



## Job Description

Title:	<b>IT Network and Security Administrator</b>
Reports to:	Director of Information Systems & Technology
EBA/Award:	South Coast Baptist College Operational Agreement 2024
FTE:	1.0 FTE
Employment Type:	Permanent – Full Time

### Position Summary

The IT Network and Security Administrator is responsible for administering, maintaining and securing the College's information technology systems and solutions, including networks, servers, firewalls, identity platforms, endpoints, and associated security systems.

Reporting to the Director of Information Systems and Technology (DIST), this role ensures the confidentiality, integrity, and availability of technology services. It leads day-to-day operations, supports systems and network administration, maintains backup and recovery readiness, and acts as an escalation point for complex incidents.

Working collaboratively within the IST Team, the position designs and maintains secure architectures, enforces security controls, and ensures compliance across all devices and platforms.

### Key responsibilities

#### Network & Infrastructure Administration

- Administer, configure, and maintain the College's wired and wireless network infrastructure, including VLAN segmentation, ACLs, routing, switching, firewalls and performance monitoring.
- Deploy and optimise wireless networks, ensuring secure authentication methods, zoning, strong coverage, and high availability.
- Implement and maintain firewall policies, VPNs, content filtering, IDS/IPS and security logging.
- Manage and maintain the College's telephony systems.
- Monitor network health, troubleshoot disruptions, and continually enhance reliability and resilience.

#### Systems Administration

- Administer and maintain Windows/Linux servers, virtualisation platforms, and SaaS systems.
- Administer, manage, and monitor the College's Microsoft 365 and Google Tenants, including Entra ID, Exchange, Teams, Intune, OneDrive, SharePoint Online, Defender, Power BI, Power Automate.
- Support system integrations, updates, and maintenance activities.
- Monitor logs and performance across infrastructure components.
- Configure and manage the PA and bell systems for announcements and scheduling.
- Configure, manage and test backup and restore, disaster recovery and business continuity processes.

#### Physical Security & Access Control

- Configure and manage access control systems, gate schedules, user permissions, and zoning.
- Administer and manage the security camera infrastructure, including footage retrieval and auditing.



- Coordinate with security vendors and authorities for ongoing reliability and reporting.
- Assist in design improvements for overall physical security posture.

#### **Identity & Access Management**

- Administer and monitor Active Directory and Entra ID environments, including lifecycle management and synchronisation.
- Configure and manage role-based access control (RBAC), group policies (GPO), and SSO.
- Configure and manage authentication and integration with third-party applications.

#### **Endpoint, Device & Patch Management**

- Perform updates, upgrades, vulnerability remediation, and compliance reporting for College devices.
- Administer Intune and MDM policies, configuration profiles, compliance rules, and deployments.
- Create and manage software deployment packages and automation.
- Remediate non-compliant endpoints and maintain Standard Operating Systems (SOE) documentation.

#### **Cybersecurity Operations & Governance**

- Lead cybersecurity operations - threat detection, triage, incident response, remediation, and post-incident reviews.
- Implement and maintain Zero Trust security principles across identities, devices, networks, and applications.
- Manage vulnerability lifecycle - scanning, prioritisation, remediation tracking, and reporting across servers, endpoints, and network systems.
- Develop and maintain cybersecurity governance documentation, procedures, and playbooks.
- Lead cybersecurity awareness initiatives and support compliance activities, including audits, risk assessments, penetration testing and security reviews.

#### **Reporting, Compliance & Vendor Coordination**

- Provide timely reports and metrics on network and server performance, cybersecurity, compliance, and IT operations.
- Maintain up-to-date technical documentation and change records.
- Ensure compliance with industry standards, best practices, and regulatory requirements for cybersecurity and data protection.
- Liaise with vendors for hardware, software, services and support.

#### **Other duties (*but not limited to*)**

- Act as an escalation point for the IST Service Desk and provide support (hardware & software) to staff and students in-person.
- Maintain an accurate and up-to-date record of enquiries/tickets and provide timely advice to staff regarding their status.
- Monitor, prioritise and resolve tickets within defined SLAs.
- Support onboarding/offboarding workflows and device provisioning.
- Create user accounts, assign licenses and permissions, and set up staff and student devices.
- Onboard new staff, students and equipment on the network and offboard exiting staff and students (permissions and hardware).
- Implement and maintain an OS imaging and deployment solution.



- Decommission old IT assets and prepare them for sale or recycling.
- Plan and schedule refresh of hardware devices.
- Maintain and update the IT asset database, ensuring IT assets are tagged and registered.
- Assist with IT budget preparation.
- Remain available to respond to cybersecurity incidents and support special events as required.

#### Selection Criteria

- Bachelor's or Master's degree in Information Technology or a related discipline
- Minimum of 4+ years' experience in similar systems, network or security administration role.
- Strong knowledge of networks, Microsoft 365, Intune, Windows Server OS, virtualisation platforms, PowerShell and scripting.
- Excellent problem-solving skills and capacity to work independently and collaboratively.
- Strong communication skills with a friendly, service-oriented approach
- Demonstrated capacity to learn, adapt and manage multiple tasks and projects.

#### Desirable

- Vendors certifications (such as Microsoft, Fortinet, HPE Aruba)
- IT Service Management qualifications such as ITIL.
- Experience working in an education environment or multi-site organisation.

#### General Requirements

- To have a personal faith and commitment to the Lord Jesus Christ.
- To actively be a part of a Church or Christian community and exemplify Christian beliefs, behaviour, and practices.
- To accept the College's Statement of Faith.
- Build co-operative and supportive relationships with the board, principal, staff, students and parents.
- Work to ensure personal best practice.
- Ensure that decision making is based on fact and is impartial and fair.
- Model the use of appropriate and proper channels of communication.
- Always act in the best interest of the College and its ethos.
- Commitment to maintaining a child-safe environment in line with the College's values and policies.
- Working With Children Card.
- National Police Clearance.
- Contribute to a safe and healthy workplace by:
  - Following WH&S instructions and policies
  - Reporting accidents and hazards
  - Generally caring for own safety and that of others, including volunteers, students, and parents.
  - First Aid certificate.

#### Other Matters

Note: This job description is comprehensive but not exhaustive, and duties may be varied at the discretion



**SOUTH COAST  
BAPTIST COLLEGE**  
*Thy Kingdom Come*

of the College in consultation with this role.

Position Held By:	
Signed:	
Date:	