



Position Description

Position Title: Service Support Administrator	Classification: Bond Level 5
Faculty/School/Office: Information Technology Services	Date Position Classified/Updated: August 2026

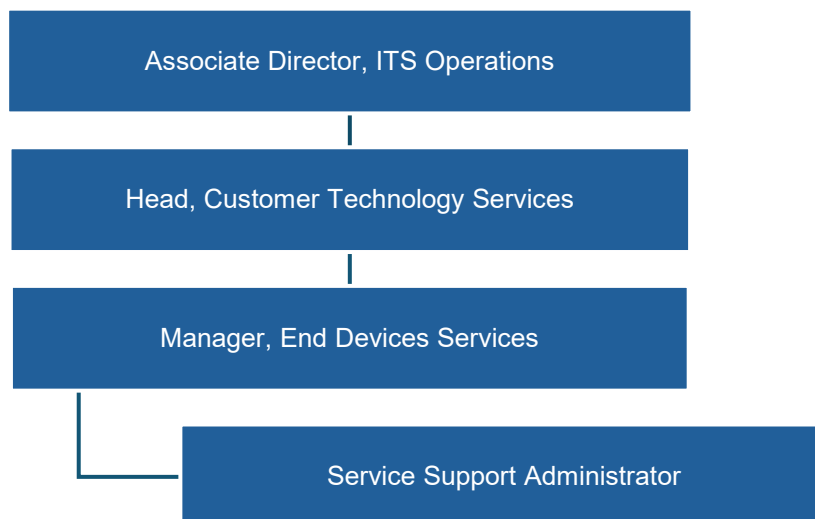
Purpose of the Position:

The Service Support Administrator is responsible for the design, implementation, support, security, and lifecycle management of the University's end user computing environment. The role administers endpoint management platforms including Microsoft Intune, Microsoft Defender for Endpoint, Windows Autopilot, operating system deployment, software deployment, and endpoint security solutions, ensuring secure, reliable, and efficient services for staff and students.

As an administrator within the End Device Services team, the position provides escalated technical support, develops and maintains standard operating environments, implements endpoint security and least-privilege solutions, automates operational processes through scripting and tooling, and contributes specialist expertise to projects and technical architecture activities. The role works collaboratively across the University to improve service delivery, resolve complex technical issues, and ensure end user computing services remain secure, compliant, and aligned with organisational requirements.

Reporting Relationship:

This position reports to Manager, End Devices Services:



Selection Criteria:

- Degree in Information Technology OR an equivalent combination of relevant industry qualifications and practical experience.
- Advanced Windows client operating system and software deployment knowledge and skills.
- Advanced Microsoft Intune knowledge and skills including configuration profiles, compliance policies, application deployment, security policies and troubleshooting techniques.
- In-depth Microsoft Defender for Endpoint knowledge including experience and skills using the Microsoft Defender portal, configuring and operating Microsoft Defender for Endpoint for attack surface reduction rules, security baselines and threat remediation.
- In-depth knowledge of endpoint security controls including anti-malware, application control and least-privilege access management.
- In-depth knowledge of DHCP, DNS and Windows network configuration.
- Experience creating, testing and deploying PowerShell scripts to manage Windows clients, install software, and retrieve data.

Desirable Criteria:

- Demonstrated experience working in a university or higher education environment.
- Relevant Microsoft Certifications and technical expertise in networking, operating systems and end point device management (including macOS, Jamf and iPadOS and Android platforms)
- Knowledge of Film and Television industry software and hardware.

Competency	Responsibility
Customer Service	• Provide responsive, professional and customer-focused support to staff and students for end user computing services. • Communicate clearly with customers regarding incident and request progress, expected timeframes, delays, outcomes and next steps. • Consult with staff, students, academics and ITS teams to understand requirements and provide advice aligned with University standards, approved ICT solutions and ITS processes. • Act as an escalation point for complex end user computing matters while maintaining appropriate customer communication and ownership through to resolution or handover. • Support a positive service experience by setting clear expectations, managing competing priorities and ensuring customers understand the available support options.
Hardware Support	• Install, configure and support approved endpoint hardware, peripherals, printers, multi-function devices and related end user computing equipment. • Maintain operational reliability of end user computing hardware through diagnosis, repair coordination, replacement and preventative maintenance activities. • Relocate, redeploy and reconfigure approved hardware to support staff, teaching, learning and operational requirements. • Provide first-line or escalated support for approved AV and meeting room equipment where aligned with End Device Services responsibilities. • Liaise with vendors and service providers to coordinate warranty repairs, maintenance, replacement and support for approved hardware. • Support approved printers and multi-function devices, including troubleshooting, maintenance coordination and escalation to vendors or internal support teams as required. • Assess and provide recommendations on approved endpoint hardware, peripheral technologies and supportability in alignment with University standards, lifecycle requirements and ITS policies. • Assist the End Device Services team to improve, streamline and automate tasks associated with endpoint hardware lifecycle activities, including refresh, redeployment, retrieval and retirement processes.
Software Support	• Plan, configure, maintain and support endpoint software and operating system deployment services using approved endpoint management platforms and tools.

	• Package, deploy, update and maintain approved application software and operating systems across managed endpoint environments. • Use Microsoft Intune, Windows Autopilot and related deployment technologies to deliver software, operating system builds, updates and configuration changes. • Liaise with software vendors, internal ITS teams and support providers to investigate, resolve and escalate software deployment, compatibility and operational issues. • Develop or support automation, scripting and tooling to improve software deployment, remediation, reporting and operational efficiency. • Identify recurring software, operating system or deployment issues and contribute to remediation through configuration changes, packaging improvements, vendor escalation or documented recommendations. • Ensure software deployment and maintenance activities align with University standards, licensing requirements, security controls and ITS processes.
Recording information and tasks	• Accurately record incidents, service requests, changes, investigations, escalations and resolutions in the IT Service Management system. • Maintain accurate hardware, software, licensing, configuration and lifecycle information in relevant asset management systems, registers and operational records. • Prepare and maintain technical documentation, procedures, knowledge articles, scripts, runbooks and support information for End Device Services activities. • Record, prioritise and track assigned tasks to support timely delivery, appropriate handover and operational visibility. • Maintain sufficient records and supporting evidence to enable troubleshooting, auditability, reporting, compliance and continuous service improvement.
Computer Lab software maintenance	• Prepare, package, test and maintain approved academic and teaching applications for computer labs, teaching spaces and student-facing managed environments in accordance with academic requirements and ITS software evaluation processes. • Coordinate and support timely deployment of academic software to relevant lab and teaching environments using approved endpoint management tools. • Conduct functional testing of academic software against documented teaching requirements, including validation with requesting academics where required. • Maintain suitable testing environments, including virtual machines where appropriate, to validate academic software compatibility, deployment behaviour and student lab readiness. • Support teaching period readiness by ensuring required academic software is assessed, tested and prepared in line with agreed academic and operational timeframes. • Investigate and remediate lab-specific academic software issues, compatibility problems or deployment failures in collaboration with academics, vendors and ITS teams.
Standard Operating Environment Maintenance	• Design, maintain and improve standard operating environments for managed endpoint devices, including Windows builds, configuration baselines, security settings and approved endpoint management policies. • Maintain alignment between SOE requirements and endpoint management configurations, including Microsoft Intune, Windows Autopilot, compliance policies, configuration profiles and deployment profiles. • Ensure SOE configurations incorporate approved endpoint security controls, least-privilege requirements, application control settings and University security standards. • Develop and execute SOE testing, validation and acceptance processes before changes are released to managed endpoint environments. • Review and update SOE components to maintain compatibility with supported operating system versions, hardware models, endpoint platforms and University requirements. • Identify and remediate SOE-related configuration, deployment or baseline issues that affect reliability, security or user experience.

	• Maintain SOE-specific technical documentation, configuration records, testing evidence and release notes to support repeatable deployment and support processes.
Other	• Contribute to Information Technology Services-wide teams, working groups and initiatives as required. • Support projects and initiatives by contributing technical expertise, implementation support, documentation and operational input as required. • Support with other duties as required.
Quality Assurance and Continuous Improvement	• Demonstrate an understanding of, and contributes to, quality assurance and continuous improvement activities relevant to the role. • Perform duties in alignment with the Bond University Strategic Plan, University policies, and established quality assurance and review processes.
Cultural Safety, Inclusion and Respect	• Demonstrate respect for diversity and contributes to a culturally safe, inclusive and discrimination free workplace. • Engage respectfully with staff, students and stakeholders from diverse cultural, linguistic and social backgrounds, including Aboriginal and Torres Strait Islander peoples. • Comply with University policies and applicable anti discrimination and workplace behaviour legislation. • Participate in relevant training or development activities that support cultural safety and inclusive practice.
Work Health and Safety Responsibilities	• Take reasonable care for own health and safety and that of others, in accordance with the Work Health and Safety Act 2011 (Qld). • Comply with University WHS policies, procedures and instructions, including those relating to psychosocial health and safety. • Promptly report hazards, incidents and risks to their manager or through established reporting mechanisms. • Where the role has supervisory or managerial responsibilities, ensure risks are assessed, appropriate controls are implemented, and workers are consulted in accordance with WHS legislation. • Complete mandatory and assigned WHS training. • Comply with return-to-work program requirements following injury/illness.

Note – the successful applicant will be required to produce a certified copy of their highest qualification received prior to commencement of duty.

It is not the intent of this position description to limit the scope of this position in any way but to give an overview of this role at Bond University. You may at times be required to work at other tasks and areas as directed by the Management.