Swansea University
Prifysgol Abertawe

Job Description: Professional Services Leadership Position

Faculty/Directorate/Service Area:	Faculty of Medicine and Life Sciences
Job Title:	Information Security and Compliance Manager
Department/Subject:	Data Science Building
Salary:	Grade 09 £46,735 to £55,755 per annum together with USS pension benefits
Hours of work:	Full time, 35 hours per week
Contract:	Fixed term until 31/03/2028
Location:	This position will be based at the Singleton Campus

Background	The Data Science building hosts several Research Centres of Excellence under one roof that undertake secure linked data analysis. These include the SAIL Databank, the Secure eResearch Platform, and Dementias Platform UK. These centres enable researchers to work together to unleash the potential of large scale data to conduct powerful new research. In addition to our main building we work through outlying centres to utilise a range of data for research within remote secure environments. Ensuring excellence in all elements of our data security is of paramount importance to the department. We need to ensure that we are legally compliant and trusted by data providers. We are looking for an individual who can help us drive and embed good practice within this environment through the development and implementation of policy. The department requires an Information Security and Compliance Manager to ensure that this area is effectively managed, is reflective of the needs of the department and external stakeholders and meets the stipulations of information security recognised standards such as ISO27001, Cyber Essentials and certifications such as the Digital Economy Act (DEA) accreditation. Working to the Head of Legislation and Due Diligence the post holder will take a lead role in all regulatory and compliance maintenance and improvement activities and will be instrumental in delivering an assurance programme across a number of work streams. Interacting with staff at all levels, as well as external organisations and visitors, the post holder will be required to develop and effectively communicate relevant protocols to all users and monitor and review the effectiveness of those systems. In addition, the post holder will help to facilitate professional standards within the building to ensure an effective and professional working environment for all users. The post holder will work jointly with other senior managers to ensure robust systems are developed and deployed to mitigate risks to the organisation. The post holder will be responsible for the security governance framework for the building and associated activities and services and will work closely with technical staff to ensure the very highest

	standards of security are maintained. The post holder will need to have an understanding of the underlying legal principles and an up to date understanding of technical principles of information security.
Main Purpose of Post	1. Produce and update security and other related policies and procedures related to formal certifications (such as ISO27001 and Digital Economy Act Accreditation) and building standard operating procedures (SOPs) 2. Provide induction training and regular security awareness training to all employees and visitors through delivering presentations and leading workshops. Responsible for both designing training materials and assessment of learning. This will be via user feedback and monitoring compliance with policies trained upon. 3. Develop, promote and manage activities to create an information security awareness ethos within the building and at satellite sites. 4. Manage and develop the information security team. 5. Keep up to data with industry developments and changes to relevant laws and codes of practice including the UK DPA 2018, GDPR and appropriate ICO materials working closely with the Head of Legislation and Due Diligence. 6. Perform information security risk assessments and serve as a lead internal auditor for security reviews and primary point of contact for any external reviews or audits 7. Management of compliance in respect of information security policies and procedures 8. Undertake reviews of all system related security plans throughout the departments associated stakeholder networks to ensure compliance and synergy with departmental strategy and plans 9. Monitor compliance with ISO 27001 and any other relevant security certifications 10. Take responsibility for continuous improvement in security and implement audit recommendations through policy. 11. Work alongside technical security colleagues (specifically the Head of Research Infrastructure and Chief Technical Officer) to ensure exemplar level practice is embedded in day to day work. 12. Assist in the delivery of the departments Data, Assets, People, Projects and API – Application Programming Interface and Trust Programmes and to actively promote compliance through transparency and proactive dialogue. 13. Monitor the risk register and incident management reports and flag issue areas and recommend responses 14. Keep updated on the subject area and advise the department on current and future information security technologies and updates 15. Build and lead networks of those involved in risk management and service delivery, to include external suppliers. 16. Provide regular update reports to Centre Directors at management board level and chair the Information Security Committee, Risk Assessment Committee and Audit Committee. 17. Own and manage the Business Continuity Plan 18. Be the responding officer for ALL security related incidents, including leading responses to breaches of SAIL user terms and conditions.

	19. Act as a point of contact for all issues and incidents relating to the physical security of the Data Science Building, including coordination of on-site contractors. 20. Ensure high levels of professional behaviour in the building and work with their line manager to provide assurance to Directors of compliance
General Duties	21. To fully engage with the University's Performance Enabling and Welsh language policies 22. To promote equality and diversity in working practices and to maintain positive working relationships. 23. To lead on the continual improvement of health and safety performance through a good understanding of the risk profile and the development of a positive health and safety culture. 24. Any other duties as agreed by the Faculty / Directorate / Service Area. 25. To ensure that risk management is an integral part of any decision making process, by ensuring compliance with the University's Risk Management Policy
Leadership Values	All Professional Services areas at Swansea University operate to a defined set of Core Values: Professional services values and it is an expectation that everyone is able to demonstrate a commitment to these values from the point of application through to the day to day delivery of their roles. Commitment to our values at Swansea University supports us in promoting equality and valuing diversity to utilise all the talent that we have. In addition you will operate to a defined set of Leadership Values: **We are Professional** We develop ourselves and our teams through continued professional development, and use feedback to improve. We create a culture that delivers successful outcomes through people, supporting, developing and challenging our teams to succeed. We involve our people in developing a vision for the future and in enabling innovation and change, improving University, team and individual performance. **We Work Together** We enable our teams to work together and across functions to deliver successful outcomes that exceed the needs and expectations of our customers. We are responsible for creating environments that demonstrate equality, foster trust, respect and challenge. We are accountable for providing clarity and direction, communicating the "big picture" and harnessing ideas and opportunities to achieve the University's vision. **We care** We create environments that identify, understand and give priority to delivering the needs of the University Community (our students, colleagues, external partners and the public). We motive and inspire our teams to provide the highest standards of personalised care and in doing so uphold the Swansea University brand.
Person Specification	**Essential Criteria:** **Leadership Values:**

1. Demonstrable evidence of creating a culture that delivers successful outcomes through people, developing and challenging teams to succeed and take pride in delivering professional services and solutions.
2. Ability to enable teams to work together and across functions to deliver successful outcomes that exceed the needs and expectations of customers, and in creating environments that demonstrate equality, foster trust, respect and challenge.
3. Demonstrable experience of creating environments that identify, understand and give priority to delivering the needs of the customer, and in motivating and inspiring teams to provide the highest standards of personalised care.

Qualifications

1. Degree in a compliance related discipline, computer science or cyber security or equivalent industry experience

Experience

2. Experience of working in a secure data driven environment
3. Experience in information security management and control
4. Extensive experience of process management and policy work within a compliance-based setting
5. Experience of developing and implementing policies and procedures within complex organisations
6. Experience of leading successful internal audits and managing audit applications to external accrediting bodies
7. Experience of achieving ISO 27001 and similar accreditations such as Cyber Essentials
8. Experience of Project Management

Knowledge and Skills

9. Knowledgeable in security access technologies
10. A broad understanding of information security risks, issues and measures and related legal requirements
11. Ability to demonstrate analysis, planning, research and creative problem-solving skills
12. Ability to transfer knowledge into practical tasks
13. Effective interpersonal, consulting, influencing and negotiation skills
14. Excellent communication and presentation skills and the ability to deliver training to staff
15. Effective writing skills and experience in developing policies, strategies and plans
16. Knowledge of data protection legislation and relevant ICO Codes of Practice
17. Be willing to undergo government security clearance vetting up to DV level.

Desirable Criteria:

18. Ability to communicate in Welsh
19. Certification as CISM, CISA or IRCA Certified Lead Assessor

Welsh Language Level	Level 1 – 'a little' - pronounce Welsh words. Able to answer the phone in Welsh (good morning / afternoon). Able to use very basic every-day words and phrases (thank you, please etc.). Level 1 can be reached by completing a one-hour training course. For more information about the Welsh Language Levels please refer to the Welsh Language Skills Assessment web page, which is available here.
Additional Information	Informal enquiries: Informal enquiries are welcome and should be directed towards: Jon Smart via email at j.h.smart@swansea.ac.uk