BRENT CYBER SECURITY STRATEGY 2022-2026:
IMPLEMENTATION PLAN

Ref#	Priority	Action	Owner	Details	Due Date
1-a	DEFEND	Implementing firewalls and scanning services	Chief Security Officer	Firewalls are in place both externally and between zones. Work is on-going to ensure all rules have a business case and are documented.	Apr-24
1-b	DEFEND	Carrying out health checks, penetration test and cyber resilience exercises to test their systems and processes	Chief Security Officer/Information Governance Lead	Health checks are carried out annually as part of the submission for Public Sector Network (PSN) code of connection. Web check from the National Cyber Security Centre (NCSC) is configured and in use. We further use early warning from the NCSC, which allows us to receive notifications of malicious activity and help investigate attacks on network quickly.	Apr-24
1-c	DEFEND	Meeting compliance regimes, e.g. PSN, PSI and the Health and Social Care Network	Chief Security Officer/Information Governance Lead	• PSN next submission due May 2024 • NHS Data Security Protection Toolkit (DSPT) next submission due June 2024 • Payment Card Industry (PCI) Compliance next quarterly scan due August 2023	Aug-22
1-d	DEFEND	Working with partners across the public sector through participation in Cyber Security Information Sharing Partnership (CiSP), Warning, Advice and Reporting	Chief Security Officer	STS is an active member of the local warning advice and reporting (WARP), Information security for London (ISfL) and Information Governance for London (IGFL). STS is currently considering options for improving the shared Service Security Operation Centre (SOC) to monitor, prevent, detect, investigate, and respond to cyber threats around the clock.	Nov-23
2-a	DETER	Network Security - Protect the networks from attack, Defend the network perimeter, filter out unauthorised access and malicious content.	Chief Security Officer/Information Governance Lead	• Applying Government's Cyber Security Guidance • 10 Steps to Cyber Security • Cyber Essentials	Apr-24

		Monitor and test security controls.			
2-b	DETER	Multi - factor authentication shall be used where technically possible, such as where administrative consoles provide access to manage cloud based infrastructure, platforms or services. Multi - factor authentication shall be used for access to enterprise level social media accounts.	STS	Where VPN and Remote Desktop Proxy (RDP) are in use, Single Sign-on (SSO) or Multi Factor Authentication (MFA) is to be used. The majority of staff working from home do so from securely configured Windows 10 laptops using direct access technology. The windows image used is checked as part of the annual IT health check. A Data Protection Impact Assessment (DPIA) to be carried out on all new systems/tools.	Apr-24
2-c	DETER	Incident management - Establish an incident response and disaster recovery capability. Test your incident management plans.	Chief Security Officer/Information Governance Lead	Run books have been developed with more to be created to address cyber incidents. Cases are managed through the current ITSM system.	Dec-23
2-d	DETER	Monitoring - Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks.	Chief Security Officer	Various monitoring is used across the estate, STS have an external Security Operations Centre (SOC). STS are continuously assessing opportunities for improvement.	Apr-24
2-e	DETER	Secure configuration - Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.	Chief Security Officer	Currently all server and end user compute builds are created using a standard format. Tools and techniques to ensure that configurations are maintained over time are being investigated. This will be done via a 3rd party tool and using Microsoft features to ensure secure configuration to minimise the attack surface.	Apr-24
2-f	DETER	User education and awareness - Produce user security policies covering acceptable and secure use of your	Chief Security Officer/Information Governance Lead	User education has been enhanced by the use of phishing simulations. Guidance has been published on the intranet to not only guide staff at work, but also provide advice on technology at home - such as the NCSC	Monthly

		systems. Include in staff training.		guidance on smart devices, SMS and email fraud.	
3-a	DEVELOP	Develop and maintain risk management framework, internal control and governance for the prevention and detection of irregularities and fraud	STS/Brent IG	Current STS digital risks fed through to Brent's corporate risk register.	Annually
3-b	DEVELOP	Process, procedures and controls to manage changes in cyber threat level and vulnerabilities	Chief Security Officer	Vigilance is maintained by reading the weekly NCSC cyber threat reports, further evidence and advice is sought from NHS cyber alerts and through engagement with the local WARP.	Weekly
3-c	DEVELOP	Operation of the council's penetration testing programme; and Cyber-incident response	Chief Security Officer/Information Governance Lead	IT health checks are carried out every year as part of the PSN submission.	May-24
3-d	DEVELOP	Introducing training for staff and elected members	Chief Security Officer/Information Governance Lead	As well as the yearly training mandated for staff, more work has taken place this year on providing phishing simulations to both staff and elected members.	Monthly
3-e	DEVELOP	Develop an incident response and management plan, with clearly defined actions, roles and responsibilities	Chief Security Officer/Information Governance Lead	Incident response playbooks have been developed and held for specific cyber events including unauthorised access, data breach, malicious code and Distributed Denial of Service (DDOS). Excersises to be carried out with nominated services Within the plans there are details of external parties and partners who can be contacted for help and advice. Including LGA, NCSC,	Apr-24

				Information Commissioners Office (ICO) and providers of cyber security tools.	
3-f	DEVELOP	Develop a communication plan in the event of an incident	Chief Security Officer/Information Governance Lead	Relevant Internal roles and responsibilities have been identified. The Information Governance team are working with STS to develop the plan within the incident response playbook excercises.	Dec-23