**[CHIEF INFORMATION SECURITY OFFICER](https://www.seek.com.au/job/77564093?ref=search-standalone&type=standout&origin=jobTitle" \l "sol=ebb63fa9b234d28c847ef00b4387e0f72bd3c7e0" \t "_blank)**

**The Organisation**  
ACME is seeking a visionary and inclusive leader who will be committed to promoting and positioning ACME as a student-centric, service-led university.

* **Exciting opportunity within our new Digital and Campus Services team**
* **Full-time, Leadership role**
* **Highly attractive remuneration package**
* **Located at our Footscray Park campus**

**The Opportunity:**

Working within a collaborative leadership team and reporting to the Chief Digital Officer and Executive Director Campus Services, the Chief Information Security Officer (CISO) is a key leadership role within the Digital and Campus Services (DCS) portfolio, providing excellence in leadership, innovation and direction for the Office of the CISO encompassing Campus Security, Business Resilience & Critical Incidents, Cyber Security and Records Management.

You will play a critical role in developing and implementing a comprehensive converged security model and plan for the University to safeguard our sensitive information, systems, and infrastructure. You will lead a team of talented professionals to proactively identify and mitigate security risks, ensure compliance with industry standards and regulatory requirements, foster a culture of security awareness and best practices, and develop opportunities to drive security innovation through external partnerships and alliances to support and enhance ACME’s overall capability.

A full list of the responsibilities or duties can be found in the position description.

**Conditions & Benefits:**

This full-time position will be offered on a 3-year fixed term contract basis. An attractive remuneration package is on offer, including an employer superannuation contribution of up to 17%.

# Interview Script

**Interview Question 1: Developing a Converged Security Model**

**Interviewer:** "Can you describe your experience in developing and implementing a converged security model for an organization?"

**Less Effective Response**

**Interviewee:** "I've worked on security models before, focusing on different areas like cybersecurity and physical security. It's important to cover all aspects."

**More Effective Response**

**Interviewee:** "In my previous role, I led the development of a converged security model that integrated physical, cyber, and information security. This model was crucial for protecting our organization’s diverse assets. We started by conducting a comprehensive risk assessment to identify potential threats and vulnerabilities across all security domains. I then collaborated with key stakeholders to design a unified security framework that included policies, procedures, and technologies tailored to our specific needs. This framework included an integrated security operations center (SOC) that monitored physical and cyber incidents in real-time. The converged model improved our incident response capabilities, reduced redundancies, and ensured a holistic approach to security across the organization."

**Interview Question 2: Leading a Diverse Security Team**

**Interviewer:** "How have you successfully led and developed a diverse team of security professionals?"

**Less Effective Response**

**Interviewee:** "I've managed security teams before. I make sure everyone knows their role and supports them as needed."

**More Effective Response**

**Interviewee:** "Leading a diverse team of security professionals requires understanding their unique skills and experiences and leveraging them effectively. In my previous role, I managed a team that included experts in cybersecurity, physical security, and business continuity. I fostered a culture of collaboration and continuous learning by encouraging cross-training and professional development opportunities. Regular team meetings and workshops were organized to discuss the latest security trends, share knowledge, and address any challenges. I also implemented a mentorship program to help junior staff grow into more senior roles. This approach not only enhanced the team's capabilities but also promoted a positive and inclusive work environment, leading to increased job satisfaction and retention."

**Interview Question 3: Promoting Security Awareness and Best Practices**

**Interviewer:** "What strategies have you employed to foster a culture of security awareness and best practices within an organization?"

**Less Effective Response**

**Interviewee:** "I've conducted security awareness training sessions and shared best practices through emails and newsletters."

**More Effective Response**

**Interviewee:** "To foster a culture of security awareness, I implemented a multi-faceted approach that included regular training sessions, awareness campaigns, and hands-on workshops. We launched a 'Security Champions' program, where employees across different departments volunteered to act as security advocates, promoting best practices and helping to disseminate important security information. Additionally, I developed a monthly newsletter that highlighted recent security incidents, emerging threats, and practical tips for staying secure. We also conducted phishing simulation exercises to test and improve our employees' ability to recognize and respond to phishing attempts. This comprehensive approach not only educated staff on security best practices but also actively engaged them in protecting the organization’s assets."

**Interview Question 4: Ensuring Compliance with Industry Standards and Regulations**

**Interviewer:** "How do you ensure compliance with industry standards and regulatory requirements in your security programs?"

**Less Effective Response**

**Interviewee:** "I make sure our security practices follow the relevant laws and standards. We have audits to check compliance."

**More Effective Response**

**Interviewee:** "Ensuring compliance with industry standards and regulatory requirements is a critical aspect of my role. I start by conducting a thorough review of the applicable regulations, such as GDPR, HIPAA, or ISO 27001, and mapping these requirements to our existing security policies and controls. I established a compliance management framework that includes regular internal audits, risk assessments, and continuous monitoring to ensure adherence to these standards. We also maintain detailed documentation and evidence to support our compliance posture, which is crucial during external audits or regulatory reviews. Additionally, I work closely with legal and compliance teams to stay updated on any changes in regulations and adjust our practices accordingly. This proactive approach helps us mitigate risks and maintain trust with stakeholders."

**Interview Question 5: Building External Partnerships for Security Innovation**

**Interviewer:** "Can you provide an example of how you've developed external partnerships to drive security innovation?"

**Less Effective Response**

**Interviewee:** "I've worked with external vendors and attended conferences to learn about new security technologies."

**More Effective Response**

**Interviewee:** "In my previous role, I actively pursued partnerships with leading technology vendors, academic institutions, and industry consortia to drive security innovation. For example, we collaborated with a university’s cybersecurity research lab to develop advanced threat detection algorithms. This partnership allowed us to leverage cutting-edge research and integrate these innovations into our security operations. Additionally, I participated in industry consortia focused on emerging threats and best practices, which provided valuable insights and facilitated knowledge sharing among peers. We also partnered with technology vendors to pilot new security solutions, such as next-generation firewalls and AI-driven security analytics, before full-scale deployment. These partnerships not only enhanced our security capabilities but also positioned us as leaders in adopting innovative security technologies."

**Interview Question 6: Handling Critical Incidents and Business Resilience**

**Interviewer:** "Can you describe your approach to managing critical incidents and ensuring business resilience?"

**Less Effective Response**

**Interviewee:** "In critical incidents, I follow the incident response plan and make sure everyone knows their roles. We also have backups in place to maintain business operations."

**More Effective Response**

**Interviewee:** "In managing critical incidents, I emphasize a structured and proactive approach. I ensure that our incident response plan is comprehensive and regularly updated, incorporating lessons learned from past incidents. During a critical incident, I coordinate the incident response team to quickly identify, contain, and mitigate the issue, while maintaining clear communication with all stakeholders. To ensure business resilience, we conduct regular business impact analyses and develop robust business continuity plans that include disaster recovery strategies, such as off-site data backups and redundant systems. We also conduct tabletop exercises and full-scale simulations to test these plans, ensuring our readiness to respond effectively to a range of scenarios. This approach helps minimize downtime and maintain operational continuity even during significant disruptions."

**Interview Question 7: Driving Security Innovation**

**Interviewer:** "How have you driven security innovation within an organization, and what were the outcomes?"

**Less Effective Response**

**Interviewee:** "I've introduced new security technologies and tools. It helped improve our security posture."

**More Effective Response**

**Interviewee:** "Driving security innovation involves not only adopting new technologies but also fostering a culture of continuous improvement and creative problem-solving. In my previous role, I launched an internal innovation lab where team members could experiment with emerging technologies, such as machine learning for anomaly detection and blockchain for secure data sharing. We collaborated with external partners, including startups and research institutions, to pilot these technologies. One successful initiative involved developing a machine learning model that significantly improved our ability to detect insider threats by analyzing behavioral patterns. The outcomes included enhanced threat detection capabilities, reduced response times, and increased employee engagement in security initiatives. This innovation mindset positioned our organization as a leader in adopting cutting-edge security solutions."

**Interview Question 8: Collaboration with Academic Institutions and Industry Consortia**

**Interviewer:** "Can you discuss your experience collaborating with academic institutions and industry consortia, and how these collaborations benefited your organization?"

**Less Effective Response**

**Interviewee:** "I've attended conferences and worked with universities on some projects. It was helpful to stay updated on new research."

**More Effective Response**

**Interviewee:** "Collaborating with academic institutions and industry consortia has been a key strategy in advancing our security capabilities. I spearheaded partnerships with leading universities to access cutting-edge research and talent. For example, we partnered with a university's cybersecurity department to research advanced threat detection techniques, which led to the development of proprietary algorithms that enhanced our SOC's efficiency. Additionally, my active participation in industry consortia, such as ISACA and FIRST, allowed us to stay ahead of emerging threats and benchmark our security practices against industry standards. These collaborations provided invaluable insights, facilitated knowledge exchange, and helped us implement innovative security measures that improved our overall security posture and response capabilities."

**Interview Question 9: Navigating Regulatory Compliance in Higher Education**

**Interviewer:** "How have you navigated regulatory compliance challenges specific to the higher education sector?"

**Less Effective Response**

**Interviewee:** "I ensure that our practices align with regulations and work with the legal team to stay compliant. We also have regular audits."

**More Effective Response**

**Interviewee:** "Navigating regulatory compliance in the higher education sector requires a deep understanding of various regulations, such as FERPA, GDPR, and HIPAA, which govern student data privacy and protection. In my role, I developed a comprehensive compliance framework that integrated these regulations into our cybersecurity policies and procedures. I worked closely with the legal and compliance teams to ensure that our data handling practices met all regulatory requirements and conducted regular training sessions for staff and faculty to raise awareness of their responsibilities under these laws. We also implemented a data classification and encryption policy to protect sensitive information. Regular internal audits and external reviews were conducted to ensure ongoing compliance and identify areas for improvement. This proactive approach not only ensured regulatory compliance but also built trust with our students and stakeholders."

**Interview Question 10: Building a Security-First Culture**

**Interviewer:** "How have you built a security-first culture within an organization, particularly in an academic setting?"

**Less Effective Response**

**Interviewee:** "I've held training sessions and sent out security updates to build a security-first culture."

**More Effective Response**

**Interviewee:** "Building a security-first culture in an academic setting involves engaging a diverse community of students, faculty, and staff. I started by integrating cybersecurity education into the university's orientation programs and curricula, ensuring that everyone had a foundational understanding of security best practices. We launched a 'Security Awareness Week' with workshops, seminars, and interactive sessions led by security experts, which included live demonstrations of phishing attacks and data protection strategies. To reinforce this culture, I established a 'Cybersecurity Ambassadors' program where students and faculty could volunteer to promote security awareness in their departments. Additionally, we implemented regular communication campaigns, using newsletters, posters, and social media, to keep the community informed about current threats and how to stay secure. This comprehensive and inclusive approach fostered a culture where security became a shared responsibility, significantly reducing the incidence of security incidents and enhancing the overall resilience of the university."