Job Title: DIS Network Officer

Unit/School: Digital Information Services

Grade: 6A/B

HERA: TBC

Core purpose of role

Responsible for the technical support, administration and development of the University's local communication systems and cloud-based service provisions. Carrying out configuration, pro-active monitoring, maintenance, support and development tasks, as is necessary, to ensure their effective security, operation and availability.

Key responsibilities and contributions

- Acting as a subject matter expert for Cardiff Met's wired and wireless services, telephony, and IT security systems within the network team's area of responsibility. Work within Cardiff Met and with suppliers to evaluate, design and/or conduct architectural reviews and advise on IT technologies, technical requirements, service implications and costs, ensuring IT security best practice is considered throughout each phase.

- Configuring and administering the University's firewalls and Network Access Control system, following best practice and departmental procedures. Managing and supporting IT infrastructure equipment, where necessary working in secure data centre areas, to carry out hardware installations, repairs and upgrades.

- Taking ownership and responsibility for solving complex technical network, telecommunication and cyber security issues, co-ordinating service providers, technical staff and user representatives, where necessary. Analysing and diagnosing faults and implementing robust and innovative solutions to resolve them.

- Providing management and pro-active monitoring for services and systems as directed. Carrying out regular audits of firewall and network logs, identifying and implementing detection and prevention mechanisms. Assisting in scans and penetration tests to identify, remediate and mitigate against vulnerabilities. Ensuring network and firewall patch levels are managed and kept up to date.

- Performing risk analysis to ensure installations, system modifications and maintenance tasks take place to meet approved requirements, standards and time scales whilst maintaining agreed levels of confidentiality, integrity and availability.

- Researching, evaluating and recommending technologies to meet the University's requirements and in line with the corporate IT standards and IT strategy where necessary producing costed proposals and/or reports.

- Undertaking training, attending workshops and online seminar to maintain an up-to-date knowledge of technology trends and developments, including those related to telecommunications and IT security, their application in Higher Education, and the countermeasures to protect against the security challenges they represent.

- Contributing to attaining and maintaining IT security-related accreditations.

- Undertaking IT related projects to meet the University's business requirements, both individually and as part of a team. Planning and co-ordination of system and infrastructure implementations and upgrades and advising on resource requirements and service implications.

- Playing a vital role in the IT Security Incident Response Team and working with other Digital Services and University staff to maintain and test Disaster Recovery and Business Continuity plans.

- Building and maintaining positive individual and team working relationships, both internal and external to Cardiff Met. Liaising with schools, departments and other stakeholders, promoting Digital Services, participating in developments and projects groups. Establishing and evaluating business requirements, as necessary, and providing advice on the network security implications and the technologies to support them. Sharing knowledge and where necessary providing training in new technologies.

- Carrying out other duties related to the provision of University's local servers, communication services and cloud-based service provisions as is directed.

Person specification

Essential qualifications / Professional memberships

- Degree in an IT related subject
  OR
- HND / HNC in an IT related subject AND equivalent professional experience (as outlined below).
  OR
- A professional relevant qualification AND equivalent professional experience (as outlined below).

Essential experience, knowledge and skills

1. Thorough knowledge of wired and wireless network and communications technologies and their application in a corporate environment, including knowledge of network routing protocols and Internet troubleshooting techniques.

2. Excellent knowledge and hands-on experience of working with network infrastructures – such as WANs, LANs, VLANS, Routers/Switches, WLCs and APs.

3. Excellent overall knowledge of IT security and technologies and their application in a corporate network environment.

4. Knowledge of secure IT service provision with awareness of implications of changes and upgrades.

5. Good knowledge and hands-on experience of working with security technologies – such as Firewalls, VPNs, file and session encryption and cryptography methods and web application security.

6. Experience in working with firewalls in a corporate network environment.

7. Considerable experience supporting and designing secure communications infrastructures and/or cloud-based platforms.

8. Experience in planning and co-ordinating technical implementations and support tasks.

9. Logical and systematic approach to troubleshooting with ability to diagnose and resolve complex technical problems and to identify underlying issues and trends.

10. Customer focused with excellent interpersonal skills and able to communicate with students and university staff at various levels.

11. Ability to work under pressure with strong decision making and analytical skills.

12. This is a hybrid role with an expectation of an average of 60% on-site and 40% remote working, along with a need to travel between University sites, depending on demand, and occasional working outside of normal business hours. Attendance of conferences and events across the UK.

Desirable

1. IT Security based qualification such as CISSP or relevant technical accreditation from a supplier such as Cisco or Microsoft.

2. Experience of Cisco networking technologies.

3. Knowledge of Network Access Control solutions.

Welsh skill requirements

Welsh is essential to our students and staff and is a key part of our provision and services. For every position at Cardiff Met, proficiency in Welsh language is either essential or desirable. You can find information about the levels by viewing our booklet: Welsh language skills levels. If a skill is listed as essential in the table below, please ensure you demonstrate this in your online application form.

Language level and general descriptor	Listening	Reading	Speaking	Writing
A1 – Beginner Can understand and use familiar everyday expressions and very basic phrases in Welsh.	Desirable	Desirable	Desirable	Desirable
A2 - Basic user Can deal with simple, straightforward information and communicate in basic Welsh.				
B1 - Intermediate user Can communicate, to a limited level, in Welsh about things that are familiar and/or work related.				
B2 - Upper intermediate user Can express myself in Welsh on a range of topics and understand most of a conversation with a native speaker.				
C1 - Fluent user Can communicate fluently in Welsh.				
C2 - Master user Can communicate fluently on complex and specialist matters in Welsh.				

Disclosure & Barring Service requirements
This post does not require a DBS check.

Supporting information
The University is a dynamic organisation and changes may be required from time to time. This job description and person specification is not intended to be exhaustive.

The University is committed to the highest ethical and professional standards of conduct. Therefore, all employees are expected to have due regard for the impact of their personal behaviour and conduct on the University, students, colleagues, business stakeholders and our community. Each employee must demonstrate adherence to our Code of Professional Conduct. In addition, all employees should have particular regard for their responsibilities under Cardiff Metropolitan University's policies and procedures.