



Job Description

Job Title: Chief Information Privacy and Security Officer (CIPSO) JTC: AJY

Salary Range: E07 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

The chief information privacy and security officer (CIPSO) is charged with the responsibility for building and maintaining an information privacy and security-conscious culture and infrastructure for the Dallas County Community College District, including 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. The CIPSO owns the District's awareness and training program for information privacy and security.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES

Proven work experience as a Chief information Privacy and Security Officer. Knowledge with computing systems, networking, and applications common to higher education environments. Capable of establishing a privacy framework and compliance structure. Understanding of new and existing compliance issues and related policies and procedures.

The ability to identify potential areas of compliance vulnerability and risk; develops/implements corrective action plans for resolution of problematic issues and provides guidance on how to avoid similar situations in the future. Ability to monitor the performance of the Compliance Program and related activities on a continuing basis, taking appropriate steps to improve its effectiveness.

Ability to establish and maintain positive working relationships in a diverse community, both internally and externally, to achieve the goals of the organization. Demonstrates strong leadership qualities and team building.

Capable of assessing situations to determine the importance, urgency and risks, and make clear decisions which are timely and in the best interests of the organization. Experience responding to alleged violations of rules, regulations, policies procedures, and Standards of Conduct by evaluating or recommending the initiation of investigative procedures. The ability to balance business objectives while interpreting the privacy practices is fundamental.

Ability to interpret technical information and communicate to users with varying levels of technology literacy. Ability to communicate effectively both verbally and in writing 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

Master's degree or higher plus four (4) year of related experience, including supervision, in a complex multi-location environment. Security certification/accreditation, such as CISSP is desirable. Requires a valid driver's license to enable travel within the college and service locations. 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

Manages the development, implementation, and maintenance of the District's information privacy and security policy, standards, and guidelines. Serves as an expert advisor to the District's senior management in the development, implementation, and maintenance of an information privacy and security infrastructure. Identifies key privacy and security program elements and coordinates whichever departments or offices throughout the District locations must be involved in building a comprehensive information privacy and security program.

Performs the functions necessary to administer the Texas Administrative Code – Information Security Standards. Stays abreast of federal, state and local laws, regulations and standards pertaining to the protection of student and employee information and determines their effect on the District to comply. Provides guidance and advocacy regarding prioritization of infrastructure investments that impact privacy and security. Chairs the District's Information Privacy and Security Program Strategic Steering Committee.

Acts as the primary control point during significant information privacy and security incidents. Develops guidelines and procedures to ensure that departments consider information privacy and security risks in both ongoing and planned operations, including purchases of new software. Collaborates with and provides leadership to location privacy and security officers. Monitors information security trends internal and external to the District and keeps District senior management informed about information privacy and security-related issues and activities affecting the organization.

Understands potential threats, vulnerabilities, and control techniques and communicates this information to location information privacy and security officers. Assists locations as necessary to investigate security breaches and pursues associated disciplinary and legal matters. Works with Internal Audit and/or other personnel both internal and external to the organization, as appropriate, on required security audits. Develops an information privacy and security awareness and training program. Works with locations and the Purchasing Department to create selection criteria for vendor products, tools, and services related to information privacy and security.

Monitors and reports regularly on District-wide information privacy and security activities and compliance as well as the effectiveness of the program. Considers physical and verbal as well as electronic use and storage of information in formulating policies and procedures. 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.

Supervises departmental staff and manages departmental budget.

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.