POWYS TEACHING HEALTH BOARD
JOB DESCRIPTION

JOB DETAILS	
Job Title:	Cyber Security Analyst
Pay Band:	7
Hours of Work and Nature of Contract:	37 hours permanent
Service Group:	Finance, ICT & Informatics
Department:	Digital Transformation & Informatics
Base:	TBC/Agile-Remote Working supported as per HB policy
ORGANISATIONAL ARRANGEMENTS	
Managerially Accountable to:	Cyber Security and Compliance Manager
Professionally Accountable to:	Director of Digital Transformation & Informatics

VALUES & BEHAVIOUR

Our Values and Behaviours are demonstrated through our 'Health Care Strategy' centred on the Needs of the Individual' through Respect, Trust, Integrity, Working Together, Kindness and Caring and Fairness and Equality.

JOB SUMMARY / PURPOSE:

The post holder will be required to provide technical expertise and operationally monitor and manage and report on Powys Teaching Health Board's IT systems and services to improve its cyber security posture, will respond to cyber incidents, and help develop and define policy, processes, and procedures to reduce the likelihood of cyber security risks and incidents.

Undertake vulnerability scanning, the monitoring of ICT systems and services and work with IT service delivery to review compliance with best practice.

Act as an escalation point for cyber security incidents and provide subject matter expert and specialist advice and knowledge, help in improving user education on cyber risks to the Health Board.

Required to adhere to the cyber security professional code of conduct and keep up to date with legislation such as Network Information Systems (NIS) regulations and Welsh national security policies and procedures, as well as assessing security advisories from external sources such as Digital Healthcare Wales (DHCW), 3rd Party Suppliers, Health Board Partners and National UK organisations NCSC, NHS Digital etc.

In particular the post holder will be responsible for:

- Contributing to the Cyber Security and Compliance Strategy
- Operational delivery of the day-to-day Cyber Security Monitoring and Management
- Deputising for the Cyber Security & Compliance Manager when required
- Present and make the case for controls and measures to deliver effective ICT security/cyber security
- Manage and maintain the Cyber Security & Compliance Service Improvement Plan
- Be a key figure for ICT Security/Cyber Security System development and support

DUTIES & RESPONSIBILITIES

Reporting to and assisting the Cyber Security & Compliance Manager in developing robust cyber security procedures based on best practice, advice, and guidelines from professional bodies as well as theoretical knowledge. Advising of relevant cyber security risks, issues and vulnerabilities with IT systems or services used across the Health Board.

Ensure all equipment is protected from Malware and other emerging threats.

Ensure security systems are in place for our local and wide area networks.

Proactive monitoring, reviewing, analysing, and interpreting of security incidents based on:-

- Alerts generated by Microsoft 365 Defender and the National DHCW IT Welsh national LogRhythm SIEM solution, and Nessus Platform.

- Monitoring and reporting of end user device and servers' security patching and vulnerabilities using Microsoft 365 Defender.

- Raising incidents, prioritising incidents dependant on the risks and vulnerabilities identified by alerts and nationally raised cyber events.

- Monitor alerts relating to abnormal user behaviour e.g., access to systems outside normal working hours, unauthorized login attempts and login failures.

- Attempts to connect by un-authorised systems to network and IT systems and applications.

- Advise the ICT Security Function on technical faults, products, industry developments.

Plan and prioritise own work ensuring effective support to all areas and delivery of key Cyber Security improvement objectives.

Monitor, report and record own projects and their timelines.

Assists in supporting the requirements of internal and external cyber security audits, penetration tests and the remediation actions that might arise from these.

Utilise benchmarking, trend information, audits, and other available information in managing Cyber Security delivery and performance.

Continually understand the changing level of cyber security threat, from a local and national perspective and react accordingly.

Produce technical documentation that provides all necessary information to allow continuing maintenance and development of systems and services.

Conduct regular and frequent vulnerability audits and assessments using a variety of tools and techniques against all networked devices and manage any identified vulnerabilities and within an agreed timeframe and produce remediation plans and actions.

Keeping abreast of new threats and vulnerabilities which could impact the Health Board and bringing key security issues and concerns to the attention of relevant ICT staff members with recommendations to resolve the security issues and ensuring that IT Senior Team receives timely advice on any potential cyber security threats to the Health Board IT Infrastructure or IT systems.

Comply with the Corporate Governance structure in keeping with the principles and standards set out by Powys Teaching Health Board.

Communication

Develop close working relationships with the ICT Team and other departments within PTHB and other health bodies to enable PTHB to deliver Cyber Security improvement objectives.

Provide and receive highly complex and potentially highly sensitive information in relation to adverse events where there may be significant barriers in accepting and delivering the management of change.

Use influencing skills to ensure collaborative working to engender a level of quality improvement across the organisation.

Develop and manage awareness programmes for end users in support of key Cyber Security objectives.

Writing and presenting reports to a wide range of groups both internal and external.

Required to regularly produce complex reports and presentations based on a range of information from a variety of sources.

Governance and Quality

Development, dissemination, and adoption of robust security standards in-line with security good practice.

Ensure an evidence-based approach to relevant audit/and or evaluation work on all aspects of quality improvement.

Collaborate with all departments within PTHB to establish a process for identification and dissemination of high-quality information to facilitate effective Cyber Security management and improvement.

Leadership

Advocate continuous improvement policies of the Information Security Management System, setting standards, benchmarking across the NHS and developing best practice.

Provide leadership and direction in situations where highly complex concepts need to be conveyed and implemented across the organisation.

Responsible for developing and implementing a Cyber Security strategy including change control, Root Cause Analysis, and error management.

Lead and advise Cyber Security Manager in relation to implementation of the PTHB Information Security Management System.

Identify the physical resources required to deliver an Information Security Management System improvement programme.

Contribute to defining the strategic cyber security direction of the organisation in developing cyber related improvements.

Other Responsibilities

Undertake other relevant duties as required by the Cyber Security and Compliance Manager. This includes representing PTHB at both internal and external meetings.

Act on behalf of the Cyber Security & Compliance Manager in their absence, deputising at relevant strategic and operational meetings as required.

Support the Cyber Security & Compliance Manager in ensuring budgets and project costs are managed and used effectively and promote value for money for PTHB.

Responsible in conjunction with the Cyber Security & Compliance Manager for the recruitment and selection of any future staff in cyber security roles.

PERSON SPECIFICATION			
ATTRIBUTES	**ESSENTIAL**	**DESIRABLE**	**METHOD OF ASSESSMENT**
Qualifications and/or Knowledge	Educated to Masters level or similar discipline relevant to an IT Security equivalent such as CISM, CISSP, CISMP Specialist knowledge of Cisco/Microsoft/CompTIA/CompTIA+ Certified Ethical Hacker, Security+ Security compliance testing Security architecture Evidence of continuous professional development Good working knowledge of NHS terms and conditions Up to date knowledge of Release and Change Management IT Service Management ITIL V3 or V4	Analysis of network penetration testing Application vulnerability assessments	Pre-employment checks Application Form
Experience	Experienced with Network segmentation and Network Access Controls (802.1x, MAB) Azure Cloud Solutions and Azure AD Intermediate to high level of experience with SIEM solutions Experience of Cyber Risk Management Knowledge and experience of industry standard technology such as: Microsoft Windows Client and Server operating systems Microsoft MDE (ATP /Defender) Relevant experience in health service or other major large-scale customer service-oriented organisation	Experience with PAM solutions Experience with SIEM Platforms	Application Form and Interview

ATTRIBUTES	ESSENTIAL	DESIRABLE	METHOD OF ASSESSMENT
Experience cont'd	Expert and detailed knowledge and experience leading, coordinating or being actively involved in the investigation and remediation of security incidents Understanding of GDPR / NIS Regulations Expert and detailed knowledge and experience in the investigation and remediation malware infections and outbreaks Detailed knowledge and experience in cyber security threat analysis and the use of software utilities to identify potential threats and eliminate false positives Skilled in the installation and configuration of endpoint and perimeter cyber-security solutions and software agents Knowledge of Cyber security best practices Experience of working with service requests Maintaining accurate records for customers and colleagues Knowledge of IT infrastructure including Networking, Firewalls, TCP/IP, Active Directory, DNS and DHCP		
Aptitude and Abilities	Highly developed problem solving and analysis skills in areas which may be complex Enthusiastic and innovative Excellent communication skills both written and verbal, demonstrate tact and diplomacy when working with others	Ability to speak Welsh	Interview

ATTRIBUTES	ESSENTIAL	DESIRABLE	METHOD OF ASSESSMENT
Aptitude and Abilities cont'd	Work within ICT Security/Cyber Security Frameworks and policies Pragmatic and strategic thinker, developer of practical and effective solutions with an aptitude for developing new skills Self-motivated and project focussed Output qualitative and quantitative risk assessments/analysis Attention to detail, accurate and a strong quality first approach Team player, self-starter, pro-active and resourceful Ability to work under pressure Willing to work as part of a team and pick up ad-hoc work as requested Excellent computer skills and experience of Microsoft Office Suite with the ability to master new applications		
Values	Demonstrate PTHB Values		Interview Application Form
Other	Ability to travel within geographical area Flexible approach to work		Application Form and Interview

GENERAL REQUIREMENTS

Include those relevant to the post requirements

- **Values:** All employees of the Health Board are required to demonstrate and embed the Values and Behaviour Statements in order for them to become an integral part of the post holder's working life and to embed the principles into the culture of the organisation.

- **Competence:** At no time should the post holder work outside their defined level of competence. If there are concerns regarding this, the post holder should immediately discuss them with their Manager/Supervisor. Employees have a responsibility to inform their Manager/Supervisor if they doubt their own competence to perform a duty.

- **Learning and Development:** All staff must undertake induction/orientation programmes at Corporate and Departmental level and must ensure that any statutory/mandatory training requirements are current and up to date. Where considered appropriate, staff are required to demonstrate evidence of continuing professional development.

- **Performance Appraisal:** We are committed to developing our staff and you are responsible for participating in an Annual Performance Development Review of the post.

- **Health & Safety:** All employees of the organisation have a statutory duty of care for their own personal safety and that of others who may be affected by their acts or omissions. The post holder is required to co-operate with management to enable the organisation to meet its own legal duties and to report any hazardous situations or defective equipment. The post holder must adhere to the organisation's Risk Management, Health and Safety and associate policies.

- **Risk Management:** It is a standard element of the role and responsibility of all staff of the organisation that they fulfil a proactive role towards the management of risk in all of their actions. This entails the risk assessment of all situations, the taking of appropriate actions and reporting of all incidents, near misses and hazards.

- **Welsh Language:** All employees must perform their duties in strict compliance with the requirements of their organization's Welsh Language Scheme and take every opportunity to promote the Welsh language in their dealings with the public.

- **Information Governance:** The post holder must at all times be aware of the importance of maintaining confidentiality and security of information gained during the course of their duties. This will in many cases include access to personal information relating to service users.

- **Data Protection:** The post holder must treat all information, whether corporate, staff or patient information, in a discreet and confidential manner in accordance with the provisions of the General Data Protection Legislation and Organisational Policy. Any breach of such confidentiality is considered a serious disciplinary offence, which is liable to dismissal and / or prosecution under current statutory legislation and the HB or Trust Disciplinary Policy.

- **Records Management:** As an employee of this organisation, the post holder is legally responsible for all records that they gather, create or use as part of their work within the organisation (including patient health, staff health or injury, financial, personal and administrative), whether paper based or on computer. All such records are considered public records and the post holder has a legal duty of confidence to service users (even after an employee has left the organisation). The post holder should consult their manager if they have any doubt as to the correct management of records with which they work.

- **Equality and Human Rights:** The Public Sector Equality Duty in Wales places a positive duty on the HB/Trust to promote equality for people with protected characteristics, both as an employer and as a provider of public services. There are nine protected characteristics: age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race; religion or belief; sex and sexual orientation. The HB/Trust is committed to ensuring that no job applicant or employee receives less favour-able treatment of any of the above grounds. To this end, the organisation has an Equality Policy and it is for each employee to contribute to its success.

- **Dignity at Work:** The organisation condemns all forms of bullying and harassment and is actively seeking to promote a workplace where employees are treated fairly and with dignity and respect. All staff are requested to report any form of bullying and harassment to their Line Manager or to any Director of the organisation. Any inappropriate behaviour inside the workplace will not be tolerated and will be treated as a serious matter under the HB/Trust Disciplinary Policy.

- **DBS Disclosure Check:** In this role you will have **no contact** with patients / service users / children **/**vulnerable adults in the course of your normal duties. You will therefore not be required to apply for a Criminal Record Bureau Disclosure Check as part of the HB/Trust's pre-employment check procedure.

- **Safeguarding Children and Adults at Risk:** Powys Teaching Health Board is fully committed to safeguarding people. Employees and workers (including agency and bank workers) are responsible for ensuring they understand what actions to take if they have reasonable cause to suspect that a child or an adult is at risk of harm and mandatory safeguarding training is completed in line with their role specific competencies.

- **Infection Control:** The organisation is committed to meet its obligations to minimise infections. All staff are responsible for protecting and safeguarding patients, service users, visitors and employees against the risk of acquiring healthcare associated infections. This responsibility includes being aware of the content of and consistently observing Health Board/Trust Infection Prevention & Control Policies and Procedures.

- **No Smoking:** To give all patients, visitors and staff the best chance to be healthy, all Health Board/Trust sites, including buildings and grounds, are smoke free.

- **Flexibility Statement:** The duties of the post are outlined in this Job Description and Person Specification and may be changed by mutual agreement from time to time.

Organisational Chart