****

**Professional Services**

**Information Services**

**Cyber Security Operations Manager**

**ZZ007667**

**Information for Candidates**

**THE POST**

Please see the attached job description and person specification.

**TERMS OF APPOINTMENT**

Full-time

Permanent

Salary is in the range £51,799 to £60,022per annum and progress to the top of the scale is by annual increments payable on 1st April each year. Salary is paid into a bank or building society monthly in arrears.

The full-time standard University hours are 37 per week which are normally from 8.30 a.m. to 5.15 p.m. Monday to Thursday and 8.30 a.m. to 4.15 p.m. Friday with one hour and ten minutes for lunch. Specific times may vary according to the Department concerned. If the position is part-time, the hours and days worked will either be as stated in the advert or discussed at interview/appointment. Overtime is not normally payable but time off in lieu may be given.

Annual leave entitlement is 32 working days in a full leave year. If you work less than 37 hours per week, your leave will be calculated on a pro-rata basis. The leave year commences on 1 October and staff starting and leaving during that period accrue leave on a pro-rata basis. In addition, the University is normally closed from Christmas Eve until New Year’s Day inclusive and on bank holidays.

The Appointee will be entitled to join the Local Government Pension Scheme. The scheme's provisions include an index-linked pension with an option to exchange some pension for a lump sum on retirement together with dependants’ benefits. Contributions by the employee are subject to tax relief.

There is a probationary period of six months during which new staff are expected to demonstrate their suitability for the post.

There is a comprehensive sickness and maternity benefits scheme.

**All interview applicants will be required to bring their passport or full birth certificate and any other 'Right to Work' information to interview where it will be copied and verified.** The successful applicant will not be able to start work until their right to work documentation has been verified.

Please note if you are the successful candidate once the verbal offer of employment has been made and accepted, references will be immediately requested. It is the University’s policy that all employment covering the past three years is referenced. A minimum of two references is required to cover this three-year period of employment or study (where there has been no employment). One of your referees must be your current or most recent employer.

The successful candidate will need to bring documentary evidence of their qualifications to Human Resources on taking up their appointment.

If the position has a requirement for Disclosure and Barring Service check (DBS) or Non-Police Personnel Vetting (NPPV), this will be stated in the advert. Further information will be provided once the selection process has been completed.

All applications must be submitted by 23:59 (UK time) on the closing date published.

For information on how to find our campus and the navigation of buildings (including accessibility), please see <https://www.accessable.co.uk/university-of-portsmouth> (click on the Access Guides tab at the top of the page, and then click on "view all access guides".



**UNIVERSITY OF PORTSMOUTH – RECRUITMENT PAPERWORK**

1. **JOB DESCRIPTION**

|  |  |
| --- | --- |
| **Job Title:** | Cyber Security Operations Manager |
| **Grade:** | 9 |
| **Faculty/Centre:** | Professional Services |
| **Department/Service:****Location:** | Information Services St Andrews Court |
| **Position Reference No:** | ZZ007667 |
| **Responsible to:** | Head of Cyber Security |
| **Responsible for:** | Cyber Security Operations Senior AnalystCyber Security Operations Junior Analyst |
| **Effective date of job description:** | June 2022 |

|  |
| --- |
| **Context of Job:** |
| Cyber-attacks are increasing in sophistication, stealth, and destructiveness. The University is re-evaluating its security capabilities in the areas of threat prevention, detection, and response. As part of this strategic approach to cyber security, we are creating a dedicated Cyber Security Team within the university’s Information Services department. |

|  |
| --- |
| **Purpose of Job:**  |
| Under the direction of the Head of Cyber Security in Information Services, the role is responsible for the development, delivery, and enforcement of comprehensive cyber security operations plan. Cyber Security runs through every aspect of the University, and it is essential that all IT services are delivered in a manner that protects the University and in particular, protects all personal and confidential data and information. This role will manage the Cyber Security Operations team who are responsible for carrying out day to day cyber security related duties such as responding to security incidents, reporting threats, vulnerabilities and attacks on the university's systems. They will also liaise with technical specialists within IS, other departments, and with external partners to agree on appropriate operational Cyber Security measures to ensure confidentiality, integrity and availability of university systems and data. The post holder will take the lead and provide a focal point for cyber security and cyber security risk matters in liaison with our Security Operations Centre.The post holder will also be required to advise and offer guidance on existing security arrangements and be actively involved in the specification, design and implementation of new services.The post holder must ensure that they keep up to date with developments in best practise, standards, and technologies within the sector and beyond. |

|  |
| --- |
| **Key Responsibilities:** |
| 1. Support the Head of Cyber Security in developing and maintaining the University’s Cyber Security Strategy, ensuring that it delivers against the University’s strategic aims.
2. Be responsible for the development and management of a robust cyber security operational plan
3. Responsible for the management and successful implementation of Cyber Security Improvement Programme, technical work packages.
4. Support the Head of Cyber Security in the development of the Cyber Security Incident Response Plan and implementation and management the plan.
5. Manage the operational activities in any Cyber Security Incident Response Team (CIRT) and support the incident response and recovery activities.
6. Support and advise your team and senior management with up to date knowledge of technology trends and developments, specifically those related to cyber security, their application in higher education, and the countermeasures to protect against them.
7. Support the development and promotion of a cyber security culture across the institution, raising awareness and increasing the University’s understanding of security through the application of policy and practice. Ensuring that this is articulated in a way that is understandable to a non-technical audience.
8. Line manage, support, challenge and develop the Cyber Security Operations team members.
9. Define and deliver clear and actionable reporting, metrics and dashboards regarding security operations.
10. Follow the IT Governance, Risk and Compliance Framework
11. Manage the activities and relationship of our externally provided Security Operations Centre. Act as a point of escalation for prioritisation and escalation of incidents.
12. Lead on the engagement with auditors or other security-related third parties to address University Cyber Security issues e.g. Janet CSIRT.
13. Be responsible for threat tracking and assessment, and lead on recommending mitigations, remediation or acceptance of cyber security vulnerabilities based on internal and external capabilities, assessments and penetration tests.
14. Attend and actively participate in the IS Security Monthly Review, feed into the risk log and monthly security report.
15. Build and maintain a strong working relationship with vendors and partners.
16. Be responsible for ensuring that stakeholders understand and establish acceptable levels of risk, and recommend activities that will proactively reduce the potential for incidents.
17. To manage budgets associated with cyber security operations and ensure ongoing costs are captured in recurrent budgets. Provide project and operational budget reports as required.
18. Support and advise on cyber security requirements for the development and delivery of new IT services.
 |

|  |
| --- |
| **Working Relationships:** |
|

|  |  |
| --- | --- |
| **Internal** | **External** |
| * Chief Information Officer
* IS Senior Management
* IS Operational Managers
* Service desk
* Project Managers
* Staff at all levels within the university
* Students
 | * Security Operations Centre
* Software, hardware, and service suppliers; including sales and technical support.
* Relevant HE sectors and national security organisations
* ICT staff in other institutions
 |

 |

1. **PERSON SPECIFICATION**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Attributes** | **Rating** | **Source** |
| **1.** | **Specific Knowledge & Experience** |  |  |
|  | IT operations management experience | E  | AF, S |
|  | Demonstrable relevant experience in methods and techniques for risk management, business impact analysis, countermeasures and contingency arrangements. | E  | AF, S |
|  | Experience in the principles, practices, tools and techniques of IT auditing. | E  | AF, S |
|  | Experience in working in a large, challenging multi-site service delivery environment, preferably in HE. | D  | AF, S |
|  | Experience in working with external partners for penetration testing | D  | AF, S |
|  | Demonstrable success in deploying methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements. | E  | AF, S |
|  | Demonstrable experience of working within agreed budget, timescales and resources to deliver successful outcomes. | E  | AF, S |
|  | Knowledge and experience in working with Information Security / Cyber Security frameworks | E  | AF, S |
|  | Practical experience of managing a Cyber Security Team of subject matter experts | E  | AF, S |
|  | Specific technical expertise in key areas including; threat intelligence, incident management and security operations | E  | AF, S |
|  | Knowledge and experience of best-practice forensic investigation in an IT environment | D  | AF, S |
| **2.** | **Skills & Abilities** |  |  |
|  | Shows aptitude for analysing and managing problems arising from incidents in the operation of information systems combined with the ability to provide innovative technical solutions. | E  | AF, S |
|  | Technical investigation skills, the ability to research and collate information from a wide variety of sources into technical reports and recommendations. | E  | AF, S |
|  | Excellent written and verbal communication skills, Able to present to a wide range of audiences ranging in the knowledge of technology, business awareness and seniority | E  | AF, S |
|  | Stakeholder and supplier relationship skills | E  | AF, S |
| **3.**  | **Qualifications, Education & Training** |  |  |
|  | Educated to degree level or equivalent experience  | E  | AF |
|  | Relevant industry qualifications (e.g. CISSP, CISM, ITIL, etc.)  | E  | AF |
|  | Membership of relevant professional bodies  | D  | AF |
| **4.** | **Other Requirements** |  |  |
|  | Handle sensitive and confidential matters, situations, and data; | E  | AF, S |
|  | Remain calm under high pressure/difficult situations. | E  | AF, S |
|  | Credibility and integrity | E  | AF, S |
|  | Positive and open in communication both verbal and written | E  | AF, S |
|  | Initiative and confidence | E  | AF, S |
|  | Analytical in approach to acquiring knowledge and information | E  | AF, S |
|  | Collaborative, able to build working networks | E  | AF, S |
|  | Commitment to service quality whilst adhering to internal procedures. | E  | AF, S |
|  | Desire to undertake further personal development and training. | E  | AF, S |

**Legend**

Rating of attribute: E = Essential; D = Desirable

Source of evidence: AF = Application Form; S = Selection Programme (Including Interview, Test, Presentation)

**JOB HAZARD IDENTIFICATION FORM**

|  |
| --- |
| **Please tick box(s) if any of the below are likely to be encountered in this role. This is in order to identify potential job related hazards and minimise associated health effects as far as possible. Please use the** [**Job Hazard Information**](http://www.port.ac.uk/departments/services/humanresources/recruitmentandselection/informationforrecruiters/essentialinformationandformsforrecruiters/) **document in order to do this.**  |
| 1. International travel/Fieldwork  |  | 13. Substances to which COSHH regulations apply (including microorganisms, animal allergens, wood dust, chemicals, skin sensitizers and irritants, welding fume)  |  |
| 2. Manual Handling (of loads/people)  |  | 14. Working at height |  |
| 3. Human tissue/body fluids (e.g. Healthcare settings, First Aiders, Nursery workers, Laboratory workers) |  | 15. Working with sewage, drains, river or canal water  |  |
| 4. Genetically modified Organisms  |  | 16. Confined spaces |  |
| 5. Noise > 80 DbA  |  | 17. Vibrating tools  |  |
| 6. Night Working (between 2200 hrs and 0600 hrs) | X | 18. Diving |  |
| 7. Display screen equipment | X | 19. Compressed gases |  |
| 8. Repetitive tasks (e.g. pipette use, etc)  |  | 20. Small print/colour coding |  |
| 9. Ionising radiation/non-ionising radiation/lasers/UV radiation  | 21. Soil/bio-aerosols |  |
| 10. Asbestos and/or lead  | 22. Nanomaterials  |
| 11. Driving on University business: mini-bus (over 9 seats), van, bus, forklift truck, drones only)  | 23. Workplace stressors (e.g. workload, relationships, job role, etc.) X |
| 12. Food handling  | 24. Other (please specify) X |

|  |
| --- |
| Some out of hours working may be necessary |

**Completed by Line Manager/Supervisor:**

|  |  |
| --- | --- |
| **Name (block capitals)** | STUART GRAVES |
| **Date** | 10th June 2022 |
| **Extension number** | 2284 |

Managers should use this form and the information contained in it during the induction of new staff to identify any training needs or requirements for referral to Occupational Health (OH).

Should any of this associated information be unavailable please contact OH (Tel: 023 9284 3187) so that appropriate advice can be given.