University of Essex

RECRUITMENT PACK

This document includes the following information:

- Job Description
- Person Specification
- Additional information

Making an application:

When completing the on-line application form you will be asked to answer questions to help you demonstrate how you meet the requirements of the post. Your answers will be used at the shortlisting and interview stages of the recruitment process. We therefore recommend that you take a copy of this recruitment pack to help with your preparation.

NOTE: You don't have to answer the questions in one attempt, but can save your incomplete application and return to it at another time. You may want to draft your answers using Microsoft Word and then copy your text into the application form. Please be aware that formatting (eg. underline, bold, bulleting) will be lost in this process. If you are using an Apple product you will need to use an alternative web browser to Safari such as Google Chrome.

- Links to Guidance Notes and Frequently Asked Questions can be found on the Search Results page. These pages will open in a new window.
- We recommend that you take a copy of this recruitment pack to help with your preparation.

A commitment to sustaining an inclusive and diverse community is one of the University's Core Values and we are keen to address any imbalances in our workforce.

The University of Essex is proud to be part of the Disability Confident scheme and is committed to supporting diversity and equality, representative of our inclusive community. As part of our commitment to this scheme any candidate who has a disability and meets all the essential criteria for the role will be offered an interview. We also work in partnership with national disability organisation DisabledGo who provide detailed online access guides to many of our campus buildings and facilities which you may find useful.

Please note: We are only accepting on-line applications for this post. However, if you have a disability that makes it difficult for you to provide us with information in this way, please contact the Resourcing Team (01206-874588/873521) for help.

Closing Date: 03 September 2017

Interviews are planned for: 20 September 2017

Produced by:
Resourcing Team
Human Resources
University of Essex
Wivenhoe Park
Colchester CO4 3SQ
United Kingdom
Tel: +44 (0)1206 873521/874588
Email: resourcing@essex.ac.uk

University of Essex

JOB DESCRIPTION – Job ref (REQ00776)

Job Title and Grade:	Cyber Security Specialist Grade 9
Contract:	Full time, permanent
Hours:	A notional minimum of 36 hours per week
Salary:	£39,324 - £46,924 per annum
Department/Section:	IT Services
Responsible to:	Director of IT Services
Reports on a day to day basis to:	Information Assurance Manager
Purpose of job:	The Cyber Security Specialist defines, describes, and implements our security architecture in conjunction with the Assistant Director of IT Services (Infrastructure) and the Network Manager.

Duties of the Post:
The Cyber Security Specialist provides the technical expertise to deal with current and emerging cyber security threats, provides the support, guidance and advice to enable business owners, systems owners and individuals to meet their responsibilities under the Information Security Policy, and influences and informs policy around the safe use of information and information systems.

The Cyber Security Specialist will have a number of key relationships within IT Service, within the wider University, and externally. Within IT services the key relationships are with systems team leaders and IT managers, the Networks Team, the Information Officer and the Cloud Services Specialist. Within the University the key relationships are with Internal Audit, IT managers, system owners, the Head of Security and academics working in the field of cyber security. Beyond the University key relationships are with law enforcement and regulatory bodies, Janet, CSIRT, UCISA, JICS, NCSC and external auditors.

The Cyber Security Specialist will be responsible for any student assistants, interns, work placements or apprentices as required. The postholder will work closely with, and be supported by, the IT Services General Office staff.

As identified in its Information Strategy, the University is a knowledge organisation and handles a huge amount of information and data of various types across its educational, research, and administrative activities. The University must act in accordance with external information legislation and regulation and ensure that its internal policies, procedures, and processes support availability, integrity, and security of the University's information assets.

The Information Assurance Manager leads work on developing a systematic approach to information security including developing policies, procedures, processes, and organisational and individual awareness of the benefits and responsibilities of working with information across its broad membership, and the Cyber Security Specialist will provide the technical expertise and support to put policy into practice.

The Cyber Security Specialist's responsibilities apply to the entire University: all campuses, all parts of the University's organisational structures, and all members.

The post will be responsible for the following:

Strategy, Policy and Planning

1. Advise on and identify the best technological solutions to support information security, and to enable staff to comply with the requirements of the Information Security Policy and related guidelines, and lead on projects to implement those solutions, working with the relevant teams (networks, systems, web).

2. Directly contribute to the support and development of the Information Security Policy.

3. Maintain the balance between security of information and systems and the need for accessibility.

Service Leadership, Delivery and Improvement

4. Provide guidance and make recommendations to relevant teams on the design, implementation and administration on the security aspects of technical services, including:
    - Enterprise class firewalls
    - Network security scanning tools/penetration testing
    - Server firewall configuration
    - Application security assessments
    - Network data encryption protocols and ciphers
    - User- and device-based network access controls and device encryption
    - Intrusion detection systems (IDS) and Intrusion protection systems (IPS)
    - Cloud services
    - Security integration

5. To act as the University's principal liaison with JANET CSIRT (Computer Security Incident Response Team); and create and lead a network of colleagues involved with security across the University, to ensure that our processes are aligned with ITSM best practice.

6. Lead on developing and reviewing arrangements for cyber security incidents, and lead on the management of those incidents, investigating, responding to, recording and remediation, and reporting internally and externally as required.

7. Liaise with the Information Assurance Manager regarding security and incidents relating to personal data or breach of any information legislation, regulation or University Policy to reduce risks and safeguard personal and other restricted data.

8. Manage IT risks, identifying vulnerabilities, including initiating internal and external vulnerability scans and tests, monitoring technical compliance, specifying required updates, and ensuring that the risks related to cyber security are properly documented and addressed through the risk register and associated documentation so that the risk register fully reflects the risk landscape.

9. Monitor emerging vulnerability trends and make recommendations for reducing their impact.

10. Keep abreast of, and understand, developments in security frameworks, including ISO27001, Cyber Essentials and PCI-DSS, identify and implement the controls that apply to the University

11. Work with IT Services teams to introduce and management the deployment of Applocker or similar on staff computers.

Communication and Collaboration

12. Take an active part in the Business Continuity and Emergency Response work of the section, attending relevant training and acting as part of the emergency response team.

13. Embed cyber security in our in our developing information culture, through activities such as building and developing relationships with University academics working in relevant areas to

share best practice, identify emerging trends and opportunities for mutual collaboration and support, and providing information and training for end users in all information security related matters.

14. Identify projects across the University that have, or may have, implications for IT security, and provide the necessary support and guidance for the relevant project managers.

15. Provide reports and service performance information as required.

16. Co-ordinate the communications for all cyber security incidents.

Investigation, Analysis and Research

17. Participate in UK forums, including attendance at relevant events, to keep abreast of developments and ensure that the University is advised about issues and good practice in information and cyber security.

18. Build relationships with key external organisations, nationally and internationally, including relevant law enforcement and regulatory bodies, Janet, JISC, UCISA, and NCSC.

Other

19. Undertake any other such duties as may be assigned from time to time by the Director of IT Services or his/her nominee.

These duties are a guide to the work that the post holder will initially be required to undertake. They may be changed from time to time to meet changing circumstances.

For Academic posts only: **It should be noted that there is a contractual requirement for some members of academic staff to undertake research duties. If this requirement applies to a post it will be clearly stated in the job description, which forms part of the contract of employment.**

Terms of Appointment:
For a full description of the terms of appointment for this post please visit:
http://www.essex.ac.uk/hr/current-staff/terms.aspx#

July 2017

University of Essex

Person Specification

JOB TITLE: Cyber Security Specialist

Qualifications /Training

	Essential	Desirable
▪ CISSP or equivalent.	☒	☐
▪ Degree in a relevant technical discipline or a degree in another combined with substantial additional experience directly relevant to this post.	☒	☐
▪ IT Service Management (ITIL) Foundation or significant experience of working in an ITIL environment.	☐	☒

Experience/Knowledge

	Essential	Desirable
▪ Substantial experience of systems design and administration within a large organisation with complex IT.	☒	☐
▪ Proven track record in improving cyber security through implementing security architecture systems and controls.	☒	☐
▪ Demonstrable experience in understanding and applying security standards, models, accreditations and security management practices, such as PCI-DSS, ISO27001 and Cyber Essentials.	☒	☐
▪ Excellent conceptual knowledge of the major components constituting a modern IT architecture and their interactions with other components.	☒	☐
▪ Knowledge of core networking concepts, such as TCP/IP, subnets and ports, in relation to cyber security.	☒	☐
▪ Proven recent experience in the design, implementation and administration of systems in a large complex environment.	☐	☒
▪ Experience of working with service development and delivery teams across a broad service catalogue.	☐	☒
▪ Experience of providing IT Services within a Higher Education environment.	☐	☒
▪ Experience of a broader set of technologies such as: VMWare NSX; Linux or Windows server management; Webserver configuration and administration (IIS, Apache etc.); User management/authentication systems such as Radius, LDAP & Active Directory.	☐	☒

Skills/Abilities

	Essential	Desirable
▪ Excellent interpersonal and verbal and written communication skills, with the ability to influence others, including senior managers, to explain technological concepts clearly and without jargon, give presentations and write clear and concise reports.	☒	☐
▪ Ability in writing scripts or code to perform monitoring and analysis.	☒	☐
▪ Highly developed analytical skills and problem solving ability, with the ability to lead others in investigating and resolving issues.	☒	☐
▪ Highly effective planning and organisational skills.	☒	☐
▪ Technical investigation skills.	☒	☐
▪ Ability to deliver excellent customer service and to continually improve the customer experience.	☒	☐

University of Essex

Other

	Essential	Desirable
▪ *Ability to meet the requirements of UK 'right to work' legislation.	☒	☐

*The University has a responsibility under the Asylum, Immigration and Nationality Act 2006 to ensure that all employees are eligible to work in the UK. Prior to commencing employment, the successful candidate will be asked to provide documentary evidence to this effect. The University may be able to offer Tier 2 Sponsorship for this role. For further information about UK immigration requirements please follow this link https://www.gov.uk/government/organisations/uk-visas-and-immigration

July 2017

University of Essex

ADDITIONAL INFORMATION

Department

IT Services

You can find more information about the department at the following link http://www.essex.ac.uk/it/

General information

Informal enquiries may be made to Sara Stock, Information Assurance Manager, (telephone: 01206 874853 e-mail: sstock@essex.ac.uk). However, all applications must be made online.

People Supporting Strategy

Please find a link to the People Supporting Strategy.

http://www.essex.ac.uk/hr/policies/docs/people-oct15.pdf

Benefits

Our staff and students are members of the University for life. We believe a person's potential is not simply defined by grades or backgrounds, but by a willingness to question, to collaborate and to push at the edges of knowledge and their own potential.

As an employer we offer a range of benefits and a commitment to career development and equal opportunities in an environment that both reflects and creates a rich interaction of people, disciplines and ideas.

- Pension scheme
- Generous holiday entitlement
- Competitive salaries
- Training and development Family Friendly policies
- On campus childcare facilities, for more information visit www.wivenhoeparkdaynursery.co.uk
- Childcare vouchers
- Relocation package for qualifying staff
- Interest free season ticket loan
- Range of optional salary exchange tax benefits (pension, childcare and bicycle schemes)

No smoking policy

The University has a no smoking policy.