**P6: Level Standards**

**GENERAL ROLE**

This level is accountable for serving in a highly advanced capacity in an area of specialization. The advanced resource capacity must be distinct from the regular or most common provision of work within the area of specialization. Positions at this level are not reflective of the majority of the workforce, but instead the most advanced functions within an area of specialization.

Incumbents:

* Serve in a subject leader and consultative capacity within an area of expertise.
* Set goals and objectives for team members to meet project initiatives and standards.
* Distribute project work.
* Evaluate and monitor the accuracy, quality, quantity, and timeliness to meet project milestones and objects.

**INDEPENDENCE AND DECISION-MAKING**

*🡪 Supervision Receive*d

* Works under direction.
* Seeks approvals when significant changes to process steps are considered and additional resources for task completion are required.

*🡪 Context of Decisions*

* Decisions are driven by departmental policy and procedures.
* Incumbents understand the smallest details of an assigned area.

*🡪 Job Controls*

* Free to plan and carry out all phases of work assignments, including the oversight of project staff.
* Has the latitude to make daily operational project decisions.

**COMPLEXITY AND PROBLEM SOLVING**

*🡪 Range of issues*

* Issues are readily identified but cannot be understood and fixed in simple cause-effect terms.
* Variables affecting the problem are generally known.

*🡪 Course of Resolution*

* Utilizing an understanding of best practices and the way similar units run elsewhere, convincingly recommends, develops, and implements capital and process improvements to the area.

*🡪 Measure of Creativity*

* Problems require integrative solutions such as how technologies, processes, resources, and people all fit together

**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 a lead over major projects within a specific administrative/programmatic function or specialty area requiring specialized education.
* Actions regularly affect a department or an office-centric outcome with departmental impact.
* Actions generally have a direct impact on controlling such things as nature of work and scope of services.
* Actions may have high-risk financial, compliance, political or safety implications.
* Performance results tend to relate 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 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.
* Proactively analyzes network traffic, system logs and other sources using security tools to identify threats or incidents within the university.
* Implements and maintains security tools and counter measures.
* Assists with triage of security requests from customers and internal teams.
* Identify and communicate 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 or assists in forensic analysis and incident response.
* Analyzes security incidents to determine root cause and prevent future occurrences.
* Develops security metrics to proactively monitor cyber threats and provide trend data for reporting.
* Performs related work as required.

**MINIMUM QUALIFICATIONS**

* Associates degree
* Four years of related experience

OR

* Bachelor’s degree
* Two years of related experience

OR

* Six years of related experience

AND

* One to three 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:**

* Concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).
* Cyber-attack stages (e.g. reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
* System administration concepts for operating systems such as Windows or Unix/Linux
* Common computer/network infections (virus, trojan, etc) and methods of infection (port, attachments, etc.)
* Physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.)
* Basic structure, architecture, and design of modern communication networks

**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