Draft Classification Standards – Rev. 03/29/2024

Information Security Analyst

Class Title	Class Code	Issue Date	FLSA
Information Security Analyst I	*XXXX*	*XXXX*	*Non-Exempt**
Information Security Analyst II	*XXXX*	*XXXX*	*Exempt**
Information Security Analyst III	*XXXX*	*XXXX*	*Exempt**
Information Security Analyst IV	*XXXX*	*XXXX*	*Exempt**

OVERVIEW:

Provides monitoring, configuration, and policy compliance to ensure the security, integrity, and privacy of university data, infrastructure, systems, applications, and physical technology assets. Works to protect systems from malicious, inadvertent, or unauthorized access, modification, or destruction. Acts on breaches with appropriate security measures, controls, containment, and recovery. Designs and implements security measures and technical solutions that provide detection, prevention, containment, recovery, and deterrence mechanisms. Monitors and assesses network, systems, and end-point device activity to identify vulnerabilities, risks, and other information security threats. Implements security controls and best practices to mitigate risks. Implements and audits to industry standard security frameworks. Delivers end-user training to support the safe handling and use of university information.

Positions are assigned to classifications within the series based on the scope and complexity of information security activities; degree of independence and judgement; experience, knowledge, skill, and ability required; degree of planning, analysis, and execution required by the position; impact and risk to the university; and nature of supervision received. Higher levels within the series build upon and include the knowledge and skill requirements and work assignments of lower levels within the series.

Information Security Analyst I – Entry level professional who applies basic professional concepts to resolve problems of limited technical scope and complexity. Normally operates under established guidelines. Follows standard practices and procedures. Assignments may be routine in nature and involve performing various duties related to protecting the integrity of campus information technology infrastructure and mitigate risks and losses associated with security threats.

Information Security Analyst II – Professional who applies acquired IT Security job skills and knowledge of IT Security concepts, principles, practices, policies, and procedures to implement and maintain information security controls, conduct risk assessments, respond to security incidents, and collaborate with IT teams and stakeholders to evaluate, recommend, and implement security technologies solutions. Draws from prior experience and knowledge of information security principles, concepts, controls, policies, and procedures to exercise judgment while identifying and monitoring security risks and threats and developing and deploying incident response plans and information security controls and solutions to protect the institution's data and information.

Information Security Analyst III – Professional who applies advanced IT security job skills, in-depth organizational and stakeholder acumen, and technical project planning skills to lead and manage information security initiatives of significant technical scope and

complexity. Exercises advanced discernment to develop and implement information security strategies, initiatives, and controls. May require the development of new approaches, techniques, and innovation to address issues. Responsible and accountable for the selection, development and proper deployment of information and cybersecurity systems, frameworks and solutions. Assess the effectiveness of security controls.

Information Security Analyst IV – Technical leader with a high degree of knowledge in information security and compliance. Problem-solving frequently requires analysis of unique issues or problems without precedent and/or structure and new approaches, methods, techniques, or innovation. Responsible for conceptualization, planning, and implementation of complex technology security solutions, initiatives, and customizations. Under the direction of management, creates strategies, policies, programs, guidelines, and procedures to ensure security objectives are achieved.

TYPICAL PROGRAMS, ACTIVITIES, AND CORE FUNCTIONS/DISCIPLINES *(May include but are not limited to)*:

- *IT Security Procurement* – Collaborates with departments to evaluate and perform security review and risk assessments of technology related products and services and determines the impact and probability of security risk based upon the CSU framework. Evaluates conformance and the compliance of vendor documentation such as product roadmaps and product compliance statements relative to CSU standards. Communicates CSU security standards and coordinates conformance to procurement procedures.
- *Policy and Compliance* – Contributes to policy and process development that prevents unauthorized intrusion, intentional or inadvertent modification, disclosure, or destruction of the campus and/or CSU information systems, IT assets, and intellectual property. Provides guidance for compliance with policy and best practices, such as data classification levels and disaster recovery. Advises and counsels management on potential risks and strategies related to data, information systems, and IT assets. Conducts assessments to ensure policy or regulatory compliance.
- *Compliance Documentation* – Creates and maintains compliance documentation, including guides, procedures, and user manuals to ensure that knowledge is shared and accessible within the organization. Ensures documentation is accurate, up to date, and accessible to relevant stakeholders.
- *Information Data Privacy* – Contributes to policy development and establishes guidelines to protect personal and institutional information. Determines what and how to collect, store, utilize, and dispose of information. Supports research and other groups to develop security infrastructure and frameworks to comply with standards.
- *Intrusion Prevention* – Develops, implements, and maintains internet and network security measures and procedures to protect the organization's digital assets from inadvertent modification, disclosure, and/or destruction. Serves as gatekeeper to prevent the breach or invasion of privacy of the campus and its community. Develops strategies for anti-virus and malware protection.
- *Identity and Access Management* – In collaboration with leadership designs and implements identity strategies and procedures that provide for best practices. Configures

access and end-user security controls to minimize business impact and risk exposure. Researches potential security incidents.

- *Server, Desktop, Cloud, and End-Point Security Administration* – Designs, implements and administers systems that monitor endpoints such as desktops, servers, cloud systems, and other systems and seeks to mitigate risks of malicious threats or other information security vulnerabilities. Seeks to identify vectors for compromise of university data or inappropriate access to systems or infrastructure. Responds to end-point security alerts and takes steps to remediate and secure systems and data. Configures system settings and other components to optimize and enhance system protection to provide for secure connectivity and operations.
- *Monitoring and Analysis* – Performs vulnerability scanning and testing of networks and applications and oversees security assessments to identify systems and networks that deviate from acceptable configurations, practices, or policy. Recommends and documents best practices for scanning/testing to mitigate and reduce vulnerabilities to university systems. Identifies exploited system and network vulnerabilities and misconfigurations to correct or strengthen university security posture. Trains automated security systems to learn patterns, anomalies, and potential risks and identify and detect suspicious behaviors.
- *Data Security Analytics* – Utilizes security analytics tools to collect, integrate and analyze data extracted from multiple sources. Monitors, detects, and documents information security threat trends to support information security goals.
- *Incident/Data Breach Response* – Coordinates efforts to remediate information security incidents, such as data exposure, network breach, data theft, computer theft, and other incidents related to information security and privacy. Investigates and responds to incidents and provides technical guidance to mitigate risks. Develop and/or maintain incident response plans, playbooks, and protocols. Participates in planning and testing for disaster recovery efforts.
- *IT Security Awareness and Training* – Develops and provides end-user education and training on topics of data security and privacy to build a culture that emphasizes security best practices.

DISTINGUISHING CHARACTERISTICS:

- Performs functions of the information security program, developing training, preventing IT-based crime, hacking, intentional or inadvertent modification, disclosure, or destruction to an organization's information systems and IT assets and intellectual property.

INFORMATION SECURITY ANALYST I

Under direct supervision, performs entry-level professional information security analysis. Performs less complex technical tasks following detailed and established procedures. Work is reviewed for accuracy and soundness of technical concepts.

Work assignments typically include some or all of the following:

- Provides technical testing and analysis of campus websites, applications, and software to maintain security and privacy.
- Implements and maintains information security controls, monitors security alerts and logs to identify and assess security risks, vulnerabilities, and threats, and responds to security incidents.
- Assists with the documentation of existing procedures.
- Assists in the research of identified risks and available mitigations.
- Assesses, tests, and implements security controls.
- Assists in the design of technical solutions to protect the university's data.
- Assists in developing procedures for data access management.
- Communicates security policies and procedures to stakeholders.
- Maintains information security documentation, records, and training materials.
- Participates and promotes security awareness and training.

MINIMUM QUALIFICATIONS:

Knowledge and Skill:

- General knowledge of principles and concepts of information security analysis.
- Network and computer skills to appropriately troubleshoot and alter systems as required.
- Organizational and time management skills to plan, organize, and prioritize work.
- Demonstrated communication and interpersonal skills to gather information from clients, communicate technical issues effectively, and produce documentation.
- Knowledge and ability to troubleshoot system issues.
- Ability to maintain confidentiality and appropriately handle sensitive data and information.
- Ability to work independently and as part of a team and build relationships with diverse stakeholders.
- Analytical skills to collect, analyze, and interpret application process problems and technology needs; to evaluate project performance and manage issues, risk and changes of scope.
- Computer skills to appropriately troubleshoot and alter systems as required.
- Ability to work with and analyze standard data sets and write reports using database, query language, and analytical tools.

Experience and Education:

An equivalent to bachelor's degree in a related field. Relevant education and/or experience which demonstrates acquired and successfully applied knowledge and abilities shown above may be substituted for the required education on a year-for-year basis.

INFORMATION SECURITY ANALYST II

Under general supervision, develops and evaluates information security systems, networks, and applications for the university to ensure confidentiality, integrity, and availability of information assets. Applies information security and cybersecurity knowledge to test vulnerabilities, deploy incident response plans, and ensure safety and security compliance of confidential data. Works independently on most day-to-day assignments with general supervision on new assignments or projects to ensure alignment with objectives. Handles multiple work priorities and is accountable for own work results.

In addition to duties performed by the Information Security Analyst I, the Information Security Analyst II typically performs the following duties:

- Designs, tests, and implements security controls.
- Evaluates and recommends security technologies and solutions.
- Communicates university security standards to vendors. Reviews vendor documentation to ensure conformance to information security and cybersecurity procurement procedures.
- Monitors security alerts and logs to identify and assess security risks, vulnerabilities, and threats including potential points of strength and vulnerability within networks, as well as adequacy of controls and security measures within systems and applications.
- Assess security controls based on cybersecurity principles and tenets.
- Properly documents all systems security implementation, operations, and maintenance activities and updates as necessary,
- Monitors and analyzes network traffic, logs analysis, and prioritizes and differentiates between potential intrusion attempts and false alarms.
- Identifies systems containing confidential data and analyzes protection of data, both in storage and in transit.
- Performs daily administration of campus information security toolsets and products.
- Performs recurring and on-demand vulnerability scanning of organization systems and cloud environments.
- Performs detailed analysis on security related incidents to determine the cause and impact of security violations. Preserves and analyzes digital evidence. Provides clear and concise reporting of the incident and implements corrective action when applicable. Provides recommendations for improving incident response procedures.
- Develops and maintains metrics, reports, and dashboards to monitor and report on the effectiveness of information security initiatives and programs.
- Provides guidance on information security policies, practices and procedures to university staff, departments, and constituents.
- Develops and maintains documentation of information security procedures for audit compliance and user support.
- Maintains database of regulatory requirements related to cyber security, data governance, state, and federal data compliance.
- Develops and delivers information security awareness programs and training sessions.
- Stays current with emerging technologies, industry trends, and best practices in information security.
- Provides lead work direction and training to technical or less experienced staff.

MINIMUM QUALIFICATIONS:

In addition to Information Security Analyst I knowledge and skill requirements, work assignments typically require:

- Working knowledge of information and cyber security principles, concepts, practices, and procedures including network security, vulnerability management, and incident response.
- Working knowledge of information security frameworks, standards, network security architecture concepts, including topology, protocols, components, principles, and best practices.
- Working knowledge of assessment, testing, and monitoring processes and tools.
- Experience with security tools and technologies including investigating and documenting risk assessments.

- Knowledge of laws, policies, procedures, or governance relevant to cybersecurity.
- Knowledge of information security audit and compliance procedures.
- Knowledge of the CSU's information classification system and its requirements for protecting the data.
- Ability to recognize vulnerabilities in campus infrastructure systems. Ability to properly prioritize remediation efforts.
- Strong detail orientation and organizational skills to plan, organize, and handle multiple assignments and incidents.
- Strong communication and interpersonal skills with the ability to present technology information to technically diverse audience in a clear and concise manner.
- Strong analytical skills to investigate, evaluate, and monitor information security threats and breaches and determine corrective actions.
- Skill in providing lead work direction and training to others.
- Proficiency in using applicable software and programming languages.

Experience and Education:

An equivalent to a bachelor's degree in a related field and two years of relevant experience. Additional experience which demonstrates acquired and successfully applied knowledge and abilities shown above may be substituted for the required education on a year-for-year basis. An advanced degree in a related field may be substituted for the required experience on a year-for-year basis.

INFORMATION SECURITY ANALYST III

Working independently under general supervision, leads information security initiatives and ensures the security of information assets. Applies advanced information and cyber security knowledge and expertise to develop and implement information security strategies, processes, procedures, and solutions. in collaboration with management, demonstrates advanced discernment in selecting methods and techniques. Decision-making is based on information security and cybersecurity best practices; data security compliance standards; university and information technology policies, guidelines, and protocols; and information security and information technology strategies and goals. Work is focused on ensuring alignment with overall objectives. Handles multiple work priorities and may provide lead work direction with accountability for results.

In addition to duties performed by the Information Security Analyst II, the Information Security Analyst III typically performs the following duties:

- Develops information and cyber security strategies and systems.
- Under the guidance of management, oversees risk, threat, vulnerability, and alert monitoring.
- Provides direction for complex forensic investigations to identify and respond to information security incidents. Collaborates with internal teams and external stakeholders to develop mitigation strategies. Develops and manages incident response plans and playbooks. Responsible for recommending and improving response processes and procedures.
- Identifying and correlating events related to system intrusion.
- Advises and counsels management on potential security risks and strategies related to data, information systems, and IT assets.

- Conducts security audits and assessments. Collaborates with internal and external auditors to address security findings.
- Deploys systems and controls according to industry standard frameworks.
- Troubleshoots campus information security toolsets and products.
- Builds playbooks and automation of daily information security response processes.
- Assesses information security operations and processes, recommends improvements where appropriate.
- Identifies and recommends hardware and software to provide the appropriate level of protection for information systems from unauthorized access and use.
- Under the guidance of management, oversees procurement requests. Performs and documents vendor and cloud service security posture assessments following university practices.
- Guides departments in the development of procedures for data access management and data lifecycle management.
- Provides information security guidance and expertise in the design and implementation of secure network architectures and systems.
- Identifies, designs, and/or implements solutions that provide detection, prevention, containment, and deterrence mechanisms to protect and maintain the integrity of campus data, infrastructure, systems, applications, and physical assets.
- Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.
- Recommends and develops information and cyber security awareness programs to enhance understanding of IT Security and its business risk.
- Designs new and recommends improvements to processes and procedures.
- Provides lead work direction, mentoring, and training to professional, technical, and other staff.

MINIMUM QUALIFICATIONS:

In addition to Information Security Analyst II knowledge and skill requirements, work assignments typically require:

- Thorough and advanced knowledge of information security frameworks, standards, and best practices.
- Thorough knowledge in cryptography technologies, key and certificate management, and provisioning.
- Demonstrates competence in independently applying advanced judgment to resolve difficult and complex information security risks and issues.
- Excellent leadership and project management skills, with the ability to manage multiple projects and initiatives simultaneously.
- Advanced skill in identify management and information security design.
- Advanced skill in overseeing and auditing systems in accordance with industry standards frameworks.
- Advanced analytical skills to understand information security problems from a broad perspective and discern applicable underlying principles to conceive and develop strategic solutions.
- Advanced skill in mentoring and overseeing the work of others.

- Advanced communication and interpersonal skills to effectively enforce information security policies and procedures and persuade stakeholders and management to create a culture of information security awareness.

Experience and Education:

An equivalent to bachelor's degree in a related field and four years of relevant experience. Additional experience which demonstrates acquired and successfully applied knowledge and abilities shown above may be substituted for the required education on a year-for-year basis. An advanced degree in a related field may be substituted for the required experience on a year-for-year basis.

INFORMATION SECURITY ANALYST IV

Working independently with minimal supervision, provides expert guidance and leadership to protect information assets and ensure compliance with regulatory requirements. Problems are highly complex and may require the creation of new procedures and information security techniques. Often leads high-impact projects with campus-wide and/or system-wide significance. Serves as a technical expert to guide information security decision making and policy development. Decision-making often requires integration and interpretation of diverse information technology disciplines, information security expertise, and persuasion and negotiation with management. Functions with a high degree of autonomy. Work often requires a high degree of technical expertise, persuasion, and leadership.

In addition to duties performed by the Information Security Analyst III, the Information Security Analyst IV typically performs the following duties:

- Develops methodologies for protecting campus confidential data and other high-risk information assets.
- Develops broad strategic solutions addressing future security concerns for the university.
- Leads technical analysis, support, and troubleshooting of assigned applications, tools, and interfaces.
- Consults with IT leadership to ensure strategy, design, and technical execution meets the needs and data security expectations of the university and federal guidelines.
- Strategizes, scopes, develops, and implements comprehensive security solutions and associated application and software deployments to ensure cybersecurity.
- Serves as a key technical advisor within the information security discipline. Under the direction of management, provides oversight and recommendations for highly complex problems and issues.
- Under the guidance of management, oversees process improvement efforts, often developing new strategic approaches and solutions.

MINIMUM QUALIFICATIONS:

In addition to Information Security Analyst III knowledge and skill requirements, work assignments typically require:

- Expert knowledge and understanding of information security methodologies and best practices including compliance and audit procedures.
- Knowledge of laws, policies, procedures, or governance relevant to cybersecurity for critical infrastructures.
- Expert knowledge and skill in applying and interpreting applicable standards, guidelines and, as appropriate, recommends organization policies, guidelines, and procedures.

- Expert analytical and organizational skills to organize, prioritize, and coordinate the successful completion of large, complex, and high impact information security projects and initiatives.
- Expert communication and interpersonal relationship skills to effectively persuade stakeholders and management regarding information security design and development options.

Experience and Education:

An equivalent to bachelor's degree in a related field and five years of relevant experience. Additional experience which demonstrates acquired and successfully applied knowledge and abilities shown above may be substituted for the required education on a year-for-year basis. An advanced degree in a related field may be substituted for the required experience on a year-for-year basis.

NOTES:

All IT professionals protect the confidentiality and integrity of data and electronic information from incidental, intentional, unauthorized release and/or preventable misuse or loss to the university. IT professionals at the university are collectively responsible for ensuring the security and protection of sensitive information, systems, and digital assets. This includes upholding data confidentiality, integrity, and availability and actively contributing to a culture of cybersecurity awareness and compliance throughout the university's technological ecosystem.

The California State University has a long-standing commitment to make its programs, services, and activities accessible to the public and the entire campus community. All professionals classified within the Information Technology Series have the expectation to support practices and techniques that align with federal and state law, as well as the CSU initiatives, coded memorandums, and executive orders.

Acronyms and technical terms used in this classification document are current as of the publication date. Subsequent technical, functional, and usage terminology and acronyms should be substituted as appropriate.