NHRS
New Hampshire Retirement System

NEW HAMPSHIRE RETIREMENT SYSTEM
CAREER OPPORTUNITY

Information Security Administrator

Interested and qualified applicants please submit resumes to the NHRS Human Resources team via email at careers@nhrs.org or apply on line

Position Title: Information Security Administrator

Functional Area: Information Technology (IT) **Date Established** 02/2022

Title of Supervisor: Director of IT **Date of Last Amendment:** 6/01/2022

NHRS Position Band/Min. Step: N/A **Collective Bargaining Unit Status:** Not in unit

FLSA Status: Exempt

Supervises: Various IT positions

SCOPE OF WORK:

The Information Security Administrator is responsible for researching, developing, implementing, testing and reviewing NHRS' information security in order to protect information and prevent unauthorized access. This position also supports security initiatives and NHRS policy adherence and awareness efforts and provides security expertise to business units and key stakeholders.

ACCOUNTABILITIES:

- Using the Risk Management Framework of record, conduct assessments of information security controls in order to measure the effectiveness of controls and identify control gaps.
- Monitor IT Security solutions for alerts, and when necessary, research and analyze available information to determine validity of alert and any actions to be taken.
- Oversee the vulnerability management program, including scanning and analysis, working closely with peers in infrastructure and applications to evaluate pre-deployment assessments, ensure closed-loop remediation process and ongoing comprehensive consistent scanning.

- Coordinate and perform security audits and system updates.
- Maintain relations with operations, management and team members to ensure compliance.
- Identify, assess, and prioritize identified risks, collect evidence, artifacts, and document findings to support conclusions, report on compliance with internal policies, controls, and standards, and provide recommendations for remediation of identified deficiencies.
- Manage remediation efforts and report on the status of control deficiencies, this will include working with external partners.
- Ensure compliance to guidance and standards such as NIST Publications, NHRS policies and procedures, and other industry best practices.
- Coordinate third-party risk assessments and IT audits. The IT Audits include physical audits of offices and remote sites.
- Manage security awareness training using NHRS approved software, and coordinate with third parties for onsite trainings and HR for tracking.
- Enforce policy adherence and manage formal policy exception requests.
- Provide timely status updates/reporting on assessments and assigned projects.
- Actively participates on NHRS' Management Team, including development and implementation of strategic planning initiatives, collaborative problem solving and various project initiatives.
- Carries out supervisory responsibilities in accordance with the organization's policies and applicable laws. Responsibilities include interviewing, hiring and training employees; planning, assigning and directing work; appraising performance; rewarding and disciplining employees; addressing complaints and resolving problems.
- Provide back up and assistance to others on the IT team, which include roles in Network and Server administration, and help desk duties.
- Other appropriate and related duties as assigned by supervisor.

MINIMUM QUALIFICATIONS:

Education: Bachelor's degree in Computer Science or a related engineering field with training in information security. Master's degree preferred

Experience: 8+ years of IT Security related work, either as a primary or secondary job responsibility. 5+ years' experience building and managing Windows server platforms. Experience using security scanners and remediating vulnerabilities, or similar tools. Experience in creating and maintaining minimum-security configuration baselines for Windows platforms and applications (i.e., Minimum Benchmarks: CISA, STIGS, NIST SP 800-53). Experience in management a plus.

Certifications: Security certifications are a plus: CISSP, Security+, CySA+.

License: Valid driver's license preferred.

SPECIAL REQUIREMENTS:
RECOMMENDED KNOWLEDGE, SKILLS, AND TRAITS:

- Experience using vulnerability scanning and pentesting tools.
- Experience with endpoint protection tools, SIEMS, MSSPs, and WAFs.
- Project and Program Management, Risk Analysis, and Risk Management.
- Proficient in Cybersecurity Awareness Programs, including training, assessments, coordinate with offsite venders to enhance security posture.
- Proficient in Microsoft Office (Word, Excel, PowerPoint, etc.)

PHYSICAL REQUIREMENTS:

- This position requires sitting (80%), standing (5%), and walking (15%).
- Requires lifting materials of approximately 20-25 lbs.
- Often requires computer responsibility, which involves extensive use of keyboard, mouse and monitor.

WORK ENVIRONMENT/CONDITIONS:

- Dayshift hours primarily, although overtime may be required in meet project deadlines.
- Physically able to participate in training sessions, presentations, and meetings.
- Work related assignments on weekends are possible.