



Senior Information Security Engineer

Job Description

Department: Information Systems
Position: Career Service
Grade: 731
Supervisory: Lead
Reports to: Division Manager - Information Security

Summary

Under general supervision of the Division Manager - Information Security, responsible for the design, development, implementation, monitoring, and maintenance of Utah County's information security programs. Protects the confidentiality, integrity, and availability of Utah County's Information Technology (IT) systems, networks, applications, and data. Assists with the creation of a comprehensive information security strategy, ensuring compliance with regulatory frameworks and best practices while mitigating security risks to County resources and infrastructure.

Essential Functions

Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

1. Design, develop, and implement comprehensive information security strategies to protect Utah County's IT systems, including networks, applications, voice, and data resources.
2. Lead the creation and integration of IT security and privacy programs to reduce the risk to County systems, applications, and data from security threats.
3. Collaborate with the Information Security Manager and other stakeholders to create and define policies, procedures, and technical strategies aimed at securing Utah County's infrastructure and ensuring compliance with applicable laws and regulations.
4. Conduct regular security assessments and audits of critical systems to identify complex vulnerabilities; design and recommend corrective actions, ensuring continuous improvement of security controls.
5. Manage security incident response efforts, including coordinating with internal and external teams to resolve and mitigate security breaches and vulnerabilities.
6. Serve as the primary escalation point for junior members of the security team, providing guidance, mentoring, and assisting in troubleshooting and resolving complex security incidents and technical issues.
7. Lead forensic investigations and provide expert technical guidance on data breach response and reporting procedures.

For Office Use Only

Job Code: 2903
Job Title: Senior Information Security Engineer
FLSA: Exempt
Effective Date: 1/6/2026
Public Safety: No

Worker's Compensation: Clerical
Background Level: I
Safety Sensitive: No
DOT: No
ML: Individual Contributor

8. Develop and lead security awareness programs and training efforts to reduce security risks and educate County employees, contractors, and partners on security best practices.
9. Establish and maintain positive business relationships with users countywide to actively market and educate them on the importance of security, cooperation, and compliance.
10. Conduct risk assessments, vulnerability management, and penetration testing to proactively identify and mitigate security threats.
11. Ensure and validate compliance with applicable regulatory frameworks and industry standards such as the Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), and other applicable standards relevant to County operations.
12. Collaborate and advise various departments, partners, and third-party vendors to enforce security requirements and address complex security concerns across the County's infrastructure.
13. Develop, review, maintain, and update documentation related to security procedures, incident response plans, system configurations, and operational workflows to ensure clarity, consistency, and compliance with internal standards and regulatory requirements.
14. Evaluate emerging threats, technologies, and security trends; develop technical assessments and recommend new tools, strategies, and technologies to strengthen the County's security posture.

Knowledge, Skills, and Abilities

- Knowledge of security concepts, principles, and best practices for protecting voice and data networks, applications, computer infrastructure, and cloud services
- Knowledge of Information security architecture, cloud security, and the use of advanced security controls in cloud platforms (SaaS, PaaS, IaaS)
- Knowledge of regulatory compliance requirements such as PCI-DSS, HIPAA, CJIS, and general data protection regulations (GDPR), and how to ensure security practices align with these standards
- Knowledge of risk management frameworks and methodologies, including conducting security audits, vulnerability assessments, and penetration testing
- Knowledge of current and emerging security technologies including but not limited to Firewalls, Remote Access Virtual Private Network (VPN), Email Security, Encryption, Vulnerability Management, Traffic Management, Endpoint Detection and Response (EDR), Managed Detection and Response (MDR), Incident Response, Identity and Access Management (IAM), Active Directory, Azure Active Directory, Cloud Security
- Skilled in strong verbal and written communication skills, with the ability to present complex security concepts to non-technical stakeholders
- Skilled in analysis and problem-solving, with the ability to develop and apply systematic approaches to resolve security-related issues

For Office Use Only

Job Code: 2903
Job Title: Senior Information Security Engineer
FLSA: Exempt
Effective Date: 1/6/2026
Public Safety: No

Worker's Compensation: Clerical
Background Level: I
Safety Sensitive: No
DOT: No
ML: Individual Contributor

- Skilled in managing and prioritizing multiple tasks in high-pressure environments while maintaining a focus on security and risk mitigation
- Skilled in using security tools such as Security Information and Event Management (SIEM), intrusion detection/prevention systems, vulnerability management platforms, and endpoint protection tools
- Ability to work in a high-pressure environment with a high volume of urgent user needs
- Ability to analyze security data and threat intelligence to proactively address vulnerabilities and improve overall security posture
- Ability to provide technical guidance and subject matter expertise to team members and internal stakeholders, fostering a culture of security awareness and compliance
- Ability to set priorities and maintain overall user satisfaction
- Ability to maintain cooperative relationships with those contacted during work activities
- Ability to ensure commitment to quality standards and processes and efficient delivery

Supervisory Responsibility

This position currently has no direct supervisory responsibility but serves as a coach and mentor for other positions in the department.

Work Environment

This job operates in a professional office environment but occasionally exposes incumbent to electrical hazards during systems installation and maintenance. This position exposes incumbent to stress due to project deadlines, systems failures, system recovery, managing employee performance, and meeting state and federally mandated requirements, regulations, and certifications. Work may expose the incumbent to high stress situations including contact with the public and others in confrontational, emotionally charged, or uncomfortable circumstances. This role routinely uses standard office equipment such as laptops, desktops, smartphones, photocopiers, shredders, and filing cabinets. The noise level in the work environment is usually moderate. The incumbent may be required to drive Utah County owned vehicles while conducting County business and must abide by the Utah County Vehicle Policy.

Physical Demands

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job.

While performing the duties of this job, the employee is required to use manual dexterity to handle, feel, and operate objects, tools and controls, and reach with hands and arms. The employee is frequently required to stand, talk, and listen. Specific vision abilities by this job include close vision and ability to adjust focus. The employee is required to type, file, and lift supplies up to thirty (40) pounds. The employee occasionally drives a motor vehicle.

For Office Use Only

Job Code: 2903
 Job Title: Senior Information Security Engineer
 FLSA: Exempt
 Effective Date: 1/6/2026
 Public Safety: No

Worker's Compensation: Clerical
 Background Level: I
 Safety Sensitive: No
 DOT: No
 ML: Individual Contributor

Position Type / Expected Hours of Work

Incumbent must work eighty (80) hours each pay period to maintain full-time status. There may be availability to work out a flex schedule ahead of time that works for both the County and the employee. Occasional evening and weekend work may be required as job duties demand.

Travel

Travel is primarily local during the business day, although some out-of-area and overnight travel may be expected, up to five (5) percent.

Required Education and Experience

1. Bachelor's degree from an accredited college or university in information security or a closely related field.
2. Four (4) years of hands-on experience in information security, including roles focused on network security, application security, and incident response.
3. Equivalent combinations of education, experience, and demonstrated work competence may also be considered.

Preferred Education and Experience

1. Preference may be given to applicants with lead or supervisory experience.
2. Preference may be given to applicants with certifications such as Certified Information Systems Security Professional (CISSP) and/or Certified Information Security Manager (CISM).
3. Preference may be given to applicants with experience in implementation of the NIST Cyber Security Framework (NIST CSF).
4. Preference may be given to applicants with a master's degree in information security or a closely related field.

Additional Eligibility Qualifications

1. Applicants must possess a valid driver's license and obtain a valid State of Utah driver's license within sixty (60) days of employment.
2. Selected applicants will be required to submit to a pre-employment drug screen and background check. Due to potential access to sensitive protected data, this position is subject to additional criminal background checks as directed by the Information Systems Department.

AAP/EEO Statement

It is the policy of Utah County Government to assure equal employment opportunity to its employees and applicants for employment without regard to race, color, religion, national origin, disability, age, sex, sexual orientation, genetic status or gender identity.

For Office Use Only

Job Code: 2903

Job Title: Senior Information Security Engineer

FLSA: Exempt

Effective Date: 1/6/2026

Public Safety: No

Worker's Compensation: Clerical

Background Level: I

Safety Sensitive: No

DOT: No

ML: Individual Contributor

Other Duties

Please note this job description is not designed to cover or contain a comprehensive listing of activities, duties, or responsibilities that are required of the employee of this job. Duties, responsibilities, and activities may change at any time.

Utah County Government is a drug-free workplace.

Acknowledgement below to be completed after an offer has been extended and accepted.

This job description has been approved by the Office of Human Resource Management in consultation with the Department Head.

Signature below constitutes an understanding of the requirements, essential functions and duties of the position.

Candidate / Employee _____ Date _____

For Office Use Only

Job Code: 2903

Job Title: Senior Information Security Engineer

FLSA: Exempt

Effective Date: 1/6/2026

Public Safety: No

Worker's Compensation: Clerical

Background Level: I

Safety Sensitive: No

DOT: No

ML: Individual Contributor