Appendix 1 – Further information on controls, resources and systems in place to provide effective cyber security services within Swansea Bay University Health Board

The controls detailed in the high level cyber security risk consisted of the following actions:-

- **Recruitment of Cyber Security Team**
- **Adopt national tools to highlight vulnerabilities and provide warnings when potential attacks are occurring.**
- **Ensure existing tools provide effective protection against potential Cyber Security attacks**
- **Ensure malicious emails coming into Swansea Bay through NHS Wales gateway are acted on efficiently and effectively**
- **A strong patching regime established to protect against any known security vulnerabilities.**
- **Effective response to alerts raised from the Anti-virus system.**
- **Ensure old systems that are no longer supported are upgraded to supported versions to mitigate against security vulnerabilities.**
- **Rollout of a Cyber Security training module to raise awareness for staff, this is essential as staff are the biggest risk for any cyber security attack.**

1. Recruitment of Cyber Security Team

At the time this risk was submitted, the Cyber Security resource was a single Band 7 WTE.

A new Cyber Security Team has now been established:-

- Band 8a Cyber Security Manager
- Existing Band 7 Cyber Security lead
- Additional two Band 6 posts as Cyber Security Specialists. (It should be noted that the Band 6 posts are currently funded by Welsh Government, and in addition to the Band 8a post are supported at risk by Digital Services).

This has allowed for the setup of a Security Operations Centre to be established in a dedicated environment for the Cyber Team to monitor cyber events in real time and adopt a proactive approach to real time security alerting and take appropriate mitigating actions and onward reporting. This is already providing benefits to the organisation in terms of identifying risks and providing rapid response to those risks.

The Cyber Security Team at Swansea Bay has strong partnership links in place. It works closely with a number of national groups as well as the Cyber Security Team at NWIS through the Operational Service Security Management Board (OSSMB). The team also has membership of the National Cyber Security Centres (NCSC) Cyber Information Sharing Partnership (CiSP) as well as the welsh WARP and Local Resilience Forum who have representatives from the Regional Organised Crime Cyber Unit TARIAN.

2. Adopt national tools to highlight vulnerabilities and provide warnings when potential attacks are occurring.

Progress has been made with the adoption of national tools provided by NWIS (Welsh Government Cyber Security Funding). The resources in the newly established team are essential in providing expert knowledge and ability to act on any issues identified.

- **Security Incident and Event Management system** (**SIEM**) – This allows for centralised logging and alerting of suspicious events across all systems and networks. Local installation has been implemented, with health board system cyber events feeding into the SIEM. Feeds from the health board Anti Virus and End Point Protection system, the SBU Smoothwall Web Proxy (Internet Filter) and the local instance of the national Active Directory which collects information on failed login attempts which could be an early warning that there is a potential cyber attack by malware that is trying different passwords to login to a system. This will provide a dashboard for security monitoring to ensure visibility of potential cyber threats and appropriate action taken by the newly formed Cyber Security team. Training for Cyber staff on operational use of the SIEM was scheduled for March 2020 but Covid digital activities across NHS Wales means that this was postponed and rearranged for a date in July via Teams. The team in conjunction with Security resources in NWIS monitor events on a daily basis. The training will ensure staff have the up to date knowledge to make the best use of the system in Swansea Bay.

- **National Vulnerability Management System** (**Nessus**) - This is a system which scans devices attached to the network for known security issues and report on the severity of them, This has recently been implemented at SBU and training for Cyber Security staff completed on May 21st 2020. This process has started with the Server team as a proof of concept.

3. Ensure existing tools provide effective protection against potential Cyber Security attacks

A number of local tools and national systems have been in place for a number of years to protect against malicious attacks. These include:

Local System	**New Activity following formation of Cyber Security Team**
Anti Virus and Endpoint Security – Kaspersky Endpoint Security renewed in 2020 which provides the Anti-Virus protection for desktop, laptop and server computers. In addition, Endpoint Security Management which forces encryption of USB memory sticks to	Cyber Team have a dashboard displaying events and proactively manage this.

protect data. Kaspersky are recognised as one of the Leaders in this field.	
Filtered Web Access – Web traffic from all devices on the HB network is sent via the Smoothwall Web Filter which provides controls around which user groups can access which content types and provides additional protection to block access on known malicious sites.	Rule sets are actively monitored and any sites highlighted as risks are actively blocked. This has been of particular importance during the COVID-19 pandemic to stop staff inadvertently accessing fake sites.
Secure File Sharing Portal – This is used to securely transfer files to people outside of the organisation to protect against confidential and person identifiable information getting into the wrong hands.	Cyber team have improved the process to securely transfer confidential and Person Identifiable documents. The process is much quicker than previously possible with a single resource and helps mitigate against work around solutions which could inadvertently result in confidential information getting in the wrong hands.

4. Ensure malicious emails coming into Swansea Bay through NHS Wales gateway are acted on efficiently and effectively

The newly established Cyber Security team have developed a process to act upon malicious emails which have inadvertently come through the national email filter. These are daily events and without the new resources, would have taken substantially longer, especially when previously there was only one resource who could be training or in a meeting.

5. A strong patching regime established to protect against any known security vulnerabilities.

The health board computer devices have excellent compliance levels with Microsoft patching. The following systems are in place to ensure compliance levels are maintained.

System	**New Activity following formation of Cyber Security Team**
Asset Management – SNOW asset management software has been deployed to health board computers and provides hardware and software inventory. This provides detail on the device hardware, software installed and who has used it. This is essential to highlighting any potential software	**Secure Managed Device Review Group** A cross team working group with Cyber Team, Infrastructure Team and Desktop Team to review the managed device estate and the plan to bring all devices to a position they are running up-to-date **operating systems** and supported hardware. SBU Service Delivery Manager chaired the All Wales Device

vulnerabilities. Microsoft SCCM is also used in conjunction with SNOW to provide updates to protect against software security vulnerabilities.	management Group to ensure Windows 7 (non supported January 2020 – extended to 2021 following the new licence agreement with Microsoft) devices were upgraded to Windows 10. Nationally SBU are leading in this across Wales **A High Risk Software Review Working Group** – Recently setup collaboration with Cyber Team and Desktop Team to perform weekly review of high risk software installed on managed devices. Compliance levels are monitored and reducing the number of agreed software for essential needs only ensure that programs are updated regularly to reduce the risk of a cyber attack on old vulnerable software. Given the amount of software installed, this work is ongoing to reduce numbers. Weekly meeting.
Server Patch Management Monitoring– Ensuring latest software updates are applied is essential in defending against security attacks on vulnerable systems. An in-house developed Server Patch Management system has been implemented to show security patch levels for the Health Board servers. A simple dashboard shows compliance levels with latest releases. This is in direct response to the national recommendation from the All Wales Stratia Report.	**Secure Infrastructure Review Group** A cross team working group with the Cyber Team and Infrastructure Team to review servers and services are using the latest supported operating systems and software.

6. Effective response to alerts raised from the Anti-virus system

As detailed in section 3.

7. Ensure old systems that are no longer supported are upgraded to supported versions to mitigate against security vulnerabilities.

There are a number of older systems running on software that is no longer updated mainly due to departments not implementing the latest versions. A plan will be developed in order to move these to supported versions. Funding for a fixed term post has been requested from capital 2020/21 but has stalled due to Covid activities. There will inevitably be further costs which will need to be funded further as identified by the fixed term post. From a Governance perspective, the Digital Service Management Group has

been established to ensure departmental representatives manage their systems in a safe and secure manner.

8. Rollout of a Cyber Security training module to raise awareness for staff, this is essential as staff are the biggest risk for any cyber security attack.

A national Cyber Security Training Package has been deployed locally, through ESR which will offer a number of modules on improving awareness around Cyber Security.

Mandatory adoption of this training package **is not in place yet**. Until this is made mandatory and the training module has been completed by all staff, the cyber security risk associated with staff ill equipped to notice phishing or fraudulent emails remain at a high level. This has been taken to the mandatory training board but no agreement has been reached to adopt this essential Cyber Security training/awareness course.

In addition, a **Phishing** (basically a hacker's phrase for conning an online user, usually through email) **Simulation Campaign and Targeted Training software package has been procured from** Welsh Government Cyber Security funding (Metaphish). This allows the Cyber Team to perform a simulated phishing attack and depending on the staff response (clicks on a malicious link or not) provides a dashboard view on how many staff are aware of phishing emails and conversely who needs additional training to ensure they don't get exploited when real risk phishing emails come in. The training material complements the training Cyber Security module within ESR but emphases the risk of phishing emails. to raise awareness of Cyber Security risks and provide essential learning to mitigate against those risks.

9. Additional Cyber Security tools procured to enhance protection

In addition, the following cyber security systems are being implemented. These were funded by Welsh Government to enhance Cyber Security defences based on local needs.

System	Additional Protection
Network Monitoring and Visibility	Procured Cisco Stealth Watch (Welsh Government Cyber Security Funding) to allow real time monitoring and provide early warning for suspicious activity of the health board computer network, as well as retrospective analysis with the use of advanced machine learning. Early warning is critical in order to stop further potential damage caused by malicious attacks and limit the impact on availability/data loss.
Local Firewalls	Procured Cisco Firepower next generation firewalls (internal) to complement the Cisco Security Centre firewalls which protects the network traffic entering and leaving the health board. These provide additional internal security protection.

A Secure Networking Group has been established. A weekly review with the Network and Cyber Security Team to review network security. This group provides expert knowledge in terms of the management of the newly procured solutions and effective proactive management of any network related security alerts from existing and new security tools.

The Health Board also has an internet link, an annual independent vulnerability check is made to ensure services are secure and mitigates against unauthorised access.