University of London
Job Specification

Job Title: IT Security Officer

Department: Information Technology and Digital Service Department (ITDS)

Section: IT Security & Business Continuity

Level: Level 06

Job Purpose:	The role holder will be responsible for supporting the department in identifying, mitigating, responding and reporting on cyber security threats, as part of the IT Security Team. As a member of this team, the role holder will significantly contribute to the IT security of all University staff, students, fellows and contractors, co-ordinating the response to IT security incidents and improving the defence of the University's IT infrastructure and information assets.
Job Content:	

1. Security Incident Detection & Response

The role holder will play a key role in the response to the University's security incidents, ranging in severity from minor abuse or policy infringements, to serious criminal activity and threats to the University's IT infrastructure, services or intellectual properties. This involves the following:

- Assist in the analysis of threat or incident alerts, data and correspondence to assess and categorise the seriousness and impact of security threats and incidents as they emerge on a daily basis.

- As part of the Incident Response Team, they will help co-ordinate the University's response to a security incident or threat by:
    - The effective communication of intelligence between affected institutions, staff, customers or students.
    - Provide technical or policy advice on how to mitigate threats or resolve incidents.
    - Advise on mitigating actions required by other departments or customers, such as network reconfigurations.
    - Undertake technical tests or analysis to measure the effectiveness of any response or mitigating actions.
    - Assist in tracking the threat or incident response from start to finish, ensuring all necessary steps are taken by staff, students or institutions.
    - Escalate Major Incidents within the team and to senior management as necessary.

- Provide incident updates within the team so they can be conveyed to the Senior Leadership/Management Team during Major Incidents.

- Liaise with a variety of security teams inside and outside the University, sharing information and helping to co-ordinate incident response. These national and international CERT teams include JANET CSIRT (JISC), CERT UK and CiSP

- Inform the operational decision to remove, or shutdown, IT services for individuals or institutions as a response to a security incident as appropriate to the situation, balancing the threat posed against the disruption caused by the service removal. Examples include:
  - Disabling user accounts
  - Disconnecting network access for whole institutions.

- Help to determine when to restore IT services post-incident, without compromising University infrastructure or security.

- Determine the cause and mechanism of security incidents, evaluate the potential threat for the University and respond accordingly.

- Inform operational security strategies on how to prevent further incidents of the same type.

- Liaise and help to prepare reports and analysis of incidents for external Agencies e.g. JANET, Police, Security Services.

- Co-ordinate with the ITDS Department & wider University as appropriate, to help create or refine policies and educational material.

2. IT Security Infrastructure & Services Development

- As well as threat and incident response, the role holder is expected to undertake work to implement or develop services that enhance the security of the University's IT infrastructure.

- Recommend new services or changes to existing services, to enhance the University's security posture.

- Contribute to all aspects of the delivery of these new services, including:
  - Identify requirements, products and solutions.
  - Undertake field testing of solutions, write technical reports and evaluations.
  - Liaise with Procurement in obtaining quotes and evaluating competing solutions.

- For new services and infrastructure implemented within the wider University, the role holder will:
  - Assist with evaluating supplier security questionnaire responses.

3. IT Security Intelligence, Risk & Threat Analysis

- The IT security threat landscape evolves on a daily basis and the challenges faced by the University in protecting its assets constantly change. To be

effective, the role holder is expected to be an emerging authority on security threats in the following ways:

- Undertake personal research to stay abreast of current threats, using intelligence gathered from various sources including specialist internet sites, police and government institutions, higher education organisations, researchers, the IT community, conferences and publications.
- Look beyond already established and known threats, apply their own initiative and investigatory work to identify threats and detect incidents previously unknown or unimagined.
- The role-holder must be able to analyse the implications of any intelligence and evaluate how the threats apply to the complicated nature of the University understanding the unique challenges this presents and formulating effective responses.

- In particular, the role holder must specifically stay abreast of the following:
  - Newly identified vulnerabilities .
  - Newly identified attack vectors.
  - Newly identified threat actors, such as criminals or foreign bodies.
  - New security solutions or capabilities.

- The role holder will analyse service logs and data for the pro-active detection of security incidents by technical means, such as custom-written scripts, database searches or activity patterns.

4. IT Security Communications, Education & Community Awareness

- The role holder will constantly engage with the wider University community, usually on a daily basis, as every security incident involves systems, services or data, belonging to an individual or department. Beyond incident response, the engagement takes other forms:

  - Provide technical advice or guidance agreed within the team, on securing IT systems, using email, meetings, presentations or online content.
  - Provide security advice, guidance or help to students and staff, requiring help with a security related incident.
  - Assist with writing news articles or email communications, addressing the whole collegiate University on current IT threats or incidents. These need to be effectively communicated to their target audience, which is not necessarily other IT staff.
  - Write intranet pages to provide advice, technical guides and security information, related to incidents and threats.

- Engage with the community outside the University including:

  - Janet CSIRT
  - CISP
  - Local and national police authorities

5. Pen Testing & Vulnerability Assessment

- The post holder will assist with the proactive Pen Testing of externally facing sites and conducting internal Vulnerability Scans including:
  - Running the tests
  - Assessing the results and taking decisive action.

- Communicating with business owners about these tests.
- Coordinating the remediation of vulnerabilities by liaising with internal developers or external parties.
- Keeping records of activities.
- Contribute towards regular management reporting.

6. To contribute to and actively promote the University's Information Security Policy and sub-policies, including the Acceptable Use Policy.

7. To actively follow and promote the University of London policies, including the University's Dignity at Work and Equal Opportunities Policy and actively promote these wherever possible.

8. To maintain an awareness and observation of fire and health and safety regulations.

9. Any other duties consistent with both the grade and scope of the post.

10. Any other duties reasonably required of the postholder by the reporting manager.

Reports to: **Responsible for:**	IT Security Manager None
Additional demands of the role:	The role may demand out of hours/weekend work and occasional travel outside of central London.

Person Specification

EXPERIENCE & PERSONAL QUALITIES

Essential:

- Experience in a SysAdmin / InfoSec role within an IT service environment.
- Excellent communication skills - Must possess the ability to convey and to present potentially complex information so that it is clear and easily understood, including the ability to design, present and run info-sec training courses.
- Committed to high standards, the post holder must be patient, level-headed and good people person, with the ability to work flexibly, and to persevere and remain effective under pressure.
- Possessing demonstrable initiative and judgment to resolve many problems independently, the post holder must be equally effective when working alone or as part of a team and with the organizational skills to be able to manage multiple tasks in a varied workload.

Desirable:

- Experience of working in Higher Education.

- Experience in resolving significant security or infrastructure incidents.

TECHNICAL KNOWLEDGE & SKILLS

Essential:

- Good Knowledge and experience of security infrastructure, solutions and operations.
- Knowledge and experience of security issues which apply to the following: Microsoft Windows, Macintosh OS X, Linux operating systems, network infrastructure, email services and desktop support.
- Knowledge and experience of essential networking concepts, such as TCP\IP, subnets and ports, as applied to security
- Knowledge and experience of IT security issues and vulnerabilities (e.g. Phishing, Social Engineering, MiTM, DDoS, etc.)
- Ability in writing scripts or code to perform analysis.
- Knowledge of SIEM technologies
- Knowledge of Vulnerability Scanning technologies
- Knowledge of Intrusion Detection technologies
- Able to adapt to changes and keep up with new technologies using their own initiative.

Desirable:

- Knowledge and experience of corporate firewall technologies.
- Knowledge and experience of cloud security technologies.
- Experience of SIEM technologies.
- Experience of Vulnerability Scanning technologies.
- Experience of Intrusion Detection technologies.

EDUCATION & PROFESSIONAL QUALIFICATIONS

Essential:

- Education to a good first-degree standard in a technical discipline, or equivalent experience
- IT Security qualifications (e.g. CompTIA Security+, OSCP, CEH)
- Working towards improving these qualifications.

Desirable:

- MSc in Cyber Security or equivalent.

Competency Requirements	Essential	Desirable
Academic Community focus	B	C
Adapting to change	C	D
Commercial awareness (optional)	B	C
	C	C

Creativity and innovation		
Customer focus	C	D
Interpersonal understanding	C	D
Leadership	B	C
Managing resources	B	C
Organisational commitment	B	C
Proactivity and planning	B	C
Problem solving and decision making	C	D
Performance Management	B	C
Resilience	C	D
Staff development and commitment to learning	B	C
Striving for excellence	B	C
Working collaboratively with others	B	C

Competencies are scored on an A-D scale, with D representing the highest demonstration of the competency.
For further information on each of the competencies and relevant levels, please refer to the University's Competency Model https://london.ac.uk/sites/default/files/governance/UoL-Consolidated-Competency-Model-%28Updated-Oct-2018%29.pdf