

JOB ROLE STATEMENT

CYBER SECURITY MANAGER LEVEL 7

DIRECTORATE FINANCE AND COMMERCIAL SERVICES
BRANCH INFORMATION MANAGEMENT **POSITION NO** VARIOUS

KEY RESPONSIBILITIES

Ensure cyber risks are identified and managed, where necessary oversee the implementation of technologies and processes to minimise the risks. Ensure the relevant cyber security frameworks are in place and managed, including a controls assurance and audit program.

KEY DELIVERIES

Cyber Security Governance, Risk and Compliance

- Manage Cyber Security and Cyber Risk throughout Main Roads.
- Manage the development and implementation of a Security Risk Management Framework for Main Roads.
- Manage the establishment and implementation of a controls insurance and audit program to support the Security Risk Management Framework.
- Manage the provision of Risk and Compliance Reports in line with the performance reporting framework.
- Manage the development of a Cyber Security Accreditation Framework.
- Manage the development and implementation of policies, standards, procedures and guidelines for Information and communication Technology (ICT) security.
- Identify problem and risk areas, design, propose and implement solutions to enhance ICT security systems and services
- Research security trends relating to the provision of ICT Services, assess for relevance to Main Roads' operating environment and recommend suitable strategies and mitigations for infiltration security vulnerabilities and security incidents.
- Initiate and manage projects designed to prepare Main Roads for responses to ICT security breaches, trends and to protect Main Roads' computer facilities, data resources and assets.
- Perform specialist investigations of security breaches and report on outcomes.
- Manage the design and development of security standards and control across a variety of technology stacks and including networks, operating systems, databases and websites.
- Review performance and availability of Main Roads' ICT Security Systems and services.

Leadership and Management

- Manage the continuous improvement of ICT Security at Main Roads.
- Contribute to the formulation of the Branch's policy and strategy.
- Manage financial, technological, physical and other resources within agreed allocations to meet agreed outcomes.
- Manage employee behaviour, performance and development.

Stakeholder Relationships

- Negotiate, consult, and liaise with Government agencies, commercial enterprise and senior management on ICT security.
- Build and enhance collaborative working relationships with internal staff and external stakeholders.
- Represent Main Roads and the Branch on working parties and forums relating to organisational ICT security.

SAFETY, HEALTH AND WELLBEING (SHW)

Responsible for active participation and performance to SHW standards as detailed by the Main Roads' Safety, Health and Wellbeing (SHW) Management System - refer to "SHW Roles and Responsibilities Procedure" on 'iRoads' intranet.

LOCATION

Main Roads is a regionalised organisation with key delivery centres operating from the Kimberley to the Great Southern regions, including the metropolitan area. The incumbent of this position may be required to undertake a role in a region for a period of time.

DYNAMIC RESOURCING

The incumbent of the position may be required to perform any other role within the incumbent's level of skill, competence and responsibility as directed by the Managing Director of Main Roads to meet the organisation's objectives and the incumbent's development.

REPORTING RELATIONSHIPS

This position reports to:

(A) TITLE AND LEVEL	POSITION NO
MANAGER ICT ENTERPRISE ARCHITECTURE OFFICE	LEVEL 8 VARIOUS

CYBER SECURITY MANAGER LEVEL 7

POSITIONS UNDER DIRECT SUPERVISION

List the position numbers, titles and levels of positions directly supervised

TITLE and LEVEL	POSITION No
ICT Security Architect	LEVEL 6
Cyber Security Operations Co-ordinator	LEVEL 6
ICT Security Officer	LEVEL 5

ALL POSITIONS UNDER CONTROL

State number of positions only

CATEGORY	NUMBER
Salaried, Wages	various
	various
	various
TOTAL	various

SELECTION CRITERIA – SHOULD BE ADDRESSED IN THE CONTEXT OF THE ROLE

ESSENTIAL:

- Comprehensive skill, knowledge and experience in:
 - managing the security of Information and Communication Technology (ICT) infrastructure and services in a large and complex organisation
 - defining, designing and developing security policies, standards and controls across a variety of technology stacks, including networks, operating systems, databases, websites and cloud technologies
 - working with discreet information and documentation
 - building and enhancing stakeholder relationships
 - managing financial, technological, physical and other resources within agreed allocations to meet agreed outcomes
 - managing employee behaviour, performance and development
 - negotiation and facilitation
- Knowledge of:
 - policies and practices on Work Health and Safety (WHS), and on EEO, diversity and equity
- Possession of a current Western Australian ‘C’ or ‘C-A’ Class (car) motor vehicle drivers’ licence or an approved equivalent.

DESIRABLE:

- A Degree in Information and Communication Technology (ICT) or other relevant discipline.

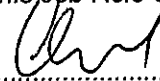
OTHER REQUIREMENTS:

Appointment to this role is also subject to:

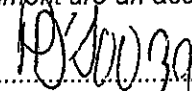
- Possession of a current National Police Clearance

CERTIFICATION

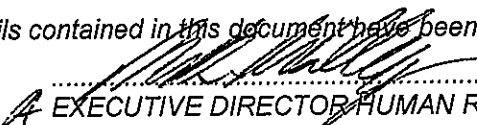
1. The details contained in this Job Role Statement have been reviewed and conform to Main Roads guidelines.

SIGNATURE  DATE 22/01/2026
BRANCH/SECTION HEAD

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

SIGNATURE  DATE 22/01/2026
EXECUTIVE DIRECTOR FINANCE AND COMMERCIAL SERVICES

3. The details contained in this document have been reviewed and conform to Main Roads guidelines.

SIGNATURE  DATE 22/1/26
EXECUTIVE DIRECTOR HUMAN RESOURCES