Government of **Western Australia**
Department of the **Premier and Cabinet**

JOB DESCRIPTION FORM

SECTION 1 – OFFICE IDENTIFICATION

EFFECTIVE DATE OF DOCUMENT: 01/09/2020

ORGANISATION: Department of the Premier and Cabinet	
DIVISION: Office of Digital Government	
BRANCH: Cyber Security Unit	
SECTION:	

CLASSIFICATION: Level 7	**POSITION NUMBER:** DPC20024
TITLE: Security Operations Centre Coordinator	
AGREEMENT/AWARD: Public Sector CSA Agreement 2019	
LOCATION: West Perth	

SECTION 2 – REPORTING RELATIONSHIPS

Manager Cyber Security (Technical)

Level 8

⇦

Other offices reporting to this office	
Title	Level
2 x Senior Cyber Security Analysts	5
Cyber Security Analyst	4
Cyber Security Project Officer	3

⇧

Security Operations Centre (SOC) Coordinator

Level 7

⇦

Officers under direct responsibility	
Title	Level
2 x Senior Cyber Security Analyst	5
Cyber Security Analyst	4

SECTION 3 – KEY RESPONSIBILITIES

Undertakes the daily operation of the Office of Digital Government – Cyber Security Unit Security Operations Centre (DGov SOC). Primarily responsible for performing security event monitoring of multi-agency networks across the WA Public Sector, incident coordination and response.

This role is responsible for development and maintenance of a whole-of-government threat intelligence and Cyber Incident Coordination program designed to support agencies in detecting, responding to, and recovering from cyber security incidents. Coordinates the SOC in the performance of incident identification, assessment, quantification, reporting, communication, mitigation and monitoring tasks.

The SOC Coordinator liaises with internal and external stakeholders, including Public Sector Agency's, interstate partners and private sector service providers, builds and maintains positive working relationships with them.

SECTION 4 – STATEMENT OF DUTIES

Summary of Duties
Details

LEADERSHIP AND MANAGEMENT

Responsible for leading and motivating staff in the development and achievement of the Office of Digital Government (DGov) Security Operations Centre business goals.

As a member of the Cyber Security Unit management team, has shared responsibility for the operations and outcomes of the Unit.

As a member of the I management team, has shared responsibility for the directions of the Directorate and is accountable for the delivery of Unit and DGov outcomes.

Develops and implements a comprehensive workforce development plan to develop staff, share strategic procurement knowledge and experience and ensures the efficient and effective delivery of services to client agencies and stakeholders.

Within the Branch, promotes a culture supportive of innovation and continuous business process improvement.

Provides proactive, timely and accurate advice to the Manager Cyber Security (Technical) and stakeholders in relation to cyber security threats, incidents and mitigations.

In an environment of constraint, ensures that resources including financial, physical, technological and information requirements are efficiently applied to maintain a high level of products/service delivery.

INCIDENT COORINDATION AND RESPONSE

Primarily responsible for coordinating the performance of security event monitoring of multi-agency networks across the WA Public Sector, incident coordination and response.

Ensure compliance to service level agreements (SLA), process adherence and process improvement to achieve operational objectives.

Revise and develop processes to strengthen the Security Operations Framework, review policies and highlight the challenges in managing SLAs.

Responsible for team & vendor management, overall use of resources and initiation of corrective action where required for Security Operations Centre.

Perform threat management, threat modelling, identify threat vectors and develop use cases for security monitoring.

Responsible for integration of standard and non-standard logs into the DGov security information and event management (SIEM) system.

Creation of reports, dashboards, metrics for SOC operations and presentation to senior management.

Co-ordination with stakeholders, builds and maintains positive working relationships with them.

PROJECT MANAGEMENT

Oversees the management of projects, including the development of project management plans.

Liaises with stakeholders in order to resolve complex disputes.

OTHER

Undertakes other duties as required to support the achievement of the DGov outcomes and outputs.

This position applies equal opportunity, occupational safety and health and ethical principles and practices in all aspects of this role whilst assisting in providing a fair, safe, enjoyable and innovative workplace.

SECTION 5 – SELECTION CRITERIA

Essential

Shapes and Manages Strategy
Anticipates, analyses and manages emerging issues to optimise performance. Leads in developing innovative solutions to complex problems.

Achieves Results
Effectively manages and leads team and organisational work deliverables. Role models collaborate behaviour and displays a strong work ethic and resilience.

Builds Productive Relationships
Builds and sustains relationship and trust with internal stakeholders and a broad network of external stakeholders to achieve mutually beneficial outcomes.

Communicates and Influences Effectively
Communicates complex information in a clear, articulate and compelling manner to engage and influence internal and external stakeholders.

Extensive knowledge of modern cyber security threats, tools and techniques
Can effectively apply the concepts, demonstrated ability to utilise relevant technology to detect and respond to identified threats.

Displays Personal Drive and integrity
Role models judgement, initiative and professionalism and encourages these standards in others. Proactively develops themselves and others.

Prerequisite

Baseline Personal Security Clearance. You will be required to complete a personal security vetting to achieve BASELINE security clearance in order for you to view and access classified resources up to and including those that are designated 'PROTECTED'. The assessment process will require your declaration on information about yourself and your immediate family members or those who are closely related to you.

Desirable

Relevant tertiary qualifications and or certificates.

Possess Industry Certification for example CISSP, CCSP, CRISC, CISM, CSXP and Security+ and/or equivalent qualifications.

Knowledge and experience in providing information security services within a government or large corporate environment.

SECTION 6 - CERTIFICATION

The details contained in this document are an accurate statement of the duties, responsibilities and other requirements of the job.

BRANCH/DIVISION HEAD

SIGNATURE: _____

DATE: _____

DIRECTOR GENERAL

SIGNATURE: _____

DATE: _____

As Manager I have reviewed the statement of duties and agree this is a current and relevant document.

NAME	SIGNATURE	DATE	INITIALLED BY HRSB

As the Employee I have reviewed the statement of duties.

NAME	SIGNATURE	DATE	INITIALLED BY HRSB