

**Cyber Security Analyst**  
New Hanover County Schools

**Job Description**

Class: Classified  
Dept: Technology

**TITLE:** Cyber Security Analyst

**QUALIFICATIONS:**

1. Bachelor's degree in Computer Science, Information Technology, or a related field or equivalent combination of education, experience, and cyber security related certifications.
2. Three or more years of experience in network administration
3. One year of experience in network security
4. Valid North Carolina driver's license.

**REPORTS TO:** Director of Network Security

**JOB GOAL:** Maintain IT security measures within NHCS. Manage vulnerabilities and threats while developing strategies to handle security incidents. Implement education programs for end user awareness as well as safety and security compliance.

**ESSENTIAL FUNCTIONS AND RESPONSIBILITIES:**

1. Follow all rules, policies and procedures of New Hanover County Schools, along with state and federal regulation pertaining to schools and technology.
2. Implement security measures and controls.
3. Secure digital files and information systems, protecting them from unauthorized access or tampering.
4. Provide technical support and monitor security access.
5. Perform regular internal and external security audits.
6. Analyze the source of security breaches.
7. Implement security tools and anti-malware software.
8. Enforce district security procedures and policies.

9. Inform management of security vulnerabilities.
10. Identify cybercrime perpetrators and liaise with the appropriate authorities if necessary.
11. Implement and maintain firewalls to protect network infrastructure.
12. Research and recommend best ways to secure company-wide IT infrastructure.

The above statements describe the general nature and level of work being performed by the individual assigned to this job. This is not intended to be an exhaustive list of all responsibilities and duties required of personnel so employed.

Terms of Employment: Twelve-month work year/At Will/FLSA Exempt

Starting Salary and/or Grade: SA-IV

Evaluation: Performance of this job will be evaluated in accordance with provisions of the Board and local policy on evaluation of personnel.

Knowledge, Skills and Abilities:

- Demonstrate a strong knowledge of endpoint protection, antivirus/anti-malware.
- Demonstrate a strong knowledge of Cisco network equipment, including but not limited to FirePOWER Threat Defense, Cisco Umbrella, Cisco ISE.
- Demonstrate strong knowledge of security devices, routers, and switches; protocols (TCP/IP, DNS, SSL,SMTP SNMP, NTP FTP, HTTP, HTTPS); network monitoring tools and security; basic office tools, spreadsheets, word processing, and presentation generation tools.
- Demonstrate a strong knowledge of Microsoft Active Directory.
- Demonstrate functional knowledge of account provisioning, management, and automation.
- Maintains detailed documentation regarding network configuration, operating procedures, and service records relating to network security.
- Demonstrate functional knowledge of general programs, policies, and practices used in educational organizations; computer software installation and training.
- Demonstrate functional knowledge of long range and strategic planning concepts; ability to effectively administer a variety of projects/abilities simultaneously.
- Ability to analyze problems, identify alternative solutions, project consequences or proposed actions and implement recommendations in support of goals.
- Demonstrate strong knowledge of cloud cybersecurity.
- Ability to interface with vendors, staff and law enforcement over security matters.