

Open Position: Security Analyst I

Location: Boston

Job Type: Full-Time, Hybrid

Salary: From \$66,600

Massachusetts Property Insurance Underwriting Association is seeking a Security Analyst to join our Information Technology Department.

The Security Analyst I is responsible for assisting in the day-to-day administration of the Information Security Management System (ISMS). The position is a crucial role within our Information Technology department focusing on security, tasked with the monitoring, analysis, and protection of our digital assets. This role supports our ongoing efforts to maintain organizational security integrity, ensure compliance with security policies, and respond effectively to security incidents.

#### **JOB REQUIREMENTS:**

This position requires a bachelor's degree in Computer Science, Information Technology, Cybersecurity, or a related field and or equivalent work experience. Proficiency in Windows, Linux, and other operating systems, including their security configurations and vulnerabilities is required. Must have knowledge of basic cybersecurity principles, including the CIA triad (confidentiality, integrity, and availability), have exposure to security tools such as firewalls, antivirus software, intrusion detection systems (IDS), and intrusion prevention systems (IPS). A basic understanding of network infrastructure, including TCP/IP protocols, DNS, DHCP, and network segmentation is required. Experience with or knowledge of tools that scan for vulnerabilities in networks and systems is also required. The position must have the ability to analyze data and security logs to identify patterns of activity that might indicate a threat and be capable of troubleshooting issues swiftly and effectively under pressure. Strong verbal and written communication skills are needed to report findings and make recommendations to both technical and non-technical colleagues and a high level of accuracy and attention to detail is crucial for detecting threats and vulnerabilities. The following certifications are preferred but not required: CompTIA Security+, Certified Ethical Hacker (CEH), GIAC Information Security Fundamentals (GISF) or similar entry-level certifications. Must be able to adapt to a rapidly changing technology landscape and new threats. Must have a willingness to work as part of a team, sharing information and learning from colleagues.

#### **RESPONSIBILITIES:**

1. Support the IT Director and IT Manager – Infrastructure and Security with defining and documenting specific information security controls, policies, and practices.

2. Compile necessary backup documentation and reports for IT controls for annual Financial and other security audits.
3. Monitor the Association's network and systems through the use of SIEM (Security Information and Event Management) tools. Analyze and review reporting of Systems such as Arctic Wolf and Mimecast with the IT Director, the IT Manager - Infrastructure and Security and the IT Manager - Software Development and Operations as necessary.
4. Configure and deploy the monthly Mimecast security awareness training videos and phishing campaigns, and review employee test results. Work with employees who fail repeatedly, and work with HR and the employee's manager/supervisor if necessary.
5. Assist the IT Manager-Infrastructure and Security in developing the content and delivery of the mandatory monthly security awareness training sessions coordinated with GFMS.
6. Use various tools to detect PII data loss in email and files on the network to determine if data is being properly handled and stored. Infractions need to be logged and reported.
7. Assist the IT Manager-Infrastructure and Security in the review and implementation of new security solutions that enhance the Association's security posture.
8. Manage quarterly AD user audit certifications with each division and subdivision across the organization, using Stealth Audit tools.
9. Review IT procedures and make suggestions where documentation is lacking.
10. Complete annual CIS 18 controls audit to ensure technical controls meet policy objectives.
11. Assist the IT Director and the IT Manager-Infrastructure and Security in the completion of third-party penetration tests, IT Control Audits, and IT Financial Audits.
12. Assist in all disaster recovery exercises and documentation.
13. All other duties and projects as assigned.

#### **ACTIVITIES REQUIRED TO PERFORM ESSENTIAL FUNCTIONS:**

To complete the essential functions of this position in a complete and timely fashion, the person must be able to:

- Remain in a stationary position 100% of the time.
- Operate a computer and other office productivity equipment as needed to meet the requirements of this position.
- Read and create both physical and electronic documents.
- Effectively communicate with employees, customers, vendors, and other internal and/or external business partners on the telephone, in writing and in person.
- Think analytically, concentrate on assigned tasks, observe, and remember detail, and make decisions sufficient to meet the requirements of this position.

- Ability to travel as needed to meet the requirements of this position.

We offer an excellent benefits package, a matching 401(k) program, pension, a hybrid work schedule and we are conveniently located in Government Center.

For more information about Massachusetts Property Insurance, please visit our website at [www.mpiua.com](http://www.mpiua.com). Interested applicants should send resumes via e-mail to [hr@mpiua.com](mailto:hr@mpiua.com) or by fax (617) 209-1072. We are an Equal Opportunity Employer.