CAJE REF: 2020/0107

GIG CYMRU
NHS WALES
Bwrdd Iechyd Prifysgol
Aneurin Bevan
University Health Board

ANEURIN BEVAN UNIVERSITY HEALTH BOARD
JOB DESCRIPTION

JOB DETAILS:

Job Title	ICT Senior Cyber Security Analyst
Pay Band	Band 6
Hours of Work and Nature of Contract	37.5
Division/Directorate	Informatics
Department	ICT
Base	Mamhilad

ORGANISATIONAL ARRANGEMENTS:

Managerially Accountable to:	ICT Network, Cyber Security & Telecoms Manager
Reports to: Name Line Manager	ICT Cyber Security Team Leader
Professionally Responsible to:	Head of ICT

OUR VALUES:

Job Summary/Job Purpose:

Aneurin Bevan University Health Board (ABUHB) has a large and complex ICT service that underpins the delivery of digital health care. ICT supports around 14,000 users and over 200 services across more than 120 sites. The adoption and expectations placed upon digital healthcare are expected to grow substantially over the next 5 years as the health board adopts mobility both in primary and secondary care settings.

The team will be required to monitor Cyber Security Systems, respond to Cyber Incidents and develop policy, processes and procedures to reduce the likelihood of a Cyber Security incident.

As a senior member of the Cyber Security Team at ABUHB you will undertake vulnerability scanning, the monitoring of Cyber Security Systems and work with third parties to review compliance with best practice. You may be required to deputise for the Cyber Security Team leader where appropriate.

You will act as an escalation point for Cyber Security incidents and provide specialist advice and knowledge to support the service operations centre as well as developing Cyber Security Training packages for both the team and the organisation. With digital becoming a critical dependency in healthcare, availability of services is essential and we must therefore instil a culture of Cyber Security from the ground up.

You will be required to adhere to the Cyber Security professional code of conduct, and keep up to date with legislation and national policies, as well as assessing security advisories from third parties.

You may be required, at times, to work outside of standard working hours. You could also be expected to join on an out of hours, on-call escalation rota. You will be required to adhere to the Cyber Security professional code of conduct, and keep up to date with legislation and national policies, as well as assessing security advisories from third parties. The post holder will undertake other relevant duties as agreed with the ICT Voice Services Team Leader, ICT Network, Cyber Security & Telecoms Manager, and Technical Services Manager commensurate with the banding of this role.

<u>DUTIES/RESPONSIBILITIES</u>:

1. Communication & Relationship Skills
   - Provides and receives complex, sensitive information relating to Cyber Security and the safe operation of the organisations ICT systems.
   - Provides and receives highly complex statistical and analytical information relating to Cyber Security.
   - Communicates highly complex information with other Cyber Security Analysts/Specialists
   - Prepares reports based on Cyber Security incident statistics and organisational compliance with Cyber Security targets
   - Coordinates staff training in Cyber Security and prepares awareness campaigns
   - Coordinates Cyber Security incident responses at organisational level

2. Knowledge Training and Experience
   - Specialist knowledge across range of Cyber Security areas, underpinned by theory and experience of statistical/ analytical techniques and procedures, acquired through degree level or equivalent and a recognised qualification in Cyber Security e.g. CISMP, CompTIA or equivalent.
   - Specialist knowledge of Cyber Security monitoring and vulnerability scanning systems.
   - Developing Cyber Security procedures based on best practice, advice and guidelines from professional bodies as well as theoretical knowledge.

3. Analytical and Judgmental Skills
   - Determines appropriate course of action when presented with complex facts relating to ICT systems and their security.
   - Analyses, investigates and resolves complex Cyber Security queries and issues/problems, where there is a range of solutions
   - Analyses complex data from a range of Cyber Security monitoring systems and vulnerability assessments and interprets information to determine options to mitigate risks.
   - Investigate user requirements which may require configuration of software and hardware.

4. Planning and Organisational Skills
   - Plans and coordinates digital asset and system patching in conjunction with critical health care services and other stakeholders within ICT.
   - Initiates and plans all work programmes and makes adjustments to meeting customers’ requirements.

5. Physical Skills
   - The role will require travel between different places of work.
   - Requires standard keyboard skills and manipulating complex data at speed.

6. Responsibility for Patient / Client Care
   - Contact with patients is incidental

7. Responsibility for Policy / Service Development
   - Implement policies and procedures and proposes changes to practices around Cyber Security that impact team, department and health board
   - Tests Cyber Security procedures
   - Ensures maintenance and knowledge management of Cyber Security Systems
   - Proposes changes to Cyber Security practices as a result of new guidelines or legislation.

8. Responsibility for Financial / Physical Resources
   - Ensure that digital assets are patched and up to date and that Aneurin Bevan University Health Board is compliant with best practices and national standards.
   - Perform audits and vulnerability assessments on the digital assets.
   - Determine hardware and software refresh cycles for equipment.

- Work with key stakeholders in ICT to ensure that compliance is retained and that where this is not possible, appropriate risks are recorded and financial profiles and risk registers are updated.
- Approves staff travel expenses where applicable.
- Manages staff Annual leave and sickness via the ESR system in line with health Board policies.

9. Responsibility for Human Resources
    - Act as a mentor to junior staff and coordinate work where appropriate
    - Day to day management of the cyber security team.
    - Required to supervise work placements Contractors and junior staff where appropriate
    - Deliver specialist training programmes for Cyber Security.
    - Develops own staff
    - Working with the ICT Management Team to contribute to the professional development of the above staff.
    - Lead, develop and motivate the team to ensure they perform to acceptable standards.

10. Responsibility For Information Resources
    - Adapt, design Cyber Security Systems to ensure compliance with Cyber Security standards
    - Work with auditors to ensure Cyber Security Systems are compliant with external assessors
    - Responsible for introducing, adapting and improving Cyber Security Systems
    - Responsible for the production of report and compliance data from Cyber Security Systems and monitoring of digital estate to ensure systems are patched and protected against known and emergent threats.
    - Presents all data and KPI's to ICT Management Board for review and propose actions and resolutions based on the data.

11. Responsibility for Research and Development
    - Day to day research into external and internal Cyber Security threats
    - Undertake vulnerability scanning and surveys of network security
    - Research and propose options to mitigate Cyber Security Vulnerabilities
    - Implements methods to capture and report Cyber Security assessment data

12. Freedom to Act
    - Act as a lead for the Health Board within the Cyber Security Team.
    - Lead analyst for NHS board level performance reports
    - Work to achieve agreed team objectives with the freedom to do this working within national standards, best practice and Cyber Security Code of conduct
    - To manage own workload

Addendum

This Job Framework is a guide to the duties you will be expected to perform immediately on your appointment. It is not part of your contract of employment and your duties may well be changed from time to time to meet with changes in the Health board's requirements.

As an employee of Aneurin Bevan University Health Board, you are required to completely conform to all relevant policies including Health & Safety, Confidentiality, Dignity at Work and the Fire Policy.

PERSON SPECIFICATION

ATTRIBUTES	ESSENTIAL	DESIRABLE	METHOD OF ASSESSMENT
Qualifications and/or Knowledge	Educated to Degree level (preferably Cyber Security) or equivalent and a recognised qualification in Cyber Security e.g. CISMP, CompTIA or equivalent level of work experience and knowledge Evidence of Continual Professional Development Good understanding of Cyber Security best practices and terminology Knowledge of Desktop, Server and Mobile devices and operating systems as well as IoT devices Knowledge of Information Assurance and Cyber Security standards and -certifications Knowledge of laws and regulations relating to Cyber Security Knowledge of common Cyber Security tools and solutions Good understanding of security monitoring and alerting solutions Good understanding of Cyber Security professional code of conduct Good understanding of the Incident Response lifecycle Good understanding of vulnerability scanning and penetration testing methodologies	Professional qualification or membership in cyber security (ISC2, BCS, NCSC, Tiger, CHECK, CREST, CompTIA etc.) Application of Cyber Security in a healthcare environment Good knowledge of one or more specialist areas such as compliance, penetration testing, or incident response. ITIL Foundation	Application Form Interview References Certificates
Experience	Experience within Cyber Security, underpinned by theory Knowledge of a range of ICT areas acquired through qualification or relevant experience Experience of Cyber Security monitoring of SIEM systems. Evidence of Cyber Security or	Experience of ICT service provision in a health care setting Experience of working in fields other than Cyber Security Delivery of training to technical and non-	Application Form Interview References

	other relevant work outside formal training or employment (voluntary, research, academia, social media etc.) Relevant experience working in Cyber Security	technical staff Report writing Procedure development	
Aptitude and Abilities	Excellent communication and interpersonal skills, verbal and written and reporting skills Ability to produce good quality documentation. Able to deal effectively with staff, customers, and suppliers at all levels Good organisational skills Good computing/keyboard skills	Ability to speak Welsh Strong interpersonal skills	Application Form Interview References
Values	Able to work as part of a Team Able to work under own initiative Self-motivated and enthusiastic with the ability to work unsupervised. Flexible approach to work and adaptable to the needs of the service. Good time keeping Proactive outlook in the resolution of customer issues. Analytical approach to tasks.	Able to work under pressure Thorough approach to completing tasks.	Application Form Interview References
Other	Must be able to travel within geographical area. May be required to work hours flexibly on occasion You will be required to work as part of an on call escalation.		Application form and interview

GENERAL 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 organisation'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:** This role does not require a DBS Disclosure Check.

- **Safeguarding Children and Adults at Risk:** The organisation is committed to safeguarding children and adults at risk. All staff must therefore attend Safeguarding Children & Adult training and be aware of their responsibilities under the All Wales Procedures.

- **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.

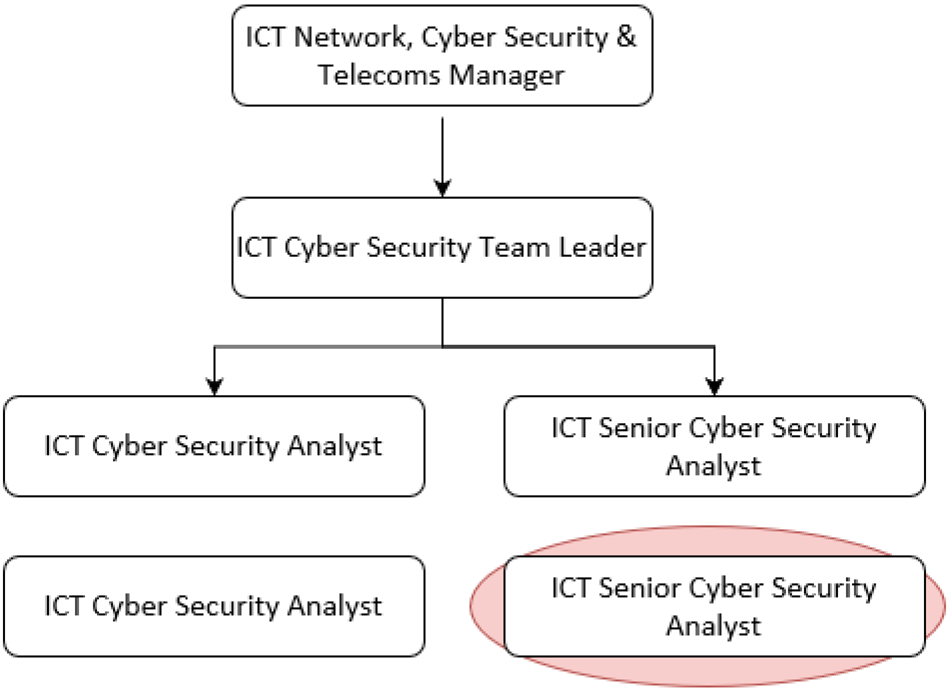
- **No Smoking:** To give all patients, visitors and staff the best chance to be healthy, all Health Board/Trust sites, including buildings and grounds, are smoke free.

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.

APPENDIX 1

Job Title: ICT Senior Cyber Security Analyst

Organisational Chart


ICT Network, Cyber Security & Telecoms Manager
ICT Cyber Security Team Leader
ICT Cyber Security Analyst
ICT Senior Cyber Security Analyst
ICT Cyber Security Analyst
ICT Senior Cyber Security Analyst

APPENDIX 2

Job Title: ICT Senior Cyber Security Analyst

<u>Supplementary Job Description Information</u>

Physical Effort

Examples of Typical effort(s)	How often per day / week / month	For how long?	Additional Comments
The role requires light physical effort.	Daily	All day	
Occasional physical effort required to carry or move equipment	A few times a year	1-2 hours	
VDU use	Daily	Continuous	

Mental Effort

Examples of Typical effort(s)	How often per day / week / month?	For how long?	Additional Comments
Concentration required when checking information and when answering queries from staff, customers; there may be interruptions to deal with.	Daily	2-3 hours	
Concentration required when creating and checking documentation for accuracy as well as analysing data.	Daily	2-3 hours	
Ability to handle multiple work streams at the same time.	Daily	2-3 hours	

Emotional Effort

Examples of Typical effort(s)	How often per week / month?	For how long?	Additional Comments
Rare exposure to emotional circumstances within the work place e.g. Failure of systems affecting whole health board.	Rarely	1-3 hours	

Working Conditions

Examples of Typical Conditions	How often per week / month?	For how long?	Additional Comments
Office conditions requiring continuous VDU usage on most days.	Daily	All day most days	
Occasional work in server rooms whilst monitoring, installing or configuring equipment.	Every few months	1-2 hours at a time	
Independently mobile between sites of work around within the health board area of operation.	Monthly	1-2 hours at a time	