|  |  |
| --- | --- |
| Last updated: | 20th March 2025 |

**JOB DESCRIPTION**

|  |  |  |  |
| --- | --- | --- | --- |
| Post title: | **Cyber Security Advisor** | | |
| School/Department: | iSolutions (Professional Services) | | |
| Faculty: | Professional Services | | |
| Career Pathway: | Management, Specialist and Administrative (MSA) | Level: | 4 |
| Post reports to: | **Cyber Security Manager- iSolutions** | | |
| Post responsible for: | n/a | | |
| Post base: | Office based- Hybrid working options available | | |

|  |  |  |
| --- | --- | --- |
| Job purpose | | |
| As a member of the Cyber Security team within iSolutions at the University of Southampton, the post holder will take a leading role in securing the Secure Data Research Environment. They will collaborate with colleagues across the university to monitor and analyse security systems, support incident response, and contribute to security measures and initiatives.   * The postholder will also play a lead role in the university’s preparation and maintenance of Cyber Security Accreditations (Cyber Essentials Plus, ISO/IEC 27001), supporting the development of a secure facility for processing sensitive research data (the "Secure Data Research" environment). | | |
| Key accountabilities/primary responsibilities | | % Time |
|  | **Technical and Operational**   * Work with colleagues from the University to Lead efforts for the Secure Data Research Environments Cyber Security accreditations (e.g., Cyber Essentials/Plus, ISO/IEC 27001), coordinating audits, managing documentation, and implementing remedial actions. Prepare leadership reports. * Assist in incident response activities, working alongside senior analysts or incident response teams to investigate security incidents, gather evidence, analyse attack patterns, and document findings. Collaborate with relevant stakeholders in iSolutions and the wider University as required. Create and implement baseline cyber security controls for the Secure Data Research Environment. * Provide support in maintaining security operations by managing and updating security policies and procedures, conducting vulnerability assessments, and implementing security patches and updates. * Maintain accurate documentation of security incidents, investigations, and remediation efforts. Prepare reports and presentations summarizing findings and recommendations for enhancing security measures. Ensure clear and concise documentation for knowledge sharing and audit purposes. * Oversee remediation of risks from security scans and tests, ensuring alignment with risk appetite before production. Conduct risk assessments for on-premise and cloud-hosted solutions, identifying control gaps and residual risks using frameworks (e.g., CIS Top 18, NIST Cyber Security Framework, ISO 27001). * Define scopes for external security testing (e.g., ITHC, Pen Testing) for public cloud and SaaS solutions. Ensure implementation of security architecture principles, designs, and controls. Support the identification and remediation of vulnerabilities and threats using industry tools. * Lead on efforts relating to the Secure Data Research Environments Cyber Security accreditations, including Cyber Essentials/Plus and ISO/IEC 27001. Coordinate internal and external audit efforts with other relevant areas of the business, and manage associated documentation and implementation of any identified remedial actions. Prepare reports as required for review by leadership. * Ensure implementation of security architecture principles, designs, and controls. * Develop security assurance documentation aligned with risk management frameworks. | 65% |
|  | **Programme Delivery**   * To design and implement operational cyber security improvement projects and programmes, throughout their entire lifecycle, in support of the University’s core mission. To work directly with the University community to capture requirements, produce proof of concepts and agree implementation details. To engineer solutions using agreed tools to meet identified requirements. * Ensure that the delivery of the digital transformation initiatives is aligned with University Cyber Security strategy, providing technical security operations input as part of the overall governance process championing Secure by Design principles in projects and platforms and fostering relationships to drive a security focused culture * Provide security expertise for major system procurements and Agile programs within the Secure Data Research Environments. * Oversee development of customer-focused processes and procedures based on industry standards (e.g., ISO 27001:2022, Cyber Essentials). * Perform Cyber Security Maturity Assessments using standards such as CIS Top 18 and NIST Cyber Security Framework. | 20% |
|  | **Expert Advice**   * Stay updated with emerging cybersecurity threats, vulnerabilities, and industry best practices through continuous learning and research. Participate in training programs, conferences, webinars, and obtain relevant certifications to enhance cybersecurity skills and knowledge. * Provide expert guidance on policies, standards, industry regulations, and best practices. Offer consultation on Secure by Design principles and information assurance. Develop IA strategies, policies, and awareness programs. Scope and explain security testing activities and recommend remediation steps. * Identify, analyse, and evaluate information risks across various projects and systems. Communicate the causes, likelihood, and impacts of information risks to stakeholders. * Maintain awareness of evolving cyber security and regulatory landscapes to inform risk management and governance. | 10% |
|  | Any other duties as allocated by the line manager following consultation with the post holder. | 5% |

| Internal and external relationships |
| --- |
| Internal:  The post holder will work closely with:   * Specialists within the Digital Service Delivery team and Information Governance team within the university. * Special Interest Groups that focus on Information Governance and Digital Services Management. * Technical specialists and service delivery teams within iSolutions, including Information Security and Infrastructure teams.   External:  The post holder will liaise with:   * External stakeholders and customers, including NIHR, NHS, NCSC, UCISA, etc. * Relevant suppliers and other external bodies   The post holder will be expected to be aware of the activities and initiatives being formulated globally within the relevant specialist area and will be expected to take part in such activities should they be relevant to, and of benefit to, the work being undertaken locally. |

| Special Requirements |
| --- |
| * Occasional travel to other University sites and supplier offices may be required. * Out of hours work may be required to resolve major incidents. * Due to the nature of Information and Cyber Security, the post holder will be expected to always maintain appropriate levels of confidentiality. |

**PERSON SPECIFICATION**

|  |  |  |
| --- | --- | --- |
| Criteria | Essential | Desirable |
| **Qualifications, knowledge and experience** | Skill level equivalent to achievement of HND, Degree, NVQ4, or relevant information/cyber security experience.  Knowledge of security frameworks such as:   * NCSC Cyber Essentials * ISO/IEC 27000 series   Knowledge of data protection legislation.   * GDPR   Data Protection Act 2018  Experience working with cloud ‘SaaS’ software products and providers.  Experience working with Microsoft Azure/Office 365 (or similar) security technologies, such as:   * Microsoft Defender family * Microsoft Sentinel * Azure MFA * Intune * Cloud App Security * Azure Information Protection * Experience with software vulnerability detection, assessment, and management | Relevant professional certification, e.g., SSCP, CCSP, Security+ |
| **Expected Behaviours** | Able to apply and actively promote equality, diversity, and inclusion principles to the responsibilities of the role.  Demonstrate the Southampton Behaviours and work with colleagues to embed them as a way of working within the team. |  |
| **Management and teamwork** | Able to harness the commitment and contribution of others across the University in building security capability.  Able to provide expert guidance and advice to colleagues across the NIHR-CC to resolve complex problems.  Able to work effectively as part of a team whilst also being able to prioritise and manage own workload. |  |
| **Planning and organising** | Able to prepare and implement a programme of activity over time to pro-actively monitor security in the NIHR-CC.  Able to plan and prioritise a range of one’s own standard and nonstandard work activities and effectively meet deadlines.  Able to plan and manage new projects or significant new activities, ensuring plans complement broader organisational strategy. |  |
| **Problem solving and initiative** | Able to identify broad trends to assess deep-rooted and complex issues.  Able to take ownership for resolving security issues and deciding appropriate solutions.  Able to identify and solve complex problems by applying judgement and initiative to tackle some situations in new ways and by developing improved work methods.  Able to conduct research into new security technologies and present recommendations.  Pro-active and able to work on own initiative |  |
| **Communicating and influencing** | Able to work with stakeholders, advising, influencing, and gaining support for security initiatives.  Able to deal with sensitive information in a highly confidential manner.  Able to communicate specialist technical information clearly and confidently to staff and non-technical stakeholders. |  |
| **Special requirements (of the postholder)** |  |  |

**JOB HAZARD ANALYSIS**

**Is this an office-based post?**

|  |  |
| --- | --- |
| Yes | If this post is an office-based job with routine office hazards (e.g.: use of VDU), no further information needs to be supplied. Do not complete the section below. |
| No | If this post is not office-based or has some hazards other than routine office (e.g.: more than use of VDU) please complete the analysis below.  Hiring managers are asked to complete this section as accurately as possible to ensure the safety of the post-holder. |

## - HR will send a full PEHQ to all applicants for this position. Please note, if full health clearance is required for a role, this will apply to all individuals, including existing members of staff.

|  |  |  |  |
| --- | --- | --- | --- |
| **ENVIRONMENTAL EXPOSURES** | **Occasionally**  (<30% of time) | **Frequently**  (30-60% of time) | **Constantly**  (> 60% of time) |
| Outside work |  |  |  |
| Extremes of temperature (e.g.: fridge/ furnace) |  |  |  |
| ## Potential for exposure to body fluids |  |  |  |
| ## Noise (greater than 80 dba - 8 hrs twa) |  |  |  |
| ## Exposure to hazardous substances (e.g.: solvents, liquids, dust, fumes, biohazards). Specify below: |  |  |  |
| Frequent hand washing |  |  |  |
| Ionising radiation |  |  |  |
| **EQUIPMENT/TOOLS/MACHINES USED** | | | |
| ## Food handling |  |  |  |
| ## Driving university vehicles (e.g.: car/van/LGV/PCV) |  |  |  |
| ## Use of latex gloves (prohibited unless specific clinical necessity) |  |  |  |
| ## Vibrating tools (e.g.: strimmer, hammer drill, lawnmowers) |  |  |  |
| **PHYSICAL ABILITIES** | | | |
| Load manual handling |  |  |  |
| Repetitive crouching/kneeling/stooping |  |  |  |
| Repetitive pulling/pushing |  |  |  |
| Repetitive lifting |  |  |  |
| Standing for prolonged periods |  |  |  |
| Repetitive climbing (i.e.: steps, stools, ladders, stairs) |  |  |  |
| Fine motor grips (e.g.: pipetting) |  |  |  |
| Gross motor grips |  |  |  |
| Repetitive reaching below shoulder height |  |  |  |
| Repetitive reaching at shoulder height |  |  |  |
| Repetitive reaching above shoulder height |  |  |  |
| **PSYCHOSOCIAL ISSUES** | | | |
| Face to face contact with public | x |  |  |
| Lone working |  |  |  |
| ## Shift work/night work/on call duties | x |  |  |