NHRS
New Hampshire Retirement System

NEW HAMPSHIRE RETIREMENT SYSTEM

Career Opportunity

Information Security Analyst

Position Title: Information Security Analyst

Functional Area: Information Technology (IT) **Date Established** 8/20/2025

Title of Supervisor: Chief IT Officer **Date of Last Amendment:** N/A

NHRS Position Band/Min. Step: M **Collective Bargaining Unit Status:** In unit

FLSA Status: Non-exempt

Supervises: None

SCOPE OF WORK:

The Information Security Analyst (ISA) is responsible for leading the development, implementation, and continuous improvement of NHRS' information security program to ensure the confidentiality, integrity, and availability of systems and data by proactively defending against unauthorized access and cyber threats. This position supports security initiatives, promotes policy adherence and awareness efforts, and acts as the primary security advisor to NHRS leadership and business units. The ISA helps translate cybersecurity risks into business terms and ensures that security strategies are aligned with organizational goals.

ACCOUNTABILITIES:

- Using NHRS' adopted framework of record, conduct assessments of information security controls in order to measure their effectiveness and identify gaps. Participates in the selection and socialization of the framework.
- 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.

- Work collaboratively on remediation efforts and report on the status of control deficiencies, engaging as needed with internal and external partners.
- Ensure compliance with guidance and standards such as NIST Publications, NHRS policies and procedures, State of NH legislation, and industry best practices.
- Lead third-party risk assessments and support internal and external IT audits, including preparation of materials, evidence gathering, and coordination with audit teams.
- Manage security awareness training using NHRS approved software, and coordinate with third parties for onsite trainings and ensure participation is documented.
- Create and maintain IT policies. Enforce policy adherence and manage formal policy exception requests.
- Provide timely status updates and report on assessments and assigned projects.
- Provide limited backup support to infrastructure and help desk functions as needed, while maintaining primary responsibility for cybersecurity program execution and risk oversight.
- Develop and maintain a risk register to track identified risks. Ensure that IT and executive staff who need to consume it have the necessary training and access. Highlight areas of high risk to executive staff and/or Audit Committee members that include deficiencies preventing resolution.
- Create reports to describe the cybersecurity posture of NHRS for various stakeholders.
- Participate in Incident Response. Take primary responsibility to ensure that the Incident Response Plan is up to date, that it is appropriately disseminated and users are trained on it throughout the organization, and that it is available as needed.
- Other appropriate and related duties as assigned by supervisor.

MINIMUM QUALIFICATIONS:

Education: Bachelor's degree in computer science or a related field with training or experience in information security. Master's degree in computer science or business preferred. Qualified work experience may be substituted for formal education.

Experience: Combined 15 years' experience in Information Security and Windows administration.

Certification: Security certifications preferred, such as CISSP, CISM, Security+, or CySA+. NHRS supports professional development and encourages continued certification and training.

License: Valid driver's license preferred.

SPECIAL REQUIREMENTS:

- Experience managing the remediation process in coordination with IT and third-party vendors.
- Experience with data manipulation and visualization, including pivot tables, data extraction and clean up, and creation of reports including various charts and drill down.
- Experience in creating and maintaining minimum-security configuration baselines for Windows platforms and applications (i.e., Minimum Benchmarks: STIGS, US-CERT).
- Demonstrated experience with SIEM platforms, log correlation, threat detection, and incident response processes. Ability to analyze anomalies and escalate incidents based on defined thresholds.
- Experience developing, maintaining, and enforcing cybersecurity policies, standards, and procedures, and facilitating policy governance processes including formal reviews and exception tracking.
- This position may require some in-state travel and the ability to work a flexible schedule, including periodic evening hours.

RECOMMENDED KNOWLEDGE, SKILLS, AND TRAITS:

- Cybersecurity principles and practices, understanding of network security, encryption, authentication, and vulnerability management.
- Regulatory and compliance, familiarity with frameworks and standards such as NIST, ISO 27001, HIPAA, or GDPR.
- Threat Intelligence, knowledge of threat actors, malware behavior, and current cybersecurity trends and attack vectors.
- Risk assessment and mitigation, ability to identify, assess, and develop strategies to minimize risks to information systems.
- Incident response and investigation, proficiency in analyzing breaches, conducting forensic investigations, and documenting findings.
- Proficiency with security tools, experience with SIEM, firewalls, IDS/IPS, endpoint protection, and vulnerability scanning tools.
- Analytical and detail-oriented, strong critical thinking skills and attention to detail for monitoring, troubleshooting, and analyzing anomalies.
- Integrity and discretion, trustworthy and ethical when handling sensitive and confidential information.

- Skilled in utilizing data analytics and visualization tools to interpret and present data effectively.
- Strong communication skills, both written and verbal, with the ability to explain complex technical concepts to a non-technical audience.

PHYSICAL REQUIREMENTS:

- The employee must have the ability to maintain regular, punctual attendance consistent with the ADA, FMLA and other federal, state, and local standards.
- Communicate with others to exchange information. (Constantly)
- Analyze accuracy, neatness, and thoroughness of the work assigned. (Constantly)
- Requires computer responsibility which involves extensive use of keyboard, mouse and monitor, and repeat motions that include the wrist, hands, and/or fingers. (Constantly)

WORK ENVIRONMENT/CONDITIONS:

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

EXPECTATIONS OF NHRS EMPLOYEES:

Commit passionately to the vision and mission for NHRS.

Exercise diligent fiduciary responsibility – Act first and foremost as fiduciaries. Whether it is an investment decision or an expense incurred to administer the System, it must be made with members in mind.

Do what is right for the member, always – Provide member service at the highest level. *Every* member should receive the *same* level of *excellent* service. Decisions must be made with the benefit of all members in mind – not that of any individual or member group.

Accept responsibility – NHRS is New Hampshire's largest locally organized financial institution. This is exemplified by bringing professional expectations to our work. Commit to doing excellent work and trust that colleagues will also.

Operate transparently – While guarding the integrity of member information, provide responsive and accurate information, data, and analysis to our many stakeholders, including members and their employee groups and associations, employers, the Legislature and its committees, and the public.

Adhere to legal frameworks that NHRS operates under – State and Federal law, constitutional mandates, IRS provisions, and NHRS rules and procedures all have a place in ensuring that fiduciary obligations are met.

DISCLAIMER STATEMENT

This description lists typical examples of work and is not intended to include every job duty and responsibility specific to a position. An employee may be required to perform other related duties not listed on the job description provided that such duties are characteristic of that position.