

VACANCY ID #210801

## EMPLOYMENT ANNOUNCEMENT



**TITLE: INFORMATION TECHNOLOGY SPECIALIST 3 (INFO SECURITY)**

**STATUS: PERMANENT NON-COMPETITIVE**

**BUREAU: INFORMATION TECHNOLOGY**

**LOCATION: LATHAM**

**SALARY GRADE (SG): PEF SG23 (\$86,681-\$109,650)**

---

We are seeking talented and motivated support staff to work with our attorneys in the State's law firm. The selected candidate will be part of a fast-paced office, gaining experience while providing public service on behalf of the State of New York. The [Attorney General](#) serves the public interest of all New Yorkers in matters affecting their daily lives, enforcing laws to protect consumers, tenants, patients, workers, investors, and charitable donors. The office coordinates statewide civil and criminal investigations, promoting economic and social justice, encouraging harm-reducing public health strategies, and preserving the state's environment.

Careers with the State offer multiple benefits, including **paid vacation leave (13+ days per year)**, sick leave, **paid State holidays off, health insurance** including vision & dental, entry into the **NYS retirement** (pension) system, education and training, eligibility for public student loan forgiveness, and **job stability with promotional opportunities**. Workplace flexibilities include multiple options for employees, including **telecommuting** (up to two days per week) and alternative work schedules.

---

### **MINIMUM QUALIFICATIONS**

Bachelor's degree with at least 15 credit hours in cyber security, information assurance, or information technology; and two years of information technology experience, at least one year of which is information security or information assurance experience.

OR

A bachelor's degree in any field with at least three years of information technology experience, at least one year of which is information security or information assurance experience.

OR

An associate's degree in any field with five years of general information technology experience at least one of which is information security or information assurance experience.

OR

At least seven years of information security or information assurance experience.

---

### **DUTIES**

Under the direction of the Manager of Information Technology Services (Information Security) 1 of the Security Operations Unit, the Information Technology Specialist 3 (Information Security) will serve as an Identity and Access Management (IAM) Administrator for Microsoft Entra, managing identity and access systems, and ensuring secure access to both on-premises and cloud-based resources. This role requires expertise in Microsoft Entra, identity governance, and authentication protocols. This role is responsible for maintaining user access, enforcing security policies, and integrating IAM systems with other security tools to ensure the integrity and security of the organization's identity management infrastructure. By controlling and securing access to critical resources, this position directly enhances the agency's ability to prevent unauthorized access and maintain a strong security framework.

- Lead the development and implementation of the IAM strategy to be aligned with business objectives and regulatory requirements in conjunction with security policy.
- Support design and documentation for IAM architecture, identity governance, and role-based access control.
- Manage security operations tasks related to identity and access management, including incident response recommended solutions.
- Identify and rectify gaps within current infrastructure as it relates to onboarding and offboarding personnel.
- Ensure IAM processes comply with industry standards (NIST, ISO, CIS) and internal policies developed by the CISO and SecOps teams.

- Conduct regular audits and assessments to identify vulnerabilities and ensure compliance.
- Assess current applications and architecture to ensure current implementations align with identity-first security strategies, best practices, and approved standards.
- Define integration methodologies for IAM solutions with existing and onboarding applications, including cloud services, on-prem systems, and third-party applications (Entra ID, Azure, on-prem Active Directory, Oracle Identity Manager (OIM)).
- Work closely with other teams within the IT bureau (O365, Windows, Linux, EA, etc) to ensure fluid cohesiveness.
- Other duties as assigned.

## **PREFERRED QUALIFICATIONS**

- 2+ years of dedicated identity and access management experience with multi-environment experience (Oracle Identity + Microsoft) a plus
- 5+ years of information technology administration experience or equivalent combination of work and educational experiences
- Intermediate to advanced knowledge of identity technologies and concepts.
- Intermediate to advanced knowledge of directories, Single-Sign On (SSO), identity federation, privileged access management, automated life-cycle management.
- Proven knowledge of security (preferred - CISSP, CISA, CISM, GPEN, GWAPT, GCIH, other GIAC certifications, OSCP, CEH, Security+, etc.)
- An understanding in application integration patterns and API-based access control
- An understanding of Microsoft Entra ID hardening, role-based access control, active directory attributes and privileged identity management
- Experience with Microsoft Entra ID by configuring and maintaining Conditional Access policies, enforcing MFA, and securing authentication methods to reduce identity-related risks.
- Experience implementing controls, identity lifecycle management and third-party integrations for automation using Microsoft Entra ID Governance
- Strong familiarity with administering and maintaining Role-Based Access Control (RBAC) in Microsoft Entra ID, including the creation of custom roles, access reviews, and ensuring alignment with least-privilege principles.
- Ability to leverage Active Directory and Entra ID user attributes to automate access provisioning and group memberships using dynamic group rules.
- Skilled in supporting Privileged Identity Management (PIM) by configuring just-in-time access to critical roles, implementing approval workflows, and conducting periodic access reviews.

## **HOURS**

The agency's hours of operation are Monday through Friday, between 8:30 a.m. and 5:00 p.m. (37.5 hours/week). Scheduling determinations depend on the needs of each Bureau and will be communicated during interviews.

---

## **ADDITIONAL COMMENTS**

For new State employees appointed to graded positions, the annual salary is the hiring rate (beginning of the Salary Range) of the position. Promotion salaries are calculated by the NYS Office of the State Comptroller (OSC) in accordance with NYS Civil Service Law, OSC Payroll rules and regulations, and negotiated union contracts.

The Office of the NYS Attorney General (OAG) cannot provide sponsorship for work authorization. Candidates need to be authorized to work in the United States to be employed by this agency. It is incumbent upon employees to maintain work authorization for the duration of their employment with the OAG. This agency does not participate in E-Verify for work authorization purposes.

## **HOW TO APPLY**

In your submission, you must provide sufficient information to determine from your resume and/or cover letter that you meet the minimum qualifications stated above. If a certificate or degree is required to demonstrate that you meet the minimum qualifications, you must provide proof that you hold the required certificate or degree. To apply, please send your resume, cover letter, and a copy of your degree/transcript (if applicable) to [HR.Recruitment@ag.ny.gov](mailto:HR.Recruitment@ag.ny.gov). Be sure to include the Vacancy # and Title of the position in the subject heading of your email.

*Candidates from diverse backgrounds are encouraged to apply.  
The OAG is an equal opportunity employer and is committed to workplace diversity.*

---

**Posted March 4, 2026**