## JOB PROFILE

| | |
|---|---|
| **Profile** | Analyst – Information Security |
| **MITA Career Level**<br>*Based on SFIA v6 Responsibility Levels* | 3 |

## SUMMARY STATEMENT

Identify, analyse and react to cybersecurity threats using a reliable set of processes and technology solutions.

## MISSION

Provide security operations support, including identification, protection, detection, response and recovery from cyber security events and incidents. The Analyst – Information Security performs real-time monitoring, analysis and response to security events and threats. As a member of the Security Operations Team, the Analyst is required to work collaboratively, to develop sufficient understanding of all roles within the team to provide assistance to other functions as required.

## DELIVERABLES

| | |
|---|---|
| **Accountable** | • Detection and monitoring of threats |
| **Responsible** | • 1st/2nd line security support |
| **Contributor** | • Resolution of incidents |

## MAIN TASKS

- Works as part of the Security Operations Team to ensure the Agency's products, systems and services are managing risk appropriately and protecting customers' interests.
- Works collaboratively with security and operational staff and consultants to ensure that security measures are implemented and operational.
- Conducts real-time monitoring of the Agency’s systems and services through established processes and procedure.
- Perform effective triage of security events throughout their lifecycle.
- Supports the Incident Response Team in containing and mitigating security breaches and incidents impacting Agency’s systems.
- Liaises with vendors in the delivery of secure services
- Provides timely and relevant details of potential security incidents to supervising security analysts as they are discovered.
- Contributes to the formulation and ongoing evaluation of the tactical and strategic direction of the Agency's cyber security operations priorities.
- Prepares and document security monitoring reports for Agency IT systems.
- Consumes incoming threat intelligence feeds and contributes to the formulation of outgoing threat intelligence.

- Keeping abreast on information security trends and security standards.
- Other duties as assigned.

## ESSENTIAL BASIC ATTRIBUTES *Based on SFIA v6 according to Responsibility Levels (Appendix I)*

| | |
|---|---|
| **Autonomy** | Works under general direction. Uses discretion in identifying and resolving complex problems and assignments. Usually receives specific instructions and has work reviewed at frequent milestones. Determines when issues should be escalated to a higher level. |
| **Influence** | Interacts with and influences colleagues. Has working level contact with customers, suppliers and partners. May supervise others or make decisions which impact the work assigned to individuals or phases of projects. |
| **Complexity** | Performs a range of work, sometimes complex and non-routine, in a variety of environments. Applies methodical approach to issue definition and resolution. |
| **Business Skills** | Demonstrates an analytical and systematic approach to issue resolution. Takes the initiative in identifying and negotiating appropriate personal development opportunities. Demonstrates effective communication skills. Contributes fully to the work of teams. Plans, schedules and monitors own work (and that of others where applicable) competently within limited deadlines and according to relevant legislation, standards and procedures. Appreciates the wider business context, and how own role relates to other roles and to the business of the employer or client. |

## ESSENTIAL PROFESSIONAL ATTRIBUTES *Based on SFIA v6 (Appendix I)*

| Code | Description | SFIA Level |
|---|---|---|
| **INAN** | Analytics | 3 |
| **CSMG** | Customer Service Support | 3 |
| **DTAN** | Data Analysis | 3 |
| **USUP** | Incident Management | 4 |
| **SCTY** | Information Security | 3 |
| **SCAD** | Security Administration | 3 |
| **TEST** | Testing | 3 |
| **ASUP** | Application Support | 4 |
| **ITOP** | IT Infrastructure | 3 |
| **NTAS** | Network Support | 3 |
| **PBMG** | Problem Management | 3 |
| **HSIN** | Systems Installation/Decommissioning | 3 |
| **SLMO** | Service Level Management | 3 |
| **CFMG** | Configuration Management | 3 |
| **CHMG** | Change Management | 3 |

## ESSENTIAL SOFT SKILLS *Based on ESCO database (Appendix II)*

Social Skills – Working with others and as a team
Attitudes and Values
Thinking – Creative and Analytical
Communication – Verbal and non-Verbal

## CERTIFICATION

| | |
|---|---|
| **Name** | Relevant Professional Certification |
| **Mandatory** | No |

## REPORTING LINE

| | |
|---|---|
| **Reports to** | Service Manager or delegate |
| **Interacts with** | Peers |
| **Supervises** | N/A |

## WORKING CONDITIONS

Normal hours with possibility to provide support in crisis situations after office hours or on weekends. Abnormal support may be required on roster basis.

Works in accordance with a pre-defined shift schedule as agreed with Management which may include night shift.

## APPENDIX I - SFIA SKILLS DEFINITION

**INAN Analytics: Level 3**

Undertakes analytical activities and delivers analysis outputs, in accordance with customer needs and conforming to agreed standards.

**CSMG Customer Service Support: Level 3**

Acts as the routine contact point, receiving and handling requests for support. Responds to a broad range of service requests for support by providing information to fulfil requests or enable resolution. Provides first line investigation and diagnosis and promptly allocates unresolved issues as appropriate. Assists with the development standards, and applies these to track, monitor, report, resolve or escalate issues. Contributes to creation of support documentation.

**DTAN Data Analysis: Level 3**

Applies data analysis, data modelling, and quality assurance techniques, based upon a detailed understanding of business processes, to establish, modify or maintain data structures and associated components (entity descriptions, relationship descriptions, attribute definitions). Advises database designers and other application development team members on the details of data structures and associated components.

**USUP Incident Management: Level 4** Prioritises and diagnoses incidents according to agreed procedures. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents. Facilitates recovery, following resolution of incidents. Documents and closes resolved incidents according to agreed procedures.

**SCTY Information Security: Level 3** Communicates information security risks and issues to business managers and others. Performs basic risk assessments for small information systems. Contributes to vulnerability assessments. Applies and maintains specific security controls as required by organisational policy and local risk assessments. Takes action to respond to security breaches in line with security policy and records the incidents and action taken.

**SCAD Security Administration: Level 3** Investigates minor security breaches in accordance with established procedures. Assists users in defining their access rights and privileges. Performs non-standard security administration tasks and resolves security administration issues.

**TEST Testing: Level 3**

Reviews requirements and specifications and defines test conditions. Designs test cases and test scripts under own direction, mapping back to pre-determined criteria, recording and reporting outcomes. Analyses and reports test activities and results. Identifies and reports issues and risks associated with own work.

**ASUP Application Support: Level 4** Maintains application support processes, and checks that all requests for support are dealt with according to agreed procedures. Uses application management software and tools to investigate issues, collect performance statistics and create reports.

**ITOP IT Infrastructure: Level 3** Carries out agreed operational procedures, including network configuration, installation and maintenance. Uses network management tools to collect and report on network load and performance statistics. Contributes to the implementation of maintenance and installation work. Uses standard procedures and tools to carry out defined system backups, restoring data where necessary. Identifies operational problems and contributes to their resolution.

**NTAS Network Support: Level 3** Identifies and resolves network problems following agreed procedures. Uses network management software and tools to collect agreed performance statistics. Carries out agreed network maintenance tasks.

**PBMG Problem Management: Level 3**

Investigates problems in systems, processes and services. Assists with the implementation of agreed remedies and preventative measures.

**HSIN Systems Installation/Decommissioning: Level 3** Installs or removes hardware and/or software, using supplied installation instructions and tools including, where appropriate, handover to the client. Conducts tests, corrects malfunctions, and documents results in accordance with agreed procedures. Reports details of all hardware/software items that have been installed and removed so that configuration management records can be updated. Provides assistance to users in a professional

manner following agreed procedures for further help or escalation. Reviews change requests. Maintains accurate records of user requests, contact details and outcomes. Contributes to the development of installation procedures and standards.

**SLMO Service Level Management: Level 3** Monitors service delivery performance metrics and liaises with managers and customers to ensure that service level agreements are not breached without the stakeholders being given the opportunity of planning for a deterioration in service.

**CFMG Configuration Management: Level 3** Applies tools, techniques and processes to track, log and correct information related to CIs, ensuring protection of assets and components from unauthorised change, diversion and inappropriate use.

**CHMG Change Management: Level 3** Develops, documents and implements changes based on requests for change. Applies change control procedures.

## APPENDIX II - ESCO DATABASE

### Social Skills

Working with Others - work as part of a team

- Accept constructive criticism
- Collaborate on tasks
- Foster social networks
- Give constructive criticism
- Share information
- Share opinions
- Share resources

### Attitudes and Values at Work

Attitudes

- Demonstrated commitment – attend to detail, attend to quality, be curious, make an effort, meet commitments, persist, show enthusiasm, work efficiently, work independently
- Handles challenges – adapts to changes, build on experience, cope with pressure, deal with uncertainty, learn from mistakes, manage frustration

Values

- Follow ethical work practice – identify environmental impact, identify ethical issues, identify social impact, make ethical choices, reflect on own work practices
- Show respect – demonstrate tolerance, show consideration, show good manners, treat people fairly, work with different viewpoints

### Thinking

Creative and Entrepreneurship

- Generate new ideas – anticipate needs, experiment, recognise opportunity, show originality, visualise completed work
- Turn new ideas into action – adapt implementation strategy, create implementation strategy, produce original work

Critical thinking

- Examine evidence – check facts, consider alternative views, consider impact of judgement, critique reasoning, notice bias
- Explore issues – ask key questions, draw conclusions, explain reasoning, identify live topics, identify patterns, make judgements, question assumptions, recognise connections

Learning

- Manage learning process – monitor learning process, plan learning, use different learning strategies
- Manage the learning self – prioritise learning tasks, reflect on learning process

Planning own work

- Follow plan – monitor progress
- Manage time – work out prioritisation of tasks
- Sets target – identify objectives and milestones

Problem Solving

- Analyse the problem – examine causes of problem, explore context of problem, identify stakeholders involved
- Plan for action – devise strategy, prioritise actions, set goals
- Take action to solve the problem – coordinate actions, evaluate success, implement strategy, multi-task, troubleshoot

### Communication

Non-verbal communication

- Respond to cultural differences

- Understands non-verbal cues – read different types of eye contact, read different types of touch, read facial expressions, understand gestures, understand postures, understand uses of personal space
- Use non-verbal cues – make appropriate use of eye contact, make appropriate use of personal space, make appropriate use of touch, use appropriate facial expressions, use appropriate gestures, use appropriate postures

Verbal communication

- Spoken interaction – debating techniques, interrogating, negotiating, persuading
- Spoken production – presentation techniques