

### SECURITY ENGINEER

**Reports to:** Information Technology Services Management

**Division:** Administrative Services

#### Our ideal candidate

You are a highly skilled and proactive security professional who designs, implements, and maintains technical safeguards to protect organizational data, networks, and systems. You excel at translating security policies and plans into actionable, technical solutions and procedures. With a strong understanding of the legal and regulatory landscape governing student data privacy and secure access in educational settings, you ensure that security practices meet the needs of a modern office environment as well as the specialized needs of Juvenile Court and Community Schools, Special Education, and Early Care and Education programs. You are detail-oriented, collaborative, and dedicated to ensuring a secure, compliant, and resilient technology environment.

#### General description

Under general direction, the Security Engineer serves as a technical lead for implementing security policy across all SBCEO systems and collaborates closely with leadership to align configurations with organizational strategy. In alignment with SBCEO security policies and plans, the Security Engineer ensures compliance with legal requirements and best practices and provides technical expertise to support secure operations countywide, across SBCEO programs and office sites, with particular attention to protecting sensitive student data and supporting school-based programs. With other ITS staff, implements and maintains security technologies, configurations, and procedures to protect SBCEO's information technology infrastructure and data.

#### Specific duties and responsibilities

- Draft and recommend SBCEO security policies and plans; execute security policies by implementing, monitoring, and maintaining technical security controls, including firewalls, intrusion prevention systems, endpoint protection, multi-factor authentication, and encryption.
- Perform ongoing security monitoring and log analysis to detect, respond to, and mitigate potential threats and vulnerabilities.
- Conduct regular security assessments, vulnerability scans, and penetration testing of networks, systems, and applications.
- Coordinate with the CTO and other ITS staff to execute incident response plans, ensuring timely and effective resolution of security incidents.
- Support the secure configuration and maintenance of networks, servers, cloud environments, and end-user devices.
- Collaborate with program administrators and ITS colleagues to ensure that security controls meet the unique requirements of SBCEO instructional programs, including Juvenile Court and Community Schools, Special Education, and Early Care and Education.
- Maintain awareness of emerging threats, vulnerabilities, and regulatory changes, providing recommendations to enhance security posture.

#### SECURITY ENGINEER

- Ensure compliance with all applicable laws and regulations related to data privacy and security, including Family Educational Rights and Privacy Act (FERPA), Children's Internet Protection Act (CIPA), and other relevant standards.
- Document and maintain security configurations, procedures, and response activities.
- Provide guidance and support to ITS staff and end-users on secure computing practices, assisting with awareness and training initiatives.
- Participate in disaster recovery and business continuity planning, ensuring critical systems can be restored securely.
- Ensure data used for Artificial Intelligence (AI)/automation complies with FERPA, CIPA, and SBCEO security policies.
- Monitor risks of generative AI and enforce acceptable use standards.
- May provide support and resources to local school districts and schools within Santa Barbara County, as assigned.
- Perform other related duties as assigned.

#### Requirements

A typical way to qualify for this classification would be:

**Education:** A bachelor's degree in computer science, information systems, electrical engineering, or a related field.

**Experience:** Three years of experience in information security in a multi-site environment that included design or implementation of secure network architectures, encryption technologies, application security, virtualization technologies, and secure coding practices.

Experience in an education or public sector setting is preferred.

Equivalent combinations of training, education, and experience that provide the required knowledge and abilities will also be considered.

### SECURITY ENGINEER

**Knowledge of:**

- Information security principles, standards, and frameworks (e.g., NIST, CIS Controls, ISO 27001).
- Network, endpoint, cloud, and application security best practices.
- Security technologies and tools, including firewalls, SIEM, IDS/IPS, anti-malware, and encryption.
- Legal and regulatory requirements for student data privacy and security (e.g., FERPA, CIPA).
- Incident response, disaster recovery, and business continuity practices.
- Risks and mitigation strategies associated with supporting diverse educational programs and sensitive populations.
- Correct English usage, grammar, spelling, punctuation and vocabulary.
- Standard office productivity software applications and modern office practices and equipment.
- Telephone and email etiquette.

**Ability to:**

- Implement and maintain effective technical security measures across complex IT environments.
- Analyze and respond to security threats and incidents effectively.
- Understand and apply legal and regulatory requirements to technical configurations and operations.
- Communicate clearly with technical and non-technical stakeholders regarding security matters.
- Collaborate with ITS team members, administrators, and program staff to support secure operations countywide.
- Document configurations, procedures, and incidents accurately and thoroughly.
- Stay current with emerging security trends, tools, and threats.
- Communicate effectively orally and in writing.
- Communicate technical information clearly to non-technical users.
- Produce a variety of written materials, including security protocols, incident reports, and draft policies.
- Collaborate effectively with ITS staff, administrators, and program staff to meet organizational needs.
- Work independently and as part of a team.
- Establish and maintain effective and professional working relationships with others.
- Exercise tact, patience, and courtesy in interactions with others.
- Interpret, explain and apply rules, regulations and policies.
- Maintain confidentiality of SBCEO data.
- Maintain accurate records, documentation, and reports.

#### SECURITY ENGINEER

**Licenses and certificates**

Possession of job-related certifications, such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), CompTIA Security+, or similar is preferred.

Possession of a valid California driver's license and the use of a dependable vehicle are required. These requirements may be waived if the incumbent is able to perform their duties efficiently using alternative means of transportation.

**Working conditions**

Work is performed primarily in an office environment, with travel to school and administrative sites throughout Santa Barbara County. May require work outside of regular hours to respond to urgent security matters or perform maintenance. Requires the ability to work in wiring closets, server rooms, and other technical spaces as needed.

**Series**

Information Technology

**Salary range 97**

*Approved by the Personnel Commission:*

*August 28, 2025*