation criteria and process for making critical decisions?
* Are there processes for recording and auditing actions and decisions?
* Are there more detailed incident response playbooks in place for incidents that are deemed highest risk?
* Has the incident response plan been tested and exercised regularly and involved members, senior officers as well as the incident response team?
* Does the plan contain clearly defined processes for each stage during the lifecycle of an incident?
* Do you have a retainer or access to security experts in a cyber incident?
* Do you have cover for out of office hours, weekends, bank holidays with your IT teams etc?
 |

### Business Continuity and Disaster Recovery Approach

|  |
| --- |
| Explain the council’s improvements to business continuity and disaster recovery planning, including establishing a prioritisation plan and ensuring that systems and data can be restored in a timely manner, minimising disruption to services. Refer to how you will involve different service areas in co designing business continuity and disaster recovery plans.Consider:* Have departmental representatives (information asset owners and other relevant stakeholders) been involved in co designing and signing off on business continuity and disaster recovery plans?
* Do you have a prioritisation plan for restoring critical services?
* Are the relevant service areas aware off the Recovery Time Objective and Recovery Point Objective?
* Do you have technical capabilities in place to respond to an attack, and implement an effective response e.g. triaging, analysing/containing, and recovering affected systems?
* Are there offline backups which can be recovered?
* What level of training has been delivered to the Executive Leadership team and incident response team?
* How will you ensure critical systems are segmented to minimise disruption in the event of a cyber incident?
 |

### Lessons Learned

|  |
| --- |
| Outline how the council will capture and analyse lessons learned from security incidents and near-misses, ensuring that improvements are made to prevent similar incidents in the future.Consider:* The policies and processes you have in place to capture lessons learned.
* Who is involved in reviewing the incident and capturing lessons learned?
* Is there a no blame culture which enable lessons to be captured transparently and fairly?
* What processes are in place to regularly review incident response planning and ensure lessons are captured from cyber incidents?
 |

## Compliance, constraints, interdependencies, and obligations

### Data Protection

|  |
| --- |
| Explain how the council will handle and protect personal data in accordance with data protection laws, including data retention, privacy impact assessments, and data breach notification procedures. |

### Compliance

|  |
| --- |
| Explain how the council will establish policies and processes which enable it to demonstrate compliance with relevant standards and regimes such as the Public Services Network (PSN). |

### Constraints and interdependencies

|  |
| --- |
| Consider any resource constraints that the council operates within which may have an impact on the development of cyber security processes for example interdependencies between networks, systems, data centres etc. |

### Legal and Contractual Obligations

|  |
| --- |
| Describe how the council will address legal and contractual obligations related to cyber security, including the use of third-party suppliers and service providers. |

## Managing progress and delivery of the strategy

### Security Metrics and Key Performance Indicators (KPIs)

|  |
| --- |
| Define the KPIs that will be used to measure the effectiveness of the cyber security strategy and identify areas for improvement.Consider:* What governance arrangement will be in place to review the progress and impact of the strategy?
* How does this link to the overall strategic context in which the council operates in?
* Who is responsible for monitoring the delivery of this strategy?
* Who is accountable for delivering the vision set out in this strategy and also managing interdependencies between the different ambitions set out in this strategy?
 |

## Conclusion

|  |
| --- |
| Provide a concluding statement that emphasises the council’s commitment to cyber security and its ongoing efforts to protect systems, data, and stakeholders.Consider who will sign off commitment on delivering the strategy e.g. portfolio holder or Executive leadership team. |