AIR TRAFFIC AND NAVIGATION SERVICES SOC. LTD

REPUBLIC OF SOUTH AFRICA

ASMCGS System Replacement

REQUEST FOR PROPOSAL: ATNS/RFP007/FY24.25/A-SMGCS REPLACEMENT

APPOINTMENT OF A SERVICE PROVIDER FOR ADVANCED SURFACE MOVEMENT GUIDANCE AND CONTROL SYSTEM REPLACEMENT PROJECT REQUIRED AT OR TAMBO INTERNATIONAL AIRPORT (FAOR) and CAPE TOWN INTERNATIONAL AIRPORT (FACT).

CYBER RISK ASSESSMENT

June 2024

The information contained within this document is confidential to ATNS in all respects and it is hereby acknowledged that the information as provided shall only be used for the preparation of a response to this document. The information furnished will not be used for any other purpose than stated and that the information will not directly or indirectly, by agent, employee or representative, be disclosed either in whole or in part, to any other third party without the express written consent by the Company or its representative

CYBER RISK ASSESSMENT QUESTIONARIRE

3rd Party Information Security Questionnaire			
Area	**Question**	**Answer YES/NO**	**Remarks**
POLICY	Is there a management approved information security policy that is enforced across the organization?		
POLICY	Is there dedicated resource/team responsible for management of Information Security with clearly defined roles and responsibilities?		
POLICY	Is there approved cyber incident management procedure/policy to ensure monitoring and management of cyber security threats and incidents?		
POLICY	Does the Incident Management Policy/Procedure include notification of affected 3rd parties/Customers during an Incident?		
POLICY	Is there a documented procedure to securely dispose of all media containing client data?		
POLICY	Is a unique user ID (and password) provisioned for each user (for access to systems, network services, and applications) to ensure accountability, and that only authorized users are granted access to systems?		
POLICY	Is there a process to review user access to systems, applications, files, and folders?		
POLICY	Is there an approved password management policy or standard?		
HR	Are background checks performed on employees before they are hired?		
HR	Are employees required to sign employment agreements?		
HR	Are your employees and contractors required to sign a non-disclosure agreement (NDA) or confidentiality agreement (CA) that requires them to maintain the confidentiality of client data during as well as post-employment?		
HR	Is there continuous awareness and training program to all employees on cyber threats and their role in protection of customer information?		
PRIVACY	Do you have a Privacy Policy which is compliant with in-scope privacy laws? (e.g. POPIA)		
PRIVACY	Have you had any personal data breaches within the last 18 months which have required notification to a data protection regulator or data subjects?		
PRIVACY	Does your Incident Management Policy/Procedure include Data breach notification requirements.		
PRIVACY	Do you have a team or person accountable for management and oversight of privacy compliance?		
PRIVACY	Have you had any regulatory enforcement action in the last 3 years relating to personal data?		
RISK/BCM	Is there a risk governance plan that includes Information Security related threats?		
RISK/BCM	Does the organization implement and continuously improve security controls for their information systems?		

RISK/BCM	Is there an internal audit, risk management or compliance department with responsibility for identifying and tracking resolution of outstanding regulatory issues related to Information Security and Privacy?		
RISK	Is there Vulnerability Management process that ensures vulnerabilities are continually monitored and mitigated.		
RISK	Is there Effective security monitoring that ensures information systems are continually monitored for threats and incidents?		
3RD PARTY	Do you have documented third-party risk management program in place for the selection, oversight and risk assessment of third-party service providers?		
3RD PARTY	Do the third-party risk management program include assessments performed on all potential third-party service providers before entering contracts with them?		
3RD PARTY	Does your third-party risk management program include background checks performed for Service Provider Contractors and Subcontractors?		
3RD PARTY	Do the contracts with all third-party service providers include Non-Disclosure/Confidentiality Agreements?		
3RD PARTY	Do the requirements include the security measures in how client data will be protected?		
3RD PARTY	Do the contracts with all third-party service providers include data breach notifications?		
CLOUD	Does the organisation enforce MFA for access to all its cloud services and remote connections into its networks?		
CHANGES	Are only the fully tested, approved and currently supported/maintained software installed into production use?		
CHANGES	Is there a documented Change Management/Change Control process that includes procedures required for all changes to production system(s) and application(s)?		