Appendix 1

Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL
MERTHYR TYDFIL
County Borough Council

Cyber Resilience Strategy

2021 – 2024

Contents:

Issue Date	Version	History of Changes	Approval By	Approval Date
13/08/2021	V1.0 DRAFT			

1. Introduction

Cyber space offers us the ability to connect all sorts of devices to the network to gain unprecedented access to a whole range of applications and services anytime, anywhere. The prosperity and economic growth of the organisation depends on the opportunity's cyberspace offers. However, concerns about the security of this domain are becoming an increasingly pressing issue. If organisation leaders and citizens lack confidence in cyber security, it stands to gravely affect participation in online activities, thereby inhibiting further development opportunities in cyberspace.

Our heavy reliance on networking technology also makes cyber space an attractive target for malicious users willing to compromise security of our communications and/or cause disruption to services that are critical to our day-to-day survival in an interconnected world. Cyber security is now a mainstream business risk; therefore, it is of the upmost importance that corporate and public sector leads understand the current threat landscape. To obtain strong cyber resilience, we must ensure we promote a comprehensive risk-based approach to cyber security, which is integrated across personnel, technical security, information assurance and physical security, which strategically encompasses Information Security, Assurance, Resilience and Governance.

2. What is cyber resilience?

Cyber Resilience focusses on ensuring that there is a combination of cyber security and business reliance processes to reduce or minimise the impact on services and systems and ensuring that they continue to provide their intended outcome (services).

An outcome (service) cannot be delivered without the following three components:

- People to operate and monitor the service
- Information and data to feed the process and to be produced by the service
- Technology to automate and support the service

3. Why do we need a cyber resilience strategy?

This strategy provides direction on how to recognise, manage and respond to the increasing threats we all face online. By doing this, we can safely reap the rich benefits offered by the digital age.

In the modern world, the protection of digital networks such as the Internet is becoming just as important. Many countries have put in place cyber resilience strategies, including the UK's Cyber Security Strategy.

Our strategy aims to build on this solid foundation and move the organisation to a stage where we all routinely recognise and manage cyber risks in the same way as we deal with other day-to-day risks to our health and prosperity.

In addition, this strategy will reference out several key information security policies and approaches designed to protect the Confidentiality, Integrity and Availability (CIA) of information. This will help to raise cyber resilience and security at a strategic level, ensuring we are able to sufficiently protect information belonging to the organisation, keeping it safe from cyber-attacks by addressing the continually evolving threat and risk landscape, whilst protecting the strategic goals of the Council. This should subsequently balance cyber safety, financial and resource obligations, whilst meeting the legal commitments of GDPR.

4. Where cyber resilience meets business objectives

It is becoming painstakingly obvious that cyber resilience and security as we know it today is a strategic risk, that streams far beyond that of information technology. The sophistication and utility of a cyber resilience strategy is based upon its ability to align itself in conjunction with business vision, objectives, and innovation projects. To manage the risk, we must implement controls across this ever-increasing, turbulent network landscape. A successful cyber resilience strategy and programme will:

- support the strategic direction of the organisation
- have the capability and technical ability to support the specific cyber security requirements of the organisation, on a consistent basis
- manage the vulnerability and threat associated with the technical landscape.

Successful cyber resilience programs will be successful when we:

- identify the actual risks
- prioritise and protect
- develop and sustain a cyber security program
- enable business performance
- optimise for business performance

This cyber resilience strategy will support the development of a culture of cyber resilience and ensure we continue to deliver our priorities for improvement as identified in the MTCBC Recovery and Improvement Plan 2020-2025:

- **Education** outcomes
- **Social care**
- Supporting our **economy to recover**
- Environmental well-being
- Governance and resources including finances
- Council-wide change
- Being sustainable
- Having a healthy organisation
- Providing quality services

This strategy will support the six themes within our digital transformation strategy to improve connections across Merthyr Tydfil:

- Connected communities
- Connected workforce and elected members
- Connected data and information
- Connected services
- Connected businesses and partners
- Connected and compliant infrastructure

5. What are the impacts of cyber-attacks?

Risks exist at every level of our daily lives – the consequences of a cyber-attack can vary from very minor inconvenience to major disruption. The cost of cybercrime will continue to increase as more business functions move online.

Our organisation relies on crucial information assets, such as databases of customer/service user details or intellectual property, that are of value to cyber criminals.

Cyber criminals often operate through stealth with some organisations seldom noticing cyber-attacks until the effects of the attack start to impact.

The direct and indirect costs of cleaning up from a cyber-attack can be high and are often unplanned for. In many cases, these costs may not be covered by conventional insurance policies.

As a public service we are reliant on digital systems. Digital networks make it possible to provide innovative and integrated public services that deliver to those in most need and promote growth. It is crucial that cyber risk is planned and budgeted for when providing these services. In turn, this will help keep citizens confident in using digital services.

6. Our Vision

Our vision is that Merthyr Tydfil County Borough Council supports business assurance and business continuity by focussing on the cyber resources on which it depends. It aims to maximise its ability to complete critical functions despite an adversary presence in the organisation infrastructure.

We will ensure that:

- Our people are well informed and prepared to make the most of digital technologies safely
- Our organisation recognises the risks in the digital world and are well-prepared to manage them
- We have confidence in and trust our digital services
- We have a growing and renowned cyber resilience approach

7. Who needs to be involved?

Cyber resilience is a shared responsibility – Welsh Government takes the lead and will encourage and engage with all sectors to promote and build a cyber resilient Wales.

The Corporate Management Team are responsible for driving forward this strategy. The Information Security Officer is responsible for ensuring that all relevant stakeholders are included in, and can actively contribute to, the implementation of measures within the strategy.

Partners of this strategy are:

- Employees and Members
- Welsh Government
- Cabinet Office
- Wales Warning and Reporting Point (WARP)
- Wales Regional Cyber Crime Unit (Tarian)
- The Cyber Resilience Centre for Wales
- Other public sector organisations

8. How can we build cyber resilience?

Achievement of the desired outcomes of the strategy will require effective leadership. With its partners, Merthyr Tydfil County Borough Council, commits to advancing research and innovation, developing education and skills amongst its employees and Members, and providing clear communication and awareness.

Becoming more cyber resilient requires a sustained and collaborative effort. We will embed cyber resilience in our strategic and operational plans. We will continue to work closely with our partners on cyber resilience and security matters. Cyber resilience must be regarded as a critical aspect of business operation and continuity.

The high-level priority actions are:

Outcome	Priority Actions
Leadership and Partnership Working	Incorporate cyber resilience into all policies
	Ensure board level commitment to cyber resilience
	Develop cyber incident reporting measures and link to wider ICT/digital and business continuity plans
	Define the standards relating to cyber resilience for procurement of goods and services
	Ensure the safety and security of online shared services systems

	Embed cyber risk and resilience assessments when developing new products, services, and processes
	Consider shared development or procurement of cyber resilient systems and tools
Awareness Raising and Communication	Develop specific and appropriate awareness-raising activity for a wide range of audiences
	Assure the public around the safe use of digital public services
	Encourage the sharing of information relating to cyber incidents, threats, and vulnerabilities across sectors
	Develop methods on how to measure impact
Education, Skills and Professional Development	Map existing cyber resilience skills to identify gaps
	Introduce cyber resilience into workplace learning and development
	Explore ways to embed cyber resilience into teacher training in schools
Research and Innovation	Establish a coherent and sustainable approach to research
	Improve the sharing of research to develop our knowledge and understanding to help us become more effective in building cyber resilience
	Establish a baseline to identify current levels of trust and confidence in digital public services
	Develop new and innovative ways to help local businesses become more cyber resilient

9. How will we implement this strategy?

This strategy is the initial framework to help build a cyber resilient organisation. It sets out high level actions which will be developed into a set of action plans post-publication. These plans will evolve to keep up with the pace of rapid and emerging digital change and the associated risks.

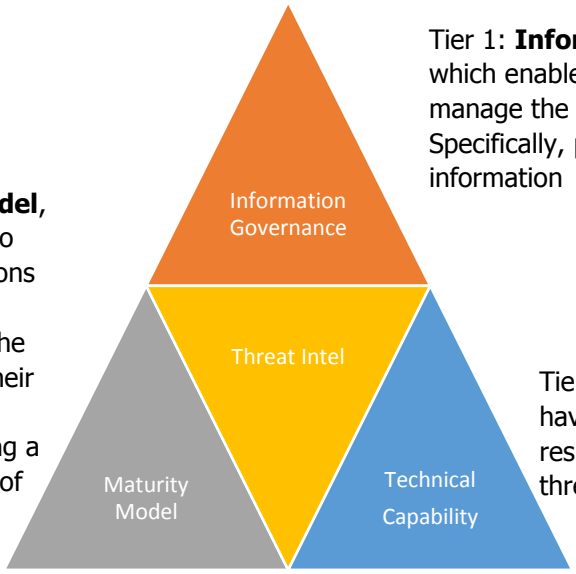
Effective implementation of this strategy and associated action plans will require input and action from every part of the organisation, from our suppliers, other public

sector organisations, law enforcement, Welsh Government and, of course, citizens themselves.

We will use a three-tier framework model to implement our cyber resilience strategy:

Tier 1: **Information Governance**, which enables us to understand and manage the way we handle information. Specifically, personal, and sensitive information

Tier 2: **Maturity Model**, which is a tool used to assess the organisations cyber resilience. Demonstrating how the organisation meets their threats is done by establishing or utilising a maturity assessment of cyber resilience.



Tier 3: **Technical Capability**, have the technical ability to responds to any potential threats

We will follow the four pillars of Cyber Resilience:

IDENTIFY – What processes and assets need protection?

PROTECT – What safeguards are available?

DETECT – What techniques can identify incidents?

RESPOND – How can we minimise and contain impacts of incidents?

FUNCTION	CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
IDENTIFY	Create an Appropriate Cyber Security Governance Process	Risk Management	• NCSC 10 Step's to Cyber Security • PCI DSS • 20 Critical Controls for Cyber Defence • CPNI Insider threat Guidance • NCSC Risk Management Collection
		Risk Appetite	• IRM Risk Appetite Statements
		Balancing Risk	• NCSC Cyber Risk Principles
	Identify and Catalogue Sensitive Information	Preparing for a breach	• ICO Guide to GDPR • ICO Guide to Accountability and Governance • Security Policy Framework • ICO Data Sharing Code of Practice
		Responding to a breach	• ISO/IEC 27000
		Reporting a breach	• Wales Accord for Sharing of Personal data
		People	• Local Public Services Data Handling Guidelines • ICO Bring Your Own Device to Work (BYOD) • Government Baseline Personnel Security Standard
		Places	• Local Public Services Data Handling Guidelines • ICO Model Contract Clauses • Cloud Security Principles • CPNI Physical Security Guidelines
		Policy	• Local Public Services Data Handling Guidelines • Cyber Essentials Scheme • ISAME
		Processes	• ICOs Conducting Data Protection Impact Assessments • GDS Blogs
		Procedures	• IStandUK on Cyber Resilience • ICO Data Sharing Code of Practise

FUNCTION	CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
PROTECT	Access to sensitive information and key operational services shall only be provided to identified, authenticated and authorised users or systems	End-to-End Visibility	• Transport Layer Security (TSL) 1.2 • HMG Minimum Cyber Standard
		Privileged Access Management	• NCSC Identity and Access Management • 10 Steps to Cyber Security (*Managing User Privileges)* • PwC Access Management Guidance • KPMG Privileged Access Management • NIST Identity and Access Management
		Access Auditing	• NCSC Introduction to logging for Security Purposes
	Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities	Protect your enterprise technology	• NCSC Public Sector DNS • FCA Cloud Infrastructure Guidance
		Protecting end user devices	• NCSC MFA Guidance • Digital NHS Identification and Authentication Guidance • Microsoft Guidance on MFA for Office 365
		Protecting Email	• DMARC Guidance • Sender Policy Framework (SPF)
		Protecting digital services	• OWASP top ten vulnerabilities • 10 Steps to Cyber Security *(Network Security)* • Financial Conduct Authority (FCA) Network Security • NCSC Web Check Blog
	High privileged accounts shall not be vulnerable to common cyber-attacks		• OWASP Top Ten Vulnerabilities • All Above Identity and Access Management Guidance • NCSC Password Guidance • NIST Password Guidance

FUNCTION	CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
DETECT	Steps are taken to detect common cyber-attacks	Patch Management	• PSN CoCo (Patch Management) • NCSC Patch Management Guidance • Digital NHS Patch Guidance • NIST Enterprise Patch Management Guidance
		Vulnerability Management	• NCSC Vulnerability Management Guidance • OWASP Vulnerability Management Guide • US-CERT Vulnerability Management • OSI Model • TCP/IP Model • NIST Vulnerability Management *(Not one size fits all)* • ISO 2002
		Threat Detection	• CPNI Intrusion Detection Guidance • NIST Intrusion Detection and Prevention Systems

FUNCTION	CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
RESPOND	Have a defined, planned and tested response to security incidents that impact sensitive information	Kill Chain Taxonomy	• Lockheed Martin Cyber Kill Chain Framework
		Incident Response	• NCSC Incident Management • NCSC Response and Recovery Planning • CREST Incident Response • NCSC Incident Response Framework/Categories • PwC UK Cyber Incident Response Guidelines

The strategy will be reviewed every three years; however, we may review some elements within the strategy more frequently due to the rapidly changing nature of cyber.

10. How will we know we are making a difference?

We will know if we are succeeding if we are able to see a step-change in the cyber resilience of our organisation, suppliers, and citizens. Our initial plan to measure success under each of the outcomes is as follows:

1. ***Our people are informed and prepared to make the most of digital technologies safely***
   Evidence example: Human Vulnerability assessment (HVA) results; training records for employees and Members; Phishing simulation results; skills analysis; public opinion surveys; number of security incidents reported.
2. **Our organisation recognises the risks in the digital world and are well-prepared to manage them**
   Evidence example: Number of incident reports; IT Health Check findings; Vulnerability management; Risk assessments; Compliance certifications.
3. **We have confidence and trust in our digital public services**
   Evidence example: Vulnerability assessments of our digital services; Supplier cyber security assessments; take-up of our digital services by the public; Public opinion surveys.
4. **We have a crowing and renowned cyber resilience approach**
   Evidence example: Annual cyber stocktake results; Compliance certifications; audit outcomes.

11. Cyber resilience roles and responsibilities

Effective cyber resilience in Merthyr Tydfil County Borough Council is delivered through the following roles and functions.

Senior Information Risk Owner (SIRO)

The Council's nominated Senior Information Risk Owner (SIRO) is the Chief Executive. The SIRO is responsible for the governance of cyber resilience and information risk within the Council. This includes 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 Resilience Strategy.

Full Council

Full Council is made up of all Councillors. Full Council will ensure full Council ownership.

Corporate Management Team (CMT)

CMT sponsor the Cyber Resilience Strategy and oversee the strategic framework through which the Council governs its cyber security.

Information Security Officer

The Information Security Officer is responsible for establishing, maintaining, and overseeing the delivery of the strategy, and program to ensure information assets and technologies are adequately protected.

ICT Department

Led by the Head of ICT, the department oversees the delivery of ICT, and makes decisions regarding technical implementations for projects, ensuring that cyber security implications are properly considered.

Information Governance Forum (IGF)

The IGF is made up of representatives from service areas across the Council, responsible for monitoring the effectiveness of the strategy.

Information Governance Team (IGT)

Along with the Data Protection Officer, the team develop and maintain a corporate inventory of all processing activities and seek legal assurance; and review contracts and ensure that GDPR changes are reflected.

Business Continuity Officer

The Business Continuity Officer will focus on ensuring continuity exists in business processes in respect of cyber resilience in all service area plans.

Information Asset Owners (IAO)

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

All MTCBC Officers and Members

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

12. Key policies relevant to this strategy

The key Council Policies that are relevant to this strategy are:

- Information Security Policy
- Antivirus Policy
- Clear Desk Policy
- Disposal of ICT Equipment Policy
- Email & Instant Messaging Acceptable Use Policy
- ICT Procurement Policy
- Information Asset Protection Policy
- Information Backup and Storage Policy
- Internet AUP
- Legal Responsibilities in relation to Information Security
- Password Policy
- Physical Security Policy
- Remote Working Policy
- Removable Media Policy
- Reporting Information Security Incidents Policy
- Social Media Policy
- Software Compliance AUP
- Unauthorised Access Policy
- Privacy Standards Policy
- Data Protection Breach Policy