NDA
National
Development
Agency

JOB PROFILE

POSITION DESCRIPTION	
Position Title	**ICT Specialist: Security**
Purpose	The ICT Specialist: Security safeguards the NDA's information assets across on-premises, cloud, and hybrid environments through security oversight, assurance, access reviews, threat monitoring, awareness, and technical oversight of ICT-managed physical-access systems. The role provides expertise in IAM, PAM, Azure, Microsoft 365, network and endpoint security, SIEM/SOC, vulnerability management and disaster recovery. It aligns security governance and strategy with business objectives, monitors compliance, and manages deviations and exemptions to support secure, reliable and resilient ICT operations.
Division	Corporate Services
Reports To	Senior Manager: ICT
Position Location	Head Office
Peromnes Grade	8
Direct Reports / Supervision	1
POSITION REQUIREMENTS	
Minimum Qualification	• National Diploma in IT • Network+, Security+ certification (COMPTIA) • Professional-level Information Security Certification (CISSP / CISM / CISA)
Advantageous	• CompTIA Cloud+ certification will be an added advantage. • CEH or ISO/IEC 27001 certification will be an added advantage.
Essential Experience	• 3 years of relevant information security experience in a corporate ICT environment.
Knowledge	• **Endpoint security:** Endpoint detection and response (EDR), anti-malware, patch management and compliance, device encryption, system hardening and device compliance monitoring. • **Network infrastructure and security:** TCP/IP, routing, switching, VPNs, firewalls, encryption, network segmentation, secure data transmission and vulnerability remediation.

	• **SD-WAN:** Overlay monitoring, traffic steering, link failover, secure branch connectivity, secure internet breakout and service-level agreement (SLA) monitoring. • **Cloud services:** Microsoft Azure; Azure role-based access control (RBAC), Azure Policy, Azure Monitor, Azure Backup, Azure Firewall, Azure networking and Microsoft Defender for Cloud. • **Microsoft 365 security:** Microsoft Entra ID, Conditional Access, multi-factor authentication (MFA), Microsoft Intune, Microsoft Exchange Online Protection, Microsoft Defender for Office 365, Microsoft Purview, and security settings for Microsoft Teams, Microsoft SharePoint Online and Microsoft OneDrive. • **Identity and privileged access management:** IAM and PAM, user lifecycle management, access reviews, RBAC, least privilege, segregation of duties and approval of privileged access. • **Disaster recovery and business continuity:** recovery time objectives (RTOs), recovery point objectives (RPOs), backup integrity, restore testing, failover, failback and ransomware recovery. • **Security monitoring:** SIEM platforms and SOC processes, including log onboarding, alert triage, incident correlation, escalation thresholds, remediation tracking and security reporting. • ICT **governance and compliance:** NDA ICT security policies, internal controls and risk policy; Zero Trust, ISO/IEC 27001, NIST CSF, COBIT, Minimum Information Security Standards (MISS), and relevant local, industry and state or enterprise IT frameworks.
Skills & Abilities	• Advanced technical skills in cybersecurity, cloud, network, endpoint, Microsoft 365, Azure, and identity environments. • Strong risk management, audit, assurance and compliance skills. • Clear communication and report writing, with the ability to translate security risks into practical advice and recommendations. • Advanced problem-solving, root-cause analysis and troubleshooting skills. • Strong interpersonal skills and effective stakeholder and service provider coordination. • Sound judgement, integrity and decisive handling of security incidents and privileged access.
Main Areas of Responsibility	
ICT Security Governance, Risk and Compliance	• Provide specialist oversight and assurance over ICT security controls, policies, standards and standard operating procedures (SOPs). • Implement approved ICT security policies, standards, procedures and control frameworks, drawing on ISO/IEC 27001, NIST CSF, COBIT, MISS and Zero Trust principles where applicable to NDA requirements. Recommend improvements based on risk assessments, audits, incidents, vulnerabilities and changes in the technology environment. • Coordinate ICT security risk assessments and maintain the ICT security risk register.

	• Assess the design and effectiveness of security controls across cloud, network, endpoint, identity, Microsoft 365 and data-processing environments. • Maintain and monitor security deviations, exemptions and control exceptions in accordance with approved governance processes. • Track audit findings, risk-treatment actions and security-control deficiencies through to implementation and evidence-based closure. • Prepare periodic cybersecurity risk, compliance and assurance reports for management and relevant governance structures. • Promote appropriate segregation of duties between security assurance, ICT operations, system administration and control ownership.
Security Monitoring and Incident Response	• Provide specialist oversight of SIEM and SOC activities. • Review security alerts, events and incidents to support effective triage, correlation, classification, prioritisation and escalation. • Coordinate relevant ICT stakeholders and service providers during cybersecurity incident investigation and response. • Support incident containment, evidence gathering, impact assessment and root-cause analysis. • Conduct or contribute to post-incident reviews and translate lessons learned into improvements to preventative, detective, response and recovery controls. • Monitor incident remediation activities and track outstanding control weaknesses. • Prepare periodic security monitoring and incident reports identifying material incidents, recurring weaknesses, trends and required management actions.
Network, SD-WAN and Firewall Security	• Provide specialist security oversight and assurance over network, internet and SD-WAN environments. • Assess secure branch connectivity, traffic steering, link failover, secure internet breakout and network segmentation controls. • Conduct security reviews of firewall rules and proposed changes, considering least privilege, appropriate authorisation, segmentation and security risk. • Review remote-access and VPN controls, routing security, encryption and secure data-transmission arrangements. • Review SD-WAN security configurations and related network-security controls against approved organisational requirements. • Monitor security-related obligations and performance of network and telecommunications service providers against applicable SLAs. • Track identified network-security risks and control weaknesses through to remediation.
Cloud and Microsoft 365 Security	• Provide specialist security oversight and assurance across Microsoft Azure and Microsoft 365 environments. • Review the design and effectiveness of controls relating to Azure RBAC, Azure Policy, Azure Monitor, Azure Backup, Azure networking, Azure Firewall and Microsoft Defender for Cloud. • Review identity, endpoint, messaging and information-protection controls implemented through Microsoft Entra ID, Conditional Access,

	MFA, Microsoft Intune, Microsoft Exchange Online Protection, Microsoft Defender for Office 365 and Microsoft Purview. • Review security configurations relating to Microsoft Teams, Microsoft SharePoint Online, Microsoft OneDrive, external sharing and mailbox security. • Identify insecure configurations, excessive permissions and weaknesses in security controls and recommend corrective action. • Monitor remediation and security improvements while preserving the responsibilities of operational administrators.
Identity and privileged access management	• Provide specialist oversight and assurance over IAM and PAM. • Review access controls across the joiner, mover and leaver lifecycle. • Review account provisioning, modification, de-provisioning, and removal of access. • Conduct or coordinate periodic user-access and privileged-access reviews. • Assess compliance with RBAC, least privilege, segregation of duties and privileged-access requirements. • Verify that access changes and privileged-access assignments are supported by appropriate authorisation. • Identify dormant, excessive, inappropriate or conflicting access and recommend corrective action. • Track IAM and PAM control deficiencies through to evidence-based closure.
Endpoint, Patch and Vulnerability Management	• Provide specialist assurance over endpoint security controls, including endpoint detection and response (EDR), anti-malware, patching, device compliance, encryption, system hardening, data loss prevention and content-filtering controls. • Coordinate and monitor the vulnerability-management lifecycle from identification and risk rating through prioritisation, allocation to responsible technical owners, remediation, re-testing and closure. • Evaluate vulnerability findings according to security risk and potential organisational impact. • Monitor outstanding vulnerabilities and escalate overdue or material exposures through approved governance processes. • Monitor vulnerability and security exceptions where remediation cannot be completed within approved requirements. • Conduct or coordinate re-testing to verify remediation. • Prepare vulnerability, patch-compliance, and remediation-status reports.

Disaster Recovery and ICT Resilience	• Provide security assurance over disaster-recovery, backup and cyber-resilience arrangements for critical ICT services. • Coordinate or support backup-integrity verification, restore testing, failover and failback exercises. • Review recovery procedures, schedules and test evidence against approved RTOs and RPOs. • Assess cybersecurity preparedness for recovery from ransomware and other significant technology incidents. • Identify resilience weaknesses and track agreed remediation activities. • Report on ICT recovery readiness and significant resilience risks to management.
Third-Party Security	• Assess security risks associated with ICT service providers, cloud services and other technology suppliers within the scope of the position; review applicable supplier security controls, contractual security requirements, service-level commitments and available assurance evidence. • Provide specialist security input into ICT procurement and technology and service provider evaluations where security requirements apply. Monitor material security incidents and control weaknesses involving ICT service providers. • Track supplier-related security findings and remediation with responsible contract, technical and business owners; escalate material unresolved third-party cybersecurity risks through appropriate governance structures. • Act as technical lead for ICT and cloud projects, coordinating technical implementation, integrating cybersecurity controls, and supporting testing and handover to operations.
Security Awareness, Advisory Support and SOPs	• Lead and coordinate cybersecurity awareness initiatives addressing the NDA's risks and emerging threats. • Provide specialist guidance to users and technical teams on access control, acceptable use, phishing, information handling, identity protection and security requirements. • Develop, review and maintain relevant ICT security SOPs. • Provide specialist escalation support on complex cybersecurity incidents and control weaknesses. • Use incidents, audit findings, vulnerability trends and recurring control deficiencies to inform targeted cybersecurity awareness interventions.

ICT-Managed Physical Access Security	• Provide specialist technical oversight and assurance over ICT-managed electronic physical-access systems and associated security technologies. • Review logical access, administrative privileges and security configurations associated with electronic access-control platforms. • Coordinate security-related technology issues with responsible internal stakeholders and service providers. • Track identified technology-security weaknesses relating to physical-access systems. • Maintain clear separation between ICT's responsibility for electronic security technology and broader organisational responsibilities for facilities and physical security.

KEY RELATIONSHIP INTERFACES	
Internal relationships (excluding reporting lines) *	**External relationships (local/provincial structures and other key parties)**
• All NDA Staff	• Service Providers • Sector Departments

Signed by: (**Job Holder)**	Authorised by: 
Date:	Date: 02/11/2026