Information Security Analyst/Administrator
Information Technology Services (ITS)

POSITION SUMMARY

The Information Security Analyst/Administrator will plan, implement, upgrade, and monitor security protocols for the protection of the organization’s computer networks and information. Reporting to the AVP for Technical Services the Information Security Analyst/Administrator works with constituents across the college - faculty, staff, and students - to develop and deliver a comprehensive security and privacy program on risk management and compliance activities. This position is responsible for security protocols related to Oxy’s information infrastructure and will work with network/system administrators to track security vulnerabilities in the information sharing network to ensure that such weaknesses in the system are addressed and remedied efficiently. This position will work continuously on security measures and applications designed to mitigate the risk of malicious intrusion into the network’s information systems.

SUMMARY OF DUTIES, RESPONSIBILITIES AND GOALS

1. Collaborates with users to discuss computer data access needs, to identify security threats and violations, and to identify and recommend needed programming or process changes.
2. Uses data encryption, firewalls, and other appropriate security tools and applications to conceal and protect transfers of confidential digital information.
3. Develops and implements plans to safeguard digital data from accidental or unauthorized modification, destruction, or disclosure; adheres to emergency data processing needs.
4. Reviews violations of security procedures; provides training to ensure violations do not recur.
5. Monitors and restricts access to sensitive, confidential, or other high-security data.
6. Performs risk assessments, audits, and tests to ensure proper functioning of data processing activities and security measures.
7. Safeguards system security and improves overall server and network efficiency by training users and promoting security awareness.
8. Determines when to update virus protection systems by monitoring current reports of computer viruses; facilitates or performs needed updates.
9. Monitors and upgrades malware, virus detection applications and other monitoring systems; conducts analysis on the information sharing structure; and tests for security vulnerabilities. Researches new anti-intrusion applications and test their efficacy against the network’s and organization’s security protocols and requirements.
10. Creates and implements policies, protocols, and procedures, and creates and presents reports based on risk analysis of the information-sharing network.
11. Directs and performs security event handling, threat hunting, threat intelligence analysis, forensic analysis, vulnerability identification.
12. Leads and engages appropriate College parties to properly address and manage cybersecurity incidents, including analysis, remediation, and recovery.

13. In partnership with members of the ITS leadership team, defines and maintains policies, standards, and practices for information and data security throughout the college, encompassing on-premise and cloud technology, third-party engagements, and academic systems. Design and execute activities, inside and outside ITS, to socialize and implement these standards.

14. Performs other duties as assigned.

QUALIFICATIONS

- Demonstrated problem-solving and analytical skills.
- Proficient, or able to gain proficiency with, a broad array of security software applications and tools.
- Thorough understanding of computer-related security systems including firewalls, encryption, and password protection and authentication.
- Ability to be self-directed and to respond to requests with short turnaround times
- Strong interpersonal skills and the ability to communicate clearly, both verbally and in writing, with colleagues, as well as possibly internal stakeholders
- Ability to prioritize and organize a heavy and varied workload, be responsive and timely, and effectively serve a range of constituents within the College.
- Technical knowledge of information security standards (e.g., NIST, ISO, OWASP, etc.), rules and regulations related to information security and confidentiality (e.g., PCI, FERPA, GLBA, etc.).
- Familiarity with/knowledge of data protection, privacy, and cybersecurity related laws and regulations.
- Strong commitment to teamwork, knowledge sharing, and communication
- Ability to coordinate remotely with teams and colleagues
- Ability to demonstrate a professional, positive attitude and adherence to ethical standards
- Critical thinking and sound judgment, especially in urgent situations
- Adaptability to address urgent situations and needs, which may occur off-hours and over the weekend
- BA or BS in Computer Science, Information Management, or related field, or equivalent experience
- More than three years of progressive experience managing a comprehensive information security and/or IT risk management program including policy development, awareness and education, application and systems development requirements, network security, penetration testing, vulnerability assessment, risk analysis, incident response, and/or governance, risk, and compliance (GRC) management.
- Experience with Security Incident, Data Breach, and IT resilience response planning, testing, auditing, and risk analysis.
- CISSP, CISM, CIPP, CIPT, CRISC, GIAC, or other security, privacy, or IT risk management certification/ accreditation preferred.
- Experience in higher education.

APPLICATION INSTRUCTIONS

Please submit a resume and cover letter explaining how your qualifications meet the requirements of the position to itsjobs@oxy.edu and resumes@oxy.edu.

ADDITIONAL INFORMATION

Occidental is an Equal Opportunity Employer and does not unlawfully discriminate against employees or applicants on the basis of race, color, religion, sex, sexual orientation, gender identity, gender expression, pregnancy, breastfeeding or related medical condition, national origin, ancestry, citizenship, age, marital status, physical disability, mental disability, medical condition, genetic characteristic or information, military and veteran status, or any other characteristic protected by state or federal law. Occidental is strongly committed to increasing the diversity
of the campus community and the curriculum, and to fostering an inclusive, equitable, and just environment within which students, staff, administrators, and faculty thrive. Candidates who can contribute to this goal through their work are encouraged to identify their strengths and experiences in this area. Individuals advancing the College’s strategic equity and justice goals and those from groups whose underrepresentation in the field are particularly encouraged to apply.

Salary is commensurate with experience and qualifications. A comprehensive benefits package is available that includes: excellent health, dental, life, and retirement benefits; tuition benefits for the employee, spouse, domestic partner, and dependents; additional extras including use of gym facilities and the College Library. For a detailed description of benefits, please visit https://www.oxy.edu/offices-services/human-resources/benefits-information.

All qualified applicants will be considered for employment, including those with criminal histories, in a manner consistent with the requirements of applicable state and local laws, including the City of Los Angeles’ Fair Chance Initiative for Hiring Ordinance.

Occidental College is committed to working with and providing reasonable accommodations to applicants with qualifying disabilities. If you need a reasonable accommodation because of a disability for any part of the application or employment process, please contact Human Resources (hr@oxy.edu).

As a condition of hire for a staff position and for appointment to a faculty position, Occidental College requires that all candidates who have received a conditional offer of employment complete an application form (if they have not already done so) and consent to a background check. Satisfactory completion of a background check, along with pre-employment verifications and references are required as a condition of employment, but only as permitted by federal, state, and local law, including the City of Los Angeles Fair Chance Initiative for Hiring Ordinance.