**P7: Level Standards**

**GENERAL ROLE**

This level is accountable for serving in an expert resource capacity in an area of specialization. Positions at this level are not reflective of the majority of the workforce, but instead the most complex functions within an area of specialization.

Incumbents:

* Serve in a subject leader and consultative capacity within an area of expertise.
* Provide analytical, technical, and advisory support to leaders and decisions makers within the same disciplinary track.
* Lead projects or initiatives within the specific area of expertise, to include leading vendors or cross-functional departments or teams.
* Research and apply better ways to effectively achieve end results by, for example, arranging/rearranging the way work is performed, changing elements of processes, and adding or deleting new or unnecessary capabilities/functionalities as needed.
* Set project objectives, immediate- and/or long-term, as a means to fulfill project initiatives.

**INDEPENDENCE AND DECISION-MAKING**

*🡪 Supervision Receive*d

* Works under general direction.
* Seeks assistance only when unique situations arise, coupled with financial impact to the division and political consequence.

*🡪 Context of Decisions*

* Work is focused on and regulated by specific department/division goals and milestones.

*🡪 Job Controls*

* Act based on own judgement as long as actions adhere to division policies and operating procedures, and remain focused on the department and division objectives and missions.
* Subject to managerial controls through conferences, review of reports, and occasional on-site visits or check-ins.
* Managerial controls are exercised on the incumbent for matters of intermediate- and long-range planning, budgetary, and human resources based matters.

**COMPLEXITY AND PROBLEM SOLVING**

*🡪 Range of issues*

* Problems are unique and unexpected.
* Challenges for problems arise due to lack of precedent.

*🡪 Course of Resolution*

* Problems require response/adaptation to changing conditions or circumstances, necessitating enterprise and new approaches with broad impacting effects.
* Problem resolution should regularly require collaboration and coordination with units internal to the division, with occasional collaboration and coordination outside the division.

*🡪 Measure of Creativity*

* Incumbents are regularly required to develop new methods/methodology for evaluation and implementation plans for new initiatives.

**COMMUNICATION EXPECTATIONS**

*🡪 Manner of Delivery and Content*

* Deliver statements and information in a combined persuasive and motivational fashion to subordinate staff, departmental and University administrators, and the campus community as a whole.

**SCOPE AND MEASURABLE EFFECT**

* Serve as an expert on specific subject matter evidenced by regularly researching and producing reports (e.g., white papers) on technical matters of systematic importance and consulting with managers throughout the division/University on specific issues in the position’s area of expertise.
* Actions regularly affect a departmental outcome with division-wide impact.
* Actions have a direct impact on controlling such things as project scope, team size and nature of assignments, operating budget, etc.
* Actions may have high-risk financial, compliance, political, or safety implications.
* Performance results tend to be related to efficiency, degree of waste/cost overruns, quality/continuous improvement, timeliness, resource allocation/effectiveness, etc.

**Job Template**

**GENERAL SUMMARY**

Uses data collected from a variety of information security tools and information sources to identify, protect, detect, respond and recover to a variety of threats to the university environment.

**REPORTING RELATIONSHIPS AND TEAMWORK**

Operates under the general direction of the Chief Information Security Officer.

**ESSENTIAL DUTIES AND RESPONSIBILITIES**

*The intent of this section is to list the primary, fundamental responsibilities of the job – that is, the duties that are central and vital to the role.*

* Leads the assessment of environments for known vulnerabilities and assist with remediation efforts.
* Acts as an information steward within the organization with a focus on the confidentiality, integrity, and availability of information.
* Proactively analyzes network traffic, system logs and other sources using security tools to identify threats or incidents within the University.
* Recommends and installs appropriate tools and countermeasures.
* Triages security requests from customers and internal teams.
* Identifies and communicates current and emerging security threats.
* Communicates security best practices to university constituents.
* Performs administrative duties on various components of the Information Security technology stack.
* Leads in forensic analysis and incident response.
* Develops security metrics to proactively monitor cyber threats and provide trend data for reporting.
* Performs related work as required.

**MINIMUM QUALIFICATIONS**

* Associates degree
* Six years of related experience

OR

* Bachelor’s degree
* Four years of related experience

OR

* Eight years of related experience

AND

* Three to five years of experience working in an information security role or supporting an information security program
* Experience in at least one information security domain including: Security Awareness, Vulnerability Management, Cyber-defense, Incident Response and Forensics, or Security Architecture

**COMPETENCIES**

**Knowledge of:**

* Computer networking concepts and protocols, and network security methodologies
* Risk management processes (e.g., methods for assessing and mitigating risk).
* Laws, regulations, policies and ethics as they relate to cybersecurity and privacy
* Cyber threats and vulnerabilities
* Cyber defense and vulnerability assessment tools and their capabilities

**Skill in:**

* Planning and organization
* Troubleshooting
* Developing and maintaining effective and appropriate working relationships
* Critical thinking, problem solving and analysis

**Ability to:**

* Provide technical training and guidance
* Communicate effectively through both oral and written means
* Respect diversity and work collaboratively with individuals of diverse cultural, social and educational backgrounds
* Prepare clear documentation
* Maintain the confidentiality of information and professional boundaries