

Position Available

POSITION TITLE: Director, Information Policy & Security Education, Duke University

JOB CODE: 2417

JOB BAND: Band E

JOB FAMILY: 08 (Information Technology)

WORK SCHEDULE: Normal hours worked

DEPT CONTACT: Scooter Freeney (scooter.freeney@duke.edu)
681-8034

SUMMARY:

The Director, Information Policy & Security Education reports jointly to Duke University and Health Systems' two Chief Information Officers and is overseen by the Information Security Steering Committee. The Director has enterprise-wide responsibility and authority regarding matters of information policy, security education and communications. The Director works collaboratively with representatives from Information Security, Legal, Internal Audit, Institutional Ethics and Compliance and central and distributed IT leaders across the campus and health system, to develop policies and best practices which ensure a secure IT environment. This position is responsible for developing and leading institutional efforts to educate faculty, staff and students regarding information policies and processes. Additionally, the Director provides strategic direction and guidance in the design and implementation of appropriate processes and controls to ensure appropriate and effective execution of information policies. The Director collaborates with appropriate technical and business leaders on risk assessment efforts, as requested. In addition to leading and directing Duke's policy development and education activities, the position plays a critical consultative role in other matters of information security (policy implementation, monitoring, assessment and reporting).

DUTIES AND RESPONSIBILITIES:

- Develops institutional policies and best practices to ensure information security and compliance with regulatory or other requirements; works collaboratively with designated officials from Duke's Legal, Internal Audit, Institutional Ethics and Compliance and Campus Police offices (and applicable health system counterparts), along with IT departments, to understand the regulatory and legal environment and its implications for Duke; ensures adequate processes for implementing consistent

policies are in place and documented and acts as coordinator between these groups on matters pertaining to information security policy and education

- Ensures appropriate risk management and compliance standards are developed and in place across the institution; takes a leadership role in driving the creation and implementation of system security and planning standards where they do not exist, and in ensuring the adequacy of those already in place; recommends and implements appropriate policies for systems procurement to ensure desired departmental or central systems meet the established systems security planning standards
- Develops and administers institution-wide information security education and training programs, ensuring institutional awareness of specified information policies; collaborates with information security leaders and specialists across the campus and health system on information security activities; communicates information security concepts and policies to senior leadership, making recommendations for changes as appropriate
- Serves as the liaison to Duke's business owners (administration, faculty and senior staff) with respect to matters of information security policy, systems security standards and education; ensures full communication to these business owners of relevant risk management and compliance standards in place at Duke
- Working with the campus and health system Chief Information Security Officers (CISOs), participates in ongoing assessment functions which categorize areas of risk within the institution, evaluates organizational risk levels and recommends actions appropriate to the level of risk (likelihood and impact); collaborates with information security leaders to determine appropriate elements and categories needed in a prioritized vulnerability scan program; works closely with Internal Audit and Institutional Ethics and Compliance to develop effective methods for educating the Duke community on both Duke-specific policies as well as those mandated by federal, state or local regulatory agencies
- Consults with information security specialists and other technical staff across the campus and health system on best practices for systems monitoring for purposes of understanding capabilities and limitations of Duke's current deployments with respect to risk abatement, to assist in future policy development or adjustments to existing policies
- Tracks industry and higher-education policy developments and best practices to maintain a thorough understanding of current and future directions, evaluating the need for similar policies or processes at Duke
- Maintains a close and effective working relationship with the Associate Vice President, Federal Relations, gaining a solid understanding of the current regulatory environment to ensure Duke's information security policies are in full compliance with federal, state or other regulatory requirements

SUPERVISORY RESPONSIBILITIES:

N/A

MINIMUM EDUCATION AND EXPERIENCE:

- Bachelors degree in communications, business and/or information management, or related field, or equivalent experience; Law or similar advanced degree preferred
- Seven to ten years current experience directly related to the duties and responsibilities specified. Experience in higher education, health system or a research environment is preferred.

KNOWLEDGE, SKILLS, AND ABILITIES REQUIRED:

- Broad knowledge of computer security issues, policies, requirements and trends
- Understanding of information security laws (including HIPPA, FERPA, GLBA, CALEA, PCI and Sarbanes-Oxley), and accepted industry practice; knowledge of NC Identity Theft Protection Act a plus
- Ability to translate technical security issues and risks to executives, as well as to non-technical staff and students
- Very strong interpersonal and communication skills, and the ability to achieve goals by collaboration and cooperation
- Ability to work effectively with a wide range of constituencies in a community that is both demographically and technologically diverse
- Previous experience developing policies, process documentation and compliance procedures, preferably in a higher ed or health system environment
- Proven ability to develop and present educational programs, awareness campaigns and/or workshops
- Knowledge of current technological developments/trends in area of information security policies and practices
- In-depth knowledge of information security issues and leading practices, especially as they apply to the university or health system environment

WORKING CONDITIONS

Normal office environment.

DATE of POSTING:

June 20, 2008

Pos#: 50470079

Req#: 400216078