Information Security Analyst			
Level	1	Location	Brisbane – Head Office
Department	IT Security Operations	Division	Information Services
Group	Office of the CEO	Direct Reports	n/a
Reports to	Head of Information Security	Manager once removed (MOR)	CISO
Created	10th December 2017	Updated	

Goals

My Role	As an Information Security Analyst, you will consult with all areas of the Virgin Australia business on information security matters. You are familiar with the concepts around penetration testing, vulnerability assessment, malware analysis and are keen to gain exposure to security incident handling in a corporate environment. In a fast-paced environment where every day is different, your flexibility, willingness to learn and ability to pick up new skills quickly are key to your success. You have a theoretical knowledge of the security domain and a logical approach to problem solving and are looking for a role to put these into practice.
	You will be monitoring and analysing firewall, routers/switch, intrusion detection systems, and enterprise data-leakage and anti-virus logs and alerts on a daily basis and will ensure your knowledge of the threat landscape remains up to date by keeping abreast of global information security events and trends.
	Your technical skills are continually expanding as you work to stay up to date on the latest methods attackers are using to infiltrate corporate networks, and you are willing to develop your communication, business engagement and technical writing skills. To be successful in this role, you will need to be an all-rounder, turning information security concepts in to practical, quality service delivery.
My Department:	The IT Security Operations Team are responsible for the operational security of our corporate computer networks, including:
	- The planning and implementation of Virgin Australia's way of handling security - Incident handling and investigations - Risk management and assessments, compliance and IT audits - Monitoring the health of security sensors and endpoints - Evaluate existing technical capabilities and systems to identify opportunities for improvement
	Working within the Information Services team, but consulting across the entire Virgin Australia business, the IT Security Operations Team have a passion for enhancing, enabling and executing business outcomes through the intelligent application of information security best practice.

Virgin Australia

1. To be Australia's airline of choice.

2. To be Australia's best customer led organisation

3. To do for corporate travellers what we did for leisure travellers in 2000

Expertise

	Must have	Great to have
Knowledge	• Broad understanding of penetration testing and incident response methodologies; • Understanding of basic information security principles including access management, data segregation and least privilege; • Understanding of basic information security principles and practices, including cloud and managed (outsourced) services;	• Airline or transport industry experience; • Experience in mobile security solutions;
Qualifications	• Bachelor-level degree in technical discipline or field (Information Security, Computer Science, Software Engineering, etc) or equivalent.	• Other relevant certifications including OSCP, CISSP, OSCE, OSWP, OSWE, OSEE, CREST, GWAPT, GPEN, GCIH, CISA, CISM
Skills	• Strong written and verbal communication skills; • Ability to identify key threat intelligence across open source channels that is relevant to Virgin Australia and its interests • Solid analytical skills to assist in investigating any irregularities across the network	• Working knowledge of common security tools such as Nessus, Nexpose, BurpSuite and sqlmap.
Experience	• Exposure to Windows/Linux/Mac operating systems • Confidence on the command line (particularly Linux) • Demonstrated interest in the information security field	• Red/blue teaming, bug bounty or Capture-The-Flag experience; • Building and configuring servers in a client/server network environment

Key Accountabilities

Accountability	Major activities	Performance Indicators
1. Internal Business Partnering	• Understand and contribute to the development of our security strategy • Monitor and improve technical	• Ensure secure operation of Virgin Australia systems and networks • Rapid response to identified security incidents with sense of

Accountability	Major activities	Performance Indicators
	security policies as stated in the IT Security Strategy for the Virgin Australia Group • Participate in IT Security audits • Maintain knowledge of new and emerging global security threats	urgency • Regular engagement with other business units on relevant security topics
2. IT Team Relationships	• Embody the customer centric service culture within the IT Security Operations team • Build and maintain effective relationships across the greater IT team • Contribute to team achievement on service delivery targets • Adherence to all corporate standards and policies	• Annual and sick leave managed against corporate policies • Ensure regular one-on-one meetings are held • Timely completion of scheduled People processes such as leave submissions and expense claims • Performance agreements & reviews • Creating and following performance development plans • Compliance to all applicable corporate standards and policies
3. Vendor Relationships	• Developing and maintaining professional relationships with key vendors in the IT Security space	• Conduct regular vendor meetings and service/product performance reviews (where applicable)

Competencies are relevant to every Virgin Australia team member. Please refer to the Virgin Australia Behavioural Guide for further detail specific to your position.

– Continuous Improvement and Strategic Focus

– Critical Thinking and Analysis

– Organisational and Social Commitment

– People and Leadership

– Personal Awareness and Effectiveness

– Service Delivery

– Vivacity

Key Interactions

Internal	• IT department • Business units across the Virgin Australia Group (Managers and team members)
External	• External Vendors, professional bodies, government and law enforcement officials.

Major Challenges

• Providing timely and high-quality analysis to key stakeholders during security incidents

- Addressing security risks in on a priority basis within tight timeframes
- Running fast, effective security incident response in an environment with multiple internal and external managed service providers
- Ensuring security culture continues to develop across the Virgin Australia business at all levels

Our Expectations

You are expected:

1. To be the ultimate Virgin Australia ambassador through living, breathing and promoting the Virgin Australia Values – Caring, Excellence, Individuality, Resourcefulness, Innovation, Enthusiasm and Integrity.

2. To demonstrate our Leadership Behaviours; Act with integrity, Be decisive, Act quickly, Listen to Guests and team members and Take responsibility.

3. To comply with and actively support all position, department and company policy and procedures

4. To be a team player – supporting a one in all in approach and a first to know, best to deal with

5. To demonstrate our Safety-First philosophy – First to find, first to fix! Ensuring that you keep our workplace fair and safe – free of all forms of discrimination and harassment and free from injury and incident.

6. To engage the very best of your personality and enthusiasm and create memorable, positive and fun experiences for all.

Sign Off

I have read and understand the requirements of this position. I agree to consult with my Manager or Leader should I not understand the key accountabilities or expectations of me. I will carry out the position to the best of my ability and understand I must meet required performance standards and targets. I accept the responsibilities of the position as outlined above.

I understand the position description for my role is constantly evolving, based on emerging priorities and shifts in organisational and department needs, and therefore will be updated from time to time.

Team member name:	Signature:	Date:
[Add name]		[Add date]
Manager/Leader's Name:	Signature:	Date:
[Add name]		[Add date]