Job description
Cyber Security Officer

06/07/2024

Company context

INTO's mission: Transforming international student academic and career success through exceptional university partnerships.

INTO University Partnerships is an independent organisation committed to expanding higher education and career opportunities for students across the globe.

We believe in the power of education to transform lives. We believe that movement of students leads to movement of ideas, which in turn creates better and more successful societies.

We connect students seeking quality international education with leading universities worldwide aspiring to widen their global reach and impact. Achieving the best learning experience and career prospects for students is central to our mission.

Since our inception in 2005, INTO has pioneered innovation in international education and created groundbreaking partnerships with 30 universities in the US, UK and Australia. We have so far helped more than 130,000 students from 190 countries realise their dream of achieving a degree from a world-class university. We also equip students to get a head start in building a career. We do this by offering exceptional academic and employability skills programmes.

We are active in over 120 countries and provide unrivalled personalised service to international students with more than 1,500 experienced staff worldwide and a global network of 2,000 recruitment partners.

Our websites have details of how we are organised and our outstanding achievements so far:

www.intostudy.com   www.intofuture.com   www.intoglobal.com   www.into-giving.com

Reporting line

The role reports to the Global IT Operations Manager

Job purpose

The new role of Cyber Security Officer plays a critical role in establishing and leading a robust cybersecurity strategy across our organisation. This role is designed to safeguard our digital assets, ensure we comply with data protection regulations, and mitigate cybersecurity risks effectively. You'll collaborate closely with IT teams and stakeholders throughout INTO, developing strategic plans, policies, and overseeing security operations to enhance our information security posture.

Key accountabilities and duties

- Strategy and Leadership:
    - Develop and implement the organisation's IT security strategy aligned with business goals.
    - Collaborate with senior management to prioritise security initiatives.
- Risk Management and Compliance:
    - Identify and assess cybersecurity risks, vulnerabilities, and threats.
    - Establish risk mitigation strategies and ensure compliance with relevant standards (e.g., ISO 27001, GDPR).
    - Conduct regular security audits and vulnerability assessments.
- Security Architecture and Infrastructure:
    - Work with IT teams to implement cybersecurity measures, including firewalls, website security, encryption, and intrusion detection systems.
    - Monitor systems for signs of unauthorised activity.
- Incident Response and Threat Intelligence:
    - Develop incident response plans and coordinate security incident investigations.
    - Stay updated with industry trends and advancements to ensure the organisation's security measures are current and effective.
    - Collaborate with external threat intelligence providers.
- Security Awareness and Training:
    - Promote security awareness among staff and educate them on best practices.
    - Conduct training sessions and workshops on security-related topics.
- Vendor Management:
    - Evaluate and manage relationships with security vendors and service providers.
    - Ensure third-party security assessments are conducted for critical vendors.

- Policy and Procedure Development:
    - Create and maintain IT security policies, standards, and procedures.
    - Regularly review and update policies based on industry trends and regulatory changes.

Qualifications and Experience:

- Bachelor's degree in Computer Science, Information Systems, or a related field
- Professional certifications such as CISSP, CISM, or CEH.
- Proven experience (at least 3 years) in IT security.
- Strong knowledge of network security, encryption, authentication, and access controls.
- Familiarity with cloud security (Azure) and mobile device security.

Skills and Competencies:

- Excellent communication and stakeholder management skills.
- Analytical mindset with the ability to assess complex security issues.
- Crisis management and incident response expertise.
- Business acumen and strategic thinking.

The job title does not define or limit your duties and you may be required to carry out other work within your abilities from time to time at our request. We reserve the right to introduce changes in line with technological developments which may impact upon your job duties or methods of working.

Location

- Brighton, UK

Safeguarding

As part of our safeguarding procedures, applicants are asked to note that:

- references will be followed up;
- all gaps in CVs must be explained satisfactorily;
- proof of identity and (where applicable) qualifications will be required;
- reference requests will ask specifically whether there is any reason that they should not be engaged in situations where they have responsibility for, or substantial access to, persons under 18;
- appropriate suitability checks will be required prior to confirmation of appointment.

This role may meet the requirements in respect of exempted questions under the Rehabilitation of Offenders Act 1974. If so, all applicants who are offered employment will be

subject to a Disclosure and Barring Serviced check before the appointment is confirmed. This will include details of cautions, reprimands or final warnings as well as convictions.