

JOB DESCRIPTION

JOB DETAILS

Job Title: Cyber Security Senior Specialist

Pay Band: 7

Directorate: Planning, Performance & Commissioning

Department: Informatics

ORGANISATIONAL ARRANGEMENTS

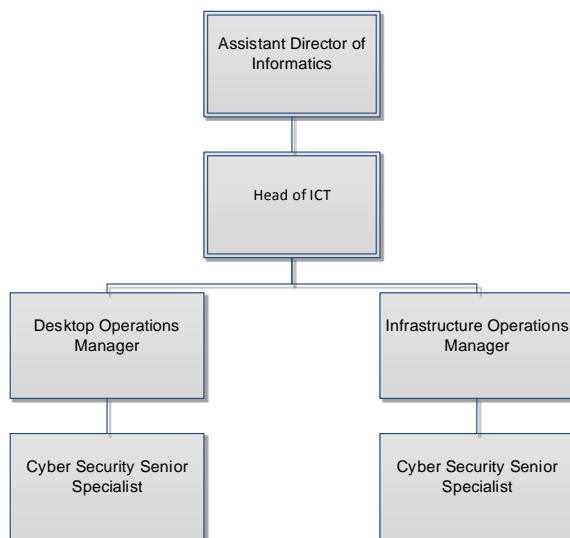
Managerial Accountable to: Head of ICT

Reports to: Desktop Operations Manager
Infrastructure Operations Manager

Professionally Responsible to: Head of ICT

Responsible For: No line management responsibilities

Organisation chart:



JOB SUMMARY / PURPOSE

The post holder 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 ICT team at Hywel Dda UHB you will undertake vulnerability scanning, the monitoring of Cyber Security Systems and work with third parties to review compliance with best practice.

You will act as an escalation point for Cyber Security incidents and provide specialist advice and knowledge across all ICT areas (including networks, systems, and applications) and to support our ICT services 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.

MAIN DUTIES AND RESPONSIBILITIES

Service Management

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.

Analyses, investigates and resolves highly complex incidents and problems associated with Cyber Security systems.

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.

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.

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

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

Service Improvement

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.

Communications

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.

Communicates highly complex analytical Cyber Security matters to non-technical staff and managers across the Health Board such as undertaking presentations to the Information Governance Sub-Committee

Prepares reports based on Cyber Security incident statistics and organisational compliance with Cyber Security targets and ensures after actions are completed across ICT and the wider Health Board.

Provides staff training in Cyber Security, undertakes complex presentations to large groups and prepares awareness campaigns.

Coordinates Cyber Security incident responses at organisational level.

Finance and Resources

Ensure that digital assets are patched and up to date and that Hywel Dda University Health Board is compliant with best practices and national standards to ensure the safe and correct use of IT equipment used by the staff of Hywel Dda UHB..

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.

Adapt, design Cyber Security Systems to ensure compliance with Cyber Security standards ensuring the safe and correct use of IT equipment used by the staff of Hywel Dda UHB.

Work with auditors to ensure Cyber Security Systems are compliant with external assessors.

Responsible for project managing the introduction of new Cyber Security systems ensuring the relevant plans and documentation is in place.

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 Team for review and propose actions and resolutions based on the data.

Uses KPI data to analyse Cyber Security trends across the Health Board.

Personal and People Development and People Management

Act as a mentor to junior staff and coordinate work where appropriate.

Required to supervise work placements Contractors and junior staff where appropriate relating to Cyber Security activities.

Deliver and plan specialist training programmes for Cyber Security.

Develops ICT staff in Cyber Security skills and competencies.

Working with the ICT Management Team to contribute to the professional development of the above staff.

Lead, develop and motivate the wider ICT team to ensure they perform to acceptable standards in relation to Cyber Security.

Information Processing

Determines appropriate course of action when presented with complex facts relating to ICT systems and their security.

Analyses, investigates and resolves highly complex incidents and problems associated with Cyber Security systems where there is no available solution yet available.

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.

Responsible for the implementation of new Cyber Security systems ensuring they meet the requirements of the Health Boards Cyber Security strategy.

Health, Safety and Security

Act within legislation, policies and procedures relating to Information Governance.
Attend statutory/mandatory training.

Ensures all equipment is tested to ensure correct and safe operation prior to introduction as a live service.

Guarantees at all times the security and safety of user information and ensures all Health Board employees and equipment complies with the relevant policies.

Quality

Undertake day to day research into external and internal Cyber Security threats.

Undertake vulnerability scanning and surveys of network security systems.

Research and propose options to mitigate Cyber Security Vulnerabilities.

Implements methods to capture and report Cyber Security assessment data.

Assists the Health Board in achieving the relevant Cyber Security certifications.

Equality and Diversity

Actively promotes equality of opportunity and diversity in own area of responsibility.

Effort and Environmental

The role will require travel between different places of work.

Attending local and national meetings.

Requires standard keyboard skills and manipulating complex data at speed.

Act as a lead for the Health Board within the ICT team.

Work to achieve agreed team objectives with the freedom to do this working as the Lead specialist within national standards, best practice and Cyber Security Code of conduct
To manage own workload.

The role requires frequent concentration and analysis of ICT and Cyber Security Systems and due to the responsive nature the work pattern unpredictable

Concentration required when analysing complex machine data with likelihood of interruptions to answer queries from staff and other user groups.

Occasional exposure to high pressure Cyber Incident Response.

Office conditions requiring continuous VDU usage on most days.

General

Any other duties consummate with current band and below as determined by the Head of ICT.

Maybe required to participate in the ICT team's on-call rota.

To be an active member of the national Cyber Security Service Management Board(s) representing the Health Board as required.

Create a personal development plan annually as part of the PADR process.

Keep skills up to date to reflect best practices in Cyber Security.

Attendance at seminars and conferences that support development of self and the role.

Ensure continuation of personal development including leadership skills, through appropriate formal and informal training as and when necessary.

Keep up to date with legislation in relation to GDPR and NISD, Caldicott principles, and confidentiality, Human Rights Act, Freedom of Information Act etc. and the latest policies.

Keep up to date on National Informatics Health Care strategies.

PERSON SPECIFICATION

ATTRIBUTES	ESSENTIAL	DESIRABLE	METHOD OF ASSESSMENT
<p>Qualifications and Knowledge</p>	<p>ITIL Foundation.</p> <p>Educated to Post Graduate 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.</p> <p>Evidence of Continual Professional Development.</p> <p>In depth specialist knowledge of Cyber Security best practices, standards, certifications and terminology.</p>	<p>Professional qualification or membership in cyber security (ISC2, BCS, NCSC, Tiger, CHECK, CREST, CompTIA etc.).</p> <p>Application of Cyber Security in a healthcare environment.</p> <p>In depth specialist knowledge of one or more specialist areas such as compliance, penetration testing, or incident response.</p>	<p>Application form.</p> <p>Certificates.</p>
<p>Experience</p>	<p>Relevant experience working in Cyber Security.</p> <p>Evidence of Cyber Security or other relevant work outside formal training or employment (voluntary, research, academia, social media etc.)</p> <p>Working with SIEM and Vulnerability scanning solutions.</p> <p>Development of training packages.</p>	<p>Experience of ICT service provision in a health care setting.</p> <p>Experience of working in fields other than Cyber Security.</p> <p>Delivery of training to technical and non-technical staff.</p> <p>Report writing.</p> <p>Procedure development.</p>	<p>Application Form.</p> <p>Interview.</p> <p>References.</p>
<p>Aptitude and Abilities</p>	<p>Ability to provide guidance and support to less experienced team members.</p> <p>Ability to communicate clearly with non-technical staff and end users.</p> <p>Ability to challenge poor behaviour</p>	<p>A broad range of ICT skills and understanding.</p> <p>Ability to speak Welsh.</p>	<p>Application Form.</p> <p>Interview.</p> <p>References.</p>

	<p>Sound judgment, decision making, and organisational skills.</p> <p>Ability to work on own initiative, organise own workload, and deliver projects with minimal support.</p> <p>Work with 3rd parties and suppliers to deliver projects</p> <p>Ability to execute vulnerability scans, and understand and present results.</p> <p>Provide clear reports to senior management.</p> <p>Able to evaluate and assist in selection of best practice security tools</p> <p>Root Cause Analysis of security incidents</p> <p>Good keyboard skills and application use.</p> <p>Enthusiastic, self-motivated, looks for opportunities to improve services, staff and self.</p> <p>Cares about the service and service continuity and is willing to go the extra mile when necessary.</p> <p>Ability to communicate with all levels of the organisation.</p> <p>Ability to embrace the following personal values and behaviours on a daily basis -</p> <ul style="list-style-type: none"> • Dignity, Respect and Fairness • Integrity, Openness and Honesty • Caring, Kindness and Compassion 		
--	---	--	--

	<p>Ability to demonstrate a commitment to our organisational values -</p> <ul style="list-style-type: none"> • Working together to be the best we can be • Striving to develop and deliver excellent services • Putting people at the heart of everything we do 		
Other	<p>Ability to travel between sites in a timely manner</p> <p>Flexible approach to needs of the service.</p>		<p>Application Form.</p> <p>Interview.</p> <p>References.</p>

GENERIC STATEMENTS

COMPETENCE

The post holder is required to participate in the Hywel Dda PDR process and work towards meeting identified development needs. The postholder is required to demonstrate ongoing continuous professional development. At no time should the postholder work outside their defined level of competence. If the postholder has concerns regarding this they should immediately discuss this with their Manager/Supervisor/Consultant. The postholder has the responsibility to inform those supervising their duties if they are not competent to perform a duty.

OUR VALUES

Hywel Dda University Health Board is a values driven organisation. The post holder is expected to uphold our values of dignity, respect, fairness, integrity, honesty, openness and caring, kindness & compassion underpin a behaviour framework which are supported by our organisational values of

- Putting people at the heart of everything we do
- Working together to be the best we can be
- Striving to deliver & develop excellent services

TEAM BRIEF

The post holder is required to actively participate in Hywel Dda Team Briefing in order to aid communication within the Health Board. Managers and supervisors will regularly deliver the Team Brief verbally to their own staff teams by means of a Core Brief and additional departmental information.

RISK MANAGEMENT/HEALTH & SAFETY

The postholder has a responsibility to themselves and others in relation to managing risk, health and safety and will be required to work within the policies and procedures laid down by the Hywel Dda. All staff have a responsibility to access occupational health, other staff support services and/or any relevant others in times of need and advice. The postholder has the responsibility for monitoring the progress on action plans in relation to risk, health and safety. The postholder has the responsibility for the development of risk profiles and a risk register within their area of responsibility. The postholder has the responsibility for developing systems to monitor performance against agreed performance indicators.

HARRASSMENT & BULLYING

The HB condemns all forms of harassment and bullying and is actively seeking to promote a workplace where employees are treated with dignity, respect and without bias. All staff is requested to report any form of harassment and bullying to their line manager or to any Director of the HB.

RECORDS MANAGEMENT

The postholder has the responsibility for timely and accurate record keeping and where appropriate in accordance with professional guidelines. The postholder has the responsibility for the creation and maintenance of records in accordance with Hywel Dda policy and the data protection act.

FLEXIBILITY STATEMENT

The developing and rapidly changing nature of the organisation will require considerable flexibility from the post holder. This job description indicates the main functions and

responsibilities for the post and is not intended to be a fully inclusive list and the duties and responsibilities specified in this job description are subject to change as the needs of the HB evolve. On agreement with the post holder, this job description will be amended, as necessary, in the event of future organisational and professional changes and/or personal development.

CONFIDENTIALITY

All staff may have access to confidential information about patients, staff or health service business. On no account must such information be divulged to anyone who is not authorised to receive it. Confidentiality of information must be preserved at all times whether at or away from work. Any breach of such confidentiality is considered a serious disciplinary offence, which is liable to dismissal and /or prosecution under current statutory legislation (Data Protection Act) and the HB Disciplinary Policy.

EQUAL OPPORTUNITIES

Hywel Dda University Health Board is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff, patients and others reflects their individual needs and that individuals or groups will not face discrimination, harassment or victimisation, or be treated less favourably on the basis of sex, pregnancy and maternity, gender reassignment, disability, race, age, sexual orientation, religion and belief, family circumstances including marriage and civil partnership. To this end, the UHB has an Equality and Diversity Policy and Equality Impact Assessment Policy and Procedure and it is for each employee to contribute to enacting these policies.

OUTSIDE EMPLOYMENT/OUTSIDE INTERESTS

Any other work or outside interests must not conflict with the duties and responsibilities of your attendance for work as an employee of the HB.

ENVIRONMENTAL

The Hywel Dda Health Board is committed to its environmental responsibilities. The Board recognizes that its activities, including energy consumption, waste generation, transportation emissions, water use and resource consumption, have a significant impact on the environment. As an integral part of its commitment to ensure high quality patient care, all staff have a responsibility to adhere to environmental policy and procedure at both an organisational level and within their own area of work to ensure legal compliance. Staff will do their utmost to minimize the environmental impacts of Health Board activities and services, and seek to continually improve operations to minimize their environmental effects. Staff should take note of relevant communications and attend mandatory training when required.

SMOKE FREE POLICY

All Health Board sites and premises and grounds are designated as smoke free areas. This policy applies to all staff, contractors/service providers, patients*, visitors and the public.

***Those patients staying in residential mental health units will be exempt under the Smoke-Free Premises (etc) Wales Regulations 2007.**

SAFEGUARDING ADULTS AND CHILDREN

Every employee of the Health Board, whatever their job, role, profession, status or place of work, paid or voluntary, has a responsibility for Safeguarding both adults and children. Staff must:

- Understand the nature of abuse and how children and adults might be at risk of harm and neglect.
- Understand their own safeguarding responsibilities and what actions they may need to take.
- Know where they can access local policies and procedures in relation to Safeguarding Children and Safeguarding Adults.
- Report allegations or suspicions of abuse to their line manager, including suspicions about a colleague or manager, irrespective of their status, profession or authority. This includes whistle-blowing
- Know how to make a Safeguarding referral to Social Services and/or the Police for both adults and children to report allegations or if they have concerns.
- Know what services, advice and support are available locally to vulnerable children and adults and how to access help needed.

INFECTION CONTROL

"The document Commitment to Purpose: Eliminating Preventable Healthcare Associated Infection: A Framework of actions for healthcare organisations in Wales stipulates that all staff must understand their responsibility and accountability for Infection Prevention & Control and the Health Board must be assured of this on an ongoing basis". IP&C is the personal and individual responsibility of all Health Board staff. All staff have a responsibility to protect and safeguard 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 Infection Prevention & Control Policies and procedures; and best practice guidance in order to maintain high standards of Infection Prevention & control.

GENERAL

The postholder needs to ensure they are familiar with their terms and conditions of service.