SENIOR INFORMATION SECURITY ANALYST IN RICHMOND, VA

Job Description

Senior Information Security Analyst

Description:

This position will conduct information security risk assessments for VCU Health in order to ensure that information security risks associated with internal and external relationships are within acceptable tolerances. In addition, she/he will help VCU Health develop new business and maintain existing customer relationships by responding to requests from external parties concerning VCU Health's own information risk management practices.
Responsibilities
• Determine information security risk profiles for various vendor and business partner services using questionnaires and knowledge of VCU Health policy and relevant industry best practices and standards.
• Clearly and professionally communicate information security risks associated with internal and external services to VCU Health business unit personnel and business leaders.
• Assess external party information security controls to ensure they meet or exceed VCU Health information security risk management requirements for the services to be provided.
• Recommend and drive solutions to eliminate, reduce, or mitigate risk, and communicate said solutions to both external parties and internal business stakeholders.
• Record pertinent documentation and communications for all assessments in VCU Health information technology (IT) governance, risk, and compliance platform.
• Report status of engagements to Information Security management, project managers, and other business stakeholders as appropriate.
• Respond to incoming requests from external parties for information concerning VCU Health information security practices by providing appropriately scoped and accurate information in a timely and professionally written manner.
Education
• Bachelor’s Degree or equivalent work experience (4 years of experience in lieu of Bachelors)
Experience
• 6 - 8+ Years of experience in IT audit, information security, information systems compliance, or information risk management that directly aligns with the specific responsibilities for this position. (Required)
• Possession and continual application of the following character traits: dependability,

integrity, decisiveness, tact, courage, enthusiasm, and sound judgement.
• Working knowledge of common information security concepts, practices, and technologies, including best practices for:
o Network defense and secure network design
o Network, operating system, and application vulnerability management
o Secure software development
o Cloud Technologies
o Logging and monitoring
o Identification, authentication, and authorization mechanisms
o Account provisioning, review, and de-provisioning
o Data loss prevention
• General knowledge of industry standard security frameworks, including the NIST Cybersecurity Framework.
• General knowledge and understanding of regulatory compliance mandates concerning data protection, including HIPAA and various state laws and regulations.
• General knowledge of IT audit and assessment concepts and practices.
• General knowledge of common web application vulnerabilities preferred.
• Industry certification preferred, including but not limited to CISSP or CISM.of understanding of System Security Plans (SSP)

Send Resume to info@intellectualpoint.com job.