**SENIOR INFORMATION SECURITY ANALYST**

**Information Security Systems Analysis:**

* Develops and executes security controls, defenses and countermeasures to intercept and prevent internal or external attacks or attempts to infiltrate company systems (e.g., email, data, e‐commerce and/or other internal or external customer facing systems, integration of information security with back up process and disaster recovery, etc.)
* Researches attempted and/or successful efforts to compromise systems security and designs countermeasures
* Monitors, maintains and provisions hardware, software, network firewalls and other security devices, and encryption systems including key management and encryption software
* Administers security policies to control physical and virtual access to systems, encryption of sensitive and confidential data, software patching, security penetration tests and other policies enforced by infrastructure components
* Provides input to management on the acquisition of the new hardware and/or software required to meet new regulatory functions or to handle the expected load increases
* Provides information to management regarding the negative impact on the business caused by theft, destruction, alteration, or denial of access to information

**Information Security Compliance, Design & Administration:**

* Monitors and administers information security processes and policies
* Completes customer and vendor assurance projects
* Works with systems or applications teams to understand compliance requirements
* Coordinates and analyzes compliance with regulations
* Analyzes emerging technology trends with security vendors and subject matter experts
* Helps to designs and architect new information security infrastructure solutions
* Designs and/or adapts security policies

**Job Level Summary:**

* Acts as a resource for colleagues with less experience
* Requires specialized depth and/or breadth of expertise
* Interprets internal and/or external business issues and recommends best practices
* Solves complex problems
* Takes a broad perspective to identify innovative solutions
* Works independently, with guidance in only the most complex situations
* May lead teams or projects

**Key Responsibilities:**

* Designs and architect’s new information security infrastructure solutions
* Leads, architects and designs new solutions to security related issues (e.g., key management infrastructure design)
* Leads more complex and/or cross-departmental information security projects from end to end; establishes and recommends a process and implements logistical aspects of the project (e.g., across McKesson policy development and/or development of security
* Gathers information to develop and document security requirements from the perspective of compliance, best practices and emerging trends across application families
* Designs and performs/coordinates audits and tests and summarizes/escalates findings; recommends and approves remedial actions
* Leads, architects and designs new solutions to security related issues (e.g., key management infrastructure design)
* Develops, documents, trains and leads teams in the execution of security controls, defenses and countermeasures to intercept and prevent internal or external attacks or attempts to infiltrate company systems (e.g., email, data, ecommerce and other internal or customer facing systems), as well as assists in the execution of the procedures
* Acts as a SME for teams developing processes for the monitoring, maintenance and provisioning of hardware, software and network firewalls and other security devices, and encryption systems including key management and encryption software as well as supporting the monitoring, maintenance and provisioning
* Partners with the business to understand business process requirements and recommends information security and data privacy policies (e.g., Reviewing application product designs from business unit development teams to advise on coding and implementation security considerations)
* Works with application teams to develop requirements and develops processes and procedures and/or optimizes existing workflows to guide activities of lower level analysts (e.g., supporting various security shared services); develops policies and endorses exceptions; recognized as an internal SME
* Leads more complex and/or cross-departmental information security projects from end to end; establishes and recommends a process and implements logistical aspects of the project (e.g., across McKesson policy development and/or development of security

**Education:**

* 4‐year degree in computer science or related field or equivalent experience
* 6+ years’ experience in administering security controls in an organization

**Key Differentiators:**

* Applies advanced knowledge, integrated with experience to design solutions across a range of products/areas and businesses
* Detailed knowledge of networking, database design, programming & scripting
* Advanced knowledge of products, platforms, systems, and/or processes supported and integration with other systems and processes
* Advanced knowledge of standards and information security policies in own and related areas
* Advanced knowledge in more than one security domain; broad knowledge of other security domains
* Advanced knowledge of industry specific, healthcare sector regulations appropriate for the business unit supported (e.g. HIPAA, ISO27001, etc.)
* Leverages specific industry and McKesson business knowledge to achieve work results
* Leverages technical and business knowledge to effectively plan and manage projects