NON-CONTRACT ROLE DESCRIPTION

JD4745

ROLE TITLE:	Senior Information Security Specialist	**ROLE DESCRIPTION NO.:**	4745
DEPARTMENT:	Information Management/Information Technology - Information Security	**HEABC REFERENCE NO.:**	18721470
REPORTING TO:	Director, Information Security	**HSCIS CODE:**	05099
CLASSIFICATION:	NCEM/Range 9	**JOB CODE:**	91346

ROLE SUMMARY

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

Reporting to the Senior Manager, Security Advisory Services, the Senior Information Security Specialist is a subject matter expert in information security standards, practices, industry trends and technologies. This position understands and anticipates information security and information management trends that could affect both local as well as cross-health sector initiatives and develops strategies and work plans to ensure the organization remains current and operates in accordance with legislative and other regulatory obligations. Functions as a lead resource in the development of tools and processes for assessing the organizational security risks associated with the deployment of information technologies.

Responsible for leading and conducting investigations, resolving security-related incidents, designing and implementing security related processes and practices across the organization.

Travel may be a requirement of this position. Transportation arrangements must meet the operational requirements of Island Health in accordance with the service assignment and may require the use of a personal vehicle.

DUTIES AND RESPONSIBILITIES:

1. Participates as a member of the IM/IT leadership team in providing research and direction related to the implementation of the strategic design, tactical and operational plans required to support the effective daily use and future evolution of all Island Health information systems and infrastructure.

2. Oversees the research, design and integration of new and upgraded security technologies by monitoring and analyzing industry trends and best practices, manufacturer design and implementation standards, and Island Health project requirements all to ensure successful integration to Island Health's environment and the continued protection of Island Health information assets and infrastructure.

3. Defines Security requirements, and provides expert research, analysis and advice, for Island Health strategic initiatives projects involvement information management and /or the deployment of information technology solutions ensuring alignment with Island Health security policy, practices, legal and regulatory obligations.

4. Reviews and assesses complex information systems architectures, designs and control specifications by conducting formal Security Threat and Risk Assessments (STRAs) and Security Assessments (SAs). Assess such design for legal and regulatory compliance gaps and risks. Communicate effectively with senior management and Island Health executive where such designs fail to meet legal and regulatory requirements or where the level of associated risk exceeds organizational risk tolerance.

5. Develops and maintains the tools and organizational processes required for conducting security risk assessments (STRAs and SAs).

6. Communicates, both verbally and in writing, with senior management, physicians and internal staff to provide interpretation and expert advice on adherence to legislation, international and eHealth information management standards and principles related to information security. Takes immediate and appropriate action as required on critical or escalated issues related to Information Security technologies.

7. 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.

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

9. Works closely with other Health Authorities, the Provincial government and other contracted vendors, manufactures and service providers to ensure that required Information Security standards and best practices are discussed and Island Health's desired outcomes are delivered. Recommends specific courses of action to address issues, gaps or opportunities.

10. Represents Island Health at provincial meetings and technical working groups as it pertains to Information Security.

11. Works closely with Island Health Privacy personnel, other Health Authorities and the Provincial government to create harmonized educational material and programs that promote Security and Privacy best practices, and ensure education and compliance with system security policies and procedures.

12. Manages and works closely with cross-IM/IT project, technology and research teams to produce technology designs and deliverables, based on Island Health's organizational priorities and requirements that are high quality, highly available and are on time and on budget, and also ensure adherence to Island Health's Privacy and Security standards.

13. Represents Information Security at the Architectural Review Board to ensure all new technologies and information systems being implemented at Island Health meet the organizational architectural standards including Privacy and Security requirements.

14. Develops, issues, and evaluates Requests for Proposal related to the provision of end-user computing equipment and services.

15. Works with external service providers to negotiate contract terms, change orders and pricing, resolve complex service issues and enhance and expand existing services.

16. Provides expert guidance to staff at all levels of the organization and takes a lead role in ensuring information security is considered throughout the design or re-design of programs services and projects and initiatives.

17. Manages assigned staff by selecting employees, directing, supervising, and evaluating staff to ensure effective performance of duties, promoting, disciplining and initiating employee terminations.

18. 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.

19. 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 Island Health. Prepares and delivers presentations to key stakeholders, management and staff.

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 at least seven (7) years' experience in a large information technology services environment. Active CISSP, CCSP, CISM, SANS GIAC, or Security + certification with healthcare experience preferred.

Skills And Abilities

- Advanced understanding of information security, governance and eHealth practices and trends, related legislation and requirements, provincial eHealth and clinical information systems.
- Demonstrated understanding of information security principles and controls to support risk management identification in electronic systems
- Demonstrated ability to review and assess complex information systems architectures, designs and control specifications, assess such design for compliance and risk, and communicate effectively with senior management and executives where such designs fail to meet legal and regulatory requirements or where the level of associated risk exceeds organizational risk tolerance.
- Comprehensive knowledge of networking concepts and core security technologies including firewalls, anti-virus, intrusion detection/prevention, monitoring/reporting.
- Knowledge of FIPPA, ISO 27002, ISO 27017, and the BC Government Information Security Policy preferred.
- Demonstrated ability to problem solve with a global perspective in order to incorporate the organization's systems and strategies when developing viable solutions to problems
- Demonstrated ability to establish and maintain effective partnerships with a variety of stakeholders while exercising maturity, tact, confidentiality and discretion
- Demonstrated ability to function in a highly dynamic environment, including working under pressure, adapting and responding to changing priorities and meeting deadlines
- 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
- Demonstrated 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
- Demonstrated ability to utilize both analytical skills and conceptual thinking to identify and resolve issues.
- Demonstrated 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
- Physical ability to perform the duties of the job.