The University of Waikato
Te Whare Wānanga o Waikato

POSITION DESCRIPTION

Cloud Information Protection Engineer (M365 & Azure)

Reports to:	Associate Director Networks, Security and Assurance
Division:	Information Technology Services
Tenure:	Permanent
Location:	Hamilton Campus
Date:	January 2026

Vision

Ko te tangata

A research-intensive university providing a globally connected, innovative and inclusive studenty experience in an environment characterised by a commitment to diversity, respect for Indigenous knowledge, and high levels of community engagement.

Values

Ko te mana o Te Whare Wānanga o Waikato ka herea ki tō tātou:
- Tū ngātahi me te Māori
- Mahi pono
- Whakanui i ngā huarahi hou
- Whakarewa i te hiringa i te mahara

The University of Waikato places a high value on:
- Partnership with Māori
- Acting with integrity
- Celebrating diversity
- Promoting creativity

1. GENERAL

Our University’s digital vision is “Digital connects us and moves us forward.”

Information Technology Services (ITS) leads digital direction, manages and protects the digital ecosystem, supports digital initiatives and delivers digital services that ensure the University can teach, research and operate successfully in a secure, resilient, connected, sustainable and future-ready digital environment.

ITS is part of the Corporate Services Group within the portfolio of the Chief Operating Officer.

2. POSITION PURPOSE

The Cloud Information Protection Engineer is a key technical role within ITS and is responsible for the design, implementation, operation, and continuous improvement of information protection, data governance, and compliance controls across Microsoft 365 and the Azure ecosystem.

The role has a strong focus on Microsoft Purview capabilities, including records management, retention and disposal policies, sensitivity labels, data loss prevention (DLP), reporting, and audit readiness.

Key responsibilities include:

- Ensuring effective implementation and operational support of Microsoft 365 information protection and governance capabilities.
- Designing and maintaining records management, retention, sensitivity, and DLP policies aligned to legal, regulatory, and institutional requirements.
- Monitoring, maintaining, and improving information protection services to ensure reliability, security, and compliance.
- Working collaboratively with Cybersecurity, Records Management, Privacy, Legal, Risk and business stakeholders to deliver effective information lifecycle management.
- Investigating, recommending, and implementing new Microsoft Purview, M365, and Azure information protection capabilities.
- Creating and maintaining documentation, standards, and operational procedures.

The role will work proactively as part of a small team, in collaboration with the M365 Platform Owner and Records Management staff, to ensure the efficient operation and utilisation of M365 functionality for improved information and records management and business productivity across the University.

3. FUNCTIONAL RELATIONSHIPS

Internal: M365 Platform Owner
ITS teams
Chief Information Officer, Deputy CIO, Associate Directors and ITS managers
Records Management team
Vice Chancellor's office, Pro Vice Chancellor’s and Directors
University staff and students

External: Vendors and strategic partners

4. KEY RESPONSIBILITIES

Information Protection Platform Provision and Support

- Configure and administer information protection functionality, especially within the University’s M365 and Azure environments.
- Provide, or coordinate third-party, Tier-3 support for information protection services.
- Ensure Microsoft 365 and Azure information protection services are monitored to detect and mitigate risks, misconfiguration, or service degradation.
- Maintain platforms in line with Microsoft best practice and supported versioning.
- Maintain accurate configuration records for information protection services.
- Ensure as-built documentation, standards, and knowledgebase information are maintained and available for Tier-1 and Tier-2 support teams.

- Create and maintain standard operating procedures (SOPs) and business-as-usual (BAU) processes.
- Establish dashboards and reporting for information protection and compliance metrics.
- Continuously assess information protection posture and maintain improvement roadmaps.
- Ensure secure operational management practices are followed.
- Ensure changes are managed through ITS change management processes.
- Provide input into licensing, capability planning, and service optimisation.
- Establish and provide regular stakeholder reporting on compliance posture and service health.

Microsoft Purview – Records Management

- Design, implement, and maintain records classification, metadata, and retention schedules.
- Configure and manage retention and disposal policies in alignment with legislative and institutional requirements.
- Ensure defensible and auditable records disposition processes.
- Support audit, regulatory, and assurance activities through evidence collection and reporting.

Data Loss Prevention

- Design and manage sensitivity labels across Microsoft 365 workloads.
- Ensure appropriate protection (encryption, access controls, markings) is applied based on data classification.
- Design, implement, and maintain DLP policies across Microsoft 365 services.
- Monitor DLP alerts and trends to identify risk and improvement opportunities.
- Support user adoption and usability of information protection controls.
- Work with stakeholders to fine-tune policies to balance protection and productivity.
- Promote and implement new Microsoft information protection features as they become available.

Team Contribution

- Engage with the M365 Information and Records Management project team and ITS Cybersecurity and Cloud Infrastructure teams to promote high performance and knowledge sharing.
- Actively participate in project and team operational activities.
- Participate in technical peer review processes to ensure changes are implemented effectively.
- Provide advice, guidance, and problem-solving assistance to other technical staff within and external to the teams.
- Provide technical support to resolve incidents, ensuring timely restoration of services and adherence to established operational and security practices.
- Build and maintain strong collaborative relationships across ITS and with key stakeholders to ensure alignment and shared success.
- Respond to infrastructure service requests and incidents in a timely manner.
- Stay current with developments in Microsoft 365, Azure, and related governance and compliance technologies, ensuring best practices are applied.
- Continuously review new capabilities and lead the adoption and implementation of technologies that enhance security, compliance, and operational efficiency.
- Comply with and undertake responsibilities set out in the University’s Health and Safety Policy.

On-call

- Provide 24 hour on-call support for the University's infrastructure and associated support systems. On-call duty will be rostered amongst the members of the team.
- When rostered on-call to promptly respond to calls and alerts received via the on-call phone, and triage and problem manage critical after-hours incidents through to resolution.

NOTE: Staff have an annual Objectives, Development and Reflection (ODR) meeting with their manager.

5. PERFORMANCE STANDARDS

The Cloud Information Protection Engineer (M365 & Azure) will be performing satisfactorily when:

- Contribution to the project team and wider ITS is positive and supportive, assisting to build a high performing team.
- Solutions are built and supportable in compliance with the University's digital architecture, principles, standards, and solution architecture patterns.
- Information protection and compliance services operate within BAU parameters.
- Service levels are consistently met.
- Procedures (documentation, SOPs, and standards) are maintained and accessible to ensure reliable and professional operation of services.
- Stakeholders are kept informed of service issues and risks.
- Microsoft 365 and Purview capabilities are configured in line with best practice.
- Compliance and audit requirements are met with minimal remediation required.
- Improvement roadmaps are maintained and actively progressed.
- Risks are appropriately identified, documented and managed.
- Positive feedback is received from business and customer stakeholders, and from colleagues.
- IT changes are managed via the change management processes and procedures.
- Knowledge of administrative tasks is shared amongst other team members.
- The ability to recognise critical issues and think strategically is demonstrated consistently and in a broad range of project types (including complex situation assessment/strategy projects/tactical work on system health).
- Proactive support/assistance is routinely provided to the other team members where appropriate.
- Interactions in the course of performing duties are conducted professionally, respectfully and collaboratively.
- Valuable contribution and participation in relevant meetings and/or projects is provided.
- Advice provided complies with professional standards, University policies and procedures and supports the University's strategic objectives.
- Safe and healthy work practices are followed that comply with University policies and procedures, relevant work standards and statutory obligations.

PERSON SPECIFICATION

EDUCATIONAL QUALIFICATIONS

Essential

- A Bachelor’s Degree in Information Technology, Computer Science or similar or maybe equivalently obtained through experience within the industry.
- Microsoft 365, Purview, Security or Azure qualifications or relevant work experience for the scope of the role.

Desirable

- Project Management certification, or relevant work experience in leading small projects or working within a self-managing project team.

SKILLS, KNOWLEDGE and EXPERIENCE

Essential

- At least 3 years’ experience in a senior cloud, Microsoft 365, or information security engineering role.
- Strong technical experience with Microsoft 365 administration.
- Demonstrated experience with Microsoft Purview (records management, retention, sensitivity labels, DLP).
- Understanding of information governance, privacy, and compliance principles.
- Experience working with Azure and identity services.
- Strong documentation and stakeholder communication skills.
- Demonstrated capability to build positive relationships with key stakeholder groups (across the organisation and industry) and ability to leverage these to achieve mutual success.
- An understanding of industry trends and significant influences in ICT, particularly as they relate to tertiary education and business operations.
- Commitment to equal opportunity and to the University’s partnership with Māori as intended by the Treaty of Waitangi. Demonstrated awareness of Māori and Pacific cultures.

Preferred

- Experience working in a tertiary institution, or experience in large enterprise environments
- Experience supporting audit, privacy, or regulatory compliance activities
- Familiarity with data classification frameworks and records management practices
- Knowledge of Private Cloud Infrastructure
- Knowledge of Microsoft Infrastructure technologies and services such as Active Directory, Azure AD, ADFS, Microsoft 365, DHCP, DNS File, Print, Group Policy etc
- Knowledge of Linux Systems
- Ability to apply information and communication technologies to achieve desired outcomes and maintain and update those skills

PERSONAL QUALITIES

- Ability to engage, present and communicate with all levels of staff and key stakeholder
- Collaboration skills and relationship building capability
- High integrity, particularly in handling sensitive information
- Strong commitment to continuous improvement and service excellence
- Flexibility and team player, seeking out and listening to the views and ideas of others
- Self-motivated and independent
- Ability to work independently and with the minimum supervision and equally well in a team/project environment
- Commitment to a culture of openness, flexibility and cooperation
- Commitment to diversity principles and the University’s partnership with Māori as intended by the Treaty of Waitangi.

March 2026