Duke University Job Description

Position Title: ASSISTANT DIRECTOR E-COMMERCE COMPLIANCE – Remote Work

Contact: Director, Electronic Commerce, christa.stilleypoe@duke.edu

This position is fully remote. All Duke University remote workers must reside in one of the following states or districts: Arizona; California; Florida; Georgia; Hawaii; Illinois; Maryland; Massachusetts; Montana; New Jersey; New York; North Carolina; Pennsylvania; South Carolina; Tennessee; Texas; Virginia or Washington, DC.

This position reports to the Director, Electronic Commerce and has a significant role in the Payment Card Industry – Data Security Standard (PCI-DSS) compliance activities for Duke University and Duke University Health System. This person will ensure corporate governance and adherence to PCI-DSS compliance, a vital service for merchants who depend on payment card transactions.

Provide leadership and guidance for Duke merchants in all aspects of the PCI-DSS with emphasis on safeguarding sensitive data, thus protecting the interests of the cardholders and business units, and the overall University brand.

Work with representatives of University and third-party vendors to ensure compliance with the PCI-DSS requirements for all payment card processing, and the Duke-related policies, technical security processes, infrastructure, and long-range planning requirements.

Serve as central resource for merchants to leverage expert knowledge on PCI-DSS. Assist with the development and maintenance of detailed compliance instructions to interpret PCI standards as relates to the Duke environment to ensure a consistent approach.

Manage annual PCI-DSS education process to ensure the mitigation of risks (training, self-assessment questionnaire, action plans, etc.). Provide guidance on Duke's policies and resources as relates to the PCI requirements. Manage and maintain a required online security awareness training program for all eligible staff and affiliates.

Assist the Director in defining, enforcing and administering centrally defined framework of policies, standards and guidelines for Duke University. Consult with merchants on the development and implementation of appropriate internal controls, including the department's related policies and procedures and supporting compliance documentation. Coordinate mitigation strategies for non-compliant issues.

Maintain up-to-date knowledge of payment card processing technologies, understanding technical developments and industry trends related to the payment card industry; assess risk, cost, and benefit.

Manage QSA (Qualified Security Assessor) relationship at corporate sponsor level to assess all Duke merchants' compliance status. Define and maintain an electronic PCI-DSS SAQ (Self-Assessment Questionnaire) schedule and external scans for all merchants within the QSA system. Analyze merchants' PCI SAQs, vulnerability scans and other supporting documentation for accuracy, completeness, and overall compliance.

Assess Duke's PCI-DSS compliance status as outlined by the specific PCI-DSS requirements, Duke framework of policies, and Duke's contracted QSA, including but not limited to merchants' vulnerability assessments, penetration testing, application assessments, wireless assessments, and security and network architecture reviews.

Direct merchant owners in developing the PCI-DSS required documentation for existing infrastructure to identify data flows and critical support systems (i.e. network diagrams, server standard, data retention and disposal policy, system locations/contacts, and related internal policies and procedures). Ensure merchants have a change management regime so all changes or additions to the infrastructure can be readily assessed for impact and security issues, creating a controlled change environment.

Manage Duke's secure network segment implemented for the exclusive purpose of processing credit cards. Responsible for maintaining approved access accounts. Coordinate bi-annual review of firewall

rules by IT Security. Initiate quarterly review of access account with merchant owners. Maintain a current inventory of all devices in the segmented network and ensure quarterly vulnerability scans are performed. Approve all requests for access and changes to the firewall rules.

Assist Director in coordinating compliance processes with DU and DUHS' Security Offices, OIT, Procurement, Corporate Risk Management, the Office of Internal Audit and other constituents to ensure compliance with PCI-DSS.

Complete an annual risk assessment of all merchants. Manage follow-up of all issues to ensure compliance with PCI-DSS requirements and Duke framework of policies. Develop informational and actionable reporting for non-compliant merchants. Direct appropriate actions and remediation steps. Serve on compliance working committee(s) as needed to follow-up, document and consult on action plans.

Provide regular reporting to Director on audit findings and issues. Apprise Director of potential risks, security, and policy violations as related to the merchant credit card processing and technology.

Perform other related duties incidental to the job described herein.

Education / Training: Work requires the organizational, analytical and communication skills normally acquired through the completion of a bachelor's degree program. Work requires a minimum of five years in a business or information technology field. Candidates with experience in the following areas are favorable:

- Technical and security audit and assessment experience and knowledge of PCI-DSS.
- Experience with financial/payment systems, electronic commerce. Strong understanding of payment processes, related systems, and PCI DSS.
- Experience with data security practices.
- Customer-facing experience in an IT environment.
- One or more industry-recognized information security or audit certifications (PCI ISA, CISSP, CISM, CISA, GSNA, IRCA, ISMS Auditor, or similar)

Skills:

- Excellent ability to communicate both verbally and in writing with all levels of an organization, including both business and technical audiences.
- Demonstrated leadership skills and ability to pull cross-functional teams together to determine short-term and long-term objectives and set priorities
- Self-motivated with interpersonal skills required to work effectively with a broad range of employees and external contacts
- Ability to manage and prioritize multiple projects/tasks simultaneously
- Understanding of information security concepts/practices. Ability to define and articulate security requirements
- Ability to query complex databases, prepare analyses, and create verbal and written reports
- Proficient use of computers; requires solid working knowledge of MS Office Suite (Word, Access, Excel, Power Point), html editing, etc.
- The candidate must be analytical, detail oriented, possess strong data management and technical skills, as well as superior customer service and organizational skills.