**INFORMATION SECURITY ANALYST II**

Position Number: 000TBA Info Security Analyst II

Department: SITIS - Information Security Office

Campus: US:IT

Date: September 2015

1. Primary Purpose of Position:

The Information Security Analyst II is responsible for maintaining the integrity, confidentiality and availability of information systems data resources and automated system components. Primary responsibilities include providing leadership to a security team, partners and clients to prevent, detect, respond and recover from security incidents. Responsible for monitoring compliance with university IT security policy and applicable law; and assisting with the investigation and reporting of security incidents and risk assessment reviews.. Develops user training and awareness through documentation, training and alert notifications.

1. Essential Duties:
2. Respond to alerts and notifications provided by various sources including an external Security Operations Center.
3. Participate in a comprehensive incident response plan and program that regularly involves representatives from various campus offices. .
4. Under the direction of the CISO, Collaborate with IT management, the legal department, safety and security, and law enforcement agencies to manage security vulnerabilities.
5. Participate in the evaluation of proposed systems, applications, and network design to determine security or data integrity implications. Assess risks and identify countermeasures, plan and implement mitigating technologies.
6. Make recommendations and participate in the development and publishing of Information Security policies, standards and guidelines based on knowledge of best practices and compliance requirements.
7. Monitor compliance with policies and standards, appropriately referring problems. Monitor and advise on information security issues to ensure the internal security controls are appropriate and operating as intended.
8. Conduct campus data classification assessment and security audits and manage remediation plans.
9. Audit and test of security control practices to ensure adherence to policy and standards to include penetration testing, software security lifecycle assessment, and threat modeling with internal and external teams to ensure information security compliance is maintained.
10. Coordinate and execute IT security projects.
11. Create, prepare and present user documentation including reference manuals, quick guides and support materials on policy and standards; training materials; web content; and campus/ITS alerts and notifications.
12. Non-essential duties:
13. Conduct security research in keeping abreast of latest security issues.
14. Actively participate in the higher education security community such as Educause, REN-ISAC, ISSA, etc.
15. Perform other related duties as assigned.
16. Supervisory Responsibilities:

This position has no direct supervisory responsibilities. As the position evolves, responsibility for the supervision of part-time student workers is anticipated.

1. Reporting Relationships:

Reports to the Chief Information Security Officer (CISO).

1. Knowledge, Skills, and Abilities:

Knowledge of system management disciplines such as security architecture, disaster recovery and coordination of network intrusion response and documentation.

Knowledge of current, network security issues, and technology developments/trends. Knowledge of the nature and sources of network security threats and methodologies/technical requirements for devising solutions.

Knowledge of industry standards for network security monitoring software and software enhancements.

Excellent communication (oral, written, presentation), interpersonal and consultative skills.

Broad, current knowledge of Internet technologies.

1. Qualifications:

**Required:**

A bachelor’s degree in Computer Science, Management Information Systems, or related field is required or an equivalent combination of education and experience.

In addition to any equivalent experience in lieu of education, five years of experience in computing or information security, including experience with Internet technology and security issues.

Professional experience supporting a network environment, routing, TCP/IP, Internet/Intranet, network security/firewalls and encryption, as well as a variety of operating systems.

CISA or GIAC certification (or a passed test toward certification) will be accomplished within the first two years of employment.

Strong analytical and problem solving skills.

**Preferred:**

A master’s degree in Computer Science, Management Information Systems, or related field or an equivalent combination of education and experience.

# Experience in auditing network security implementation access and violations against policies, procedures, and regulations; performing diagnostics for complex multi-tasking security problem; integrating security controls across service applications; implementing and maintaining vendor supplied security software; participating on disaster recovery planning team.

Experience in security policy development, security education, risk analysis and compliance testing.

Experience in a higher education environment.

Knowledge of information security standards (e.g., ISO 27000 series, NIST, etc.), rules and regulations related to information security and data confidentiality (e.g., FERPA, HIPAA, PCI, etc.) and desktop, server, application, database, network security principles for risk identification and analysis.

CISSP, GIAC, or other security certifications desired.

Experience in network penetration testing, application vulnerability assessments, risk analysis and compliance testing.

**University services reserves the right to assign reasonably related additional duties and change or reassign job duties.**

Signatures: The signatures indicate the employee and immediate supervisor have reviewed the job description and had the opportunity to edit the document.

Employee: Date:

Immediate Supervisor: Date: