



## JOB PROFILE

POSITION DESCRIPTION	
<b>Position Title</b>	<b>ICT Specialist: Security</b>
<b>Purpose</b>	The position is responsible for performing ICT security access control, monitor systems, create awareness and related administration in order to create and maintain technology driven physical security infrastructure for ICT environment and protection of the NDA information. In addition, the position is responsible for the alignment of information security governance with the business objectives, information security strategy including compliance measurement, deviations and exemptions.
<b>Division</b>	Corporate Services
<b>Reports To</b>	Senior Manager: ICT
<b>Position location</b>	Head Office
<b>Peromnes Grade</b>	
<b>Number of Direct Reports/ Supervision</b>	1

POSITION REQUIREMENTS	
<b>Minimum Qualification</b>	<ul style="list-style-type: none"> <li>National Diploma in IT</li> <li>Network+, Security+ certification (COMPTIA) or equivalent</li> <li>Professional level Information Security Certification (CISSP / CISM / CISA) or equivalent.</li> </ul>
<b>Essential Experience</b>	<ul style="list-style-type: none"> <li>3 years relevant information security experience within a corporate ICT environment</li> </ul>
<b>Knowledge</b>	<ul style="list-style-type: none"> <li>Good knowledge and understanding of industry best practice with regards to IT Security controls such as: Anti-Virus/Anti-Malware, Patch management, Remote Access VPN, data and web content filtering, Data Loss Prevention</li> <li>Good knowledge and understanding of company internal control procedures and risk policy</li> <li>Good knowledge and understanding of NDA IT security policies and procedures</li> </ul>

	<ul style="list-style-type: none"> <li>• Good knowledge and understanding of relevant desktop and server hardware and software</li> <li>• Knowledge of Security and different levels of Encryption and Authorisation Schemes</li> </ul>
--	---

<b>Skills &amp; Abilities</b>	<ul style="list-style-type: none"> <li>• Excellent communication skills</li> <li>• Problem-solving</li> <li>• Interpersonal skills</li> <li>• Decisiveness</li> <li>• Integrity</li> <li>• Resilience</li> <li>• Strong ICT technical ability</li> <li>• Good report writing skills</li> <li>• Risk Management skills</li> </ul>
-------------------------------	--

<b>Main Areas of Responsibility</b>	
<b>Information Security</b>	<ul style="list-style-type: none"> <li>• Develop plans to safeguard computer files against unauthorized modification, destruction or disclosure.</li> <li>• Monitoring for data violations internally and externally.</li> <li>• Manage and monitor internal and hosting FIREWALL rules in conjunction with Networks.</li> <li>• Identify accurate causes of security violations.</li> <li>• Implementation of appropriate remedies to ensure data and systems security.</li> <li>• Perform periodical reporting on violations and notification to ICT Senior Manager</li> <li>• Proactive implementation of fixes and patches to block viruses and attacks to the entire ICT system environment.</li> <li>• Maintain industry best practices with regards to ICT Security controls such as: Anti-Virus/Anti-Malware, Patch management, Remote Access VPN, data and web content filtering, Data Loss Prevention, etc.</li> <li>• Maintain awareness of ICT security trends and vulnerabilities, e.g. major virus outbreaks.</li> <li>• Conduct proactive and effective communication (Intranet, email, posters) of risks and vulnerabilities to staff.</li> <li>• Implement an appropriate ICT security support to NDA staff.</li> <li>• Ensure that the data transmissions are encrypted and configure firewalls to conceal confidential information during transmission.</li> <li>• Implement and manage password authentication to keep unauthorized users from accessing sensitive data files.</li> <li>• Modify security files to incorporate new software, correct errors, and change user access status.</li> <li>• Perform risk assessments and tests on running data processing activities and security measures.</li> <li>• Train staff about computer security and promote security awareness and security protocols.</li> <li>• Participate in testing exercise of Disaster Recovery Plan as per schedule.</li> <li>• Implementation of ICT Security Strategic plan.</li> <li>• Maintain, administer and backup of ICT security servers and applications.</li> <li>• Develop and maintain SOP's/ guidelines regarding access control to Service Desk, Desktop and Information Security.</li> <li>• Management of physical access to NDA Offices.</li> </ul>

<b>General Technical Support</b>	<ul style="list-style-type: none"> <li>• Provide desktop technical support to all NDA Users</li> <li>• Provide Network, Server &amp; E-mail User Support</li> <li>• Log, investigate and follow-up and resolve logged calls on ICT helpdesk</li> </ul>
----------------------------------	--

<b>KEY RELATIONSHIP INTERFACES</b>	
<b>Internal Relationships - other than reporting lines (manager and subordinates). *</b>	<b>External Relationships (With Local/Provincial structures and other key parties, specify)</b>
<ul style="list-style-type: none"> <li>• All NDA Staff</li> </ul>	<ul style="list-style-type: none"> <li>• Service Providers</li> <li>• Sector Departments</li> </ul>

Signed by:  <b>(Job Holder)</b>	Authorised by:
Date:	Date: