As a Security Technician IT, you will assist in implementing and maintaining information technology security systems to secure all Airports Authority information assets in compliance with internal information security policies, industry best practices, and Federal security standards.

JOB DESCRIPTION

- Security Technician IT
- Works under the general supervision of Chief Information Security Officer.
- Serves in the Information Security Department of the Office of Technology located at the Washington Dulles International Airport.

Assists in implementing and maintaining information technology security systems and procedures. Performs related functions.

GENERAL RESPONSIBILITIES

- Participates in the monitoring, testing, and reporting on the confidentiality, integrity, and availability of information assets in compliance with Airports Authority information security policies and other security and compliance standards.
- Assists in the implementation, operation, and maintenance of technologies used by the Airports Authority Security Operations Center (SOC).
- Works with the Network Operations and Service Desk teams to help address information security related issues.
- Assists in the management of the Airports Authority Security Information and Event Management (SIEM) systems to provide real-time monitoring, correlation of security events, notifications, reporting, and dashboard views.
- Performs configuration management tasks to ensure critical devices and applications send automatic security event notifications to devices for security incident response and investigation and comply with information security policies and regulations.
- Assists with managing the intrusion prevention and detection systems to identify, log, block, and report malicious activity occurring within Airports Authority networks and systems. Assists with deployment, configuration, and monitoring of appliances.
- Helps resolve security alerts and escalates high risk events to the appropriate technology team for resolution.
- Works to manage and configure the Airports Authority's Web content monitoring tool and provides reports to the Chief Information Security Officer and other Office managers concerning employee internet usage.
- Assists in reviewing firewalls to ensure rules are appropriate for the protection of information and systems. Helps ensure firewall changes have been reviewed and approved by the Information Security Director prior to their deployment.
- Conducts continuous vulnerability scans and penetration testing on all networks.
- Assists in the review of the Airports Authority patch management processes and recommends improvements when deficiencies are identified.

- Monitors, tests, and reports user computing activities (such as failed logins, account lockouts) and reviews internal network and remote user access to ensure access management processes are working as designed.
- May serve as a member on the Security Incident Response Team (SIRT).
- Keeps abreast of security industry developments to proactively identify threats.
- Performs other duties as assigned.

QUALIFICATIONS

1. One year of experience in information technology security including:
    a) Detecting IT system vulnerabilities
    b) Configuring or reviewing firewalls.
    c) Assisting in conducting security assessments.

KNOWLEDGE, SKILLS & ABILITIES

1. Ability to use IT system detection tools and/or penetration testing tools to safeguard IT data and systems.
2. Knowledge of, and ability to use, configuration management tools.
3. Ability to rapidly learn and use new software and information technology systems.
4. Ability to perform general analyses of data and information and make recommendations.
5. Ability to speak and write effectively.
6. Skill in using a computer and modern office suite software, with emphasis on information security systems/software.

PREFERRED QUALIFICATIONS

- Bachelor's Degree in Information Technology or Information Security.

EDUCATION

- A high school diploma, a Certificate of General Education Development (GED), or an equivalent combination of education, experience, and training.

CERTIFICATIONS AND LICENSES REQUIRED

- None

NECESSARY SPECIAL FACTORS

- Work is typically reviewed in progress and upon completion for quantity, quality, timeliness, teamwork, customer service, and other factors.