Job Description Form

Position Title: ICT Security Tester

Classification	HSO Level G7
Employment Instrument	Health Salaried Officers Agreement
Organisation	Health Support Services
Business Unit	ICT
Function	Security and Risk Management
Location	Perth Metropolitan Area

KEY ROLE STATEMENT

As part of the Health Support Services (HSS) ICT Business Unit, the ICT Security Tester is responsible for:

- Simulating cyberattacks to identify and report security flaws on computer systems, networks and infrastructure, including internet sites and provides reports and recommendations for remediation within systems to ensure compliance with policies and regulatory requirements.
- Conducting cyber security assessments for the ICT Security and Risk Management Directorate.

REPORTING RELATIONSHIPS:

Chief Information Officer
XHE

↑

Director, Security and Risk Management
HSO Level G14

↑

This position

↑

Directly reporting to this position:

Title	Classification	FTE
NIL		NIL

ORGANISATIONAL CONTEXT:

Health Support Services (HSS) is the shared service centre for the WA public health system. We provide a suite of services to more than 55,000 employees across WA's public health services and hospitals. Our services include:

- Information, communication and technology services (ICT)
- Procurement and supply
- Workforce services, including payroll, recruitment and appointment, NurseWest and workforce data
- Financial services
- Delivery of customer-driven programs and projects

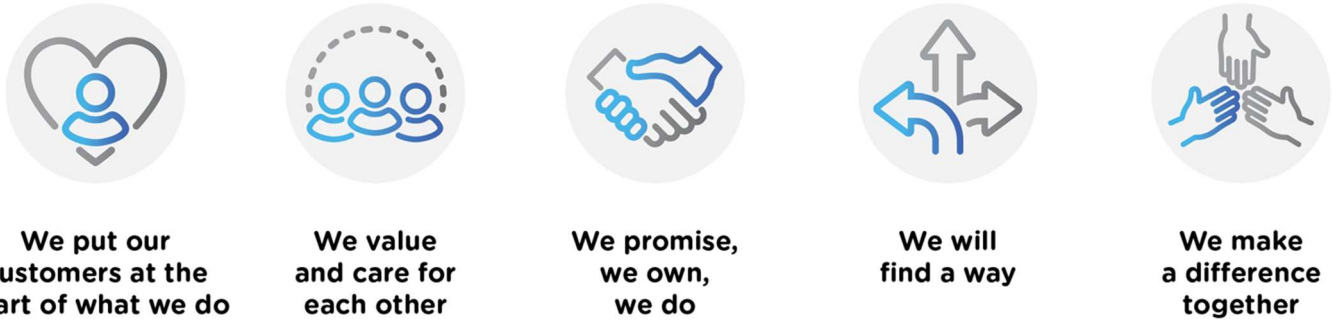
Our vision is to provide great services to our customers, be known as a valued partner, and support the health of all Western Australians. We seek to achieve this by delivering on our purpose of supporting our customers to provide excellent health care.

Whether you work in our corporate offices, at our customer sites, or out at our warehouses – collectively, our focus is on providing simple, reliable, responsive and sustainable services.

We are a workforce of over 1,400 innovative, dedicated and enthusiastic people. We embrace diversity and believe that our best services come from a workplace where varied perspectives and experiences are welcomed and encouraged.

We are undergoing a major business transformation to establish HSS as a modern shared services organisation and we're seeking the right people to grow our team.
It is an exciting time in the health sector and a defining period for HSS.

HSS VALUES



Our values guide our behaviours and the way we interact with our customers and each other.

BUSINESS UNIT ROLE:

The ICT Business Unit provides solution development, implementation, transition and operations support for the WA health system's clinical and corporate business systems. This includes the strategic planning, architecture and ongoing management of the WA health system's ICT network, applications and infrastructure, provision of ICT support to WA health system customers and the management of ICT security and risk (including security of patient data).

POSITION RESPONSIBILITIES:

HSS Participation (Team):

- Manages and contributes to the well-being and achievements of the team.
- Ensures staff and team members are held accountable for demonstrating the HSS values.
- Sets clear standards for performance, providing support when required and acknowledging individual and team achievements.
- Promotes self-development amongst team members, providing opportunities for further learning.

HSS Participation (Self):

- Maintains a culture of putting customers at the heart of everything we do and demonstrates a constant approach to the organisation, values and behaviours.
- Contributes effectively to business improvement and change management activities.
- Undertakes all duties in accordance with the WA health system's Code of Conduct, WA Public Sector Code of Ethics, Occupational Safety and Health and Equal Employment requirements, and other relevant legislation.
- Proactively contributes to maintaining the HSS Occupational Safety and Health Management (OHS) Framework.
- Takes personal accountability of own performance, and participates in all performance development activities.
- Collaboratively engages with team members, encouraging discussion whilst harnessing different viewpoints creating positive outcomes for key stakeholders.

Role Specific Responsibilities and Key Outcomes:

- Uses cyber security tools and systems to conduct penetration testing, ethical hacking and associated assessments to identify security vulnerabilities in networks, systems and web applications.
- Analyses and assesses security protocols, firewalls, and security technologies to ensure they are robust and provides recommendations for any improvements.
- Performs and reviews compliance testing to ensure adherence to cyber security policies, standards.
- Creates detailed reports and recommendations from penetration testing and assessment findings and recommends remediation strategies.
- Ensures all identified breaches in security are promptly and thoroughly investigated and that any system changes required to maintain security are implemented.
- Liaises and co-ordinates with external vendors and agencies to define the scope of penetration tests.
- Conducts retest of identified vulnerabilities and validates the recommended remediation implemented.
- Communicates effectively with clients and stakeholders, to ensure that penetration testing findings and that tailored solutions are understood and acted upon.
- Provides proactive, timely and accurate advice to the Director, Security and Risk Management and stakeholders in relation to penetration testing findings and associated projects.
- Manages security compliance responsibilities for both internal and external audit requirements as they relate to penetration testing and associated assessments.
- Supports the roll out and adoption of all security policies, process and tools across the organisation.

- Coordinates the activities of Security Incident Response Team as needed, or requested, in addressing and investigating security incidents that arise.
- Identifies and facilitates implementation of continuous improvements.
- Monitors the implementation of information security controls.
- Schedules and conducts periodic security audits.
- Tracks status on control breaches and coordinate required actions.
- Actively engages with internal and external stakeholders to continually improve the information security capability of HSS ICT.

SELECTION CRITERIA:

ESSENTIAL CRITERIA:

1. Demonstrated high level knowledge and experience using a range of penetration testing tools and methodologies to identify and manage ICT risks and security vulnerabilities in a complex and varied ICT security environment.
2. High level communication skills including the ability to develop reports for stakeholders with a proven ability to clearly communicate findings and recommendations to technical and non-technical stakeholders.
3. Well-developed analytical, conceptual, problem solving and research skills with a proven ability to identify and provide innovative solutions and mitigation plans for ICT security issues.
4. Technical proficiency in security protocols, firewalls, web application security and a strong understanding of related concepts and industry best practices.
5. Strong understanding of risk management process, including risk analysis techniques and treatment action plan for risk mitigation.

DESIRABLE CRITERIA:

1. Web application security: understanding of web application architecture and the OWASP Top 10 vulnerabilities.
2. Ethical hacking: ability to use the same tools and techniques as malicious hackers to identify vulnerabilities in systems.
3. Offensive Security Certified Professional (OSCP) certification and GIAC Penetration Tester (GPEN) certification.
4. Previous experience within the public and/or health sector.
5. Current knowledge of legislative obligations for Equal Opportunity, Disability Services and Occupational Safety & Health, and how these impact on employment and service delivery.

APPOINTMENT FACTORS

Appointment is subject to:

- Completion of 100 point identification check
- Successful Criminal Record Screening Clearance
- Successful Pre-Employment Integrity Check
- Pre-Employment Health Assessment

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

Version control	Description	CRC Approval Date	Registered Date
Vs 1.0	JDF Created	25/03/2024	26/03/2024