Class Code:…………0847
Position #:(NUNC)……….
Developed by:…………GB
Reviewed by:…………..SG
Approved by..…………LK
Date:…………………..2/08

UNIVERSITY OF RHODE ISLAND

Position Description

TITLE:	Associate Director, Information Security
DIVISION:	Academic Affairs (ITS)
REPORTS TO:	Vice Provost for Information Technology Services
GRADE:	16
SUPERVISES:	Supervises professional, technical and support staff as assigned

BASIC FUNCTION:

Reports to the Vice Provost for ITS and works directly with all campus departments including ITS to coordinate security efforts and resources to maximize information security. Advise the Vice Provost on security-related practices and policies to mitigate information security-related risks to the University's information systems and networks. Serve as the university's primary responder to technology-related incidents involving the suspected compromise of university networks, computing, or electronic information. In the course of investigating, restoring, and advising the campus on information security, the Associate Director for Information Security regularly has access to highly sensitive and confidential information such as personal email files, electronic personnel files and actions, and all manner of administrative data in potentially any office on campus including all top administrators such as the president, provost, all vice presidents, deans, and directors. Such access requires the University's highest level of confidentiality and security.

ESSENTIAL DUTIES AND RESPONSIBILITIES:

Serve as the University's primary technical contact regarding the security of information systems and networks, which includes coordinating activities with University users and campus network and system managers (including ITS). Serve as the University's Registered Agent for notification regarding the Digital Millennium Copyright Act (DMCA).

Serve as the University’s primary responder to computer incidents.

Manage forensic requirements for campus users and IT systems.

Perform as liaison to the University Legal Counsel involving law enforcement, subpoenas, warrants, and other legal issues related to technical data or systems.

Provide technical guidance and facilitate the development of disaster recovery and business continuity plans, tests, and policies.

Advise, develop, create and maintain information security policies for the Vice Provost of ITS and University.

Evaluate campus technology security, developing technical and operations recommendations and solutions, concerning hardware, software and procedures.

Implement and coordinate proactive efforts for the University’s information systems and networks to mitigate information security risk.

Conduct internal audits of information technology systems and services using industry best practices, applicable laws and University policies.

Provide information, recommendations, and training to both ITS and University staff on technology security as well as security equipment, procedures, software and the installation of security components.

Establish standards and implement procedures required by State and Federal law and associated regulations to ensure that information systems and networks are compliant such as with: HIPAA, FERPA, ECPA, CFAA, PII, COPA, and TEACH.

Maintain a professional level of expertise and knowledge of the latest technology risks and remedies through external training and seminars, as well as the ongoing review of security literature.

Provide input, and recommendations to the vice provost on issues that have an impact on the University security infrastructure.

OTHER DUTIES AND RESPONSIBILITIES:

Monitor systems and networks for proper security procedures, configurations, software revision levels and signs of compromise or intrusion.

Publish recommended procedures and guidelines for all users of the University's information systems in order to keep incidents of systems from becoming a risk to University network and infrastructure.

Other duties and responsibilities as assigned.

LICENSES, TOOLS AND EQUIPMENT:

Workstations and multiple operating systems, network testing, monitoring and sniffing tools; system and network vulnerability (hacking) tools; CISSP, GIAC or comparable certification; intrusion detection system experience, PKI and certificate management experience; Cisco routers and switches.

ENVIRONMENTAL CONDITIONS:

This position is not substantially exposed to adverse environmental conditions.

QUALIFICATIONS:

Required: Bachelor's degree in computer science, or related field; a minimum six years of information systems experience in progressively responsible roles; an understanding of systems and network administration, including best practices for industry standards; working knowledge of network security technologies such as VPN, firewall, and WLAN as well as computer security technologies for UNIX and PC systems such as antivirus, WLAN security, and middleware; excellent interpersonal skills; ability to work collaboratively with a wide range of technology staff in different units; ability to communicate technical information to non-technical people such as end-users, the media, senior management as well as legal and law enforcement professionals; and guide technical as well as non-technical campus constituents toward increasing their use of best practices regarding information security. Preferred: Master's degree in computer science or related field; direct experience as a manager of information security for an organization; experience in developing information security policies, guidelines, and best practices; CISSP, GIAC or comparable certification; intrusion detection system experience; PKI and certificate management experience; experience with Cisco routers and switches.

ALL REQUIREMENTS ARE SUBJECT TO POSSIBLE MODIFICATION TO REASONABLY ACCOMMODATE INDIVIDUALS WITH DISABILITIES.