

JOB DESCRIPTION

JOB DETAILS

Job Title: Cyber Security Manager

Pay Band: 8a

Directorate: Finance Directorate

Department: Digital Services

ORGANISATIONAL ARRANGEMENTS

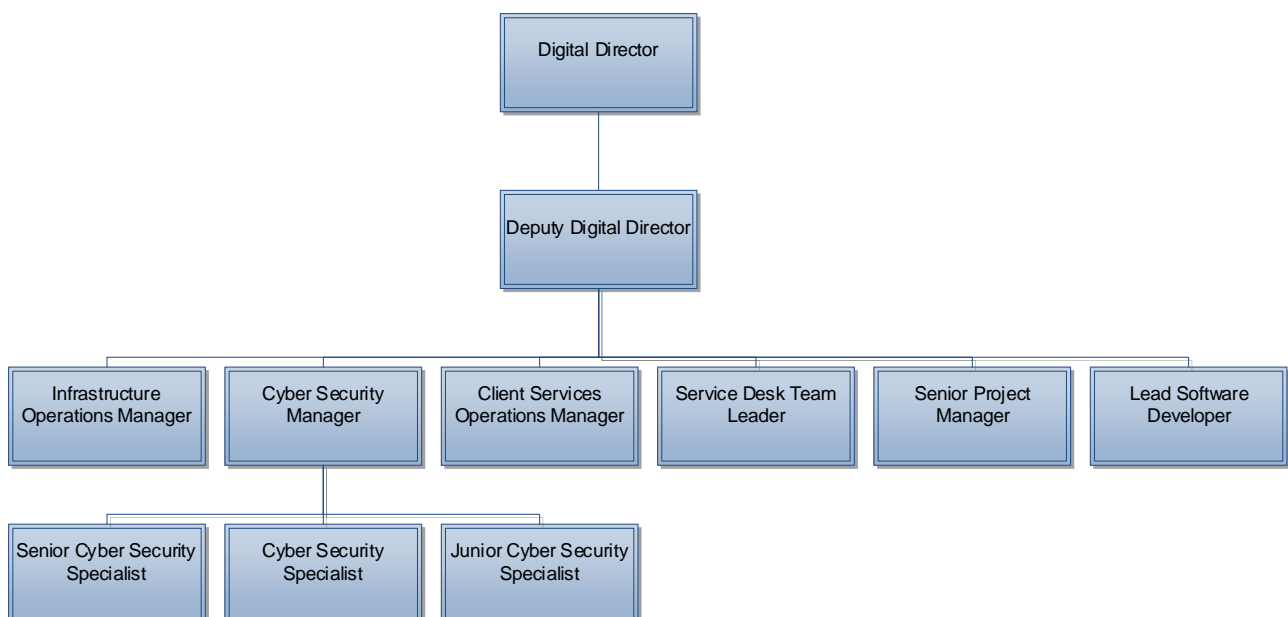
Managerial Accountable to: Deputy Digital Director

Reports to: Deputy Digital Director

Professionally Responsible to: Deputy Digital Director

Responsible For: Cyber Security Team

Organisation chart:



JOB SUMMARY / PURPOSE

The primary responsibility of the Cyber Security Manager is implementing, maintaining, and improving security within both new and existing Health Board Digital systems. This is a critical role within Hywel Dda University Health Board in terms of developing effective Cyber Security strategies, controls, and management of the operational Cyber Security team.

The post is a senior position within the Digital Operations team, supporting the strategic development for Cyber Security services. The post will require travelling across Health board sites, other sites across NHS Wales for national meetings and further for attending supplier briefings and conferences.

The post holder will have acquired a high level of cyber security technical knowledge and understand the relevant Digital Security standards and guidelines such as ISO27001 / Cyber Essentials +.

The post holder will be an advocate for knowledge sharing and collaboration within the team and across the Digital Operations department and undertake Performance Appraisal and Development Reviews (PADRs) for the Cyber Security team, identifying training needs and agreed objectives for the team.

MAIN DUTIES AND RESPONSIBILITIES

1. Service Management

- a. Undertake the creation and maintenance of the Cyber Security strategy to support the overall Digital Services Strategy.
- b. Keep up to date with National Cyber Security Centre advice and ensure guidance is appropriately communicated to the Deputy Digital Director for the potential adoption across the Health Board.
- c. Management and completion of Vulnerability Assessments and Penetration testing working with stakeholders to track remediation of outstanding vulnerabilities.
- d. Work closely with other teams within the Digital Operations team to ensure operational systems are appropriately monitored and protected against Cyber Security threats.
- e. Maintain and manage the Cyber Security risk register ensuring regular review and actions to mitigate are progressed.
- f. Ensure effective provision of an incident response and forensic investigation for Cyber breaches.
- g. Be a member of the NHS Wales security groups as required.
- h. Responsible for cyber security policy implementation across Digital Operations.
- i. Ensure Informatics policies and procedures are implemented within the Cyber Security team, propose changes as appropriate.
- j. Undertake evaluation and redevelop where necessary the procedures within the Cyber Security service area. These redevelopments may impact on all service areas throughout the Health Board.
- k. Keep up to date with legislation in relation to General Data Protection Regulations (GDPR), Caldicott principles, confidentiality, Human Rights Act, Freedom of Information Act, and any other relevant legislation.

2. Service Improvement

- a. Work with all Digital Operations teams to achieve Cyber Essentials + certification for the Health Board.
- b. Ensuring the Health Board is compliant or has an action plan working towards compliance with the Network and Information Systems Direct (NIS-D).
- c. Certify new applications from a cyber-security perspective following the relevant assurance processes.
- d. Propose areas of improvement identified by Key Performance Indicators and Cyber Security risks.
- e. Dissemination and adoption of industry standard security methodologies in line with security good practice.
- f. Identify new services as technology advances to improve cyber security services. Working closely with the Deputy Digital Director to secure funding and procurement.
- g. Occasionally undertake research and development to identify and validate any proposed additional security technologies.
- h. Ensure effective testing processes are undertaken for new hardware and software for Cyber security systems to improve and enhance the service, working closely with the Digital Operations teams.

3. Communications

- a. Be a member of the Cyber Security Information Sharing Partnership (CiSP) forum.
- b. Ensuring cyber security threat intelligence is monitored and appropriate defences are acted upon.
- c. Be a member of the Cymru WARP Group, a public sector Wales Cyber Security liaison group.
- d. Represent the Health Board on All-Wales forums and projects relating to Cyber Security and provide feedback to the senior team and security team on issues and outcomes discussed.
- e. Communicate Cyber Security issues to both Digital Services and other Health Board staff as well as third parties. Agree course of action and provide direction to help resolve issues.
- f. Develop and deliver formal and informal, Cyber Security presentations to groups of staff – both internally and externally providing advice on highly complex Cyber Security matters.
- g. Ensure that all Cyber Security Service developments and improvements are reported and highlighted to Senior Managers within Digital Services.
- h. Chair service team meetings and disseminate information as requested by the Deputy Digital Director.
- i. Develop and maintain a strong working relationship with all members of the Digital department.
- j. Liaise with Clinical and Business Managers, Departmental Managers, Information Asset Owners, and all users of Digital throughout the organisation including external suppliers.
- k. Work closely with suppliers, maintenance contractors and distributors to maintain Cyber Security systems as appropriate through effect supply chain management.
- l. Manage the development and content of the Cyber Security pages on the Health Board Intranet including publication of Key Performance Indicators.
- m. Ensure Cyber Security awareness is embedded in the organisation supported by an effective communication campaign, cyber bulletins, phishing campaigns and incident notifications.

- n. Provide highly specialist advice for anything related to Cyber Security across the Health Board.

4. Finance and Resources

- a. Ensure appropriate maintenance contacts are in place for all Cyber Security systems.
- b. Identify key equipment and hold an accurate up to date list of hardware, firmware, and software revisions. Annually review maintenance contracts and participate in procurement of contracts.
- c. Assist the Deputy Digital Director in the management of budget for Cyber Security services. Ensuring value for money as well as delivery of effective and robust cyber security services.
- d. Ensure technical refresh requirements are submitted to the Deputy Digital Director on an annual basis. All equipment and software must have end of life dates recorded so long-term capital refresh planning can take these into account and ensure timely replacement of equipment and software.
- e. Escalate reliability issues to the Deputy Digital Director.
- f. Ensure all Health Board Cyber Security systems have up to date Systems Operating Procedures (SOPs) and are reviewed regularly.
- g. Advise and manage the development, installation, and commissioning of new Cyber security systems.
- h. Specify Cyber security system requirements for Digital Operations and the wider Health Board Digital services. Advise on national procurements as requested by the Deputy Digital Director.
- i. Responsible for management and safe use of the Health Board's Cyber security systems.

5. Personal and People Development and People Management

- a. Provide professional leadership and support to Digital Operations teams on Cyber related matters.
- b. Manage Cyber Security staff including recruitment, appraisal, development, and task allocation. Construct Job Descriptions, Person specifications.
- c. Ensure Performance Appraisal and Development Reviews (PADRs) for the Cyber Security team are undertaken in line with Health Board timescales, identifying training needs and agreed objectives for the team.
- d. Ensure Cyber Security staff undertake mandatory training in line with Health Board timescales.
- e. Monitor sickness and absence within Cyber Security Staff in line with Health Board policy.
- f. Ensure that scheduled work has correctly allocated resources, is completed within timescale, to agreed quality standards.
- g. Be involved in the appointment of Cyber Security posts.
- h. Responsible for the line management of the Cyber Security team including the management of sickness and absence.
- i. Develop and deliver formal, Cyber Security presentations to groups of staff – both internally and externally.
- j. Ensure Digital staff are trained in the effective use of Cyber Security tools.
- k. Assist Deputy Digital Director in the management of budget for Cyber Security resources. Ensuring services are delivered in budget.

6. Information Processing

- a. Provide and receive highly complex and potentially highly sensitive information in relation to cyber events.
- b. Ensure Information Resources are protected by effective Cyber Security controls in line with relevant NHS strategies and industry standards.
- c. Gather and evaluate complex data from multiple security logs sources both local and national, identify trends in relation to threats, suspicious and malicious activity, and following analysis / options appraisals create prioritised security improvement plans.
- d. Ensure all Cyber security logs are monitored and kept up to date working closely with the Cyber Security and wider Digital Operations teams.
- e. Create regular complex reports and presentations on cyber security matters.
- f. Creation, collation and publication of monthly Key Performance Indicators (KPIs).
- g. Assess the security impact and implications of incidents and events and report as appropriate.
- h. Responsible for the operation of Cyber Security systems across the organisation.

7. Health, Safety and Security

- a. Act within legislation, policies and procedures relating to Information Governance and Cyber Security.
- b. Attend statutory / mandatory training.
- c. Ensures all equipment is tested to ensure correct and safe operation prior to introduction as a live service.
- d. Always guarantees the security and safety of user information and ensures all Health Board employees and equipment complies with relevant policies.

8. Quality

- a. Provide technical advice within the organisation to align with national cyber security strategies where relevant.
- b. Undertake Cyber Security Audits in collaboration with the Welsh Audit Office and Internal Audit.

9. Equality and Diversity

- a. Actively promotes equality of opportunity and diversity across the Cyber Security Team.

10. Effort and Environmental

- a. The role will require travel between different places of work.
- b. Attending local and national meetings.
- c. Requires standard keyboard skills.
- d. Work to achieve agreed team objectives deciding how to achieve these working to cyber security principles and regulations.
- e. The role requires frequent concentration and analysis of systems whilst undertaking fault analysis.
- f. Work pattern will be unpredictable at times whilst dealing with digital incidents and problems affecting critical services.
- g. Concentration required when analysing complex data with likelihood of interruptions to answer queries from staff and other user groups.
- h. Office conditions requiring continuous VDU usage on most days.

11. **General**

- a. Any other duties commensurate with current band and below as determined by the Head of Digital Operations.
- b. Undertake out of hours support as part of a rota providing 24x7 support services.
- c. Keep up to date with legislation in relation to confidentiality, such as data protection, Caldicott principles, Human Rights Act, Freedom of Information Act, NIS-D and GDPR.
- d. Always promote digital services both within the organisation and wider across NHS Wales.
- e. Develop a personal development plan annually as part of the Personal Development Review process.
- f. Keep skills up to date and relevant in order to carry out appropriate tasks in the areas of Client Services.

PERSON SPECIFICATION

ATTRIBUTES	ESSENTIAL	DESIRABLE	METHOD OF ASSESSMENT
<p>Qualifications and Knowledge</p>	<p>Educated to Master's Level in a relevant Digital subject or equivalent experience.</p> <p>Cyber security qualifications (Ethical Hacking, CISSP, CISM) or working towards</p> <p>Detailed working knowledge of application and network security</p> <p>Detailed knowledge of requirements for Cyber Essentials Plus CE+</p> <p>Detailed understanding of the Network Information and Information Systems Directive (NIS-D)</p> <p>Good working knowledge of the BS ISO/IEC 27002 Information Security standard</p>	<p>Management Qualification or equivalent</p> <p>Membership of professional body, e.g. BCS</p> <p>ITIL Foundation qualification</p> <p>A clear understanding and appreciation of the processes supporting clinical care and the approaches required to design and implement the supporting Security environment</p>	<p>Application form</p>
<p>Experience</p>	<p>Detailed experience and knowledge of procurement processes, policies and understanding of Standing Financial Instructions and Digital Procurement policies.</p> <p>Experience of using relevant industry standard Security products and tools.</p> <p>Significant experience at a senior management level within a Digital environment.</p> <p>Track record of achievement at a senior management level.</p>	<p>Experience of dealing with major Digital private sector providers in delivering major security projects and solutions.</p>	<p>Application form and interview.</p>

	<p>Track record of innovation and implementation.</p> <p>Expert knowledge of Root Cause Analysis and Error Management.</p>		
Language Skills		<p>Welsh Speaker (Level 1)</p> <p><i>Full details around the expectations associated with level 1 may be found at the bottom of this page</i></p>	Interview
Aptitude and Abilities	<p>Excellent communication and interpersonal when dealing with highly technical information to a wide range of stakeholders across organisational boundaries.</p> <p>Demonstrably managed and motivated successful technical teams.</p> <p>Ability to quickly understand and apply new technologies.</p> <p>Ability to develop and maintain effective working relationships across multi-functional teams, in particular how to engage with users (technical and non-technical) in defining requirements and implementing solutions.</p> <p>Ability to lead by example and influence others.</p> <p>Ability to motivate, build and promote team working.</p> <p>Able to work under own initiative and manage time/priorities effectively.</p> <p>Sound judgement and</p>	<p>Thorough understanding of Digital and its application to healthcare</p>	Interview

	<p>decision making involving highly complex facts or situations.</p> <p>Excellent technical and organisational skills. Able to manage complex workloads, multi-task in complex and sensitive environments.</p> <p>Good letter, report, and documentation writing skills.</p> <p>Excellent presentation skills.</p> <p>Able to adapt to change and keep up with new technologies using own initiative.</p> <p>Ability to identify and embrace change in the drive towards continuous improvement.</p>		
<p>Values</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 		<p>Interview</p>

Other	<p>Ability to travel between sites in a timely manner.</p> <p>Flexible approach to meet the needs of the service.</p>		Interview
-------	---	--	-----------

Level 1 Welsh

(Please note that for this particular post level 1 in spoken Welsh is desirable but not essential)

Listening/Speaking: Pronounce Welsh words, place names, department names, etc. Greet and understand a greeting. Use basic every day words and phrases, e.g. thank you, please, excuse me, etc. Understand / pass on simple verbal requests of a routine / familiar / predictable kind using simple language, e.g. 'May I speak to...'. State simple requests and follow up with extra questions / requests in a limited way.

Reading/Understanding: Understand simple key words and sentences on familiar / predictable matters relating to own job area, e.g. on signs, in letters.

Writing: Fill in simple forms, note down simple information, e.g. date and venue of a meeting, Welsh address, etc.

GENERIC STATEMENTS

NHS CODE OF CONDUCT FOR MANAGERS

The post holder will be expected to adhere to the standards laid down in the NHS Code of Conduct for Managers and at all times act in a manner that reflects and promotes the values of the HB. The post holder must ensure all activity and service objectives are effectively met in compliance with HBs standing orders and SFIs, scheme of delegated authority and employment legislation.

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 on-going 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.

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.