



Classification: Information Technology Specialist I

Title: Information Security Officer

Posted: November 15, 2018

Permanent, Full-Time

Range A: \$5,118.00 - \$6,859.00

Range B: \$5,628.00 - \$7,543.00

Range C: \$6,179.00 - \$8,280.00

Not Your Average State Agency

The California Student Aid Commission (CSAC) is the principal state agency responsible for administering \$2 billion dollars in financial aid programs for students attending public and private universities, colleges, and vocational schools in California. Our Mission is to make education beyond high school financially accessible to all Californians.

We are located in Rancho Cordova, in a great office complex near Zinfandel and Hwy. 50. There is plenty of parking and it is free!

Highlights of the Job

Under the general supervision of the Information Technology Services Division, (ITSD), Chief Information Officer, the incumbent works in the Commission's Information Security Office and performs all expert specialist functions as an Information Security Officer (ISO). In this capacity, the incumbent works as ISO to develop and implement all aspects of information security, physical security, privacy plans, policies, processes, procedures and standards; including electronic copy, hard copy, and any other media maintained and owned by the Commission. The Information Security Officer, is responsible for the information security of all of the Commission's Technical Architecture and for the Technology Disaster Recovery planning for all CSAC systems.

The incumbent is also responsible for Information Security Training for all CSAC staff, which includes but is not limited to: contract and vendor staff, State employees, retired annuitants and student assistants. This position will ensure CSAC staff members are sufficiently informed as how to abide by CSAC Information Security policy guidelines. The incumbent will have interactions with both internal and external entities in the development of security and privacy policies, processes and procedures.

Minimum Qualifications

<https://www.calhr.ca.gov/state-hr-professionals/Pages/1400.aspx>

Desirable Qualifications

- Knowledge of cybersecurity operations and incident response practices and experience leading security analysts and technical staff in finding and remediating security threats.
- Experience in vulnerability assessment, threat assessment, risk management, and remediation planning.
- Experience in developing, implementing, training and managing security training.
- Experience in developing and managing Interagency Agreements.
- Experience in performing all aspects of a security subject matter expert and IT support subject matter expert within an organization.
- Experience in conducting and supporting security audits.
- Experience in developing business continuity plans.
- Excellence in customer service.

- Strong technical writing/documentation skills
- A positive and professional attitude.
- Ability to manage time effectively and work independently.
- Experience identifying, analyzing and responding to Information Security risk factors.
- Comprehensive understanding of applicable security software.
- Act as a subject matter expert to the Commission for security software purchases and implementations.
- Understanding of network and data communications, including interoperability of different computer systems.
- An ongoing desire to learn.
- 2 years of experience with Information Systems
- Strong IT Troubleshooting skills
- Requires ability to assist in interpreting, establishing, documenting, and monitoring the Information Systems Security Program
- Must have effective verbal and written communication skills
- Knowledge of applicable laws and regulations
- Self-starter/leader who can anticipate department needs in a proactive (versus, reactive) manner
- Ability to develop and interpret data and manage resources
- Ability to motivate and influence others
- Ability to review potential risks and prioritize multiple competing projects
- Experience in reviewing and developing Information Technology security policies
- Current with existing cyber threat landscape. Required to stay current with latest trends and developments
- Knowledge of cybersecurity policies and industry best practices such as the National Institute of Standards and Technology (NIST) special publications and the Center for Information Security Top 20 Security Controls.
- Windows Server Administration including DHCP, DNS, AD, DFS, Group Policies and Printing
- Experience as an Information Security Officer for a state government department, state government agency, or large multi-national private sector corporation.
- Security Professional certifications; specifically, Certified Information Systems Security Professional (CISSP)
- Cybersecurity Penetration Technical Certifications; such as GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) and/or GIAC Penetration Tester (GPEN)

Who Should Apply

Applicants must have current list eligibility for appointment to this class, currently a State employee who has transfer eligibility (transfers must meet the minimum qualifications for the advertised class, per CCR Rule 250), or currently in an Information Technology Specialist I position. Other methods of appointments will be considered, including Training & Development (T&D) Assignments. Applications will be screened and only those that best meet the requirements of the job will be considered. Appointment is subject to SROA/Surplus provisions. SROA and Surplus candidates are encouraged to apply. Surplus candidates must submit a copy of their surplus status letter.

All applicants, regardless of the type of eligibility, must meet the Minimum Qualifications of the classification. To view the Minimum Qualifications, please go to <http://www.calhr.ca.gov/state-hr-professionals/Pages/job-descriptions.aspx> and enter the classification code or classification title you wish to review. In addition, please attach all required supporting documents (i.e. transcripts/diploma, license, and/or required certificate) to your application.

Eligibility is determined by the completed information on your Std. 678 and/or résumés; please ensure applications and/or résumés contain completed information or your application may not be accepted.

How to Apply/Final Filing Date

Please reference **RPA #18-032, JC-134844, Position #270-701-1402-XXX, Information Technology Specialist I**, in the 'Job Title' section on the application, Std. 678. Please clearly state basis for eligibility on your application (i.e., SROA, Surplus, Re-employment, reinstatement, transfer, list eligibility, or Training & Development Assignment). College transcripts may need to be submitted with your application, to verify the educational requirements of the class, if applicable. Please refer to the "minimum qualifications" to determine whether transcripts may be needed. Applications **will not** be accepted by fax or email.

Electronic submission of applications and résumés, through your CalCareer account at www.jobs.ca.gov, is preferred and will be accepted **Until Filled**. If you need assistance with the electronic application process, please contact the Personnel Office by email at Personnel@csac.ca.gov.

You may also submit your application and résumé by mail or in person to:

CA Student Aid Commission
P.O. Box 3210
Rancho Cordova, CA 95741-3210
Attn: HR-Recruitment

CA Student Aid Commission
11040 White Rock Rd.
Rancho Cordova, CA 95670
Attn: HR-Recruitment

AN EQUAL OPPORTUNITY EMPLOYER TO ALL REGARDLESS OF AGE, ANCESTRY, COLOR, EXERCISING THE RIGHT TO FAMILY CARE AND MEDICAL LEAVE, DISABILITY (MENTAL AND PHYSICAL), GENDER, GENDER IDENTITY OR EXPRESSION, GENETIC INFORMATION, MARITAL STATUS, MEDICAL CONDITION, MILITARY OR VETERAN STATUS, NATIONAL ORIGIN, POLITICAL AFFILIATION, RACE, RELIGIOUS CREED, SEX (INCLUDES PREGNANCY, CHILDBIRTH, BREASTFEEDING AND RELATED MEDICAL CONDITIONS), OR SEXUAL ORIENTATION OF ANY PERSON.

IT IS THE OBJECTIVE OF THE STATE OF CALIFORNIA TO ACHIEVE A DRUG FREE WORKPLACE. ANY APPLICANT FOR STATE EMPLOYMENT WILL BE EXPECTED TO BEHAVE IN ACCORDANCE WITH THIS OBJECTIVE BECAUSE THE USE OF ILLEGAL DRUGS IS INCONSISTENT WITH THE LAW OF THE STATE. THE RULES GOVERNING CIVIL SERVICE, AND THE SPECIAL TRUST PLACED IN PUBLIC SERVANTS.



CALIFORNIA STUDENT AID COMMISSION

DUTY STATEMENT

I. Position Identification:

Employee Name:	Vacant
Classification:	Information Technology Specialist I
Working Title:	Information Security Officer
Position Number:	270-701-1373-xxx
Location:	11040 White Rock Rd. Rancho Cordova, CA 95670
License/Other Requirement:	N/A
Date Prepared:	November 9, 2018
Effective Date:	TBD

Function: *(Summary of Responsibilities)*

- | | |
|--|--|
| <input type="checkbox"/> Business Technology Management | <input type="checkbox"/> Information Technology Project Management |
| <input type="checkbox"/> Client Services | <input type="checkbox"/> Software Engineering |
| <input checked="" type="checkbox"/> Information Security Engineering | <input type="checkbox"/> System Engineering |

Under the general supervision of the Information Technology Services Division, (ITSD), Chief Information Officer, the incumbent works in the Commission's Information Security Office, and performs all expert specialist functions as Information Security Officer. In this capacity, the incumbent works as the ISO to develop and implement all aspects of information security, physical security, and privacy plans, policies, processes, procedures and standards, including electronic copy, hard copy, and any other media maintained and owned by the Commission. The incumbent is responsible for the information security of the Commission's Technical Architecture and for the Technology Disaster Recovery planning for all CSAC systems. The incumbent is also responsible for Information Security Training for all CSAC staff, which includes, but is not limited to: contract and vendor staff, State employees, retired annuitants and student assistants. This position will ensure CSAC staff members are sufficiently informed as to how to abide by CSAC Information Security policy guidelines. The incumbent will have interactions with both internal and external entities in the development of security and privacy policies, processes and procedures.

Reporting Relationships:

Reports directly to: The Chief Information Officer.

II. Program Identification:

The California Student Aid Commission is responsible for administering financial aid programs for students attending public and private universities, colleges, and vocational schools in California. The Commission's central mission is to make education beyond high school financially accessible to all Californians.

The Information Technology Services Division (ITSD) supports CSAC in the delivery of state services and information to our internal and external stakeholders through information technology service management using the Information Technology Infrastructure Library (ITIL) framework.

As a valued leader of the Enterprise Services Team, you make it possible for the CA Student Aid Commission (CSAC), to improve by providing expert level consultation, being innovative, resourceful, and flexible, reporting to work as scheduled; working cooperatively with team members and others; and treating others fairly, honestly, and with respect. Your efforts are important to each member of the team, as well as students and schools we serve.

III. Essential and Non-Essential Job Functions:

Essential Functions:

Candidates must be able to perform the following functions with or without reasonable accommodations.

- 35% Administer the Department's Information Security Program:
- Develop processes and procedures to ensure the agency's policies, procedures and compliance of security standards are met.
 - Coordinate activities to ensure all staff complete security awareness training, complete confidentiality statements, and safeguard data at all times.
 - Educate and make staff aware of all security compliance requirements set forth by the State ISO office, and agency security policy.
 - Ensure CSAC satisfies the State Information Security policy including but not limited to: ensuring annual Security Risk Assessment is completed as specified by the State ISO and submitted to the CA ISO control agency with program compliance certification.
- 10% Lead activities with Departmental personnel on IT projects by reviewing project and contact documentation to determine the need and appropriateness of proposed security provisions and reviewing proposed modifications to existing electronic information processing systems to ensure appropriate security safeguards are maintained.
- 10% Lead activities in the development and maintenance of the Department's Business Continuity Plan, which is designed to allow effective and efficient recovery of critical and essential business functions in the event of a disaster. Lead the annual Disaster Recovery exercise, including ongoing policies and procedures for preparation of a disaster.
- 10% Develop policies and procedures for reporting incidents involving intentional, unintentional or unauthorized use, modification, access, or destruction of the Department's information assets. Coordinate investigations of alleged incidents of security violations.
- 10% Evaluate requests for release of personal/confidential information and authorizing or denying requests based on existing laws, regulations, and policies. Facilitating and/or overseeing IT risk assessments to identify potential vulnerabilities that could threaten the security of the Department's information assets
- 10% Develop security policies, procedures, and criteria for the collection, storage, access, and destruction of the Department's information assets. The policies and procedures provide the operational guidelines and delineate roles and responsibilities of Department entities for assuring the security and integrity of information assets.

- 5% Consults with and advises the Chief Information Officer and Executive staff on information security matters.
- 5% As Information Security Officer, represent the Department in coordinating information security issues and requirements with State control agencies, federal agencies, other state and local agencies, and individuals.

Non-Essential Functions:

- 5% Other duties as required.

IV. ADA Requirement:

Alternatives will be provided for incumbents who are unable to perform the non-essential functions of the job due to a disability covered under the Americans with Disabilities Act

V. Physical Requirements:

Ability to operate and utilize office machines required to perform work tasks, such as copiers, faxes, calculators, personal computer, etc. These job duties may require the incumbent to work under demanding conditions and irregular hours during peak periods. Requires sitting for long periods of time while using a personal computer or reviewing documents and working papers.

VI. Working Conditions:

Employee's work is to be performed within an office environment, and is equipped with standard or ergonomic office equipment, as needed. Attend meetings in designated conference rooms and be willing to travel to off-site meeting locations.

VII. Attendance:

Must maintain regular and acceptable attendance. This position is subject to on call and standby time and periodic off-shift, weekend work. This position is work week group "E" which is exempted from coverage under the Fair Labor Standards Act (FLSA). A work week group "E" or salaried employee does not receive overtime compensation and may be required to work specific hours to provide services when deemed necessary by management. Employees who are excluded from FLSA shall not charge paid leave for absences of less than whole day increments or docked for absences of less than a whole day.

VIII. Signature

By signing this document, I acknowledge that I have read and understand all the requirements and information above and will receive a copy of this Duty Statement.

Applicant/Employee Certification of Essential Functions: I certify that I possess essential personal qualifications including integrity, initiative, dependability, good judgment, and ability to work cooperatively with others; and a state of health consistent with the ability to perform the assigned duties as described above 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 Personnel Office).

Professional Conduct: As an employee of the CA Student Aid Commission, I shall conduct business in a professional and ethical manner by demonstrating integrity, honesty, good judgement, courtesy, and respect at all times. I shall be sensitive to, and responsible for, the efficient, economical, and legal implementation of all business operations.

Employee Signature

Date

Supervisor Signature

Date

*Duties of this position are subject to change and may be revised as needed or required.