



Classification: Computer Information Technology Specialist II (CITS II)
Information Security Unit - Application Security

Title Code: V08005

Pay Range: 33

POSITION SUMMARY:

This position provides professional and advanced technical expertise as it relates to application security. The position works closely with the Information Security Officer as well as staff within the Missouri State Highway Patrol's troops and divisions, and local criminal justice agencies by providing guidance and technical expertise on highly complex information security issues and deployments. This position also assists the Information Security Officer with creating, designing, implementing and maintaining a state wide information security program for the criminal justice community. This position performs application security related functions including static and dynamic code analysis and provides guidance to application development teams on secure coding practices throughout the software development lifecycle. An employee in this position performs peer level reviews of products produced by other personnel and acts as a key member of the Patrol's security incident response team. This position reports to the Information Security Officer and works under general supervision, but is expected to use extensive technical knowledge and initiative to meet goals and objectives.

DESCRIPTION OF DUTIES PERFORMED:

(Any one position may not include all of the duties listed nor do the listed examples include all tasks which may be found in positions of this class.)

Performs highly technical analysis of application development project plans and associated source code and platforms; provides guidance to project managers and project development teams on secure coding practices; acts as a subject matter expert in the area of application development security and secure coding practices and software development.

Reviews new and legacy applications for vulnerabilities, providing vulnerability assessments and mitigation recommendations.

Provides support to both MSHP and partners in regards to implementing highly complex cybersecurity issues.

Performs administrative duties over security control/protections related to application security.

Assists in investigating security incidents and incident response.

Assists with preparing and participating in presenting cybersecurity information through written documentation and oral presentation to different types of audiences; this includes meeting with technical and business staff of criminal justice agencies

Provides guidance on security requirements for RFPs, grant applications and applicable security policy development.

Performs programming and application development, creating and developing reports and forms as needed.

Documents, reviews, and updates security policies and procedures for MSHP and local agencies by reviewing, interpreting and applying industry standards as well as local, state and federal statutes and regulations

Participates in computer systems disaster recovery plan maintenance and implementation for MSHP.

Performs security testing and monitors the MSHP security infrastructure.

Classification: Computer Information Technology Specialist II (CITS II)
Information Security Unit - Application Security

Title Code: V08005

Pay Range: 33

Page 2

Meets with members of the local and state criminal justice community to discuss cybersecurity issues.

Assists in the research and review of security infrastructure hardware and/or software.

May act as a lead worker to other personnel as it relates to application security.

Performs other related work as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES:

Extensive knowledge of the principles of information security and information technology systems analysis, design, testing and documentation.

Extensive knowledge of the general operating principles and capabilities of computer hardware and software.

Extensive knowledge of secure coding practices and the secure software development lifecycle.

Thorough knowledge of the elements of cybersecurity as well as networking, application development, server software and hardware.

Thorough knowledge of software reference libraries and related utility programs.

Thorough knowledge of computer security best practice standards.

Thorough knowledge of computer networking protocols.

Thorough knowledge of computer operating systems.

Thorough knowledge of data protection methods.

Working knowledge of various software coding languages.

Working knowledge of national information sharing tools and techniques.

Working knowledge of agency's functions and their interrelationships.

Working knowledge of the principles of cost benefit analysis.

Working knowledge of the principles of project management.

Working knowledge of the principles of disaster recovery.

Working knowledge of continuing trends and developments in information technology and cybersecurity.

Working knowledge of various computer platforms.

Working knowledge of the information strategic planning process.

Working knowledge of the systems management process.

Classification: Computer Information Technology Specialist II (CITS II)
Information Security Unit - Application Security

Title Code: V08005

Pay Range: 33

Page 3

Possess good organizational skills.

Possess research and analysis skills.

Possess basic code analysis skills.

Ability to utilize highly technical analytical tools.

Ability to prepare and interpret system configuration documentation.

Ability to prepare and maintain standards, policies, procedures, guidelines and technical manuals.

Ability to handle restricted and confidential information in a professional manner and maintain the information as such.

Ability to communicate in English clearly and concisely, both orally and in writing.

Ability to establish and maintain harmonious working relations with others.

Ability to work with material that may be of a sexual nature relating to criminal activity (e.g., written material, photographs, and/or verbal language, etc.)

Ability to create and present materials for training programs.

Ability to work hours as assigned.

MINIMUM EXPERIENCE AND EDUCATION REQUIRED:

(The following represents the minimum qualifications used to accept applicants, provided that equivalent substitution will be permitted in case of deficiencies in either experience or education.)

Possess a Bachelor's degree from an accredited four-year college or university in Information Security, Cybersecurity, Information Assurance, Information Systems, Computer Programming or a related field; AND five years of experience in the areas of information security, cybersecurity, or information assurance fields.

Preference may be given to those possessing current certification(s) in Information Security and/or work experience and knowledge in all areas of application security, to include: security coding practices, secure SDLC, legal requirements, privacy policy, AAA principles, OSWAP standards, SQL databases, web and application development, and the concepts vital to ensuring confidentiality, integrity and availability of protected data and systems.

NECESSARY SPECIAL REQUIREMENTS:

Must be a United States Citizen, or a legal resident of a country participating in the Visa Waiver Program (VWP).

Must possess and maintain a MULES Certification within one year of hire.

Classification: Computer Information Technology Specialist II (CITS II)
Information Security Unit - Application Security

Title Code: V08005

Pay Range: 33

Page 4

FLSA STATUS: Partial-exempt

WORK SCHEDULE: An employee in this position works an eight-hour shift as directed; however, working hours are subject to change at the discretion of the commanding authority.