UNIVERSITY OF CANBERRA

POSITION DESCRIPTION

Position Title:	Head of Cyber Security
Business Unit:	DITM
Appointment Level:	SM0
Reporting To:	CIO
Number of Direct Reports:	6
Delegation Band:	
Position Number:	TBA

THE UNIVERSITY OF CANBERRA

The University of Canberra is a young University anchored in the national capital and works with government, business, and industry to serve our communities and nation. The University of Canberra challenges the status quo; always pursuing better ways to teach, learn, research, and add value – locally and internationally.

Our purpose is to provide education which offers high quality transformative experiences; to engage in research which makes a difference to the world around us; and to contribute to the building of just, prosperous, healthy, and sustainable communities.

The University of Canberra has recently established its long-term ambitions through its new decadal strategy: *Connected*. Through its three objectives (Connected to Canberra, Connected for life and Connected UC), the University of Canberra aims to build sustainable communities through deep collaborations that are locally focused and globally relevant, partner for life with our students to shape our economic, social and cultural futures and deliver an outstanding, digitally connected experience that removes barriers to accessing higher education.

OUR PURPOSE AND VALUES

Our purpose and values are the heart of this university. They describe our core identity: who we are and how we behave at the University of Canberra. They were developed by our people for our people.

GALAMBANY

Together we work to empower, connect and share knowledge with our people, cultures and places

BUSINESS UNIT OVERVIEW

The services provide include:

- Cybersecurity, Projects and Innovation – incorporating the planning, architecture and new capability functions of project management, business analysis and project delivery, cybersecurity management and awareness as well as the development and implementation of a university wide AI capability and innovation.
- Operations – incorporating the vendor management office and audit and compliance services for vendor operations including desktop support, service desk, applications and database management; and the provision of unit business management and support, print and audio-visual functions, registry and switchboard functions.
- The outcomes for the unit include:
- Transformational technical change - technology strategy that is aligned with the student value proposition of a seamless experience and fit for a living, learning, working campus community.
- Innovation - developing an innovation IT culture where technology is situational and innate and aligns technology initiatives with University goals.
- Lead the development of the digital business roadmap to ensure its integration with the University strategic planning process, and the resulting outcomes.
- Act as a champion and change agent in leading the organisational changes required to establish a "spirit of digital" and sustain University digital capabilities.
- Ensure that the University is developing the digital assets and capabilities that are essential to medium and long-term survival.
- Collaborate with the professional units and faculty to develop and exploit new digital business solutions to create a competitive edge for the University.

POSITION PURPOSE

The Head of Cyber Security, reporting to the CIO, provides strategy, leadership and management of all Cyber Security across UC. Drive efficiency and innovation across the University to improve cyber security and response in a cost-effective and efficient manner.

PRIMARY RESPONSIBILITIES

The occupant of this position will be required to:

- Provide leadership and strategic direction as the owner of and responsible for Cyber Security Strategy and annual roadmaps for UC
- Provide leadership and manage the Cyber Security team including performance, professional development, mentorship and supporting a work environment that fosters innovation and collaboration.
- Manage of new cyber security tools, systems and processes.
- Lead change activities across the University to improve the cybersecurity maturity level of the University.
- Translate technical information into effective communications to brief the Executive on how cybersecurity programs align to the University's Strategy and Digital Strategy.
- Manage the organisation's incident response program and coordinate response activities in the event of a security incident.
- Management of the development of objectives, plans and IT strategies for cyber security supporting the strategic direction of the University.
- Responsible for the design, specification, and selection of cyber security systems for the University.

- Apply experience and knowledge of cybersecurity requirements for an enterprise environment, to conduct cybersecurity audits & reviews, according to best practices, relevant frameworks, maturity models and latest threat detection.
- Application of Creative planning and problem-solving skills in the management of complex issues and services with a focus on quality outcomes.
- Build and maintain effective working relationships with vendors and across cybersecurity within the higher education and government sectors.
- Continue to undertake cybersecurity professional development as relevant to ensure skills and knowledge are current.
- Managing cyber security staff that run the day-to-day operations and processes and technologies that include, but are not limited to:
    - Vulnerability management
    - Network detection and response
    - Endpoint detection and response
    - Email security services
    - Micro segmentation
    - Server workload hardening and firewall administration
    - Logging
- Conduct regular research to maintain current knowledge of cybersecurity threats and apply this to increase the University's cybersecurity maturity.
- Undertake duties relevant to the position classification.

KEY CAPABILITIES

Key Capabilities	Descriptors
1. Leadership	1.1 Proactively addresses challenging issues and takes responsibility for seeing issues through. Manage team members to recognise barriers and overcome them. 1.2 Connects the University Strategic Plan with the Portfolio and reinforces connections with other staff. 1.3 Builds and communicates a clear and compelling path for others to choose to be committed and engaged. 1.4 Champions and role models effective change while working to engage and enthuse others to embrace a vision of change.
2. Effective Communication	2.1 Adjusts message and delivery appropriate to audience. 2.2 Listens to others and effectively communicates ideas. 2.3 Produces accurate and effective information in a timely and efficient manner. 2.4 Influences and negotiates persuasively.
3. Collaboration	3.1 Creates opportunities for communities of work colleagues. 3.2 Looks beyond self and immediate team to add value to the whole University. 3.3 Develops relationships with external parties. Seeks and acts on opportunities to connect external parties and partners to the University.
4. Delivers results	4.1 Delivers on agreed outcomes and escalates issues as appropriate. 4.2 Identifies opportunities to improve processes and takes opportunities to problem solve to deliver outcomes.

	4.3 Responds effectively to changing circumstances and prioritises.
5. Business Acumen	5.1 Understands the purpose of own position and how this contributes to the objectives of the University. 5.2 Manages resources effectively. 5.3 Understands the commercial context the University operates in.
6. Service	6.1 Delivers seamless customer focused service underpinned by simplified and efficient processes. 6.2 Understands and anticipates the needs of our students and partners and can convert these into commercial outcomes.
7. Digital Literacy and Innovation	7.1 Demonstrates the ability to work fluently across a range of tools platforms and applications to achieve complex tasks. 7.2 Demonstrates the capacity to adopt and develop new practices with digital technology in different settings; to use digital technologies in developing new ideas, projects, and opportunities. 7.3 Incorporates digital literacy skills into own learning and the learning of others e.g., students, peers, supervisees. 7.4 Appreciates the legal, ethical and security guidelines in the management, access and use of data.

While at work, you must take reasonable care that your actions or omissions do not adversely affect the health and safety of other persons. This includes:

• comply, so far as you are reasonably able, with any reasonable instruction that is given by the University to comply with the WHS Legislation

• cooperate with any reasonable policy or procedure of the University relating to health or safety at the workplace that has been notified to workers

• assume any additional duties as outlined in the WHS Procedure: Resources, Responsibility and Accountability

Note: This position requires a skill level that assumes knowledge or training equivalent to graduate qualifications, or extensive relevant experience, or an equivalent combination of relevant experience and/or education/training.