

POSITION DESCRIPTION

This position description serves as the official classification document of record for this position. Please complete the information as accurately as you can as the position description is used to determine the proper classification of the position.	
2. Employee's Name (Last, First, M.I.)	8. Department/Agency TECH, MGMT AND BUDGET - IT
3. Employee Identification Number	9. Bureau (Institution, Board, or Commission) Center for Shared Solutions
4. Civil Service Position Code Description INFO TECH PRGMR ANALYST-E	10. Division Enterprise Identity & Access Management
5. Working Title (What the agency calls the position) IAM Support Analyst - ITPA 11	11. Section
6. Name and Position Code Description of Direct Supervisor POST, COREY G; INFO TECH MANAGER-3	12. Unit
7. Name and Position Code Description of Second Level Supervisor EBIG, NATHAN; STATE ADMINISTRATIVE MANAGER-1	13. Work Location (City and Address)/Hours of Work Phoenix Bldg. 222 N. Washington Sq., Lansing, MI / 8AM-5PM Monday-Friday
14. General Summary of Function/Purpose of Position	
<p>This position will function as the analyst responsible ongoing operations for the Enterprise Identity and Access Management (EIAM) solution for the State of Michigan (SOM) branded as "MILogin". The analyst is responsible for administering, supporting and implementing policies and procedures for system architecture at MILogin, including the implementation of MILogin solution security, proactive monitoring, capacity planning, configuration and release management, performance management, high availability, disaster recovery and other service delivery components and functions.</p> <p>MILogin is an enterprise single sign-on and identity/access management solution which enables the State of Michigan to establish, manage, and authenticate user identities for Web and Mobile SOM IT systems. This solution is used across all state departments and provide access to over 300 various IT systems to Michigan citizens and business entities, as well as all SOM employees. This solution also provides an identity management service for Michigan local governments.</p> <p>This position is in the Enterprise Identity and Access Management (EIAM) team. The team is responsible for managing and administering the complex Enterprise Identity and Access Management (EIAM) core infrastructure environment as well as other installations through-out the State of Michigan currently providing application authentication services.</p>	

15. Please describe the assigned duties, percent of time spent performing each duty, and what is done to complete each duty.

List the duties from most important to least important. The total percentage of all duties performed must equal 100 percent.

Duty 1

General Summary:

Percentage: 70

The analyst level position will manage the onboarding of the enterprise level Identity and Access management architecture for all of Agency Services, IT systems and projects. Plan, develop and administer identity and access management technology related policies and procedures.

Individual tasks related to the duty:

- Under directions from senior level Analyst and Architect, verify implementation, manage and administer agency specific or enterprise software and tools including the installation, configuration, testing, tuning, monitoring, updating and patching.
- Develop guidelines and procedures for middleware performance i.e., uptime, response time, through-put, reliability, scalability, etc.
- Develop the guidelines and procedures for performance tuning.
- Evaluate and recommend software fixes to resolve problems.
- Perform incident management response tasks and assist facilitation of incident management response activities across multiple groups.
- Audit the software security administration access.
- Coordinate with and provide technical advice to the Project Manager to develop project plan.
- Research, evaluate, and recommend ALM tools including but not limited to requirements management tools, source code management tools, issue/defect tracking tools etc.
- Develop and manage configuration management standards, processes, and policies.
- Design Change Management repositories (example source code repository).
- Provide remediation for escalated CI issues.
- Define qualitative and quantitative Key Performance Indicators for the Change Management process.
- Facilitate Team start of day meetings.
- Participate in System incident response as needed, work to resolve incident within SLAs.
- Respond to end user tickets as assigned.

Duty 2

General Summary:

Percentage: 20

Participate in identity and access management systems projects and project teams.

Individual tasks related to the duty:

- Work directly with the client to provide a standards-based end to end designed solution and capture details to satisfy business requirements. Coordinate with telecommunication, directory services, standards and policies, and security to determine feasibility and validate ensuring provided solution is in line with defined standards. Document the detailed provided solution.
- Plan, coordinate and validate in-scope activities for regular Disaster Recovery testing for the assigned area of the identity and access management technology systems. Oversees the completion of implementation tasks being tested ensuring implementation, configuration, and testing methodologies best meet the customer requirements.
- Manage the development and testing of client enterprise level components, API's and related databases.
- Coordinate various activities with DTMB Enterprise Architecture, Office of Enterprise Security and Bureau of Strategic Policy.

Duty 3

General Summary:

Percentage: 10

Documentation and Testing

Individual tasks related to the duty:

- Manage the development of testing plans, scenarios and test data to ensure compliance and fit with the overall system.
- Manage architecture components and documentation versions using the established configuration management process and tools.
- Document training materials for new processes.
- Ensure the implementation of security standards in identity and access management technology systems and designs. Be familiar with, provide research, documentation and input (when applicable) to Enterprise Security standards.
- Coordinate and validate the support and maintenance activities for identity and access management technology systems.
- Maintain technical identity and access management technology methodology and best practices.

16. Describe the types of decisions made independently in this position and tell who or what is affected by those decisions.

Decision maker on the following:

- Technical plan – all development projects and systems users.
- The best approach to resolve technical issues and troubleshoot problems – all development projects and system users.
- Develop and administer design related policies and procedures – all development projects, and system users.

17. Describe the types of decisions that require the supervisor's review.

- Decisions regarding any purchasing.
- When decision impacts team, agency and/or section goals and priorities.
- Changes in policies, standards and procedures affecting team, section and agency that may need to be passed to supervisor for approval.
- Approval of requested hardware and software purchases as per normal departmental approval processes.

18. What kind of physical effort is used to perform this job? What environmental conditions in this position physically exposed to on the job? Indicate the amount of time and intensity of each activity and condition. Refer to instructions.

- Normal office environment and climate-controlled computer room.
- Extensive use of VDT and keyboard: 85 - 100%
- Infrequent equipment transport and setup: 1 – 5%
- Frequent heavy workloads and mandatory deadlines: ongoing
- Some travel: 5 – 10%
- May require use of personal vehicle.
- Over-time or on-call time is possible.

19. List the names and position code descriptions of each classified employee whom this position immediately supervises or oversees on a full-time, on-going basis.

Additional Subordinates

20. This position's responsibilities for the above-listed employees includes the following (check as many as apply):

- | | | | |
|----------------------------|------------------------------------|----------------------------|-----------------------------------|
| <input type="checkbox"/> N | Complete and sign service ratings. | <input type="checkbox"/> N | Assign work. |
| <input type="checkbox"/> N | Provide formal written counseling. | <input type="checkbox"/> N | Approve work. |
| <input type="checkbox"/> N | Approve leave requests. | <input type="checkbox"/> N | Review work. |
| <input type="checkbox"/> N | Approve time and attendance. | <input type="checkbox"/> N | Provide guidance on work methods. |
| <input type="checkbox"/> N | Orally reprimand. | <input type="checkbox"/> N | Train employees in the work. |

22. Do you agree with the responses for items 1 through 20? If not, which items do you disagree with and why?

Management prepared.

23. What are the essential functions of this position?

As an analyst for the Enterprise Identity and Access Management (EIAM) team, this position is responsible for new implementations and ongoing operations of the EIAM solution for the State of Michigan (SOM) branded "MILogin". This analyst is responsible for administering, supporting and implementing policies and procedures for system architecture at EIAM, including the implementation of EIAM solution security, proactive monitoring, capacity planning, configuration and release management, performance management, high availability, disaster recovery and other service delivery components and functions.

Competencies: Technical /Professional Knowledge and Skills, Planning and Organizing Work, Adaptability, Initiating Action and Customer Focus.

24. Indicate specifically how the position's duties and responsibilities have changed since the position was last reviewed.

The updated PD replaces references to MILogin/EIAM with the modernized MICAM platform, updates the supervisor information and work location, and revises duty descriptions to emphasize more hands-on operational tasks such as system monitoring, implementing upgrades, and ALM process support. It also updates educational requirements to current IT classification standards and adjusts system counts and terminology to reflect the newer MICAM environment.

25. What is the function of the work area and how does this position fit into that function?

The function of the Center Shared Solution EIAM section is to provide an enterprise single sign-on and identity and access management solution which enables the State of Michigan (SOM) to establish, manage, and authenticate user identities for Web and Mobile SOM IT systems. This solution is used across all state departments and provide access to over 300 various IT systems to Michigan citizens and business entities, as well as all SOM employees. This service also is utilized as an identity management service for Michigan local governments and other states. The position also provides an agency and State enterprise view of architecture design and integration to keep DTMB consistent with statewide technology and standards.

26. What are the minimum education and experience qualifications needed to perform the essential functions of this position.

EDUCATION:

Information Technology Programmer/Analyst 9

Possession of an Associate's degree with 16 semester (24 term) credits in one or a combination of the following: computer science, data processing, computer information systems, data communications, networking, systems analysis, computer programming, information assurance, IT project management or mathematics.

Information Technology Programmer/Analyst P11/12

Possession of a Bachelor's degree with 21 semester (32 term) credits in one or a combination of the following: computer science, data processing, computer information systems, data communications, networking, systems analysis, computer programming, information assurance, IT project management or mathematics.

EXPERIENCE:

Information Technology Programmer/Analyst 9

No specific amount or type is required.

Information Technology Programmer/Analyst P11

No specific type or amount is required.

Alternate Education and Experience

Information Technology Programmer/Analyst 9

Educational level typically acquired through the completion of high school and two years of experience as an application programmer, computer operator, IT Technician, or two years (4,160 hours) of experience as an Information Technology Student Assistant may be substituted for the education requirement.

KNOWLEDGE, SKILLS, AND ABILITIES:

Required:

- Strong Working knowledge of system administration of UNIX, Windows, or Linux operating systems.
- Knowledge in Identity and Access Management.
- Ability to quickly learn and implement new technologies and procedures
- Ability to troubleshoot application issues under pressure.
- Ability to work as a team member, ability to be a self-starter.
- Ability to communicate well, both verbally and in writing.

Recommended:

- Knowledge of IBM Access Management.
- Knowledge of IBM Identity Manager
- Knowledge of JavaScript, .NET or Spring Development Frameworks.
- Knowledge of Azure DevOps Methodology
- Knowledge of ITIL practices

CERTIFICATES, LICENSES, REGISTRATIONS:

N/A

NOTE: Civil Service approval does not constitute agreement with or acceptance of the desired qualifications of this position.

I certify that the information presented in this position description provides a complete and accurate depiction of the duties and responsibilities assigned to this position.

Supervisor

Date

TO BE FILLED OUT BY APPOINTING AUTHORITY

Indicate any exceptions or additions to the statements of employee or supervisors.

N/A

I certify that the entries on these pages are accurate and complete.

MARCELINA BREWER

Appointing Authority

3/3/2026

Date

I certify that the information presented in this position description provides a complete and accurate depiction of the duties and responsibilities assigned to this position.

Employee

Date