

Head of Cyber Security and Resilience

Job Specification

Date created: January 2025

JOB DESCRIPTION

Employment status: Permanent, full time

Hours: Full time hours at UCEM are 35 per week, Monday to Friday 9.00 a.m. to 5.00 p.m. and this role follows this pattern

Location flexibility: The place of work for this role is **Horizons based**, with the majority of your working week spent at our office in Reading and the rest at your home; the exact split of days/hours is negotiable but must include a minimum of **three** working days per week spent at Horizons (you may work more in the office should you wish)

Please note the following:

- When you work at Horizons you must attend on core office days only
- Core office days are Tuesday, Wednesday, and Thursday
- The building is closed to staff on Fridays
- You can only attend the office on Mondays if you have worked a minimum of three other core days
- Working at home is only possible if your environment meets certain conditions – see the **Attachment** to this Job Specification document – and if not, you need to work at Horizons

Department: Chief Operating Officer

Line manager: Director of Technology

Role summary

The Technology Directorate is responsible for the provision, maintenance, and adoption of all UCEM systems, providing excellent support and customer service to approximately 280 internal staff, 300 remotely based Associate Lecturers, and around 4,000 students in 100+ countries.

As Head of Cyber Security and Resilience, you will take the lead in managing UCEM's cyber security infrastructure, ensuring the establishment of policies, procedures and technology solution in support of our response to the continued cyber threats. You will be responsible for shaping and implementing a Cyber Security and Resilience strategy, as well as leading day-to-day management and operations. You will be committed to ensuring the continuous enhancement of relevant policies and processes, adapting to the changing threat landscape and leading UCEM's response to the ever-increasing cyber security risks.

Job Specification

This is an exciting time for UCEM as we will soon embark on our next 5-year strategy with a focus on Digital transformation. This role will be key to contributing to this endeavour, as well as ensuring the safe and reliable Technology operations as a key member of the Technology leadership team.

Role accountabilities and responsibilities

Strategy formation and implementation

- Design and develop a fit for purpose cyber security and resilience strategy that aligns with institutional priorities contained within the organisations overarching Digital strategy.
- Shape and progress an associated suite of documents (including robust cyber security policies, procedures and standards) that will support the continued roll out of cyber security awareness.
- Design, manage and monitor cyber security KPIs, reporting on progress against set metrics.
- Lead on the audit and renewal of various cyber related certifications and accreditations, ensuring these are maintained and improved upon where possible (e.g. PCI-DSS, Cyber Essentials Plus).
- Spearhead cyber security training and awareness initiatives, working with relevant teams to monitor completion and reach.
- Continuously observe emerging threats, reviewing and adapting strategy where appropriate and necessary.
- Maintain and utilise up to date knowledge of security trends, news and technology through relevant threat intelligence sources (e.g. Jisc CSCIRT, NCSC).
- Provide specialist advisory support to the senior leadership team to inform decision making on all matters relating to cyber security.

Incident management

- Develop and continuously improve incident response protocols, tools, processes and procedures (including incident response and preparedness plans).
- Run regular tests to ensure effectiveness of defences, identifying and improving upon any risk areas.
- Coordinate rapid response to reported cyber security incidents. This includes managing investigations and drafting lesson learnt reports.
- Collaborate with colleagues across UCEM to mitigate and manage security incidents and risks.
- Ensure all systems and services are monitored for their security, availability and resilience. Ensure appropriate controls, audits, alerts, escalations, mitigations and response plans are in-place.
- Contribute to technology resilience and recovery plans as part of UCEM business continuity and disaster recovery planning.

Budget management

- Devise and oversee the cyber security budget to ensure resources meet institutional requirements and needs.
- Manage and maintain strong working relationships with relevant suppliers, ensuring favourable terms in line with the relevant budget spend.
- Consider and implement cyber security solutions that align to the needs and priorities of UCEM.

General

- Cultivate and maintain strong working relationships with peers and colleagues across teams and departments.
- Promote positive associations with technology initiatives through business partnering and stakeholder engagement.
- Contribute to a culture of continuous improvement and support, both in and outside the Technology directorate.
- Where appropriate, deputise for the Director of Technology as part of the Technology leadership team.

Job Specification

Line management responsibility:	NONE. However, it is anticipated that this may become part of this role in the future depending on the cyber strategy.
Budget responsibility:	YES
<u>In this role you will liaise with:</u> Technology Team, Internal staff, Associate Lecturers, Students, 3 rd Party Suppliers and Contractors.	

PERSON SPECIFICATION

Assessment Criteria: A = Application I = Interview T = Test

X denotes both essential and desirable requirements plus how these will be assessed

Qualifications and training	Essential	Desirable	A	I	T
Degree level qualification	X		X		
One or more Cyber qualifications i.e. CISSP, CISA, CISM, CISA, CRISC or relevant experience	X		X		
<i>Please be aware that as part of onboarding processes, we will seek original documentary evidence of the relevant academic and/or professional qualifications which you include within your job application</i>					
Previous experience	Essential	Desirable	A	I	T
Working in a senior cyber operations leadership role where technology is a business-critical service	X		X	X	
Developing and implementing a Cyber Security strategy, roadmaps, associated capabilities and governance across multiple teams/workstreams	X		X	X	X
Defining a cyber incident response plan and leading on incident response	X		X	X	X
Ensuring the achievement and maintenance of security and Cyber certifications i.e. Cyber Essentials Plus, PCI-DSS etc	X		X	X	
Developing and implementing a business continuity and disaster recovery strategy	X		X	X	
Working in Higher Education or Public sector		X	X		
Skills, knowledge, and aptitudes	Essential	Desirable	A	I	T
Understanding of current Cyber security frameworks, standards and best practices e.g. NIST CSF, ISO27001 etc including how these can be mobilised/implemented	X		X	X	X
Knowledge and experience of commissioning and leading assurance activities i.e. Pen Test, security reviews/audit, supplier security reviews etc	X		X	X	

Job Specification

Understanding of technologies used to manage, monitor identity and audit user activity	X		X	X	
Understanding of threat management, vulnerability scanning and threat monitoring tools	X		X	X	
Knowledge of secure configuration, secure by design etc.	X		X	X	
Knowledge of Business continuity and Disaster recovery practices, standards etc.	X		X	X	
Other requirements or special requirements	Essential	Desirable	A	I	T
Alignment to the UCEM core values of Passion, Integrity, Excellence and Support; all employees are expected to demonstrate our values at work: https://www.ucem.ac.uk/core-values/	X			X	
Commitment to delivering positive outcomes for our students; we want our students to be successful	X			X	
You must be prepared to undertake compulsory online training should you be appointed; this includes Data Protection, Health & Safety, Safeguarding, Prevent, EDI, and Anti-bullying, Harassment and Sexual Misconduct	X			X	

PAY & BENEFITS

- Salary range £60,000 to £70,000 per annum (depending on experience).
- 26 days paid holiday (rising to 28 with service) plus paid bank/public holidays plus up to 5 paid closure days (typically between Christmas and New Year); all per holiday year Full Time Equivalent. Our holiday year runs from 1 August to 31 July. We also have a holiday buy and sell scheme in place. Sometimes UCEM does not need to close for 5 days per year and any balance, for example 1 day, can be used as a paid Wellbeing Day to take time out for your own physical or mental health.
- Pensions auto-enrolment to the Universities Superannuation Scheme (this is not a salary exchange/sacrifice scheme). You may opt out.
- Policies in place for all types of family-friendly statutory leave with enhanced pay available from day one of employment (in addition to statutory pay, where applicable).
- Wellbeing support and full access to the Employee Assistance Programme, as well as the Thrive Mental Wellbeing app. Several UCEM employees are trained Mental Health First Aiders and can support staff.
- Cycle to Work and Electric Vehicle salary sacrifice schemes and access to Tax-Free Childcare (Government scheme).
- For Horizons based roles, we may in the future be able to offer parking on site however you must not assume this will be possible. Every now and then we may have a spare parking space become available and you can ask to join the waiting list. UCEM is keen wherever possible, to encourage staff to commute as sustainably as possible.
- Life assurance cover.
- Employer-funded Health Cash Plan (Simplyhealth) and voluntary dental insurance (Unum).
- Charity giving options available including one voluntary paid day, per annum.
- As a UCEM employee you will have access to Microsoft Office 365 applications for personal use. You will also have access to range of lifestyle discounts (savings on everyday purchases) and access to two learning platforms.

On the Join the team page of our website, you will find the full list of employee benefits at UCEM

Job Specification

APPLICATION PROCESS

IMPORTANT! All job applications must be sent to recruitment@ucem.ac.uk and if you apply via a jobs board, please make sure you have sent all required documents otherwise we will be unable to consider your application. In addition, if you apply for this job on the recommendation of an existing UCEM employee, please make sure to mention their name within your application.

To apply for this role, please send the following to recruitment@ucem.ac.uk (you will receive an auto-response):

1. Your up-to-date CV;
2. A covering letter or email message outlining your suitability* for the role; AND
3. A completed **Recruitment Check Form** which is available from the *Current vacancies* page of our website.

The above items constitute a **complete** job application.

*We hope you take time to consider the UCEM values when you prepare your job application. You may also wish to consult our vision and strategy document: <https://www.ucem.ac.uk/our-vision/>

We are committed to driving forward our sustainability agenda to secure a sustainable future and our long-term ambition is to be the world's most sustainable university. We recommend you visit our website to find out more about our **Sustainability Strategy**: <https://www.ucem.ac.uk/sustainability/>

If you are an existing UCEM employee, we request you inform your current line manager of your intention to apply for this role.

NO AGENCIES: We are not using agencies for this vacancy, and we cannot accept any CV submissions. Please do not contact us as we can only repeat this message.

Informal discussion

If you are unsure whether to apply, perhaps because you do not meet all essential criteria, we encourage you to call the hiring manager to discuss this further (details below). If you are excited by this vacancy do not rule yourself out; it still might be worth applying.

For an informal discussion about the role please contact Kevin Wilkinson on 0118 467 2428 or email k.wilkinson@ucem.ac.uk

For all enquiries, please contact HR on 0118 467 2454 / 2433 or email recruitment@ucem.ac.uk

Closing date and next steps

Wednesday 12 February 2025 at noon.

HR will screen all applications in person and all applicants will receive a response confirming the status of their application. We value the time taken to make a job application and the interest shown in UCEM.

Interview details

Dates for interview will be advised to you later in the process.

Please indicate on your Recruitment Check Form any dates that you cannot make, up to 4 weeks from the closing date. This helps us to plan interviews should you be shortlisted, prior to contacting you.

Applications may be reviewed prior to the closing date and occasionally, you may be invited to interview ahead of the closing date.

Interviews are normally carried out over Zoom, Microsoft Teams, and we may invite you to visit our Reading office, especially when this is your place of work.

Job Specification

Please be prepared for a two-stage interview process, held on different dates. As part of the interview process, you will meet with a member of the Senior Leadership Team. Sometimes we may conduct a telephone interview at first or second stage.

Equality, diversity, and inclusion

Here at UCEM we champion equality, diversity, and inclusion in our workforce. We celebrate diversity and the strengths it brings to our staff body, our student community and our Board of Trustees, recognising that people are key to our success. Our aim is to attract, develop and retain a diverse workforce, therefore we welcome and encourage applications from all backgrounds.

Pre-employment checks

UCEM undertakes thorough pre-employment screening as part of its recruitment process. Given we have contracts with Government offices, we make sure our checks comply with the Baseline Personnel Security Standard (BPSS). Checks will include identity, right to work, basic disclosure criminal record check, and three years of employment history.

Job Specification

Attachment – homeworking environment

UCEM is a **flexible employer** and flexibility is built into different places of work location. As such, it is reasonable to ask employees to adhere to some **general principles and ways of working**, in order to make sure flexibility offers value to everyone, including UCEM.

In addition, if all or part of your working week involves working at home, your home environment must meet certain conditions. Otherwise you will be required to work in the office at Horizons.

General principles

- All employees regardless of place of work will be required to take an online Display Screen Equipment (DSE) assessment and repeat this at such intervals as may be instructed by the Facilities Management Team. The purpose of this is to look after your health and safety at work.
- All employees must adhere to UCEM IT Security and Data Protection policies in their place of work.
- All employees will be expected to be accessible to colleagues during their normal working hours and ensure their Outlook Calendars reflect the accurate place of work.
- All line managers will be expected to be accessible to their team and will be responsible for ensuring the performance of their team.

Remote (Home) requirements and conditions

- Where your place of work involves working at home, you must have suitable conditions in which to work.
- As a minimum, your UK home location must be able to accommodate the UCEM technology and equipment. What this means in practice is that you must have sufficient space in which to house the technology and equipment safely and securely.
- In all cases, UCEM technology and equipment can only be handled and used by you, the employee. It must not be accessible to any other household member, at any time.
- When you are working remotely as part of the DSE assessment, you will be required to provide evidence that your working environment meets DSE requirements, such as providing a photo of your workstation setup.
- You must also provide a secure and reliable internet connection which allows you to work as effectively as if you were in Horizons, **including undertaking video and audio calls and connecting permanently to the VPN.**
- In the case of known broadband outage you should plan to work at Horizons or elsewhere – noting that elsewhere must still meet the place of work requirements. Should you be unable to do either of these options, you will be required to take holiday. In the event of unexpected outage, you should discuss with your line manager whether you need to find an alternative place of work or take holiday.
- For the avoidance of doubt, the provision of the required broadband, will be self-funded.
- It is expected that you will house technology and equipment at a suitable work desk, which gives you the space needed to work safely and confidentially. This space in your home must be away from other household users, such as space in a room which is not frequented by other household members.
- Your work environment must remain professional at all times. This means you must be able to work remotely without interruption from household members and noise, and your surroundings should mirror what an office environment would look like (clean/tidy, free of clutter and distractions).
- It is not appropriate to work from a sofa or other location which is not in keeping with presenting a professional work environment. Opting to use the blurring function on Teams/Zoom is not an acceptable workaround.
- If you do not have space to accommodate these requirements or your circumstances change, you are not permitted to work at any location other than Horizons.