Cyber Resilience Strategy

2022 - 2027

CONWY
CYNGOR BWRDEISTREF SIROL
COUNTY BOROUGH COUNCIL

Conwy - Sir flaengar sy'n creu cyfleoedd

Conwy - a progressive County creating opportunity

Table of Contents

1. Foreword

Information and data are vital to every part of the delivery of Conwy County Borough Council's services. As we continue with our Digital Transformation ambitions to modernise the way we work and provide greater choice in how people access information and services, we need increasingly robust security measures to protect against cyber-threats and disruption to our Information Technology (IT) infrastructure.

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

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

This strategy demonstrates our commitment and the key actions we will take over the next five years to further build on a trusted digital environment for Conwy. We will strengthen and secure the Council from cyber-threats by investing in our systems and infrastructure, deterring our adversaries, and developing a wide range of responses; from basic cyber hygiene to the most sophisticated defences. We will also ensure that we are prepared to deal with issues that may cause significant disruption to IT systems and infrastructure.

Cyber-attacks will continue to evolve, which is why we will continue to work to stay ahead of all threats. Given the growing reliance on IT together with frequency and complexity of attempted cyber-attacks we will also ensure processes are in place to help minimise impact on services in the event of a successful attack or significant disruption to our IT infrastructure and systems.

This Cyber Resilience Strategy underpins the Conwy Digital Strategy; which outlines how the Council will maximise technology to realise its vision to develop Conwy as a progressive County creating opportunity. Furthermore, it contributes to Conwy's corporate priority of ensuring People in Conwy are safe and feel safe by ensuring we take steps to protect personal data and promote cyber security to ensure our citizens stay safe online.

The measures outlined in this strategy will safeguard trust and confidence in the way we operate and deliver our services, supporting Conwy to remain at the forefront of the digital revolution.

Councillor Charlie McCoubrey,
Leader, Conwy County Borough Council

2. Introduction

This document sets out Conwy County Borough Council’s application of cyber resilience measures protecting our information systems, the data held on them and the services we provide from significant disruption, unauthorised access, harm or misuse.

It is our commitment to the County’s citizens, visitors, businesses, partners, officers and members as well as our commitment to maintaining secure systems and data in the local and national interest.

3. What is Cyber Resilience and why is it important?

Cyber Resilience is the ability to prepare for, respond to and recover from cyber-attacks or a wider disruption to Council IT systems or infrastructure which may impact on our services.

It has emerged over the past few years because traditional cyber security measures are no longer enough to protect organisations from the spate of persistent attacks, it is equally important for the Council to be able to demonstrate its resilience in the event of significant disruption to IT systems.

Cyber security is the more specific practice of ensuring the confidentiality, integrity and availability of information.

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

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

Cyber security is important because in order to effectively deliver services Conwy Council collects, processes, and stores large amounts of data on systems, computers and other devices at our data centres or in externally hosted (cloud) data centres. 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.

Conwy County Borough 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.

Adoption of good Cyber Resilience measures is crucial in ensuring our services are kept up and running as well as being prepared in the event of an attack or disruption to systems. 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 citizens and through damage to the council’s reputation.

4. Strategic Context

The overarching vision in the Council's Corporate Plan is "Conwy – A progressive county creating opportunity". We are working in a changing and demanding environment. Our vision is to be progressive in managing change and to use it to create opportunities; to safeguard what we have, and to build on this to accommodate change. This vision is a shared endeavour. We want to strengthen our relationship with citizens so that we can work together to improve the county. In all that we do, from educating children, caring for the vulnerable, recycling waste, regulating businesses, to providing leisure facilities and theatre performances to name but a few, we want to be progressive and creative so that we maximise the opportunities available to the communities within Conwy county

The plan sets out how we will maximise the use of digital technology and digital channels to provide more effective and efficient access to services. It also explains that we will exploit advancements in technology to transform the way our staff deliver their day to day work, looking at the tools they use as well as the facilities and locations where they work.

This Cyber Resilience Strategy supports delivery of the Corporate Plan (2022-2027) and the Digital Strategy (2022-2027) by providing a framework for the Council to securely harness the benefits of the digital revolution for the benefit of all stakeholders. It is essential to the efficient running and evolution of the Council.

This Cyber Resilience Strategy sits alongside the Digital Strategy supported by a suite of operational policies governing how officers and services should utilise technology and systems hosted locally or externally in a safe and secure manner.

5. Purpose and Scope

The Council's Digital Strategy has outlined four key priority areas targeting development of a truly Digital County – Digital Workforce, Digital Services, Digital Connectivity and Digital Economy. The scale of change represents significant shift in the journey to digitally transform the Council.

This Cyber Resilience Strategy has been developed in response to a number of successful and high profile cyber-attacks on public and private organisations. The purpose of the strategy is to give assurance to people accessing Council services and other stakeholders of our commitment in delivering robust information security measures to data from misuse and cyber threats. It aims to safeguard their privacy through increasingly secure and modern information governance and data sharing arrangements - both internally and with partners.

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

This strategy is intended to cover all Conwy County Borough Council information systems, the data held on them, and the services they help provide. It also sets out ways in which the Council will promote cyber security to citizens to help them stay safe online.

6. The Challenge

Conwy County Borough Council is using an increasing range of technology solutions and infrastructure including our web sites, management systems, and apps which are accessible from a wide range of devices including laptops, PCs, tablets or smartphones.

Increasing aspects of our services and systems are accessed online: corresponding with residents and local businesses, carrying out case work, providing support through contact centres, offering services and payments through the web, reviewing reports or papers for council meetings and meeting on digital platforms.

This direction of travel is expected to continue and accelerate; making effective cyber resilience measures ever more crucial in protecting against new types of threats, risks and vulnerabilities and ensuring the Council is equipped to recover in the event of significant disruption.

UK and Welsh Government guidance advises all public bodies to be fully prepared for the consequence of a successful cyber-attack and significant disruption of access to IT systems.

It is a collective responsibility for all areas of the Council to remain alert and vigilant to the risks of possible cyber-attack and disruption. Given the increasing complexity and scale of unauthorised attempts to infiltrate or affect systems – we must work on the premise that it’s “not if, but when” an attack will cause significant disruption services and it is essential to ensure we are prepared should such an event arise.

7. Threats

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

There are a range of threats that the Council must consider and take steps to protect against as part of any Cyber Resilience Strategy and to ensure effective cyber security measures are in place regardless of whether systems are hosted in Conwy's data centres or externally by a third party.

Threat Type	Details
A) Cyber criminals 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.
B) Hacking / Hacktivism	Hackers may try to access vulnerable systems as a challenge or to highlight security flaws. 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 services are disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Hacktivist groups have successfully used distributed denial of service (DDoS – when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of a number of councils already.
C) Insiders (Officers, Partners and Members within the Council)	Officers or members 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 however the most common occurrence is linked to human error or a lack of awareness about the particular risks involved.
D) 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 the software supplier and before protection systems such as anti-virus products have been updated with latest information to protect against the attack type. 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.
E) Loss of Data Centre(s) or Infrastructure	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

Threat Type	Details
	otherwise that impact upon council IT systems. Operating resilient, secure data centres is critical for service continuity.
F) Espionage	Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. Disruption of communications lines and internet connectivity to limit UK capacity to conduct business could also have severe consequences.
G) Terrorist Organisations	Some terrorist groups demonstrate intent to conduct cyber-attacks. 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.

8. 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** – Software running in data centres and on devices should be updated and checked regularly and effectively. It is essential that the systems are fully updated with latest security protection 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.

- **Infrastructure Maintenance** – Maintaining core ICT infrastructure within a secure environment, with appropriate security updates and maintenance plans in place are also essential considerations.

- **Software Access** – To ensure systems have sufficient user and system authentication, data authenticity verification, or data integrity checking features that prevent uncontrolled access to systems.

- **Training and Skills** – It is fundamental that all employees, members and partners have an understanding of cyber security and how their working practices should support this. Promoting awareness of citizens around keeping safe online can also help to reduce risks of loss of personal information.

9. 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.

At Conwy County Borough Council, cyber security risks and consequences of an attack are registered on the corporate risk register. Further cyber security and resilience related risks are also identified in the IT & Digital Transformation risk register.

Regularly reviewing risks and mitigation measures to maintain appropriate levels of protection is key to maximising the Council’s levels of protection against disruption to IT systems and potential loss of data.

A key mitigation measure to help deal with consequence of a cyber-attack and/or significant period of disruption to IT systems is for Services to ensure they incorporate provision to operate effectively without access to IT systems or services including steps to populate systems with information once IT services are restored.

10. Our Approach, Principles and Priorities

To mitigate against the multiple cyber resilience related threats the Council faces, a strategic approach is required to underpin collective and individual actions. This will include:

Ensuring the threat of cyber-attack and loss of data or systems is identified as a corporate risk ensuring our staff, elected members and partners understand responsibilities around risk mitigation actions.

Deploying systems and controls which help to identify possible threats, protect against attack and support the resilience of our IT infrastructure, systems and devices.

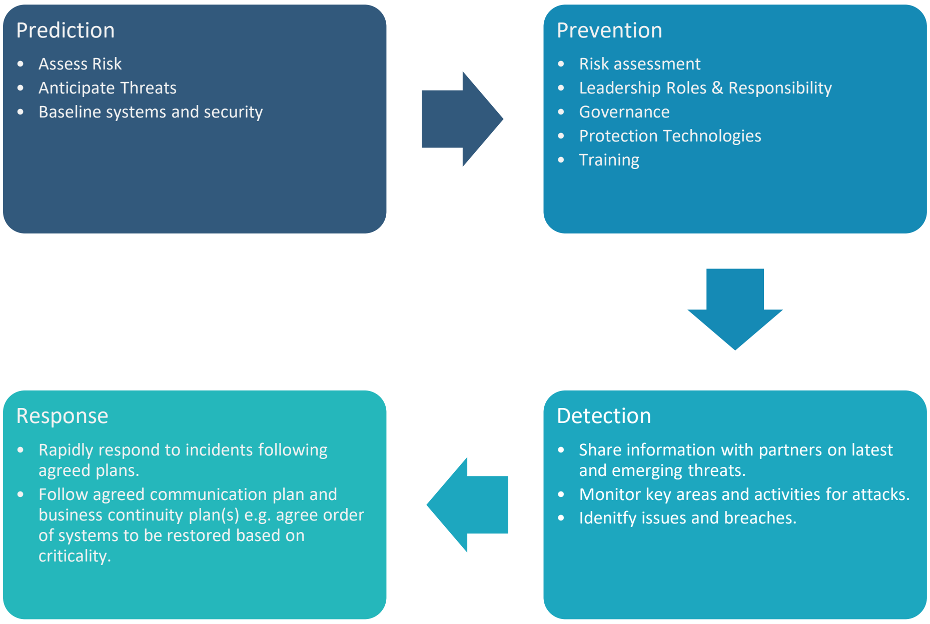
Cyber Awareness training to help mitigate insider threats, understand supply chain risks and ensure all officers understand the issues and their responsibilities.

Maintaining appropriate accreditations that require annual externally administered reviews of the Council's protection measures. These will include adoption of the Cyber Essentials Plus scheme controls, Public Sector Network (PSN) and Payment Card Industry (PCI) compliance. Through also working to comply with standards set out in other frameworks including elements of ISO 27000 we can work to ensure that the council will be able to identify, mitigate and protect against information security risks in a prioritised and resourceful fashion.

Equally, there is an obligation on Council Services sourcing systems hosted on Cloud Platforms or delivered through "Software as a Service" to ensure equivalent levels of assurance are maintained.

Setting out the approach to service delivery within service continuity plans in the event of a cyber-attack or significant and prolonged disruption it IT services.

The diagram below shows the key steps for protecting the Council from cyber related threats and disruption to IT services:



Prediction

- Assess Risk
- Anticipate Threats
- Baseline systems and security

Prevention

- Risk assessment
- Leadership Roles & Responsibility
- Governance
- Protection Technologies
- Training

Detection

- Share information with partners on latest and emerging threats.
- Monitor key areas and activities for attacks.
- Idenitfy issues and breaches.

Response

- Rapidly respond to incidents following agreed plans.
- Follow agreed communication plan and business continuity plan(s) e.g. agree order of systems to be restored based on criticality.

Key Steps to Protecting the Council

11. 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 Conwy County Borough Council ICT infrastructure, systems and data regardless of hosting provider. Where systems are sourced or hosted externally, any contract should ensure equivalent levels of cyber resilience assurance that are appropriate for the information held can be provided throughout.

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 citizens, visitors, businesses, officers, elected members and partners in gaining the knowledge and ability to defend themselves.

Actions:

Security Systems

- Implement firewalls, software protection, threat detection and scanning systems.
- Ensure approriate protection within back-up and recovery systems.

Health Checks and Testing

- Carrying out health checks and penetration testing across our infrastructure.
- Cyber resilience exercises to test recovery of our systems and processes.
- Ensure service continuity plans include cover for periods of IT disruption.

Accreditations and Compliance Regimes

- Maintaining Cyber Essentials Plus accredititations and meeting compliance requirements for Government Code of Connection (Co-Co) for Public Sector Network (PSN) and Payment Card Industry (PCI) which require good cyber hygiene, to connect to government private networks.

Working with Partners

- Working with partners across the public sector through participation in groups including the SOCITM WARP group to support information sharing, warning, advice and reporting.

DETER

The Council and partners remain a target for all forms of aggression in cyberspace. This will involve detecting, understanding, investigating and disrupting hostile action against Council IT infrastructure and systems.

Actions:

Governance

- Applying government and industry cyber security guidance, e.g. Cyber Essentials.
- Maintaining risk registers to ensure the Council IT infrastructure remains reselient and protected.
- Ensuring a schedule of internal audits are in place to monitor compliance with the strategy.

Technology and Information

- Network Security including firewall protection.
- Anti-Virus protection.
- Email systems protection.
- 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, through device encryption for users abd/or tokens where administrative consoles provide access to administer infrastructure, platforms or services.
- Complex passwords should be used to access all accounts with rules set to disable unused accounts within agreed time limits. Accounts with high levels of access to Council systems will be strictly controlled with high level password complexity and further reduced time limits on in active accounts.
- Infrastructure components shall be changed from default values and shall not be easy to guess.
- Malware prevention.
- Removable media controls.
- Secure configuration.

Agreed Policies, Plans and Guidance.

- Maintaining effective IT and Information Security Policies.
- Publication of good practice on the intranet.

Training & Awareness

- Educating users can help detect, deter and defend against Cyber threats.
- Emailing and publication of information on key emerging or current threats.
- Promoting awareness of cyber security steps with our citizens through training and messaging on social media and from libraries.

DEVELOP

The council will continually review and develop our Cyber Resilience protection measures to address the risks faced by our services given the reliance on IT infrastructure and systems.

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

Actions:

Risk Management

- Develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud.
- Process, procedures and controls to manage changes in cyber threat level and vulnerabilities.

Manage Vulnerabilities.

- Managing emerging vulnerabilities that may allow an attacker to gain access to critical systems.
- Operation of the council's penetration testing programme; Cyber-incident response processes and Disaster Recovery Strategy.

Training & Awareness

- Ensure Council IT users are aware of latest risks and appropriate actions to take.
- Consider training requirements for officers and members to maintain levels of awareness.

Incident Response Planning

- Maintain an incident response and management plan, with clearly defined actions, roles and responsibilities.
- Prepare Disaster Recovery Plans to include an agreed prioritised list of systems for recovery as agreed by the Senior Leadership Team(SLT).
- Develop a communication plan in the event of an incident which includes notifying (for example) the relevant supervisory body, senior accountable individuals, communcations team, WARP, National Cyber Security Centre (NCSC), Welsh Government and the Information Commissioner's Office (ICO) or law enforcement as applicable (not exhaustive).
- Ensure Services include mitigation in continuity plans to minimise disruption as a result of a signifcant cyber attack or loss of ICT services as well as re-populating systems with data lost or note entered as a result of any disruption.

12. Measuring our Cyber Resilience

Throughout this period of digital transformation, the Council has committed to delivering robust information security measures to protect residents and stakeholder data from misuse and cyber threats, safeguarding 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:

- Manage cyber security governance processes and maintain appropriate external cyber resilience certifications.
- Ensure Cyber Resilience is included on the Council's corporate Risk Management Framework.
- Ensure policies/procedures are in place to review user access requirements.
- Ensure Services maintain cyber-specific responses within Service Continuity Plans.
- Maintain an incident response and management plan, with clearly defined actions, roles and responsibilities together with prepared plans for priority recovery of systems. A copy of all incidents shall be recorded regardless of the need to report them.
- Within IT Disaster Recovery Planning – Ensure testing exercises are undertaken against most likely threats and undertake recovery exercises to ensure systems can be recovered in accordance with agreed priorities.
- Undertake regular reviews of systems and ICT infrastructure in place to ensure vulnerabilities are removed or mitigated.
- Review vendor management – ensuring Services have processes in place throughout any contract for assessment of third party system providers' own cyber resilience. This should ensure externally hosted data and systems are appropriately secured (See Appendix 3).
- Continue to explore active cyber defence tools and new technologies to ensure Conwy has the appropriate solutions to protect against threats.
- Maintain appropriate accreditations and compliance to ensure our cyber resilience measures are externally reviewed.
- Provide relevant cyber security and information protection training for staff and elected members.
- In partnership with Corporate Improvement and Development and Emergency Planning, consider a schedule of cyber incident related exercises, within the wider cycle of multi-agency incident response and recovery exercises.
- Support delivery of cyber security awareness initiatives and training to citizens through libraries and other sources.

13. Cyber Resilience Governance Roles and Responsibilities

Effective cyber resilience governance in Conwy delivered through the following roles and functions.

Role	Responsibilities
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 Resilience Strategy.
Strategic Leadership Team (SLT)	SLT which includes the Council's Board of Directors sponsor the Cyber Resilience Strategy and oversee the strategic framework through which the Council governs its information resources.
Senior Leadership Team (SLT)	SLT are responsible for ensuring their services are prepared to deal with a significant disruption or loss of IT services within service continuity plans and ensuring officers are aware of good practice in respect of protecting information and maintain cyber security. Ensuring system suppliers provide evidence of effective cyber resilience with regard to their services is also a key consideration. Agreeing on a prioritised plan for recovery of systems and devices in the event of significant downtime.
Senior Information Risk Owner (SIRO)	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 officers, partners and members having a role to play.
Head of IT and Digital Transformation	The ITDT Service make recommendations and decisions regarding technical implementations to ensure the Council maintains effective and appropriate levels of cyber security protection. This includes ensuring that cyber security implications are reviewed and any necessary changes are properly considered.
Information Governance Group (IGG)	The IGG is comprised of senior representatives from each service area. The group are responsible for overseeing the delivery of the Cyber Resilience Strategy and monitoring its effectiveness.
Digital Board	The Digital Board oversees implementation of Conwy's Digital Strategy. They ensure that risks, issues and dependencies are proactively managed and make decisions in relation to any risks and issues that have been escalated in relation to the digital transformation programme.
Information Asset Owners (IAO)	Information Asset Owners are responsible for all processing of personal data within their business area.
All Conwy County Borough Council Officers and Members	It is the responsibility of all officers and members to comply with the standards set out in this Cyber Resilience Strategy.

14. Appendix 1 – Standards

Cyber Essentials

Welsh Government have mandated all public sector organisations in Wales to participate in The National Cyber Security Centre's "Cyber Essentials Plus" scheme as a method of ensuring a range of protection measures are in place. Conwy County Borough Council participate in the scheme and are assessed annually for compliance.

About Cyber Essentials - NCSC.GOV.UK

Public Sector Network Compliance

To enable access to shared government networks and ensure all stakeholders adopt appropriate security standards to minimise cyber related threats, the Council is assessed at least once every two years to ensure compliance with agreed standards. Certification of compliance helps to ensure measures in place within the Council help to protect data, systems and wider networks.

Public Services Network (PSN) compliance - GOV.UK (www.gov.uk)

Payment Card Industry Data Security Standard (PCIDSS)

For assurance on the security measures adopted by the Council to ensure secure collection of payments through payment cards, the Council is also annually reviewed for PCIDSS compliance.

Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards

BS EN ISO/IEC 27000:2020 Information technology. Security techniques. Information security management systems.

The Council will also work to ensure cyber resilience measures in place are aligned to the standards set out in British Standards Institute's document which sets out standards for cyber security and data protection,

15. Appendix 2 – NCSC: 10 Steps to Cyber Security

Risk Management Regime

Embed an appropriate risk management regime following the ISO27k standards, across the organisation.

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

Secure Configuration

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

Network Security

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

Managing User Privileges

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

User Education and Awareness

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

Incident Management

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

Malware Prevention

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

Monitoring

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

Removable Media Controls

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

Home and Mobile Working

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

16. Appendix 3 – NCSC – The Cloud Security Principles.

The National Cyber Security Centre provide advice and guidance on selection of Cloud platform and Software as a Service providers that meet the Council's security needs. Services should engage with/seek assurance from suppliers before entering (and during) any contract that their system is robust, secure and adopts appropriate cyber resilience controls.

Links to NCSC guidance pages for selection or assessment of external providers is provided below.

Cloud Security Principles

Cloud Security Shared Responsibility Model

Lightweight Approach to Cloud Security (for Services NOT holding or processing sensitive data).

NCSC RECOMMENDED PRINCIPLES FOR CLOUD SECURITY AND QUESTIONS FOR THIRD PARTY PROVIDERS.
Principle 1 – Data in Transit Protection What measures does your organisation adopt to adequately protect data against tampering and eavesdropping as it transmits across networks inside and external to the Cloud?
Principle 2 – Asset Protection & Resilience How are the data and assets storing or processing it protected against physical tampering, loss, damage or seizure? Where is the data held to ensure compliance with data protection legislation?
Principle 3 – Separation Between Customers What security boundaries are in place to ensure other customers cannot access or affect the service or data of Conwy County Borough Council?
Principle 4 – Governance Framework Which security governance framework is in place to coordinate and direct your management of the service and information within it?
Principle 5 - Operational Security What measures do you employ to ensure the service is operated and managed securely in order to impede, detect or prevent attacks?
Principle 6 – Personnel Security Please confirm if any of your personnel have access to the Council's systems and data? Where this is the case, please provide details on how you ensure trustworthiness of staff, any cyber security awareness and information governance or data protection training, technical measures in place that audit and constrain potentially damaging actions?
Principle 7 – Secure Development Please outline your approach to design, development and deployment of your system or service minimising and mitigating against threats to the system security or availability?

Principle 8 – Supply Chain Security Where any third parties have access to customer data or the service on behalf of your company, please provide details of how you ensure those providers meets appropriate security standards to maintain resilience and security of the system and Council data?
Principle 9 – Secure User Management Does your system include an access model that allows the Council to implement a role based access controls across the service and data held on the system? How can access to this service be securely managed to prevent unauthorised access and alteration to resources, applications or data.
Principle 10 – Identity & Authentication Please advise how all access to service interfaces are constrained to a securely authenticated and authorised identity, which may belong to either a human user or a machine?
Principle 11 – External Interface Protection Please explain how any external or less-trusted interfaces of the service are identified and defended appropriately. This includes external APIs, web consoles and command line interfaces.
Principle 12 – Secure Service Administration Please provide details of how the design, implementation, and management of the your administration systems follow enterprise good practice, recognising their high value to attackers.
Principle 13 – Audit Information & Alerting for Customers Please provide information on how your organisation would identify security incidents and what information sources you would use to determine how and when and incident occurred? How will you provide audit information or security alerts when attempted attacks are detected?
Principle 14 – Secure Use of the Service What measures and steps are in place to ensure the Council meet's its data protection responsibilities? Is the system or service being provided secure by design and by default?