Habib University
shaping futures

Job Description

Position Title	Information Security Administrator
Department	Information Technology
Reporting To	Director IT
Type of Position	Full Time

POSITION DESCRIPTION

The position requires an experience and proactive approach to vulnerability, risk, threat, data protection, incident, investigation, audit and compliance management. Continuous improvement in information security processes to ensure the confidentiality, integrity, and availability of university information resources. Oversee and manage contract with SOC service provider, ensuring adherence to SLAs and terms.

DUTIES AND RESPONSIBILITIES

Security Strategy and Implementation:

- ✓ Develop and implement cyber security strategies, policies, and procedures tailored to the university's needs.

Security Infrastructure Management:

- ✓ Deploy, configure, and maintain security systems such as firewalls, intrusion detection/prevention systems, anti-malware solutions, VPNs, and authentication mechanisms.
- ✓ Monitor security infrastructure for vulnerabilities and perform regular security assessments and audits.

Vulnerability Management:

- ✓ Perform and assist in regular vulnerability assessments and penetration testing on university systems and networks.
- ✓ Develop and track remediation plans and work with IT teams to address identified vulnerabilities.

Manage SOC Services Monitoring:

- ✓ Assess SOC service providers based on security needs, performance, and compliance with organizational standards.
- ✓ Oversee and manage contracts with SOC service providers, ensuring adherence to SLAs (Service Level Agreements) and terms.

Incident Response and Investigation:

- ✓ Develop and maintain incident response plans and procedures.
- ✓ Lead incident response efforts during cyber security breaches or incidents.
- ✓ Conduct digital forensics investigations to determine the root cause of security incidents.

Risk Assessment and Mitigation:

- ✓ Identify and assess security risks to university systems and data.
- ✓ Recommend and implement risk mitigation strategies and controls.

Security Monitoring and Threat Intelligence:

- ✓ Monitor security logs and alerts to detect and respond to potential threats.
- ✓ Stay updated on emerging cyber threats and technologies through threat intelligence sources.

Audit and Compliance:

- ✓ Responsible for facilitating IT/IS audits to assess the effectiveness of information technology controls and ensure compliance with regulatory requirements and industry standards.
- ✓ Work closely with internal stakeholders, external auditors, and management to plan, execute, and manage ISO 27001 audits across the institution.
- ✓ Document control processes, ensuring the accuracy and integrity of ISMS documentation, and supporting ISO 27001 compliance efforts.

Security Awareness and Training:

- ✓ Conduct security awareness programs and training sessions for university faculty, staff and students.
- ✓ Promote a culture of cybersecurity awareness across the university community.

REQUIRED JOB SPECIFICATIONS	
Required Qualification	✓ Bachelor's degree in Information Security, Computer Science, Information Technology, or related field. (Relevant certifications and experience may be considered in lieu of degree). ✓ Industry-recognized cyber security certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), CompTIA Security+ or similar is preferable. ✓ Certified ISO 27001 Lead Auditor or similar certification is preferred.
Required Experience	✓ Proven experience (4+ years) in information security operation center roles, with specific experience in incident response, threat detection, and vulnerability management. ✓ Practical proven hands-on experience of deploy, configure, and maintain security systems such as firewalls, intrusion detection/prevention systems, anti-malware solutions, VPNs, and authentication mechanisms. ✓ Strong technical proficiency in networking protocols, security tools (e.g., SIEM, SOAR, IDS/IPS), and operating systems (e.g., Windows, Linux). ✓ Strong knowledge of ISO 27001 standards and experience in implementing and maintaining ISO 27001 certification.

REQUIRED JOB COMPETENCIES (Technical and Soft Skills)		
S#	*Competency*	*Criticality (High / Low / Medium)*
1.	Analytical and problem-solving skills with attention to detail.	Medium
2.	Communication skills and ability to work collaboratively in a diverse environment.	Medium
3.	Hands-on experience with SIEM and SOAR, DLP etc.	High
4.	Hands-on experience with SOC.	High
5.	Vendor Management	Medium