## CSUB JOB ANNOUNCEMENT

<table>
<thead>
<tr>
<th>Position Title:</th>
<th>CHIEF INFORMATION SECURITY OFFICER (Administrator II)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recruitment #:</td>
<td>#2143</td>
</tr>
<tr>
<td>Full/Part-Time:</td>
<td>Full-Time</td>
</tr>
<tr>
<td>Employment Type:</td>
<td>MPP – this administrative position is part of the California State University Management Personnel Plan. No tenure or permanent status can be achieved within the MPP.</td>
</tr>
<tr>
<td>Bargaining Unit:</td>
<td>M80</td>
</tr>
<tr>
<td>Salary:</td>
<td>The salary is competitive, depending upon qualifications and experience of the successful candidate. This administrative position is part of the California State University Management Plan and includes an excellent benefits program.</td>
</tr>
<tr>
<td>Department:</td>
<td>Information Technology Services</td>
</tr>
<tr>
<td>Available:</td>
<td>Immediately</td>
</tr>
<tr>
<td>Special Conditions:</td>
<td>Background/ Fingerprint &amp; Credit Check</td>
</tr>
<tr>
<td>Sensitive Position:</td>
<td>Yes</td>
</tr>
<tr>
<td>Posted:</td>
<td>April 14, 2017</td>
</tr>
<tr>
<td>Closing Date:</td>
<td>For priority consideration, application materials must be received by April 28, 2017, however, the position will remain open until filled.</td>
</tr>
</tbody>
</table>

Positions are open to all interested applicants, both on and off campus, unless this is an on-campus only recruitment.

### APPLICATION PACKET REQUIREMENTS

This position requires (including those on campus) submission of:
- A standard CSU, Bakersfield job application (download at: [http://www.csub.edu/bas/hr/EmployRecruit/Job%20status%20Inquiry/index.html](http://www.csub.edu/bas/hr/EmployRecruit/Job%20status%20Inquiry/index.html))
- Names of three professional references
- Copy of degree/transcripts/typing certificate, if required
- Brief description of how you are qualified for this position by virtue of your interest, aptitude, education and experience required.

The Chief Information Security Officer (CISO) provides thought leadership around technology, policy/practices, and governance dealing with information security and data management. Reporting to the Associate Vice President and Chief Information Officer the CISO will lead a small team of security specialists focused on providing a best-in-class security program for CSUB. The CISO is part of the Information Technology Services leadership team and serves a key role on information technology governance committees that establish the roadmap for technology implementation at CSUB. The CISO will be responsible for developing/enhancing a comprehensive security program for CSUB that allows us to optimize our security posture. The CISO will facilitate data management best practices, security governance, and the development of security policies and processes.

**California State University, Bakersfield** is committed to Equal Employment Opportunity. Applicants will be considered without regard to gender, race, age, color, religion, national origin, sexual orientation, genetic information, marital status, disability or covered veteran status.
DUTIES:

A. University and Program Leadership
   1. Responsible for the strategic leadership of CSUB’s information security program
   2. Provide guidance and counsel to the CIO and the university leadership team, working closely with senior administration, academic leaders, and the campus community in defining objectives for information security, while building positive relationships.
   3. Oversee the formation and operations of a university-wide information security organization that is organized toward a common goal in information security.
   4. Promote collaborative, empowered working environments across campus, removing barriers and realizing possibilities.
   5. Manage institution-wide information security governance processes, chair the Information Security Advisory Committee and lead the Information Security Liaison in the establishment of an information security program and project priorities.
   6. Lead information security planning processes to establish an inclusive and comprehensive information security program for the entire institution in support of academic, research, administrative information systems and technology.
   7. Establish annual and long-range security and compliance goals. Define security strategies, metrics, reporting mechanisms and program services; and create maturity models and a roadmap for continual program improvements.
   8. Stay abreast of information security issues and regulatory changes affecting higher education at the state and national level. Participate in national policy and practice discussions, and communicate to campus on a regular basis about those topics. Engage in professional development to maintain continual growth in professional skills and knowledge essential to the position.
   9. Provide leadership philosophy for the Information Security Office to create a strong bridge between organizations, build respect for the contributions of all. Bring groups together to share information and resources and create better decisions, policies and practices for the campus.
  10. Mentor the Information Security Office team members and implement professional development plans for all members of the team.
  11. Represent the University on committees and boards associated with the Institution's System and in national and regional consortiums and collaborations.

B. Policy, Compliance and Audit
   1. Lead the development and implementation of effective and reasonable policies and practices to protected/confidential data and ensure information security and compliance with relevant legislation and legal interpretation.
   2. Lead efforts to internally assess, evaluate and make recommendations to management regarding the adequacy of the security controls for the University’s information and technology systems.
   3. Work with agencies and external consultants as appropriate on required security assessments and audits.
   4. Coordinate and track all information technology and security related audits including scope of audits, colleges/units involved, timelines, auditing agencies and outcomes. Work with auditors as appropriate to keep audit focus in scope, maintain excellent relationships with audit entities and provide a consistent perspective that continually puts the institution in its best light.
   5. Provide guidance, evaluation and advocacy on audit responses.
   6. Work with university leadership and relevant responsible compliance department leadership to build cohesive security and compliance programs for the university to effectively address state and federal statutory and regulatory requirements.
   7. Develop a strategy for dealing with increasing number of audits, compliance checks and external assessment processes for internal/external auditors, PCI, ITAR, HIPAA, and FISMA.

C. Outreach, Education and Training
   1. Work closely with IT leaders, technical experts, deans and administrative leaders across campus on a wide variety of security issues that require an in-depth understanding of the IT environment in their units, as well as the research landscape and federal regulations that pertain to their unit’s research areas.
   2. Create education and awareness programs and advise operating units at all levels on security issues, best practices, and vulnerabilities.
   3. Work with campus groups such as Network Managers, Information Security Liaisons and technical organizations such as Information Technology Services to build awareness and a sense of common purpose around security.
   4. Pursue student security initiatives to address unique needs in protecting identity theft, mobile social media security and online reputation program.

California State University, Bakersfield is committed to Equal Employment Opportunity. Applicants will be considered without regard to gender, race, age, color, religion, national origin, sexual orientation, genetic information, marital status, disability or covered veteran status.
D. Risk Management and Incident Response
   1. Keep abreast of security incidents and act as primary control point during significant information security incidents. Convene a Security Incident Response Team (SIRT) as needed, or requested, in addressing and investigating security incidents that arise.
   2. Convene Ad Hoc Security Committee as appropriate and provide leadership for breach response and notification for the University.
   3. Develop, implement and administer technical security standards, as well as a suite of security services and tools to address and mitigate security risk.
   4. Provide leadership, direction and guidance in assessing and evaluating information security risks and monitor compliance with security standards and appropriate policies.
   5. Examine impacts of new technologies on the Institution's overall information security. Establish processes to review implementation of new technologies to ensure security compliance.

REQUIRED QUALIFICATIONS:

- Bachelor's degree in computer science, MIS, or related field.
- 5-7 years of lead, supervisory, or managerial experience in security management.
- Demonstrated ability to manage, motivate, and evaluate professional IT staff.
- Proven working knowledge in security, data management, and governance.
- Possesses excellent information security program, audit, compliance, policy and governance skills.
- Formal certification (CISSP, CISM, CRISC) and/or formal training in information security standards and best practices (ISO 27001/2, COBIT).
- Proven track record of creating and maintaining an information security practice or service.
- Knowledge of Higher Education policies and best practices in regards to HIPAA, FERPA, etc.
- Possess strong collaboration and team building skills.
- Knowledge of security and data management issues.
- Experience in managing an information security area, program or office.
- Experience in effective problem solving, negotiation and decision making skills to address critical issues affecting the business.
- Possess solid communication skills including written and interpersonal.
- Demonstrated experience in service management and a strong customer service ethic.
- Must be willing to travel and attend training programs off-site for occasional professional development.
- Must be able to work overtime, occasional holidays, and adjust working hours to meet special jobs. May be called back periodically to perform work as needed on an emergency basis.
- Regular and reliable attendance is required.

PREFERRED QUALIFICATIONS:

- Graduate degree
- Knowledge of risk management techniques and best practices
- Successful experience leading a unionized workforce.
- Demonstrated skills in an institutional/educational environment utilizing a customer-oriented and service-centered attitude.

SCREENING: Only those applicants possessing experience most directly related to the immediate needs of the office will be invited to appear before a Qualifications Appraisal Board for the purpose of appraising training, experience and interest in the position.

BACKGROUND CHECK: A background check (including a criminal records check) must be completed satisfactorily before any candidate can be offered a position with the CSU. Failure to satisfactorily complete the background check may affect the application status of applicants or continued employment of current CSU employees who apply for the position.

SENSITIVE POSITION: Sensitive positions are designated by the CSU as requiring heightened scrutiny of individuals holding the position, based on potential for harm to children, concerns for the safety and security of the people, animals, or property, or heightened risk of financial loss to the CSU or individuals in the university community.

California State University, Bakersfield is committed to Equal Employment Opportunity. Applicants will be considered without regard to gender, race, age, color, religion, national origin, sexual orientation, genetic information, marital status, disability or covered veteran status.
MANDATED REPORTER: The person holding this position is considered a “mandated reporter” under the California Child Abuse and Neglect Reporting Act and is required to comply with the requirements set forth in CSU Executive Order 1083 as a condition of employment.

DESIGNATED POSITION: If the duties of this position include participation in decisions that may have a material financial benefit to the incumbent, the selected candidate will be required to file Conflict of Interest Form 700: Statement of Economic Interest when they first occupy the position, and on an annual basis, complete ethics training within 6 months of appointment, and attend this training every other year thereafter.

GENERAL INFORMATION: It is the policy of California State University; Bakersfield to hire only United States citizens and aliens lawfully authorized to work in the United States. All new employees will be required to present documentation verifying their right to accept employment. You will also be requested to present a social security card at the time of initial appointment in compliance with state payroll regulations. State regulations require that every state employee sign the Oath of Allegiance prior to commencing the duties of his/her State employment, except legally employed non-citizens. These individuals are required to sign the Declaration of Permission to Work.

APPLICATION PROCEDURE: Official California State University, Bakersfield application forms must be completed in full and received in the Human Resources Office by 5:00 p.m. on/or postmarked by the specified closing date, unless otherwise indicated. Resumes are welcomed but will not be accepted in place of the official application. E-mailed or faxed applications or resumes will also not be accepted.

Applications are available outside the Office of Human Resources and may be downloaded from the Human Resources website. Candidates who reside outside the city of Bakersfield may contact the Office of Human Resources and request that an application be mailed to their residence. It takes a minimum of 4-6 weeks from the closing date for a position to be filled.

To check the status of your application, go to the Human Resources’ Job Opening/Status Inquiry page at http://www.csub.edu/bas/hr/EmployRecruit/Job%20Status%20Inquiry/index.html and click on the “Job Status” icon link. Applicants will not receive individual notifications. Upon submission, all application materials become the exclusive property of California State University, Bakersfield and will not be copied or returned.