



**STATE OF NORTH CAROLINA**  
invites applications for the position of:  
**IT Security Engineer**

**JOB CLASS TITLE:** IT Security & Compliance Specialist II

**POSITION NUMBER:** 65027809

**DEPARTMENT:** State Board of Elections

**DIVISION/SECTION:** Information Technology

**SALARY RANGE:** \$74,987.00 - \$121,857.00 Annually

**RECRUITMENT RANGE:** \$74,987 - \$100,600

**SALARY GRADE / SALARY GRADE EQUIVALENT:** IT08

**COMPETENCY LEVEL:** Not Applicable

**APPOINTMENT TYPE:** Time-Limited Full-Time

**WORK LOCATION:** Wake County

**OPENING DATE:** 12/02/20

**CLOSING DATE:** 12/17/20 5:00 PM Eastern Time

**DESCRIPTION OF WORK:**

\*\*\*This position is grant funded and time limited up to 3 years. Additional years of service is contingent upon fund availability and management discretion\*\*\*

Max Salary: **Up to** \$100,600 (subject to education and qualifications)

**Description of Agency:**

The State Board of Elections oversees the enforcement of federal and state laws, rules, and procedures governing the conduct of elections, voter registration, and campaign finance activities in North Carolina.

**Primary Purpose of the Position:**

The Information Technology Security Engineer is responsible for the operation of agency security infrastructure, technical security guidance in the application of best practices, and ensuring that the configuration of agency systems, applications and networks are in compliance with agency security policies. This position requires broad technical expertise, sophisticated problem solving and critical thinking, excellent documentation skills, security experience, and the ability to communicate complex topics clearly and effectively.

The primary goal of this position is to ensure the proper function of agency information security systems and solutions on a day to day basis.

This position is also required to identify, plan, document, execute, and report on continuous improvement activities related to security and other tasks as assigned.

Successful candidates will demonstrate the desire and ability to learn skills to grow into activities required for the position where the candidate does not currently possess such skills.

This position will be subject to a background check. DHS carries all security clearances for SBE. This position may require the receipt and ongoing maintenance of a security clearance.

## Description of Duties

### Operational Activities

- Daily operation of security solutions within the agency to include implementation and operational support
- Conducts first responder activities related to security incident response (This includes alerting information security leadership, working with the affected parties to identify if there is a problem, capture appropriate data, and work through appropriate remediation activities)
- Coordinates the general maintenance and installation of security applications and appliances
- Assists with security event monitoring and review as well as any remediation efforts
- Performs activities relating to security testing, project driven security improvements, and additional security operations activities as tasked
- Continuously evaluates current security solutions effectiveness and provides input for future improvements; this includes analysis and selection of security solutions, as tasked.
- Oversees general health of all security appliances and applications in the environment
- Addresses security related cases and tickets both as assigned and proactively
- As tasked, review of software and solutions at the agency from a security perspective
- As tasked, reviews and recommendations of firewall rule additions/modifications and some security policy exceptions

### Business Activities

- Develops implements and maintains the technical methods, procedures and processes associated with securing agency systems, applications, and networks in compliance with agency security policies
- Works with agency IT, development, and other personnel to consultatively provide technical security advice and best practice recommendations, also provides education and guidance on agency security practices and policy.
- Actively contributes to and helps maintain the agency Information Security run book and associated documentation
- Interfaces with vendor support to troubleshoot and maintain the functionality of vendor provided solutions
- As tasked, facilitates security focused code review of internally developed applications

### Policy & Compliance Activities

- Proactively works with agency IT personnel to identify and remediate security risks
- Embraces technological change while seeking to ensure that it is deployed in a secure manner
- Provides technical support for **both internal and external** security audits, **security-related audit issue tracking**, and risk assessments
- As tasked, documents, and reports on internal investigations of possible security violations
- As tasked, and where appropriate, conducts analysis and creates reports such as those relating to vulnerability management, tracks and assists with remediation where necessary
- As tasked, conducts access and security activity reviews (internal and external), reports findings, and assists with remediation where appropriate

### Initiative & Continuous Improvement

- Self-manages security-related projects and initiatives and takes ownership of security tickets through resolution
- Maintains a regimen of self-study to stay current on the latest security exploits, technologies, and news to protect agency networks, applications and systems from current and future attacks and exploits
- Follows company policy regarding internal controls as well as complies with agency policies to ensure that the employee and the company act legally and with the highest standards of ethics and integrity

## **KNOWLEDGE, SKILLS AND ABILITIES / COMPETENCIES:**

### **Required**

- 2+ years of technical IT experience in systems, networks, and applications
- 2+ years of experience in a security-related position
- Operational experience in both Windows and Linux operating systems
- Understanding of configuration management, general server administration, different authentication technologies, network services and protocols
- Understanding of risk assessment
- Understanding of scripting and programming
- Must be self-directed, have excellent initiative and organizational skills
- Excellent communication and prioritization skills
- Exhibit a strong ability to handle multiple demands with a sense of urgency, drive, and energy
- Works well in a fast-paced environment with the ability to deliver on time
- Proven track record of meeting commitments with the highest standards of ethics and integrity
- Flexibility and adaptability to changing needs and demands dictated by business and IT requirements
- Minimal travel may be required

### **Suggested**

- 3+ years of experience in IT or security-related positions
- Strong operational knowledge of Information Security technologies including hardware and software for servers, network, applications (including web and mobile), security and messaging platforms; such as, VPN, Firewalls, IDS/IPS, Vulnerability Management, Penetration Testing, MFA/SSO, SAML, SSL/TLS (key use and management), Directory Services, Threat Detection & Mitigation, Antivirus/EDR, Proxy and Filtering, and SIEM/Log Collection and how these systems apply operationally to information technology systems
- Understanding of incident response and related forensics and data preservation processes
- Understanding of identity and access management concepts, applications, in both on premise and cloud-based uses, especially Microsoft Windows Active Directory (security, groups, and role membership)
- Understanding of system and software life cycle management as it pertains to security,
- Familiarity with security frameworks such as NIST, COBIT, RMF, CMMC or others
- Experience working in a large-scale enterprise environment

## **MINIMUM EDUCATION AND EXPERIENCE REQUIREMENTS:**

Bachelor s degree in Computer Science, Computer Engineering or an Information Security degree or closely related field from an appropriately accredited institution and two year of experience in IT Security or closely related area; or Bachelor s degree from an appropriately accredited institution and three years of experience in IT Security or closely related area; or Associate s degree in Information Systems Security from an appropriately accredited institution and three years of experience in IT Security or closely related area; or an equivalent combination of education and experience.

## **SUPPLEMENTAL AND CONTACT INFORMATION:**

All applicants must complete and submit a State application for employment using the NEOGOV Online Job Application System (<http://www.oshr.nc.gov/jobs/>) for the State of North Carolina. To receive credit for your work history and credentials, you must list the information on the online application form. Any information omitted from the application cannot be considered for qualifying

credit. Attached or incorporated resumes (including Text Resumes on application form) WILL NOT be used for screening for qualifying credit. Please make sure you complete the application in full. "See Resume" or "See Attachment" will NOT be accepted. Other attachments (except a DD-214 copy) will also be accepted, but not used in screening for qualifying credit. Applicants are required to scan and attach a copy of their DD-214 (Form 4 or Certificate of Release or Discharge from Active Duty) or discharge orders if they wish to obtain Veteran's preference. Applicants may be subject to a criminal background check.

**Due to the volume of applications received, we are unable to provide information regarding the status of your application over the phone. To check the status of your application, please log in to your account and click "Application Status". It is not necessary to contact the Human Resources Office to check the status of an application.**

If you are having technical issues submitting your application, please call the NEOGOV Help Line at **855-524-5627**. If there are any questions about this posting, other than your application status, please contact the Elections and Ethics Human Resources Office.

### CONTACT INFORMATION

NC Board of Elections  
Human Resources Management Office  
430 N. Salisbury Street  
Raleigh, NC 27603  
Phone: 919-814-0700

---

APPLICATIONS MAY BE FILED ONLINE AT:  
<http://www.oshr.nc.gov/jobs/index.html>

Position #65027809-12022020  
IT SECURITY ENGINEER  
SC

NOTE: Apply to the department listed on posting  
An Equal Opportunity Employer, NC State Government

[noreply@nc.gov](mailto:noreply@nc.gov)

---

### IT Security Engineer Supplemental Questionnaire

- \* 1. I understand that the budgeted salary for this position is limited to \$100,600. If offered this position, the salary offered will be within the posted recruitment range.  
 Yes    No
- \* 2. Which of the following best describes the highest level of post-secondary education you have attained?  
 No college  
 Some college  
 Associate Degree  
 Bachelor's Degree  
 Master's Degree or higher
- \* 3. If you have a Bachelor's degree or higher, please indicate your major(s). If you do not have a Bachelor's degree, type "N/A."
- \* 4. Do you have experience responding to security incidents?  
 Yes    No
- \* 5. Do you have experience writing or modifying scripts?

Yes  No

\* 6. Do you have working knowledge of industry best practice, i.e., NIST Standards, etc.?

Yes  No

\* 7. Do you have experience in commercial or open source tools?

Yes  No

\* 8. If you do have experience in commercial or open source tools, please specify.

\* 9. Which of the following best describes your experience with network infrastructure, including routers, switches, firewalls and associated network protocols and concepts?

None

Less than 2 years

2 - 3 Years

3 - 4 Years

4 - 5 Years

5+ years

\* 10. Do you hold any Security certifications?

Yes  No

\* 11. If you answered "yes" to the previous question, please indicate the Security Certifications you hold.

\* Required Question