



## Position Information

**Employee Name:**

**Position Title:**

Senior IT User Access Administrator

**Program:**

Information Technology

**Work Unit:**

Systems Services

**Classification:**

Information Technology Specialist II

**Report To:**

Information Technology Manager I

**Collective Bargaining Identifier (CBID):**

R01

**Fair Labor Standards Act (FLSA) Status:**

Not Covered, Exempt. Work Week Group E

**Information Technology Domain(s):**

Software Engineering

## Special Requirements

**Conflict of Interest Designation:** Not applicable.

## Program Information:

We keep the tech backbone of the State Fund business strong, secure, and running smoothly—so our teams can focus on protecting what matters most to our customers. Whether it's behind-the-scenes systems or front-line support, we're here to make sure everything works. Reliable infrastructure, responsive service, and a mindset of continuous improvement—ensuring that every system, service, and user experience reflects our dedication to excellence, reliability, and trust.

## Purpose/Scope:

Under general direction of the Systems Services Manager (Information Technology Manager I), this position will be responsible to:

- Design new technologies, architectures, and solutions that will support security requirements
- Optimize and implement architecture solutions for IBM Security Identity Services at State Fund
- Optimize and implement architecture solutions for Certificate authentication Services (PKI) at State Fund
- Monitor and assess security controls, conduct security impact analyses, and report system security statuses for ISAM, ISIG, ISIM systems and PKI Architecture
- Lead and mentor project teams and State Fund department teams in security Identity systems
- Create and implement backup and recovery strategies for IBM and PKI security systems
- Monitor and conduct audits of system capacity, performance, and traffic analysis to ensure Confidentiality, Integrity and Availability for IBM Identity security systems and PKI.

## Essential and Marginal Functions:

In all aspects of performing the following functions the incumbent will:

- Comply with the Code of Conduct
- Maintain regular and predictable attendance and communication availability during working hours
- Establish and maintain effective working relationships and provide quality customer service in a timely manner.
- Follow State Fund's Equal Employment Opportunity principles
- Maintain a safe work environment
- Defend State Fund against fraudulent activities
- Maintain good customer relationships with internal and external business partners and stakeholders
- Properly maintain assigned equipment

*This duty statement outlines the primary responsibilities and expected outcomes of the position. It is not intended to provide an exhaustive list of all job duties. Employees may be required to perform additional tasks as assigned, including work in other functional areas.*

### Description of Duties

25% Essential

#### 1. Provide system design consultation, advice and recommendations

- a. Design new technologies, architectures, and solutions that will support security requirements
- b. Optimize and implement architecture solutions for IBM Security Identity Services at State Fund
- c. Optimize and implement architecture solutions for Certificate authentication Services (PKI) at State Fund
- d. Create and implement backup and recovery strategies for IBM and PKI security systems
- e. Lead and mentor project teams and State Fund department teams in security Identity systems

25% Essential

#### 2. Identify and resolve complex hardware/software issues within the Identity management and PKI systems

- a. Design, implement, monitor, and maintain the system Identity management and PKI systems environment and infrastructure.
- b. Review, install, configure, and implement new releases of Identity management and PKI systems software.
- c. Test and validate any software installations and changes.

20% Essential

#### 3. Timely reviews of auditing, security and system events for Systems Integrity analysis

- a. Monitor and conduct audits of system capacity, performance, and traffic analysis to ensure Confidentiality, Integrity and Availability for IBM Identity security systems and PKI.

20% Essential

#### 4. Analyze and optimize systems to ensure maximum up time and performance of Identity security Systems

- a. Monitor and assess security controls, conduct security impact analyses, and report system security statuses for ISAM, ISIG, ISIM systems and PKI Architecture

10% Essential

#### 5. Respond to Incidents and requests timely

- a. Timely respond to incoming incident and requests timely
- b. Timely respond to system generated alerts for servers and related systems
- c. Conduct necessary critical analysis and correlation of alerts and incident cases for escalation and resolution

## Required Knowledge Areas:

- Advanced knowledge of Windows 2019/2022 Server Operating Systems
- Proficient knowledge of PKI configuration, troubleshooting, and best practices
- Advanced knowledge of Identity Authentication methodology including Kerberos, LDAP, and SSO integrations
- Proficient knowledge of Multifactor Authentication systems such as PIM or Centrify
- Proficient knowledge of System specifications design, documentation, and implementation methodologies and techniques.
- Proficient knowledge of Business continuity and technology recovery principles and processes
- Proficient knowledge in Principles, methods and procedures for designing, developing, optimizing, and integrating systems in accordance with best practices.

## Required Skills and Abilities:

- Skill in supporting IBM identity Management Systems (minimum of 4+ years of robust technical experience)
- Skill in analysis techniques used to resolve issues or proactively prevent issues from developing
- Ability to act as a mentor
- Skill to manage multiple projects and tasks.
- Skill to work independently and execute on appropriate decisions points.
- Skill to achieve results according to objectives.
- Skill to communicate professionally and effectively, verbally and in writing, (including the ability to negotiate credibly and persuasively) with a variety of “stakeholders”.

## Work Environment:

### Physical Requirements:

- Computer data entry, frequent positioning of self to move and transport light objects, and telephone work; mobility to various working areas.
- Incumbent works in the usual office environment.

### Travel:

- Travel to various work sites and locations for training and/or meetings.

### Emergency call backs:

- Emergency call backs.

### Work Hours:

- On call availability may be needed, including 24/7 coverage as needed.

---

**Supervisor’s Statement:** I have discussed the duties of the position with the employee

|                          |                       |             |
|--------------------------|-----------------------|-------------|
| Supervisor Name (Print): | Supervisor Signature: | Date:       |
| <div></div>              | <div></div>           | <div></div> |

**Employee’s Statement:** I have discussed with my supervisor the duties of the position and have received a copy

|                        |                     |             |
|------------------------|---------------------|-------------|
| Employee Name (Print): | Employee Signature: | Date:       |
| <div></div>            | <div></div>         | <div></div> |