Judicial Council of Georgia
Administrative Office of the Courts
JOB ANNOUNCEMENT

Information Security Officer

Recruitment Period: Submit resume by May 15, 2018

Number of Positions: One (1) position

FLSA Status: Exempt

Salary: $80,000-$90,000

Position Location: Atlanta, Fulton County

Job Summary

The Administrative Office of the Courts seeks to fill a full-time Information Security Officer position within the Information Technology Division. Under limited supervision, the Information Security Officer performs critical tasks to support network viability. The Information Security Officer (ISO) serves the agency as a primary point of contact for cybersecurity planning, implementation, and response.

The Information Security Officer focuses on ensuring that network systems and devices are properly secured and tests systems to identify and defend against security threats including unauthorized access, modification and/or destruction. The Information Security Officer also works actively with managers, staff, and consults with judicial partners to train employees in security awareness and procedures.

The Information Security Officer provides technical assistance and guidance to network administrators and coordinates installation, configuration, security and support of a local area network, wide area network, internet system, computers, desktops and/or mobile devices.

The position offers a competitive fringe benefits package including health, dental, and vision insurance. Employees also earn both sick and annual leave in addition to 12 paid holidays per year.

Primary office hours are 8:30 am to 5:00 pm, Monday through Friday. Occasional evening/night or weekend availability and travel may be required for critical and planned maintenance or unplanned outages or events. This position is located in Atlanta, Fulton County, with some teleworking options available.

Job Responsibilities and Performance Standards:

1. Serves as the agency's Information Security Officer (ISO)

    - Works with other ISOs across the state to identify threats and appropriate defense and mitigation strategies
    - Participates in statewide cybersecurity tests and exercises as appropriate
    - Trains fellow employees in security awareness and procedures

- Serves as a security resource and provides guidance and technical assistance to other staff
- Works with external partners to coordinate security of data transfers and systems
- Serves as a resource to the Judicial Branch for consultation on security related matters
- Responds to security incidents in accordance with agency protocols
- Conducts agency level testing and coordinates internal exercises to ensure that agency is prepared to respond to security events and natural disasters
- Coordinates with other appropriate agencies to respond to incidents as needed

2. Installs, secures and supports network operating systems for the JC/AOC

- Plans, coordinates, and implements network security measures to protect data, software, and hardware
- Implement network security policies, application security, access control and data safeguards
- Tests network components and applications, and evaluate results as needed to ensure all users can securely access applications
- Assures that software is properly licensed (registered) and that unauthorized copies are not made or used
- Coordinates synchronization of multiple storage area networks to insure data redundancy, integrity and availability
- Reports unresolved questions to appropriate personnel
- Maintains and secures network VPN access for remote users and remote offices
- Utilizes diagnostic tools and other resources as appropriate

3. Defends systems from unauthorized modification and access

- Regularly monitor network traffic for any unusual activities
- Install and support security software and tools like anti-virus tools, firewalls and manage patch management
- Implement application security, access control, network security policies and data safeguards
- Identifies and implements security measures that are appropriate to the information and systems to be protected
- Regularly tests security systems and strategies and documents weaknesses and vulnerabilities identified
- Develops and implements new defensive systems as needed to defend against new threats and vulnerabilities identified through testing

4. Designs, configures, and tests the development and support of networks. Recommends standards, specifications and methodologies for the network operations of the Judicial Council/Administrative Office of the Courts (JC/AOC)

- Establish and analyze security requirements for existing networks and new systems
- Perform networking and vulnerability scanning assessments
- Update and develop disaster recovery protocols and business continuity plans

5. Coordinates and oversees the operation and security of all Local Access Network (LAN) systems. Maintains security and integrity of LAN systems

    - Coordinates and/or performs the troubleshooting and diagnostics of all LAN components and applications as needed
    - Coordinates and/or performs the maintenance of current documentation on LAN components and/or applications per the agency requirements
    - Controls and maintains inventory of assigned network and server equipment per agency guidelines

6. Develops and updates business continuity and disaster recovery protocols

    - Coordinates and performs data backups and disaster recovery operations
    - Coordinates, reviews and participates in regular back-up procedures and ensures others comply with back-up procedures
    - Coordinates and/or conducts recovery of LAN systems as required/needed
    - Develops, updates, and recommends protocol

7. Coordinate and provide user, vendor and customer security training

    - Work with customers and vendors to identify and classify data that needs to be protected
    - Determine security measures best suited to the information being protected
    - Explain security measures being taken to staff, customers, contractors, and vendors
    - Coordinate security training and documentation to ensure that security protocols and clearly understood and can be followed by staff, customers and vendors
    - Monitor security compliance and report ongoing issues to management for remediation if needed

8. Maintains a consistently high level of quality, customer-focused orientation when conducting business and providing services and products to users

9. Maintains a high level of technical skill by attending and completing various seminars and training courses and reading appropriate literature. Communicates this knowledge to others as required

10. Attends and supports activities of the Judicial Council Technology Committee.

Minimum Job Requirements:

- Bachelor's Degree in Information Technology, Computer Science or a related field from an accredited institution; or four years equivalent work experience may be substituted.
- Three years' experience working with Microsoft server administration, design and implementation in an enterprise environment.
- Experience working with virtualization technologies, including VMware and Citrix XenApp
- Three years' experience with server and application deployment and administration.
- Three years' data backup and recovery design, implementation and administration in windows environments.
- One year experience actively designing, implementing and managing security of network systems

- Strong oral and written communications skills
- Previous experience with one or more of the following firewalls such as Checkpoint, CISCO, Juniper or McAfee

Preferred Qualifications:

- Related Microsoft Certifications (MCSE and/or MCSA)
- CompTia Network + or equivalent
- CompTia Security + or equivalent
- Experience with Cisco UCS, switches, routers and firewalls
- Experience with SAN and backup technologies

To apply:
Applicants must submit a resume to resume@georgiacourts.gov by close of business **May 15, 2018**. This position is subject to close at any time once a satisfactory applicant pool has been established.

Subject line must include: Information Security Officer

Additional Information:

Due to the volume of applications received, we are unable to provide information on application status by phone or email. All qualified applicants will be considered, but may not necessarily receive an interview. Selected applicants will be contacted by the hiring manager to complete next steps in the hiring process.

Applicants who require accommodations for the interview process should contact resume@georgiacourts.gov or call 404-463-0638. The JC/AOC will attempt to meet reasonable accommodation requests whenever possible.