# NON-CONTRACT ROLE DESCRIPTION

JD2538

| | | | |
|---|---|---|---|
| **ROLE TITLE:** | Specialist, IM/IT Security | **ROLE DESCRIPTION NO.:** | 00371 |
| **DEPARTMENT:** | Information Management/Information Technology (IM/IT) | **HEABC REFERENCE NO.:** | 1872549 |
| **REPORTING TO:** | Manager, IM/IT Security | **HSCIS CODE:** | 05050 |
| **CLASSIFICATION:** | NCEM/Range 8A | **JOB CODE:** | 05050P |

## ROLE SUMMARY

In accordance with the Vision, Purpose, and Values, and strategic direction of the Vancouver Island Health Authority (Island Health) patient and staff safety is a priority and a responsibility shared by everyone; as such, the requirement to continuously improve quality and safety is inherent in all aspects of this position.

Reporting to the Manager, IM/IT Security, the Specialist, Information Management/Information Technology (IM/IT) Security works as a subject matter expert and lead resource in reviewing existing and proposed computer-based application and data access services. Works within IM/IT and with other VIHA business areas to ensure processes and practices support organizational information security policies and standards.

Responsible for monitoring and tracking use of VIHA data processing infrastructure, conducting investigations and resolving electronic data processing security-related incidents. Recommends and implements security processes, technologies and access methods that align with industry security standards and support the secure, uninterrupted operation of all VIHA technology services.

The Specialist, IM/IT Security deals with sensitive and critical situations and provides training and education to IM/IT and other staff on VIHA security procedures, policies and standards.

## DUTIES AND RESPONSIBILITIES:

1. Provides interpretation and expert advice, both verbally and in writing, to internal staff, physicians and management on legislation, international and eHealth information management standards and principles related to information security.

2. Manages complex and cross-agency security breach and violation investigations, including collection and appropriate handling of forensic evidence, conducting risk analysis, electronic audits and on-going investigations using an enterprise risk approach. Leads, coordinates and directs case management and documentation amongst the Integrated Breach Response Team. Liaises with external parties such as provincial government ministries and peer health authorities.

3. Evaluates breach root causes, implements and recommends resolution strategies, including disciplinary action, and practical quality improvement opportunities and risk controls targeted at strengthening organizational, operational and technical controls.

4. Participates in the development and application of security safeguards and system access controls for new and existing information technology services, ensuring alignment with VIHA security policy and practices.

5. Reviews and assesses operational processes both current and planned to ensure alignment with VIHA security policy and industry best practice.

6. Conducts periodic compliance reviews, risk analysis, electronic audits and ongoing investigations.

7. Evaluates the security risks associated with information systems and systems infrastructure by conducting formal Security Threat and Risk Assessments (STRAs) and Security Assessments (SAs) to assess risk, ensure accurate and complete documentation of security controls, and to ensure alignment with VIHA policies and legislated security obligations.

8. Lead monthly meetings involving stakeholders from various VIHA user-departments to review newly released patches and based on the VIHA enterprise risk management framework, determine the urgency and criticality of deploying them to VIHA systems.

9. Reviews security logs and violation reports investigating and evaluating root causes, implements and recommends resolution strategies, practical quality improvement opportunities and risk controls targeted at strengthening organizational, operational and technical controls and/or escalating as required.

10. Participates in the development of formalized procedures for the creation, modification, management, and deletion of user accounts and other access controls. Ensures access requests are consistent with VIHA standards and have received appropriate authorization.

11. Provides expert guidance to management and physicians and takes a lead role in ensuring information security is considered throughout the design or re-design of programs services and projects and initiatives

12. Develops and implements changes to existing procedures for secure management of data and information systems access controls.

13. Initiates partnerships and effectively maintains critical external linkages and partnerships with provincial and federal government agency representatives, regulatory bodies, legal representatives , external private companies and partners, researchers and the public to gather, provide, clarify or manage information security requirements

14. Initiates partnerships and effectively maintains critical internal linkages to ensure development of a consultative approach to mutual problem solving, enhancing communication, proactively anticipating and resolving issues and supporting the implementation of required changes.

15. Researches, creates, compiles and evaluates security information management performance metrics. Completes reports including Briefing Notes and statistical reports on specific subjects such as breach management score cards, progress of the corporate security educational program within VIHA. Prepares and delivers presentations to key stakeholders, management and staff.

16. Participates in the development of technology solutions that align with industry and VIHA security standards. Evaluates and recommends third party information security products to meet VIHA security and confidentiality requirements.

17. In collaboration with VIHA Network services, provides direct and indirect support for network security solutions such as Firewalls, Intrusion Prevention Systems, Antivirus and Internet Filtering technologies.

18. Effectively participates and represents the Health Authority on provincial and local committees or task groups. Represents the Manager, IM/IT Security as required

19. In collaboration with Information and Privacy personnel, works with VIHA programs to ensure education and compliance with system security policy and procedures. Promotes security best practices and performs both formal and ad-hoc information protection training.

20. Performs other related duties as assigned.

**QUALIFICATIONS:**

**Education, Training And Experience**

A level of education, training and experience equivalent to a Bachelor's degree in Computer Science and five years' experience in a large information technology services environment.

**Skills And Abilities**

- Good working knowledge of IM/IT security principles, management, tools and procedures.

- Comprehensive knowledge of core security technologies including firewalls, anti-virus, intrusion detection/prevention, monitoring'/reporting.
- Recent relevant experience working with Windows desktop and server technologies in a large information technology environment required.
- Good working knowledge of networking concepts and technologies.
- Knowledge of FIPPA, ISO 27002 and the BC Government Information Security Policy preferred.
- Active CISSP, SANS GIAC, or Security + certification and healthcare experience preferred.
- Advanced understanding of information security, governance and eHealth practices and trends, related legislation and requirements, provincial eHealth and clinical information systems.
- Solid understanding of information security principles and controls to support risk management identification in electronic systems.
- Ability to problem solve with a global perspective in order to incorporate the organization's systems and strategies when developing viable solutions to problems.
- Ability to establish and maintain effective partnerships with a variety of stakeholders while exercising maturity, tact, confidentiality and discretion.
- Ability to function in a highly dynamic environment, including working under pressure, adapting and responding to changing priorities and meeting deadlines.
- Ability to keep skill set up-to-date with new technologies as they are introduced to the workplace.
- Excellent facilitation, coaching, conflict management, planning and interpersonal skills, with the capability of providing leadership and interacting comfortably with a variety of disciplines at all levels of the organization.
- Ability to assess complex situations and make appropriate recommendations.
- Excellent written and oral communication skills coupled with the ability to write or edit high quality business documents.
- Ability to utilize both analytical skills and conceptual thinking to identify and resolve issues.
- Ability to work independently and effectively under time pressure to meet deadlines, balance work priorities and resolve issues appropriately.
- Demonstrated superior organizational, time management , listening and recording skills.
- Use of a personal vehicle to travel between multiple sites.
- Physical ability to perform the duties of the job.