State of Michigan
Civil Service Commission

Capitol Commons Center, P.O. Box 30002
Lansing, MI 48909

Position Code

1. ITPRANEF03N

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)** MI Cybersecurity & Infrastructure Protection
4. Civil Service Position Code Description INFO TECH PRGMR ANALYST-E	**10. Division** Michigan Office of Cyber Security
5. Working Title (What the agency calls the position) IT Security Analyst	**11. Section** Michigan Security Operations Center (MiSOC)
6. Name and Position Code Description of Direct Supervisor NEVAI, THOMAS L; INFO TECH MANAGER-3	**12. Unit**
7. Name and Position Code Description of Second Level Supervisor WAIER, BRENDA; STATE ADMINISTRATIVE MANAGER-1	**13. Work Location (City and Address)/Hours of Work** Lansing, MI / 8-5 shift, overtime and on-call may be required

14. General Summary of Function/Purpose of Position

The Security Analyst position works as a member of the Incident Response Team. The Security Analyst position remediates cyber incidents and vulnerabilities while maintaining the confidentiality, integrity, and availability of State of Michigan data.

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: 55**

.Technical security analyst assists with the completion of low to mid-level cyber investigations involving the security of the State of Michigan network.

Individual tasks related to the duty:

• Creates security procedures to ensure adequate security procedures have been developed to identify and classify cyber events.
• Performs investigation of low to mid-level incidents and tickets, following established procedures. Documents standard operating procedures for undocumented incidents.
• Correlates information and creates security plans to mitigate incidents.
• Assesses risks and scope for low to mid-level security incidents.
• Assists with creating specifications and implementation of security hardware and software. Implements corrective action as needed.
• Provide control responses on security risk assessment results.
• Tracks metrics on the performance of security responsibilities, controls, and design.
• Assists with the training of incoming analysts in roles and responsibilities.
• Transfers knowledge to subsequent analysts and other staff on duty.
• Participates in audits and implements identified remediation as necessary to ensure the effectiveness of enterprise security controls.
• Escalates as necessary.

Duty 2

General Summary: **Percentage: 40**

Technical Security Analyst performing duties related to the Incident Response team.

Individual tasks related to the duty:

• Remediates low to mid-level Incident Responses when working to resolve incidents.
• Assists with Incident Response for cyber event detection, correlation, response, and recovery.
• Monitors Incident Response tools that are used to collect and analyze data to meet program reporting and evaluation requirements. Incident data includes incident tickets serviced, requests sent through to the IR team, IR actions, and the results of IR investigations.
• Responds to all cyber security related events for the State of Michigan.
• Maintains the use of emerging data security technologies, develops standards and procedures, and promotes the usage of automated tools.
• Provides information to management on trending threats and routine updates on the progress and status of active events.
• Interfaces with other agencies to assist and provide information on active events and remediation.
• Documents after-action reports.
• Participates in On-Call rotation.
• Escalates as appropriate to ITPA 12 or management

Duty 3

General Summary: **Percentage: 5**

Maintain knowledge of “state of the art” IT security technologies and developments in new technologies and/or methodologies where feasible.
Executes / Develops security procedures.
Provides input for continuous security improvements within the MiSOC.
Provides input on audits and system security plans.

Individual tasks related to the duty:

• Attend training classes, seminars, and conferences to keep abreast of “state of the art” IT security technology.
• Keep abreast of IT security developments and activities through interface with IT security groups such as the Computer Emergency Response Team (CERT).
• Research new methodologies and provide input to management regarding the purchase of new security technologies.
• Continuous learning to determine best IT security practices.
• Other duties assigned by management.

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

Decisions involving the development of the IT security systems. These decisions impact the confidentiality, integrity and availability of the sensitive data on the entire State of Michigan network.

Forensics
Decisions involving the processing of DTMB-0130’s, DTMB-0134’s and DTMB-0244’s. These decisions are confidential in nature and relate to Personally Identifiable Information (PII).

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

Decisions regarding the acquisition of new security technologies, as well as system changes affecting enterprise-wide operational tools.
Forensics
Decisions regarding Law Enforcement investigations, sensitive employee investigations and the receipt of a Search Warrant for State of Michigan data.

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.

• The position operates in a normal office environment, performing duties within the assigned workspace.
• Tasks can be completed routinely seated at a desk, visiting others at their desks, in the context of meetings and meeting rooms.
• Work requires extensive use of personal computers including keyboards and monitors.
• This position is subject to stress and pressure to resolve problems quickly and effectively.
• There are frequent deadlines that are imposed by external forces; heavy workloads are possible and overtime during development projects may be required.
• Duties may involve lifting of 25 pounds or less.

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):

N Complete and sign service ratings.
N Provide formal written counseling.
N Approve leave requests.
N Approve time and attendance.
N Orally reprimand.

N Assign work.
N Approve work.
N Review work.
N Provide guidance on work methods.
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?

Prepared by management.

23. What are the essential functions of this position?

• Security Analysts in the Michigan Security Operations Center review and validate security procedures to ensure adequate security procedures have been developed to identify and classify cyber events.
• Ensures that all identified events are promptly and thoroughly investigated.
• Reviews correlated information and builds a security plan to identify and mitigate a response.
• Reviews security incidents for actual or potential breaches or non-compliances and ensures that all identified events are promptly and thoroughly investigated.

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

The updated MiSOC ITPA 11 Security Analyst PD narrows the role from broad enterprise security, forensic tools, and physical security work to a focused Security Operations Center Incident Response role. Duties now emphasize investigating and remediating cyber incidents, monitoring IR tools, documenting actions, on-call rotation, and supporting SOC operations. Physical security, background checks, penetration testing, and compliance-heavy duties found in the older PD were removed. Time allocations were restructured to reflect 55% investigations, 40% incident response, and 5% professional development, aligning the position specifically with MiSOC’s operational mission.

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

In their efforts to serve the citizens of the State of Michigan, state agencies are using information technology to deliver and support many of their programs and initiatives. DTMB through the Chief Information Officer (CIO) is responsible for providing the IT services that support the agencies' business goals and objects. The Bureau of Cybersecurity and Information Protection is responsible for cybersecurity and physical security. The Office of Michigan Cyber Security (MCS) reports to the Chief Security Officer who reports to the CIO. MCS was created to provide leadership for an enterprise-wide information security program. One of the sections of this information security program is the Michigan Security Operations Center (MiSOC). This section is involved with Regulatory and Standards Compliance; Security Risk Management; Data Security, Digital Forensics; Incident Management; Threat Analytics; IT Security Systems development, design, operations and Maintenance; Network and Telecommunications Security; on an enterprise basis. This position is a senior security analyst in this section.

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:

Two years or more of professional IT experience is preferred. Considerable knowledge of IT security technologies is preferred. Broad knowledge of server administration, network technologies, asset management, databases, is helpful.
Must possess excellent communication skills, both verbal and written, and be able to work well in a team environment and handle multiple tasks.
Maintains knowledge of the security tools, concepts, regulatory requirements, standards, and practices in tools, software, networking and operating systems, hardware tools.

CERTIFICATES, LICENSES, REGISTRATIONS:

• The position may work overtime, different shift schedules and/or weekends.
• Employment requires passing a drug test and background check.
• The position also requires the passing a LEIN background investigation.

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	3/3/2026
Appointing Authority	**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**