



Job Description

Position Title:	Infrastructure & Cyber Security Manager
School / Entity:	Central Office
Reports to:	Director of Technology
Direct reports:	2
Award:	Independent Schools NSW (Professional and Operational Staff) Cooperative Multi-Enterprise Agreement 2025
Classification:	Level 5.2 (Salary to be negotiated based on market and individual skillset)
Management Level	Level 5
Date created / revised	August 2026 Review due August 2029

What's it like working at St Philip's Christian Education (SPCE)?

St Philip's is focused on providing quality education in a caring, secure, and challenging learning environment based on Christian beliefs, values, and practice.

Our organisation's core values are:

- Christ First - we want to honour Christ in all things.
- Serve One Another - we want to appreciate the unique God-given potential of each person.
- Strive For Excellence - we want to aim to do our very best all the time.
- Do What Is Right - we want to always behave in a Christian manner.
- Build Community - we want everyone to feel they belong.

What's it like working in the Central Office?

The Central Office exists to:

- Ensure the organisation remains true to its Christian Mission
- Ensure that all activity and endeavours result in better outcomes for our students
- Pursue growth opportunities
- To facilitate the efficient functioning of the schools

Rationale:

The Infrastructure & Cyber Security Manager leads the design, implementation, and ongoing management of SPCE's network, server, and cyber security infrastructure. This role manages the network engineering team, champions the organisation's cyber security posture, and ensures robust, secure, and resilient IT operations across all campuses and entities, in alignment with the NIST Cybersecurity Framework and SMB1001 mitigation strategies.

The Infrastructure & Cyber Security Manager will assist the Central Office in the following ways:

Personal Christian Life:

- Promotes the vision and ethos of the organisation and its schools
- Maintains an active involvement in a local Christian evangelical fellowship
- Attends and participates in staff devotions and prayer meetings
- Participates in professional development relating to the philosophy and practice of Christian Education

Key Responsibility Areas:

- **Infrastructure Management**
 - Design, own, and maintain the organisation's multi-year infrastructure roadmap, with a strong focus on hybrid cloud architecture and positioning SPCE for future growth and scalability.
 - Lead the planning, deployment, and maintenance of all network and server infrastructure (on-premises and cloud)
 - Oversee performance, capacity, and availability of core systems and services
 - Ensure all systems are documented, monitored, and maintained to high standards
 - Oversee the creation, deployment, and maintenance of Standard Operating Environments (SOE) for Windows and Apple devices, including patch management and compliance with security standards (e.g., JAMF Pro, Intune)
 - Own the governance, security, and lifecycle management of network-connected AV, collaboration, and communications platforms.
 - Manage and optimise cloud infrastructure (M365, Azure, SaaS), ensuring robust security measures and alignment with NIST and SMB1001
 - Ensure all infrastructure and security practices comply with relevant legislation, standards (including NIST and SMB1001), and school policies
- **Cyber Security Leadership**
 - Develop, implement, and maintain the organisation's cyber security strategy and policies, aligned with the NIST Cybersecurity Framework and the SMB1001
 - Own and continuously improve the cyber security posture, including risk management, incident response, and compliance
 - Conduct regular security audits, vulnerability assessments, and awareness training
 - Promote a cyber-aware culture across the organization
 - Collaborate closely with the organisation's outsourced SIEM partner to manage the solution, ensuring log sources are correctly configured, tickets are triaged and managed by the internal team, and monthly SIEM reporting is delivered.
 - Develop and present governance reports and dashboards for the Director of Technology, providing visibility into infrastructure health, security posture, compliance status, and progress against the roadmap.

- **Disaster Recover & Business Continuity**

- Develop, maintain, and regularly test disaster recovery and business continuity plans for all critical systems
- Ensure systems and networks are resilient and backups are verified and tested on a regular basis.
- Develop and conduct cyber security table top exercises and simulated disasters for ICT and leadership teams.
- **Team Leadership & Development**
 - Manage, mentor, and develop the network engineering team (2 direct reports)
 - Set clear objectives, provide regular feedback, and foster a culture of excellence and collaboration
 - Oversee team workload, professional development, and succession planning
- **End User Support & Service Delivery**
 - Ensure high-quality end user support is delivered by the team, including device deployment, troubleshooting, and user training
 - Ensure timely and effective communication with stakeholders via service/helpdesk systems
- **Project Delivery & Continuous Improvement**
 - Lead the research, review, and selection of new technologies, tools, and platforms to support the infrastructure roadmap, ensuring alignment with strategic objectives and security frameworks (NIST, SMB1001).
 - Manage the end-to-end quote and proposal process for infrastructure and security solutions, preparing clear recommendations and business cases for presentation to the Director of Technology.
 - Oversee vendor relationships, including contract negotiation, performance management, and ongoing evaluation to ensure value, compliance, and strategic fit.
 - Identify and implement service improvements, automation, and emerging technologies (e.g., AI, cloud security, IoT)
 - Collaborate with other ICT and school teams to ensure alignment with organisational goals

Privacy, Data Breach & Supplier Governance

- Support the organisation's approach to privacy, data protection, and information security, including compliance with the Privacy Act 1988, the Australian Privacy Principles, and relevant Australian privacy laws.
- Maintain and support privacy and data breach response processes, including assessment, escalation, containment, investigation, record keeping, and notification where required under the Notifiable Data Breaches scheme.
- Implement supplier governance practices, including supplier vetting, due diligence, approved supplier lists, contract requirements, and ongoing review of supplier privacy, security, and operational risks.
- **Training & Stakeholder Engagement**
 - Lead the development and delivery of ICT training packages related to infrastructure and cyber security for ICT staff
 - Oversee and champion the cyber security awareness training for all staff

Workers WHS Responsibilities:

Workers have a responsibility to:

- Participate in the development of a safe and healthy workplace.
- Comply with instructions given for their own safety and health and that of others, in adhering to safe work procedures.
- Co-operate with management in its fulfilment of its legislative obligations.
- Take reasonable care to ensure their own safety and health and that of others, and to abide by their duty of care provided for in the legislation.
- To report any injury, hazard or illness immediately, where practical to their supervisor.
- Not place others at risk by any act or omission.

Key Relationships:

Director of Technology, Senior Network Engineer, Network & Systems Engineer, Applications Manager, Central Office ICT Team, Service Delivery Team, Project Manager, School Leadership, and Executive Team, Service Delivery Manager, External vendors and service providers.

Judgement and Decision Making:

- Use own judgement, initiative, and critical thinking skills to develop and build solutions, and resolve issues and incidents as they arise.
- Decisions of a non-routine or politically sensitive nature must be referred to the Team Leader.
- A capacity to identify important issues and risks
- At all times the incumbent is required to comply with organisation policies and procedures.

Management Skills:

- Ability to effectively plan, organise and manage own time to achieve targets and meet deadlines.
- Ability to supervise staff
- Demonstrate a strong commitment to change processes.

Interpersonal Skills:

- Ability to show understanding and patience in communicating with staff and third-party vendors.
- Friendly yet professional communication style.
- Excellent written communication skills.
 - Actively participate in a team environment to:
 - Share workloads & knowledge
 - Solve problems collaboratively
 - Assist each other with management of projects
 - Collectively make decisions.
- Open to change and innovation.
- Show leadership qualities and ambitions, with a drive to help and develop others.

Qualifications and Experience:

- Bachelor's degree in Information Technology, Computer Science, Cyber Security, or related field
- Minimum 5 years' experience in network/server administration and cyber security
- Demonstrated experience with cloud infrastructure (M365, Azure), firewalls, endpoint security, and incident response
- Strong knowledge and practical experience with the NIST Cybersecurity Framework and the SMB1001 mitigation strategies
- Experience with SOE management, patching, and device fleet administration
- Desirable:
 - Proven experience managing technical teams
 - Industry certifications (e.g., CISSP, CISM, CCNP, Microsoft, Azure, Palo Alto, CrowdStrike, JAMF, Intune, Aruba, or similar)
 - Experience in education or not-for-profit sector
 - Experience with automation, AI, or emerging security technologies

Conditions Of Employment

- Four weeks' annual leave; January is the busiest time for the ICT Department—annual leave during this period is restricted and requires prior approval
- Remuneration and conditions in line with or above the Independent Schools NSW (Professional and Operational Staff) Cooperative Multi-Enterprise Agreement 2025
- Requirement to hold and maintain a valid Working With Children Check (WWCC)

We'll encourage you along the way

We will partner with you to support your performance and ongoing development to ensure you are fully prepared for future challenges as this position and our organisation adapts and grows.

Declaration

I acknowledge that I have read and understood the requirements and responsibilities of this position and have discussed the JD and the key responsibilities of the role with SPCEF Ltd. I declare that I am able to fully undertake the inherent requirements of this role.

Employee Name:	
Employee Signature:	
Date:	