

Position Description

POSITION:	IT Technical Support Specialist – FTC to 30 June 2027.
REPORTS TO:	IT Manager
BLUE KNOT VALUES:	We lead with hope With empathy, compassion and understanding, we advocate for and support people to heal and recover from complex trauma We uphold integrity As individuals and teams, we are accountable, transparent and inclusive; always delivering quality and excellence. We drive change As innovative thought leaders, we build trauma-informed communities to transform the lives of people affected by complex trauma.

ABOUT THE ROLE:

The IT Technical Specialist is responsible for strengthening Blue Knot's internal technical capability and maturing its Microsoft 365 and endpoint environment, with particular focus on Entra ID and Intune. Reporting to the IT Manager and providing day-to-day supervision and technical leadership to the IT Support Analyst, the role provides advanced Level 2 support and Helpdesk oversight while strengthening operational cybersecurity across CrowdStrike, Mimecast and Microsoft 365.

The role holder will drive sustainable opportunities for standardisation, automation, self-service and proactive remediation, while contributing to selected Level 3 technical activities and developing Level 1 capability through coaching and knowledge transfer. Success will be reflected in a more secure, reliable and supportable technology environment, with improvements that are documented, repeatable and organisationally sustainable.

KEY RESPONSIBILITIES

Below is an outline but non-exhaustive list of responsibilities.

1. Microsoft 365, Entra & Endpoint Management

- Administer, troubleshoot and mature Microsoft 365 organisational capability, with particular focus on Entra ID and Intune, including identity and access, SSO, endpoint configuration and compliance.
- Oversee the remote management, configuration, patching and remediation of Blue Knot endpoints, ensuring all devices remain secure, compliant and supportable across a fully remote workforce.
- Develop, implement and maintain Intune policies and capabilities across device configuration, application deployment, compliance, update and patch management rings, and proactive remediation.
- Review and improve user and device lifecycle processes, including provisioning, offboarding, authentication, licensing and application access.
- Use Microsoft administrative tools, PowerShell, logs and telemetry to investigate issues and identify opportunities for secure automation and standardisation.
- Support SharePoint Online and the broader Microsoft 365 environment as required.
- Ensure technical changes are appropriately assessed, tested, validated, documented and implemented in accordance with change management requirements.

2. Cybersecurity & Compliance

- Support and strengthen operational cybersecurity across Blue Knot's fully remote workforce, with CrowdStrike as a key source of endpoint security, vulnerability and security-posture information, supported by Mimecast, Intune, Entra ID and other relevant security platforms.
- Monitor and investigate endpoint, identity, email-security and vulnerability findings, prioritising and coordinating remediation and validating outcomes.
- Identify and implement SaaS security and configuration improvements, using capabilities such as CrowdStrike Falcon Shield to assess security posture, prioritise risks and drive remediation.
- Undertake technical investigation and support response to cybersecurity incidents, including vulnerability management, remediation, escalation and identification of preventative actions.
- Contribute to ongoing improvement of security controls aligned with organisational requirements, including Essential Eight, privacy and least-privilege principles.

3. Advanced IT Support & Helpdesk Oversight

- Oversee day-to-day Helpdesk operations, ensuring incidents and requests are appropriately prioritised, progressed and resolved within agreed service expectations.
- Provide the primary Level 2 escalation point for matters requiring deeper technical investigation, root-cause analysis, complex remediation, configuration or policy change, while supporting Level 1 staff to develop capability through appropriate involvement in more advanced technical activities.
- Apply sound technical judgement within delegated authority escalate matters requiring strategic direction, significant organisational or architectural change, risk acceptance or management approval to the IT Manager.
- Undertake structured root-cause analysis, identifying preventative actions and opportunities to reduce recurring support demand.
- Review Helpdesk and security information to identify trends, service gaps and opportunities for system, process, equipment or training improvements, and providing resulting recommendations with corresponding implementation plans including success measures.
- Coordinate escalation to approved vendors and specialist third parties where required, providing appropriate technical investigation and diagnostic information.

4. Automation, Improvement & Technical Implementation

- Identify and implement opportunities for automation, self-service, proactive remediation and standardisation that reduce repetitive manual IT activity.
- Develop or contribute to PowerShell scripts and other appropriate automation and remediation solutions.
- Support the deployment and integration of new applications and SaaS solutions, considering dependencies, compatibility, security, licensing and operational impacts.
- Analyse operational and technical information and provide recommendations for service and technology improvement.
- Work with the IT Manager to prioritise technical improvements according to organisational benefit, risk and available resources.

5. Technical Leadership & Knowledge Transfer

- Provide day-to-day supervision, technical guidance and coaching to the IT Support Analyst.
- Develop Level 1 capability through structured troubleshooting, technical involvement and knowledge transfer.
- Develop and maintain technical runbooks, SOPs, configuration documentation and knowledge articles.

- Ensure technical solutions and processes are sufficiently documented and transferable to the ongoing IT function.
- Through clear end user centric communication skills, provide technical training and communicate complex technical matters effectively to technical and non-technical stakeholders across the organisation.

6. Teamwork & Service Delivery

- Work collaboratively with the IT Manager, IT Support Analyst, staff, vendors and other stakeholders.
- Proactively develop trusted relationships with Blue Knot staff.
- Maintain clear, timely and professional communication.
- Foster a respectful, supportive and safe working environment.
- Contribute constructively to technical planning, service improvement and broader team discussions.
- Be open to giving and receiving constructive feedback to support personal, team and organisational growth.
- Support broader IT functions during periods of high demand, leave and rostered support requirements.

7. Professional Development

- Participate in team meetings as a mandatory requirement, and staff meetings, as appropriate.
- Attend professional development training to enhance capability and as required.

8. Quality and Safety

- Support the continuous improvement of Blue Knot processes in line with trauma-informed principles, best practice and Blue Knot's purpose, values and Code of Conduct.
- Comply with all relevant policies and procedures.
- Promote a safety and quality culture and follow quality and safety management processes including our Technical Governance Framework, and in support of our Clinical Governance Framework.

QUALIFICATIONS & EXPERIENCE

Essential

- IT qualification (Certificate IV in Information Technology and / or undergraduate degree) or equivalent demonstrated professional experience in alignment with this role's responsibilities.
- Minimum 5 years' relevant professional IT experience, including demonstrated experience in Level 2 technical support, Microsoft 365 administration, endpoint management or a comparable technical role.

- Demonstrated hands-on experience independently administering and troubleshooting Microsoft 365, Entra ID and Intune, including identity and access, endpoint management, compliance, application deployment and remediation at a Level 2 or above.
- Demonstrated ability to independently investigate and remediate complex technical issues, undertake root-cause analysis, interpret system logs and telemetry, and validate successful resolution.
- Experience with PowerShell or equivalent scripting/automation.
- Sound knowledge of cybersecurity principles including endpoint and identity security, MFA, least privilege and vulnerability management.
- Demonstrated ability to produce fit for purpose technical documentation.
- Staff supervision experience that demonstrates provision of technical guidance, coaching and knowledge transfer that has improved both capability of direct reports and overall service performance.
- Strong communication, prioritisation and problem-solving skills.

Highly Desirable

- Relevant Microsoft certification, particularly MD-102, SC-300 or equivalent.
- Experience with CrowdStrike Falcon and/or Mimecast.
- Experience with SharePoint Online, endpoint automation, proactive remediation and employee self-service.
- Experience supporting a fully remote workforce and/or operating within an Essential Eight-aligned environment.

COMPETENCY SUCCESS MEASURES

Technical Capability: Independently investigates and resolves complex issues using structured analysis, sound technical judgement and validated solutions in line with organisation protocols and decision-making authority.

Microsoft Platform Maturity: Improves the consistency, security, automation and supportability of Microsoft 365, Entra and Intune.

Cybersecurity & Prevention: Strengthens operational cybersecurity and identifies underlying causes and preventative actions that reduce risk and recurrence.

Service Improvement: Uses Helpdesk and technical information to identify trends and implement practical improvements, automation, self-service and remediation.

Technical Leadership: Provide day-to-day supervision, technical guidance and coaching to the IT Support Analyst, supporting high quality and consistency of Helpdesk service delivery.

Knowledge & Sustainability: Ensures technical solutions and processes are appropriately documented, repeatable, transferable and supportable by the ongoing IT function.

AVAILABILITY & OTHER REQUIREMENTS

- This is a full-time, home-based position working 38 hours per week and operating nationally.
- Participate in rostered weekend and public holiday IT support alongside other members of the IT team and work flexibly where reasonably required.
- Maintain required National Police Check/Criminal History Check and Working with Children Check clearances.
- Maintain a safe and WH&S-compliant home office and reliable internet connection suitable for the role.
- Occasional travel or work from other Australian locations may be required.

Job Demands Checklist (Pre-Employment)

Job Title

IT Technical Support Specialist

Purpose

This checklist outlines the inherent requirements and key demands of the above job role.

This document will be required to be reviewed by candidates at time of commencing recruitment.

The [Candidate Completion Section](#) is to be completed by the applicable candidate at time of offer to confirm awareness of the role demands and to clarify any reasonable adjustments that may be required to support fulfillment.

This information is not used to exclude candidates, but to support transparency and safety. It will be considered alongside reasonable adjustment obligations.

It may also be used to provide information about the position to a health professional for the purpose of conducting a pre-employment medical, or to support a return-to-work program following a workplace incident, injury, or other relevant governance protocol.

Candidate Instruction

Please review the frequency of the role demands below (do not amend).

1. Physical & Ergonomic Demands (Remote Work Context)

Task	Rarely	Occasional	Frequent	Constant
Percentage performed per day (average)	(1–5%)	(6–33%)	(34–66%)	(67–100%)
Prolonged sitting/standing (sedentary work)	☐	☐	☐	✓
Screen-based work (computer use)	☐	☐	☐	✓

Task	Rarely	Occasional	Frequent	Constant
Percentage performed per day (average)	(1–5%)	(6–33%)	(34–66%)	(67–100%)
Repetitive hand/wrist movements (typing, mouse)	☐	☐	☐	✓
Use of headset / phone / video equipment	☐	☐	✓	☐
Maintaining correct ergonomic posture (desk, chair, screen setup, etc.)	☐	☐	☐	✓

2. Sensory & Cognitive Demands

Task	Rarely	Occasional	Frequent	Constant
Percentage performed per day (average)	(1–5%)	(6–33%)	(34–66%)	(67–100%)
Visual concentration (screen reading, documentation)	☐	☐	☐	✓
Hearing (phone, video, online communication)	☐	☐	✓	☐
Speaking (phone, video, online communication)	☐	☐	✓	☐
Sustained concentration / attention	☐	☐	☐	✓
Multitasking / task switching	☐	☐	✓	☐
Processing complex or sensitive information	☐	☐	☐	✓

Task	Rarely	Occasional	Frequent	Constant
Percentage performed per day (average)	(1–5%)	(6–33%)	(34–66%)	(67–100%)
Decision-making under time pressure	☐	☐	☐	✓

3. Psychosocial Demands

Task	Rarely	Occasional	Frequent	Constant
Percentage performed per day (average)	(1–5%)	(6–33%)	(34–66%)	(67–100%)
Exposure to distressed people (e.g. crisis, grief, trauma impacts)	✓	☐	☐	☐
Exposure to traumatic, distressing or emotionally challenging content (hearing, reading or viewing)	✓	☐	☐	☐
Managing risk situations with persons that may demonstrate unpredictable behaviours.	☐	✓	☐	☐
Emotional labour (supporting others while regulating own emotional responses)	☐	✓	☐	☐

4. Remote Work Demands

Task	Rarely	Occasional	Frequent	Constant
Percentage performed per day (average)	(1–5%)	(6–33%)	(34–66%)	(67–100%)
Working remotely without immediate in-person support (virtual)	☐	☐	☐	✓

Task	Rarely	Occasional	Frequent	Constant
Percentage performed per day (average)	(1–5%)	(6–33%)	(34–66%)	(67–100%)
Limited informal peer interaction	☐	☐	☐	✓
Debriefing, supervision and escalation pathways delivered virtually	☐	☐	☐	✓
Managing boundaries between work and home	☐	☐	☐	✓
Debriefing access after critical incidents is prioritised over noncritical incidents	☐	☐	☐	✓

5. Work Environment (Home-Based)

Task	Rarely	Occasional	Frequent	Constant
Percentage performed per day (average)	(1–5%)	(6–33%)	(34–66%)	(67–100%)
Maintaining privacy and confidentiality	☐	☐	☐	✓
WH&S safe & ergonomically compliant workspace setup (lighting, space, desk, chair, etc.)	☐	☐	☐	✓
Use of multiple digital systems/platforms	☐	☐	☐	✓
Reliance on stable internet and connectivity	☐	☐	☐	✓

7. Supports, Supervision & Safety Measures Provided

Control Area	Yes	No
Ergonomic self-assessment	✓	☐
Supervision provided (clinical roles)	☐	✓
Remote team and 1:1 manager meeting cadence	✓	☐
Access to debriefing / critical incident support (clinical roles)	☐	✓
Escalation pathways for core risk situations notified	✓	☐
Access to wellbeing supports (EAP or equivalent)	✓	☐

Candidate Completion Section

1. Reasonable Adjustments

Do you require any adjustments to safely fulfil the inherent requirements of this role?

☐ No	☐ Yes (please specify below)

2. Acknowledgement

Privacy

Information collected will be handled in accordance with privacy legislation and HR governance responsibilities.

Candidate statement: I have reviewed the inherent requirements of the role and understand the key demands and the terms of this document. My signature below is my acknowledgement of this, and that I have listed any reasonable adjustments that would enable me to undertake the role.

Candidate Name:

Candidate Signature:

Signature Date: