## Position: Technical Security Analyst Date: 17/06/2022

Department: IT Version Number: 5

# JOB DESCRIPTION

## Summary of Role

A group role handling the end-to-end internal and external Cyber Security requirements within in Air Business. This role is the core of a Security Operations Centre in conjunction with the Air Businesses Cyber Security Partner.

A hands-on role that requires a high-level of IT security technical understanding that will be working closely with people across the business on a combination of strategic and operational projects to implement defences to support the organisations IT security.

Working alongside and reporting to the ABD IT Systems Manager, ABS Head of IT Operations and SOC partner the role will involve supporting IT management on providing IT cybersecurity technical capabilities to the IT teams and the overall business.

The role requires supporting cybersecurity for a wide area of technical systems and software solutions, as well as reporting on the cybersecurity environment, threats, vulnerabilities, trends and advising and implementing technical solutions and processes to ensure best possible cybersecurity for the company.

## Principle Responsibilities

* Work with a group wide hybrid SOC with a designated partner and improve the security operation process
* Technical system configuration and system hardening, management of firewall rules, networking, penetration testing, analyzing log files and anti-virus solutions. Manage anti-virus implementation, patching and security configuration for cloud systems, servers, workstations, applications, mobile and other devices and ensure all are kept up to date in accordance with the IT Security Policy
* Act as technical security incident escalation point for Air Business. Take a proactive approach to cybersecurity incidents in conjunction with the IT Systems Manager, Head of IT Operations and SOC Partner. Resolve urgent concerns and action technical resolutions accordingly in response to any incidents. Conduct post-incident technical reviews, advise, and implement improvements to systems, processes, and employee engagement
* Supporting the organisation's security strategic framework and implementation plan, including technical input into the Information Security Management System
* Own IT security incident management processes, creating, managing processes, identifying improvements and reporting on incidents
* Staying alert and informed on national/international cyber security alerts and advise on any implications this may cause the organisation
* Set up and lead internal working groups to manage Access Control, ensuring that security permissions, groups, users, and other permission entities are kept in accordance with company policies
* Review and update security technologies and frameworks
* Own Cyber Security Awareness campaigns including defining the content, defining, and measuring metrics, and demonstrating the effectiveness of awareness activities
* Ensure that in-house, cloud and application systems are fulfilling the security standards
* Have a practical understanding of the latest information technology security trends, threats, advising the business of the best approach and taking the lead in preventing and resolving cybersecurity threats
* Able to understand, assess, prioritise, and resolve risks to the company and to the IT systems, within security and technology areas. Work closely with all departments in ensuring good cybersecurity practice across the company, including in office and warehouse environments, remote sites and for employees working from home
* Alongside the IT Systems Manager, Head of IT Operations, and partner SOC, support the outcomes of internal and external IT audits and certifications. Respond to identified areas of improvements from audits and certification reviews, advising on practical approaches, implementing technical solutions, and reviewing the implemented solutions and processes regularly
* Provide technical input to support IT management in the creation and maintenance of Group IT security policies and procedures, technical security designs, standards, and support policies
* Support theData Protection Officer & Privacy Managers in implementing GDPR requirements, including Right to be Forgotten Requests, Subject Access Requests, responding to technical security queries in tender documents and supporting security in all data flow processes and policies
* Manage vulnerability scanning solutions, including internal and external penetration and vulnerability testing. Understand the root causes of vulnerabilities, identify, and implement resolutions and report on status
* Ensure highly sensitive data systems, such as CCTV, HR systems, comply with security requirements and advise on technical solutions to data protection issues
* Understand the technical requirements for security in code and privacy in design, with both internal and external development teams to ensure the delivery of development security best practice for new systems and upgrades to existing systems and software solutions
* Provide regular reporting (metrics) to the IT Leadership Group on the status of cybersecurity in the business, such as patching levels, security events, threats, trends, vulnerabilities and create and oversee action plans to resolve concerns
* Support and execute security tests and table-top exercises across the IT estate, analyse outputs and implement technical remediation projects as necessary with third parties to prevent data or financial loss to the UK businesses

## Person Specification & Key Skills

* Experience of working in a small team within a heavily regulated and fast-paced environment
* Competent in cyber security technologies: Firewalls, intrusion detection, assessment tools, encryption, certificate authority, etc.
* Solid technical understanding of IT systems from a cybersecurity perspective, including access controls, patch management solutions, anti-virus systems, networking, cloud infrastructure, vulnerability scanning systems, servers, workstations, and applications
* Able to work proactively and independently to identify and report on cybersecurity threats
* Strong analytical skills to analyse security requirements and relate them to appropriate security controls
* Excellent writing and reporting skills, able to deliver reports on cybersecurity threats, patching status, vulnerabilities, etc. Able to present data in a clear and intuitive manner
* Able to work both alone and as a member of the IT team, working proactively alongside the Infrastructure, Service Desk and Development teams to identify and report on cybersecurity threats and implement cybersecurity best practice in all areas
* Good understanding of the Data Protection Act and the General Data Protection Regulation
* Sufficient understanding of compliance requirements such as ISO27001 and PCI DSS and how technical systems can be managed to meet compliance needs
* Sufficient understanding of development practices and methodology to be able to support delivery of security and privacy in code and design and report on status

## Qualifications

* Previous experience in IT system administration, IT development and/or IT security roles
* Good knowledge and competence in the cybersecurity field, including knowledge of various standards such as ISO27001, Cyber Essentials, COBIT, PCI
* Security qualifications such as CISSP, SSCP desirable
* Ability to assess and benchmark security controls in common cloud platforms including Office 365, Google Suite, Azure
* Degree in an IT field desirable.

## LOCATION

This position is located at our Head Office in Hatfield, Hertfordshire or our office in Haywards Heath, West Sussex and is a hybrid working position. It will require occasional travel to the other office.

*It is the company’s intention that this job description is seen as a guide to the major areas and duties for which the jobholder is accountable. However, the business will change, and the jobholder’s obligations are bound to vary and develop, so the job description should be seen as a guide and not as a permanent, definite and exhaustive statement.*