Brent	**Cabinet** 7 March 2022
	Report from the Strategic Director for Customer & Digital Services

Brent Cyber Security Strategy update

Wards Affected:	All
Key or Non-Key Decision:	Key
Open or Part/Fully Exempt: (If exempt, please highlight relevant paragraph of Part 1, Schedule 12A of 1972 Local Government Act)	Open
No. of Appendices:	One Appendix 1 Brent Cyber Security Strategy 2022-2026.
Background Papers:	None
Contact Officer(s): (Name, Title, Contact Details)	Stephen Skeete, Information Governance Lead Customer & Digital Services Tel: 020 8937 1570 Email: Stephen.Skeete@brent.gov.uk Rehana Ramesh, Head of Digital Transformation Customer & Digital Services Tel: 020 8937 1935 Email: Rehana.Ramesh@brent.gov.uk Sadie East, Director of Transformation Customer and Digital Services Tel: 0208 937 1507 Email: Sadie.East@brent.gov.uk

1.0 Purpose of the Report

1.1 The purpose of this report is to present Cabinet with the draft Brent Cyber Security Strategy 2022-2026 for agreement. The draft strategy builds on the 2019-2023 strategy that was agreed in October 2019. The Cyber Security Implementation Plan provides an update on progress in implementing the Brent Cyber Security Strategy.

2.0 Recommendations

2.1 Cabinet agrees the Brent Cyber Security Strategy 2022-2026 as set out in Appendix 1.

3.0 Detail

Brent Cyber Security Strategy 2022-2026

3.1 A Cyber Security Strategy was first agreed by Cabinet in 2019 in response to high profile cyber-attacks on public and private organisations. The Brent Cyber Security Strategy 2022-2026 builds on this strategy, and incorporates learning from cyber-attacks experienced by other local authorities. The central aim of this strategy is to significantly fortify the council's services against cyber-attacks, in line with the governments Cyber Security Strategy 2022-2030.

Brent's strategy is also aligned with the Shared Technology Service (STS) Cyber Security strategy and the STS Technology Roadmap sets out plans for ensuring the infrastructure for Brent and the other Councils in the shared service are kept secure.

3.2 The Cyber Security Implementation Plan has been developed as a key framework for delivering the Brent Cyber Security Strategy. The Cyber Security Implementation Plan aims to comply with the principles of the government backed scheme - Cyber Essentials - and to follow the "10 Steps to Cyber Security" framework as published by the National Cyber Security Centre in 2012 and most recently updated in 2021.

3.3 The council achieved Cyber Essentials accreditation in in February 2022.

3.4 In addition to Cyber Essentials, STS has also implemented a cloud based corporate back-up solution by Rubrik to counter ransomware attacks such as the high profile attack on Hackney Council's IT Network in 2020.

3.5 Other achievements to date include:

- Multi factor authentication (MFA) has been implemented for all Office 365 access.
- Annual training is mandated for all staff and phishing simulations to both staff and elected members.
- Replacement of all end-of-life mobile phones to ensure that they continue to be in support from the vendor, thus receiving security updates.
- Monitoring of guidance released from the National Cyber Security Centre and implementing those recommendations where appropriate, such as a new password policy due to be communicated Q1 2022.
- Meeting compliance regimes, e.g. Public Services Network (PSN), Payment Card Industry (PCI) and the Health and Social Care Network.
- Incident management – Playbooks have been developed to test and measure our incident response and disaster recovery response capabilities.

3.6 Government Cyber Assessment Framework (CAF)

The Brent Cyber Security Strategy 2022-2026 is aligned with the Government's new Cyber Security Strategy and incorporates the Governments Cyber Assessment Framework (CAF) once developed. The CAF (developed by the National Cyber Security Centre) describes 14 principles and KPIs that organisations are expected to achieve during 2025-2030. The CAF is an assessment framework that provides a systematic and comprehensive approach to assessing the extent to which risks to essential functions are being managed by organisations. Aligning with this framework will enable the council to establish and maintain appropriate and proportionate cyber security, and embed security by design.

4.0 **Risk management and audit**

Risk management:

4.1 The risk of cyber-attack is monitored as a key risk on Brent Council's strategic risk register. The risk is owned by the Managing Director of the Shared Technology Service and mitigations include the new Rubrik backup solution.

4.2 There are a number of other activities which mitigate the risk which also include:

- Anti-Virus is in use across the STS estate and pattern files are updated regularly.
- Both web filtering and mail filtering are in place for all staff.
- As well as the yearly PCN/PCI, an in depth penetration test was carried out by Dionach, an external specialist.
- Continual work is being conducted in making sure that versions of Windows and the applications are supported and have the latest security updates.
- Significant investments have been made in purchasing the tools needed to keep our systems safe and a forward plan has been built to ensure that we are able to respond to the ever changing threat landscape.
- Brent and the partnering councils in STS have a 24x7 third party Security Operations Centre monitoring any unusual activity and will disable and remove any detected threats.
- A range of internal communications campaigns have taken place to raise awareness of the threat of phishing and other risks. This included a presentation at Brent Tech Week.

4.3 The number of improvements made has seen a reduction in cyber investigations. Progress is monitored in the quarterly Shared Service Joint Committee.

Internal audit:

4.4 On 3 November 2020, Brent Council held a cyber-security workshop facilitated by Internal Audit. This was a self-assessment review of the organisation's cyber security arrangements and the demands on its security functions managed by

the Shared Services and within the council. This was timed as the council aimed to advance its cyber security 'deter, defend, detect' strategy.

4.5 A review has been planned as part of the 2021/2022 audit plan, as agreed by the Council's Audit Committee, with the objective of evaluating the design of the council's security controls developed to prevent and detect security and data incidents given the increased reliance on technology by council staff when working from home and the potential for emerging opportunistic threats.

5.0 Financial Implications

5.1 The STS Technology Roadmap was agreed by Cabinet in June 2021. This included £10m infrastructure investment over 4 years for Brent including activities to support cyber security. Cyber Protection is one of five key themes of the roadmap.

6.0 Legal Implications

6.1 None

7.0 Equality Implications

7.1 None

8.0 Consultation with Ward Members and Stakeholders

8.1 The Lead Cabinet member with responsibility for ICT (the Deputy Leader) has been informed and consulted during the development of the current and updated Cyber Security Strategy 2022-2026.

9.0 Human Resources/Property Implications (if appropriate)

9.1 None

Report sign off:

Peter Gadsdon
Strategic Director, Customer and Digital Services