CABINET – 30TH NOVEMBER 2022

SUBJECT: **CYBER SECURITY STRATEGY 2022-2025**

REPORT BY: **CORPORATE DIRECTOR EDUCATION AND CORPORATE SERVICES**

1. PURPOSE OF REPORT

1.1 To present to Cabinet the draft Caerphilly CBC ('Council') Cyber Security Strategy 2022 – 2025 ('Strategy'), **Appendix A**.

1.2 To recommend endorsement and implementation of the Strategy.

2. SUMMARY

2.1 The Strategy sets out the Council's application of information and cyber security standards to protect our information systems, the data held on them, and the services we provide, from unauthorised access, harm or misuse. The Strategy is our cyber security commitment both to the people we represent and the national interest; and emphasises the importance of cyber security in the role of all Council employees.

2.2 Information and data are vital to every part of the Council's business. As we continue with a digital programme that is transforming the way we work and how local people access information and services, we need increasingly robust security measures to protect against cyber threats.

2.3 The Strategy sets out the challenges we face as a Council to the type of threats and vulnerabilities in relation to:

Cybercriminals	Physical
Cyber Crime	Terrorists
Hacktivism	Espionage
Insiders	Systems
Zero-day Exploit	Training and Skills

2.4 The Strategy is supported by an implementation plan and critical success factors. Together with clear definitions on governance roles & responsibilities and the required standards that we as a Council need to meet on an ongoing basis.

3. RECOMMENDATIONS

3.1 To endorse and implement The Strategy.

4. REASONS FOR THE RECOMMENDATIONS

4.1 To ensure that the Council is continuously improving its Governance and security arrangements and has a fit for purpose Strategy and approach to cyber security.

5. THE REPORT

5.1 The Strategy has been produced in response to the increasing threat from cyber criminals and a number of successful and high-profile cyber-attacks on public and private organisations. Its purpose is to give assurance to residents and other stakeholders of the Council's commitment in delivering robust information security measures to protect resident and stakeholder data from misuse and cyber threats. To safeguard their privacy through increasingly secure and modern information governance and data sharing arrangements, both internally and with our partners.

5.2 The Council will continue its vision for developing and managing its interface with customers and its digital environment. Pursuing this vision against an increasingly complex public service landscape as we face substantial social, economic, and political challenges. The Strategy supports that key area of focus and includes protecting an ever-increasing agile workforce, growth in the uptake of technologies such as cloud-based systems, internet-enabled services, mobile devices, high-speed broadband and together with the digital agenda on utilising/sharing more data of all forms to develop public services means that cyber security will be increasingly tested.

5.3 The Strategy is designed to further enhance and strengthen the Council's security position. The Council has already built a model to ensure that it has a healthy and systematic security posture that protects against most types of threats. The Model follows industry best practices such as the National Cyber Security Centre (NCSC), National Institute of Standards and Technology (NIST) & Warning, Advice and Reporting Point (WARP) a community-based service where members can receive and share up-to-date advice on information security threats, incidents, and solutions.

5.4 Through delivery of this strategy, the Council will comply with and embed the principles of 'Cyber Essentials Plus'; a government-backed, industry-supported scheme to help organisations protect themselves against common online threats. The Council will also follow the "10 Steps to Cyber Security" framework published by the National Cyber Security Centre.

Conclusion

5.5 The Strategy underpins and enables the Council's Customer and Digital Strategy, which continues to ensure we harness the benefits of technology to improve the lives and life chances of all local people. The measures outlined in this Strategy will safeguard trust and confidence in the way we operate and deliver our services, supporting the Council to remain at the forefront of the digital revolution.

5.6 The Strategy demonstrates our commitment and the key actions we will take to further establish a trusted digital environment for the Council. Cyber-attacks will continue to evolve, which is why we will continue to learn and work at pace in an attempt to stay ahead of all threats.

6. ASSUMPTIONS

6.1 All details stated within this report and Strategy are reflective of all issues known as of September 2022.

6.2 Any amendments to the Strategy due to changes in legislation, policies and/or cyber security best practice will be the responsibility of the Head of Customer & Digital

Services in consultation with Corporate Director for Education & Corporate Services and Cabinet Member.

7. SUMMARY OF INTEGRATED IMPACT ASSESSMENT

7.1 The Strategy positively impacts all aspects of the IIA.

7.2 This strategy will contribute to our progress towards the well-being goals and other relevant legislative requirements. Embracing digital innovation in safe and secure way can lead to greater economic opportunities and a more prosperous and resilient society. Equipping people with the digital skills they need and designing services securely around the user will also improve social cohesion, create a more healthy and equal society with well-connected communities and contribute to a thriving Welsh language.

7.3 The full IIA can be accessed via Cyber Strategy IIA

8. FINANCIAL IMPLICATIONS

8.1 There are no financial implications.

9. PERSONNEL IMPLICATIONS

9.1 There are no personnel implications.

10. CONSULTATIONS

10.1 This report has been sent to the Consultees listed below and all comments received are reflected within this report.

10.2 The draft Strategy was presented to Governance and Audit Committee on 14 June 2022 and Members of the Committee raised the following points:

a. A Member queried whether CCBC employed a digital auditor within the audit team. Members were advised that there is not a specific IT auditor within the audit team. Members were introduced to the Senior Information Security Officer who advised Members that he worked outside of Digital Services (within Procurement and Information Services), in order to have a more independent view of the Councils' IT and security policies (this is inline with best practice). Members were also advised of a recent vacancy within the department for an Information Security Manager and also the possibility of an apprenticeship position going forward.

b. A Member sought clarification on cyber-crime and fraud and queried whether there were arrangements for the integration of risks for these areas. Members were advised that there are risk registers at different levels within the authority and that cyber security is on the high-level risk register with mitigating actions. Members were also advised that further clarification on this matter will be evident when the risk registers are produced for the next meeting in October.

10.3 Moved and seconded that the Governance and Audit Committee considered the Draft Cyber Security Strategy in order for the Committee to gain the required assurance to

fulfil its role and to note the report and verbal Strategy update. By way of Microsoft Forms and verbal confirmation this was unanimously agreed.

11. STATUTORY POWER

11.1 Local Government Act 2001

Author: Ian Evans, Procurement and Information Manager;
evansi1@caerphilly.gov.uk

Consultees: Cllr Nigel George, Cabinet Member for Corporate Services and Property,
Christina Harrhy, Chief Executive,
Richard (Ed) Edmunds, Corporate Director for Education and Corporate Services,
Elizabeth Lucas, Head of Customer and Digital Services,
Robert Tranter, Head of Legal Services and Monitoring Officer,
Stephen Harris, Head of Financial Services and S151 Officer,
Wesley Colyer, Senior Information Security Officer,
Edward Thomson, Information Security Officer,
Carl Evans, Corporate Information Governance Manager and DPO,
Mark Brett, Lead Advisor, Silverthorn Associates,
Governance and Audit Committee (14 June 2022),
Digital Leadership Group,
Customer and Digital Services Management Team,
Cyber Security Forum, Corporate,
Cyber Security Forum, Education,
PDM (9 November 2022).

Background Papers:

Appendices:

Appendix A Cyber Security Strategy 2022 – 2025.