Briefing Note

CITY OF WOLVERHAMPTON COUNCIL

Title:	**Cybersecurity Update**	**Date:**	**20/09/2021**
Prepared by:	**Jai Ghai**	**Job Title:**	**Head of Digital and IT**

Intended Audience: Internal ☒ Partner organisation ☐ Public ☐ Confidential ☒

1.0 Purpose

1.1 The purpose of this report is to provide information and assurance regarding how the City of Wolverhampton Council (CWC) manages the strategic risk in relation to cyber security.

2.0 Background

2.1 Recently there has been a significant increase in cyber-attacks, including ransomware, targeting public sector organisations. In response, the NCSC (National Cyber Security Centre) have emphasised the urgent need to take steps to mitigate the ransomware threat to the sector and increase cyber security awareness and efforts.

2.2 Several steps have been taken by CWC to increase local security and to put appropriate measure in place for prevention and remediation, if the worst does happen, ensuring our data, workforce and technical architecture is protected.

3.0 City of Wolverhampton Council's Approach

3.1 Cyber security is a key priority for the Council and monitored rigorously through the strategic risk register. The City of Wolverhampton Council are one of the few councils in the country that are **Cyber Essential Plus certified**, an accreditation process that involves auditing and testing of digital and IT systems and controls by a 3rd party. Alongside this, the Council maintains its **Public Sector Network (PSN) accreditation** which allows it to transact safely with public sector and health organisations.

3.2 CWC has a robust Information and Cyber Security Policy, and the key areas of focus in relation to cyber security are:

- Identity and access management
- Information protection
- Threat protection
- Compliance and Governance

3.3 Best practice guidance from the NCSC have already been adopted into digital and IT solutions. New procedures implemented include non-functional and functional requirements to ensure 3rd parties and solutions meet stringent guidelines to safeguard the Council and its data. All proposed new solutions and the upgrade of existing solutions go through the Digital and IT's internal Technical Design Authority (TDA) ensuring necessary controls and processes are in place, to ensure our network and data are maintained before being procured and post procurement. TDA provides strict governance, guidance and advice.

3.4 To reduce the impact of cyber-attacks, in particular ransomware and to maintain our security status, Digital and IT continue to deliver against the following key actions, which are resourced in the MTFS:

- Measures continue to be adopted Council wide to maintain good security controls e.g. multi-factor authentication, locking devices when moving away from screens etc.
- Issues highlighted by 3rd party audits are implemented quickly to reduce exposure to attacks e.g. the requirement for complex passwords and blocking the use of common words.
- 3rd party Office 365 backup solution to reduce the impact of a ransomware attack against data hosted in the Microsoft Cloud.
- 3rd party offsite back solution to reduce the impact of a ransomware attack against on-premise data e.g. Agresso.
- Data loss prevention measures are implemented which include the tagging of documents and emails such that the use of these can be controlled based on the classification.
- Increase the Audit log retention for compliance monitoring from 3 to 6 months.
- Increase capability in the secondary datacentre to active-active.
- As part of a continued programme of investment in cyber security, the Council will continue to deploy **Protect**, **Detect** and **Respond** solutions across its estate. Further detail on this is provided in appendix 1.

Appendix 1

In order to maintain a leading edge in cyber security, investment has been made in Microsoft to provide a set of integrated solutions to keep CWC safer from cyber-attacks, as follows: