



Job Description

Job Title: District Coordinator, Information Privacy & Security JTC: DAS

Salary Range: N06

FLSA: Exempt

Since 1965, we have served more than 3 million students. Dallas County Community College District (DCCCD) is one of the largest community college systems in the state of Texas, which includes seven independently accredited colleges located around the Dallas/Fort Worth area.

POSITION SUMMARY

Responsible for assisting the Chief Information Privacy and Security Officer, in initiating, developing and maintaining an information privacy and security conscious culture and infrastructure for the Dallas County Community College District. This will include assistance with developing and administering the District's information privacy and security policy, strategy and vision, assessing privacy and security risks, and coordinating information privacy and security efforts across the District. Information Privacy and Security includes physical and verbal, as well as electronic use and storage of information.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES

Knowledge of Information Technology systems, Federal and State Information Privacy Laws, and IPSO applications, common to higher education environments. Ability to understand the risk management element of IPSO and the management of risk in a business, or higher education environment.

Ability to exercise strong analytical and critical thinking skills, with strong attention to detail and accuracy with the ability solve critical problems. Ability to succeed in a busy environment, where multi-tasking is essential, and the quality of work must not be compromised. Ability to work independently and with limited supervision.

Demonstrated ability to collaborate and build professional working relationships in a diverse environment. Excellent time management and organizational skills to fulfill the mission and goals of the organization.

Ability to utilize computer technology to access data, maintain records and generate reports. Must have strong conflict resolution and project management skills. Ability to analyze information, research and make timely decisions. Desire and ability to quickly learn about the activities and specificities of the unique business model, advanced technology capability and evolving regulatory environment.

Ability to interpret technical information and communicate to users with varying levels of technology literacy. Communicate effectively both verbally and in writing, as well as establishing and maintaining effective working relationships, with a wide variety of external professionals and in-house staff from diverse backgrounds. Strong knowledge and experience providing effective customer service.

PHYSICAL REQUIREMENTS

Normal physical job functions performed within a standard office environment. Reasonable accommodations may be made to individuals with physical challenges to perform the essential duties and responsibilities.

MINIMUM KNOWLEDGE AND EXPERIENCE

Bachelor's degree or higher in related field plus three years of related experience in a complex multi-location environment. Official transcripts will be required. *** Will be subject to a criminal background check. Some positions may be subject to a fingerprint check. ***

ESSENTIAL DUTIES AND RESPONSIBILITIES

Responsible for supporting, developing, initiating and maintain an information privacy and security conscious culture and infrastructure for DCCCD. Assist with developing and administering the districts information privacy and security efforts across the district. Identify policies and procedures and programs designed to identify and mitigate risk associated with district security.

Conduct cybersecurity risk assessments covering district assets that could be affected by a cyber-attack and reduce those risks through collaboration, technical controls, training/education and development of programs and materials. Responsible for providing professional and comprehensive direction to all district locations on best practice, that will mitigate security risks as well as monitor trends and provide direction to other compliance professionals. Utilize computer technology to access data, maintain records and generate reports.

Responds to internal and external requests, which may include researching and analyzing data and replies, making recommendations within approved policies and procedures and approved channels. Identifies district-wide organizational needs and establishes working relationships with all functional areas of the district in support of security awareness program goals. Assists in the prioritization of initiatives; keeps management abreast of status of initiatives and maintains overall focus on completion of initiatives.

Provides leadership and guidance to a variety of staff, outlining compliance requirements and best practices. Assists with monitoring and evaluating program effectiveness; including but not limited to, working with Internal Audit and/or other personnel both internal and external to the organization as appropriate and on required security audits. Works with Risk Management and/or other personnel both internal and external to the organization as appropriate, on the information privacy and security incident response model. Ability to handle multiple projects consecutively, while meeting objectives and timetables.

Must complete required DCCCD Professional Development training hours per academic year. Must have excellent communication skills and the ability to interact with diverse internal/external stakeholders and constituents within the DCCCD community network.

Performs other duties as assigned.

The intent of this job description is to provide a representative summary of the major duties and responsibilities performed by incumbents of this job and shall not be construed as a declaration of the



total of the specific duties and responsibilities of any particular position. Incumbents may be directed to perform job-related tasks other than those specifically presented in this description. Position requires regular and predictable attendance.