

Job Template: Information Security Analyst 1

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 1
Job Category: P	Job Level: 4
FLSA Status: E	Job Code: E30000

P4: Level Standards

GENERAL ROLE

This level is accountable for directly providing service to any assigned work unit at the University. The service can focus on a single or a variety of job functions with varying degrees of independence. Positions at this level may supervise student or support employees.

Incumbents:

- Put into effect what is required by defined job duties and responsibilities following professional norms or established procedures and protocols for guidance.
- Alter the order in which work or a procedure is performed to improve efficiency and effectiveness.
- Recommend or implement modifications to practices and procedures to improve efficiency and quality, directly affecting the specific office operation or departmental procedure or practice.

INDEPENDENCE AND DECISION-MAKING

→ *Supervision Received*

- Works under direction.

→ *Context of Decisions*

- Decisions should involve selecting an approach from among alternatives, timing when certain tasks should be performed, determining how to best use available resources, and other similar choices.
- Decisions require more coordination and collaboration among different sources, taking into consideration the roles and impact on work outside the immediate organization.

→ *Job Controls*

- Has the latitude to make decisions on projects that they are accountable for delivering on.
- Free to plan and carry out all phases of work assignments.

Job Template: Information Security Analyst 1

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 1
Job Category: P	Job Level: 4
FLSA Status: E	Job Code: E30000

COMPLEXITY AND PROBLEM SOLVING

→ *Range of issues*

- Assignments are defined as less reoccurring or cyclical tasks, and primarily consist of development or refinement of programmatic or administrative objectives.

→ *Course of Resolution*

- Resolution and project completion require substantial planning and scheduling within the department in order to obtain and align resources when and where needed.

→ *Measure of Creativity*

- Problems are not amenable to strict technical resolution, requiring innovative thinking.

COMMUNICATION EXPECTATIONS

→ *Manner of Delivery and Content*

- Regularly provides information on finished materials to others.
- Diplomatically and effectively deliver information difficult to understand or in contrast with a student or customer's views.

SCOPE AND MEASURABLE EFFECT

- Incumbents may supervise a small homogenous department, with proportionate responsibility to perform daily responsibilities similar to the work of subordinate staff.
- Actions typically affect an individual, item, event, or incident, etc.
- Actions taken are generally done to meet reporting requirements or regulatory guidelines, or to satisfy internal checks and balances and/or existing standards.
- Incumbents are typically designated as a lead or frequently assigned project leadership roles within a specific administrative/programmatic function or specialty area.

Job Template: Information Security Analyst 1

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 1
Job Category: P	Job Level: 4
FLSA Status: E	Job Code: E30000

- Generally, have a more direct impact on a larger action or process, such as serving as an approver in a process, where the process is “owned” by a different work unit.

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’s information systems security.

REPORTING RELATIONSHIPS AND TEAMWORK

Operates under the general supervision 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.

- Assists with analysis of network traffic, system logs, and other sources using security tools to identify threats or incidents within the University.
- Implement and maintain new security solutions.
- Assists with triage of security requests from customers and internal teams.
- Communicates security best practices to University constituents.
- Performs administrative duties on various components of the Information Security technology stack.
- Aids in analysis of security incidents to help determine root cause and prevent future occurrences.
- Reports on security metrics to proactively monitor cyber threats and provide trend data for reporting
- Performs related work as required.

MINIMUM QUALIFICATIONS

Job Template: Information Security Analyst 1

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 1
Job Category: P	Job Level: 4
FLSA Status: E	Job Code: E30000

- Associates degree
 - Four years of related experience
- OR
- Bachelor's degree
 - Two years of related experience
- OR
- Six years of related experience

COMPETENCIES

Knowledge of:

- Computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)
- Internet applications (SMTP email, web-based email and chat clients, VoIP)
- Host-based security products and how those products affect exploitation and reduce vulnerability

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

Job Template: Information Security Analyst 2

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 2
Job Category: P	Job Level: 6
FLSA Status: E	Job Code: E30001

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 Received*

- 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*

Job Template: Information Security Analyst 2

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 2
Job Category: P	Job Level: 6
FLSA Status: E	Job Code: E30001

- 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: Information Security Analyst 2

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 2
Job Category: P	Job Level: 6
FLSA Status: E	Job Code: E30001

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.

Job Template: Information Security Analyst 2

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 2
Job Category: P	Job Level: 6
FLSA Status: E	Job Code: E30001

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

Job Template: Information Security Analyst 2

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 2
Job Category: P	Job Level: 6
FLSA Status: E	Job Code: E30001

- 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

Job Template: Information Security Analyst 3

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 3
Job Category: P	Job Level: 7
FLSA Status: E	Job Code: E30002

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 Received

- 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.

Job Template: Information Security Analyst 3

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 3
Job Category: P	Job Level: 7
FLSA Status: E	Job Code: E30002

- 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.

Job Template: Information Security Analyst 3

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 3
Job Category: P	Job Level: 7
FLSA Status: E	Job Code: E30002

- 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: Information Security Analyst 3

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 3
Job Category: P	Job Level: 7
FLSA Status: E	Job Code: E30002

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.
- Triage 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.

Job Template: Information Security Analyst 3

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 3
Job Category: P	Job Level: 7
FLSA Status: E	Job Code: E30002

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

Job Template: Information Security Analyst 3

Occupational Group	Information Technology
Job Family	IT Security
Job Path	IT Security
Job Title	Information Security Analyst 3
Job Category: P	Job Level: 7
FLSA Status: E	Job Code: E30002

- 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