

**YOUR EFFORTS WILL MAKE FI\$Cal A SUCCESS  
DUTY STATEMENT**

<b>CLASSIFICATION TITLE</b> Information Technology Specialist I	<b>DIVISION NAME</b> Information Technology Division, Enterprise Security Services Office, Information Systems Security Management, Policy and Assessment Unit
<b>WORKING TITLE</b>  Policy and Standards Analyst	<b>POSITION NUMBER</b>  333-350-1402-XXX
<b>EMPLOYEE NAME</b>  VACANT	<b>EFFECTIVE DATE</b>  June 7, 2023

You are a valued member of the Department of FISCAL. You are expected to work cooperatively with team members and others to provide the highest level of service possible. Your creativity and productivity is encouraged. Your efforts to treat others fairly, honestly and with respect are important to everyone who works with you.

**GENERAL STATEMENT**

Under the general supervision of the Information Technology Manager I (ITM), the Information Technology Specialist I (ITS I) will serve as Policy and Standards Analyst, to develop and oversee privacy compliance program, security policies, guidelines, and standards. The incumbent will ensure compliance with industry standards, state and federal security requirements, and promote privacy and data security awareness throughout the organization.

The duties for this position are focused in the Information Security Engineering domain, however, work may be assigned in the other domains as needed.

**SUPERVISION RECEIVED**

Reports directly to the Information Technology Manager I, within Enterprise Security Services Office (ESSO), Information Systems Security Management Section.

**SUPERVISION EXERCISED**

None.

**ESSENTIAL FUNCTIONS**

The incumbent must be able to perform the essential functions with or without reasonable accommodation. Specific duties include, but are not limited to, the following:

<b><u>% OF TIME</u></b>	<b><u>ESSENTIAL FUNCTIONS</u></b>
<b>35%</b>	<ul style="list-style-type: none"> <li>Oversee privacy training and communications to increase understanding of privacy policies and legal obligations.</li> </ul>

	<ul style="list-style-type: none"> <li>• Ensure compliance with privacy practices and apply sanctions for non-compliance.</li> <li>• Review data and privacy projects, develop procedures, and ensure consistency with privacy goals and legal obligations.</li> <li>• Provide leadership in privacy and security projects, handle complaints, track access to protected information, and facilitate reviews.</li> <li>• Establish an internal privacy audit program and provide guidance on privacy policies and procedures.</li> <li>• Monitor systems to maintain privacy protections and conduct privacy impact assessments.</li> <li>• Administer requests for disclosure of personal information and align security and privacy practices.</li> <li>• Develop procedures for vetting vendors and ensure compliance with privacy and data security policies.</li> <li>• Provide guidance on privacy and data security obligations to ensure compliance.</li> <li>• Coordinate with legal counsel and regulatory bodies to address privacy considerations and maintain appropriate consent and authorization forms.</li> </ul>
<p><b>30%</b></p>	<p><b>Risk Management</b></p> <ul style="list-style-type: none"> <li>• Develop and establish a risk management strategic plan for the organization that includes a determination of risk tolerance.</li> <li>• Advise senior management on cost/benefit analysis, risk levels, security posture, information security programs, policies, processes, systems, and elements.</li> <li>• Interpret patterns of noncompliance and prepare audit reports that identify technical and procedural findings to determine their impact on levels of risk and provide recommended remediation strategies/solutions.</li> <li>• Evaluate cost/benefit, economic, and risk analysis to ensure that security improvement actions are evaluated, validated, and implemented in the decision-making process. Advise senior management on cost/benefit analysis of information security programs, policies, processes, systems, and elements.</li> </ul>
<p><b>20%</b></p>	<p><b>Information Security Awareness Training</b></p> <ul style="list-style-type: none"> <li>• Develop and maintain a role-based security awareness training program that effectively reduces the “human factors” risks to FI\$Cal.</li> <li>• Educate staff on information security and privacy protection responsibilities.</li> <li>• Manage and ensure all FI\$Cal personnel complete Security Awareness Training annually.</li> </ul>

	<ul style="list-style-type: none"> <li>• Collect and provide security awareness training metrics to FI\$Cal leadership.</li> <li>• Ensure all FI\$Cal personnel complete Security Awareness Training upon onboarding.</li> <li>• Work with the Communications team to develop security articles for publication on the FI\$Cal intranet and newsletter.</li> </ul>
<b>10%</b>	<p><b>Collaboration</b></p> <ul style="list-style-type: none"> <li>• Support the organization's privacy compliance program, working closely with the other departmental units, Chief Information Security Officer, Chief Information Officer, legal counsel and the business units.</li> <li>• Assemble, organize and otherwise prepare documents for audits and assessments</li> <li>• Collaborate with stakeholders to ensure policy awareness and compliance.</li> <li>• Participate in the review of the System Security Plan to assure implementation of sound security principles and adherence to security requirements as outlined in NIST, FIPS, SIMM and SAM.</li> </ul>
<b><u>% OF TIME</u></b>	<b><u>MARGINAL FUNCTIONS</u></b>
<b>5%</b>	<ul style="list-style-type: none"> <li>• Perform other related duties as required to fulfill FI\$Cal's mission, goals and objectives. Additional duties may include, but are not limited to, assisting where needed within the team/unit, which may include special assignments.</li> </ul>

Please note that the time percentages mentioned in this duty statement are approximate and subject to change. These percentages are provided as a general guideline to help understand the expected allocation of time for different tasks and responsibilities. However, actual time allocation may vary depending on the specific circumstances and priorities at any given time.

**KNOWLEDGE AND ABILITIES**

All knowledge and abilities of the Information Technology Associate classification; and

Knowledge of: Information technology governance principles and guidelines to support decision making; complex and mission critical business processes and systems; principles, methods and procedures for designing, developing, optimizing, and integrating systems in accordance with best practices; system specifications design, documentation, and implementation methodologies and techniques.

Ability to: Formulate and recommend policies and procedures; perform effectively in a fast-paced environment with constantly changing priorities; establish and maintain project priorities; apply federal, state, department, and organizational policies and procedures to state information technology operations; apply systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems; positively

influence others to achieve results that are in the best interests of the organization; consider the business implications of the technology to the current and future business environment; communicate change impacts and change activities through various methods; conduct end-user training; collaborate closely with technical subject matter experts such as database administrators, network engineers, and server administrators to ensure systems are secure and meet compliance requirements; assess situation to determine the importance, urgency, and risks to the project and the organization; make decisions which are timely and in the best interests of the organization; provide quality and timely ad hoc project information to executives, project team members, and stakeholders; develop decision making documents; and assess and understand complex business processes and customer requirements to ensure new technologies, architectures, and security products will meet their needs.

### **SPECIAL REQUIREMENTS**

The incumbent will use tact and interpersonal skills to develop constructive and cooperative, working relationships with others, e.g., stakeholders, customers, management, peers, etc., to facilitate communication to improve the work environment and increase productivity. **Fingerprinting and background check is required.**

### **WORKING CONDITIONS**

The incumbent may need to be on-site to carry out their duties. This position requires the ability to work under pressure to meet deadlines and may require excess hours to be worked. The incumbent should be available to travel as needed and is expected to perform functions and duties under the guidance of the Department of FI\$Cal's core values. The incumbent provides back-up, as necessary, to ensure continuity of departmental activities.

This position requires prolonged sitting in an office-setting environment with the use of a telephone and personal computer. This position requires daily use of a copier, telephone, computer and general office equipment, as needed. This position may require the use of a hand-cart to transport documents and/or equipment over 20 pounds (i.e., laptop, computer, projector, reference manuals, solicitation documents, etc.). The incumbent must demonstrate a commitment to maintain a working environment free from discrimination and sexual harassment. The incumbent must maintain regular, consistent, predictable attendance, maintain good working habits and adhere to all policies and procedures.

**SIGNATURES**

I have read and understand the duties listed above and I can perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the assigned HR analyst.)

---

Employee Signature

Date

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

---

Hiring Manager Signature

Date

HR Analyst

**Date Revised: 6/16/2023**