JOB DESCRIPTION

Job Title:	Cyber Security Manager
Campus:	Hendon
Grade:	9
Salary:	Within the range of £51,423 - £59,224 per annum inclusive of OLW
Period:	Permanent - Full time
Reporting to:	CCSS Infrastructure Manager
Supervisory responsibility for:	1 x Analyst Programmer/System Administrator (Cyber Security Team)

Overall Purpose: To oversee the operations of the University's Cyber security solutions and to establish an enterprise security stance through policy, architecture and training processes. Additional tasks will include the selection of appropriate security solutions, and oversight of any vulnerability audits and assessments. The Cyber Security Manager is expected to interface with peers within CCSS and the wider University as well as relevant external agencies to both share the corporate security vision with those individuals and to solicit their involvement in achieving higher levels of enterprise security through information sharing and co-operation.

Principle Duties:

1. To manage varying staff resources and budget assigned to the Cyber Security Team

2. To have oversight of the University's systems and technical architecture (current and proposed), and advise on the suitability of the: design; tools; activities; control measures and processes, required to mitigate known and emerging regulation and cyber security risks. In doing so document risk findings and take a risk based approach to prioritisation of recommendations.

3. Develop and direct implementation of security standards, policies, processes and best practices for the organization.

4. To ensure an effective programme of vulnerability and compliance assessment of IT systems and processes is in place, ensuring that threats to the University's technologies are identified and tracked to remediation or accepted mitigation.

5. Maintain an effective cyber incident management response plan. Coordinate the response to Cyber security incidents and investigations, managing them in a professional manner including computer forensics for evidence gathering and preservation. Ensure appropriate and sensitive handling of affected staff and students and efficient liaison with external and law enforcement agencies when required.

6. To lead the selection, implementation and operation of cyber security services and solutions

7. Retain oversight and monitor the University's network and systems and coordinate regular Cyber Security Reviews within the University and with supplier organisations by conducting assessments of systems, processes and infrastructure and making recommendations to minimize risks identified.

8. To work closely with the CCSS managers, peers within CCSS and the wider University as well as with key contacts within External agencies, to proactively identify and drive policy and process improvements to ensure that University policies and procedures for Cyber Security are effective are adhered to.

9. To provide high quality Cyber Security guidance documentation and training.

10. To lead by example and provide good security guidance and advice on best practice to service managers, staff at all levels and students of the university and partner organisations.

11. To provide high quality guidance and assistance to faculty staff in research projects with challenging information security requirements.

12. To represent the University on Cyber Security matters and liaise with external agencies (E.g. JISC, UCISA, CiSP, SORBS) where required, ensuring that any information requested is provided on a timely and secure basis.

13. To take an active part in University committees and task groups, and to represent the University at external meetings and conferences, and participate in the (virtual) Information Security team spanning CCSS and University staff responsible for DPA, Prevent, and Records Management & Information Security.

14. To keep up to date with Information and Cyber security trends, threats and control measures, to be an active member of the Information security manager communities, particularly those working within HE, JISC, CISP and CESG

15. To maintain high levels of professional conduct, including but not limited to: co-operative engagement in tasks set; the exercising of initiative to suggest, through line managers, improvements to the service provided; and clear and professional styles of communication at all times.

16. To lead and manage cybersecurity projects, ensuring completion to deadlines and within budget. In doing so undertake planning, costing, project management, liaison with suppliers

17. To assist in business continuity preparation and testing by developing and maintaining backup procedures and Disaster Recovery documentation for the security infrastructure to ensure that business requirements are met in a timely manner and to accurately reflect user requirements.

18. To manage other activities that may arise through evolution, growth or restructuring.

19. Such duties appropriate to the grade, as may be directed by the Infrastructure Group Manager or Director of Computing and Communications Systems Service or nominated representative.

20. To maintain a very high level of knowledge in relevant technical and legislative areas, at present this includes: PCI, UK DPA, EU GDPR, U.S. Privacy Shield, Prevent, ISO27001 and similar data and security standards, Network and Routing concepts, Security concepts, Microsoft Authentication and provisioning technologies, Microsoft Windows, MacOS, Encryption Technologies.

21. To maintain a very high level of knowledge of cybersecurity equipment and technologies to enable the evaluation, selection, testing, installation and monitoring of new / enhanced systems. At present this includes VPN, MIS Firewall, Proxies, Anti Virus services, Radius Servers, IDS, Cloud Access Security Brokers (CASB) and User and Entity Behaviour Analytics (UEBA), SIEM, Certificate Renewals, TCP/IP suite of protocols including DNS, Internet, SuperJANET, Microsoft and Unix server operating systems.

Hours: 35.5 hours per week for 52 weeks per year. Overtime will be required from time to time.

Leave: 30 days per annum, plus six extra days taken in conjunction with National Holidays.

Flexibility: Please note that given the need for flexibility in order to meet changing requirements, the duties/ location of this post and the role of the post-holder may be changed after consultation.

PERSON SPECIFICATION

Selection Criteria:

1. Bachelor's or master's degree in computer science, management information systems, business administration, or related discipline or significant equivalent work experience.

2. Certification in information security (CISSP, CSSLP, CCFP, CISM, etc.) or comparable work experience.

3. Excellent communication skills and the ability to work well with people at every level with staff within the University and with external suppliers.

4. Excellent resilience to pressure, requiring the ability to manage competing high priority workloads while fulfilling responsibilities that are significant as the risks of non-compliance are serious, ranging from financial penalties to reputational damage

5. Experience managing cybersecurity projects successfully though their whole lifecycle, including: defining security requirements; business case development; project planning; supervising 3rd party suppliers and internal staff in the implementation of solutions; defining and agreeing operational parameters; retiring services

6. Experience of overseeing 3rd party contractors providing cybersecurity managed services

7. Experience of managing and mentoring technical development staff and co-ordinating activities with internal staff and suppliers.

8. Professional experience of effective cybersecurity management, including
    a. incident management and evidence gathering,
    b. change management and participating in Change and Emergency Change Boards
    c. conducting risk analysis/assessments,
    d. undertaking cyber security reviews
    e. developing and communicating policy changes
    f. providing guidance and advice to end users

9. Experience in assessing an implementing security and risk standards eg ISO 2700X, Cyber Essentials, NIST, ITIL, COBIT, PCI

10. Experience with Microsoft Windows Server 2008/2012 /RedHat Linux/Unix OS

11. Ability to react to high pressure dynamic changing environments

12. Strong problem solving and analytical skills with the ability to create and develop clear policies, standards and procedures

13. Genuine enthusiasm and passion for all things Information and Cyber Security, actively keeping up-to-date with changing trends and emerging threat

14. Knowledge of national and international regulatory compliances and frameworks such as ISO, SOX, BASEL II, EU DPD, HIPAA, and PCI D, Prevent GDPR

15. Proven ability to analyse and recommend pragmatic & practical solutions to complex business and technical problem

16. Willingness to work outside normal hours and travel between University and Service Partner locations.

17. An excellent technical knowledge of cyber security management and approaches derived from in depth experience of this field, and a high level of knowledge of these technologies in a medium sized organisation.

18. In depth understanding of data communications issues, including a reasonable knowledge of communications protocols and available Security hardware and software products.

19. A high level of experience at a technical level of current versions of VPN, MIS Firewall, Policies, ISA Proxy, Outlook Web Access Proxy, Anti Virus software, Radius Servers, IDS, Syslog Service, Certificate Renewals, TCP/IP suite of protocols including DNS, DHCP, Microsoft and Unix operating systems

20. In depth experience of relevant technical and legislative areas, at present this includes: PCI, UK DPA, EU GDPR, U.S. Privacy Shield, Prevent, ISO27001 and similar data and security standards, Network and Routing concepts, Security concepts, Microsoft Authentication and provisioning technologies, Microsoft Windows, MacOS, Encryption Technologies.

21. Exposure and experience of the following:
    - Firewall Management (Boundary, MIS, Device)
    - Cloud Access Security Broker Services
    - Anomaly Detection
    - User and Entity Behaviour Analytics
    - Security Information and Event Management
    - Security policy creation and management

22. Significant proven experience of some of the following: Microsoft Exchange, SQL*Server, Oracle RDBMS, NTP, Certificate Renewals, Office 365 and Azure.

23. Detailed technical knowledge of vulnerabilities, threats, attack methods, and infection vectors (Anatomy of a Hack).

24. A solid foundation in computer networking fundamentals & security control, firewalls, routing and the various threats applicable to the various OSI Networking layers.

25. Demonstrable understanding of application security (web based) and how to protect business services through multiple protection mechanisms (controls).

No Parking at Hendon campus: There are no parking facilities for new staff joining our Hendon campus, except for Blue Badge holders. If you are applying for a post at our Hendon campus please ensure you can commute without a car.

Information on public transport to Hendon can be found here:
http://www.mdx.ac.uk/aboutus/Location/hendon/directions/index.aspx

We offer an interest-free season ticket loan, interest-free motorbike loan, a cycle to work scheme and bicycle and motorbike parking and changing facilities.

Flexible working applications will be considered.

The postholder should actively follow Middlesex University policies and procedures and maintain an awareness and observation of Fire and Health & Safety Regulations.

What Happens Next ?

If you wish to discuss the job in further detail please contact Anita Pearman on (020) 8411 4111.
If selected for interview, you will hear directly from someone in the School/Service, usually within 3 weeks of the closing date.