

**CURRENT EMPLOYMENT OPPORTUNITIES  
QUALIFICATION SHEET**

**This position is currently vacant within the Tollway.  
The Human Resources Section will accept applications, with resumes from:**

**November 2, through November 16, 2009**

\*\*\*\*\*

<u>DEPARTMENT</u>	<u>POSITION</u>	<u>SALARY</u>
Information Technology	Security Administrator	\$51,490.00/Yr (G-6)

**JOB QUALIFICATIONS:**

**To be selected for a position,** an applicant must (1) meet the minimum requirements of the job posting, (2) pass a written exam (if applicable), (3) satisfy a background check (which may be extensive), and (4) pass an oral interview, during which the interview will further evaluate the applicants qualifications.

**Internal Applicants** who are current employees must have worked in their current position long enough to pass probation to be eligible to apply for the position. In addition, applicants are also subjected to an internal investigation which includes an evaluation of their work record, safety and discipline records, their performance assessments and time and attendance records (including late starts and early quits) for the preceding 12 months. (Authorized absences will not be included for purposes of assessing whether attendance is satisfactory.)

**EDUCATION:**

- Bachelors Degree in Computer Science or related field is required.
- Certification in one or more areas related to network/computer security is required.

**EXPERIENCE / SKILLS / ABILITIES REQUIRED:**

- 1-3 years experience with network administration and general network security.
- Previous work experience and a good understanding of TCP/IP, network protocols, VPN, IPSEC, port forwarding, and networking.
- A thorough understanding of network logging, patch management, anti-virus management and basic domain administration skills.
- Previous experience in a rapid and changing business environment.
- Must be willing to carry a phone for on call support.
- Must be able to respond to after hours calls and incidents.
- Good people skills related to service and responsiveness.
- Must be able to follow and understand the direction of the security technology.
- Must be able to deal with critical and industry specific pressures.
- Must be able to work independently w/minimal supervision.
- Must have good problem definition and problem resolution skills.
- Must be detail oriented, analytical, highly organized, have good oral and written skills, and be able to handle a variety of tasks in an efficient manner.

**SKILLS AND ABILITIES DESIRED:**

- Familiarity with PCI DSS.
- Skills in general network domain administration, including user management.
- Familiarity with MARS security appliances.
- Managing firewall logs and syslogs and conducting daily log review.
- Familiarity with WSUS and other patch and update management programs.
- Ability to work directly with end-users and non-technical personnel for security issues.
- Ability to work in a confidential environment.
- Ability to assist with incident investigation and response.
- Familiarity with Cisco MARS a strong plus.
- Hands on knowledge of configuration of Cisco routers and switches.
- Skills in WAN technology, SONET, frame relay, leased lines, and virtualized networking.

**Applicants interested in applying for this position can apply in person at our [Downers Grove Office](#) located at 2700 Ogden Ave. between the hours of 8:00 a.m. to 4:30 p.m. Monday through Friday. Applications can also be printed out by clicking on the [Application link](#) and mailed to:**

**Illinois Tollway – Human Resources  
2700 Ogden Ave.  
Downers Grove, IL, 60515**

**All applications must be received by the application deadline indicated on the qualification sheet or Internet site.**

## **POSITION DESCRIPTION**

### Security Administrator

---

#### **POSITION PURPOSE:**

To participate as a member of the Information Technology Security team and be responsible for day-to-day tasks which contribute to overall network security, including log review, patch management, software license monitoring and other security tasks.

#### **DIMENSIONS:**

1000 PC Workstations and laptops  
40-60 Windows Servers  
Cisco IDS / IPS appliances and routers  
Microsoft ISA Server

#### **NATURE AND SCOPE:**

The incumbent reports directly to the IT Security Manager. Incumbent will perform monitoring of network security logs, patch management, and general network monitoring. Incumbent will assist with upgrades to network hardware and software components as required. Incumbent will participate in troubleshooting, documentation, and correction of network outages & security threats. Incumbent will respond to the needs and questions of users for general technical support, access, resources, and security. The incumbent will also monitor computer programs that control user access to the ISTHA network and review access security for network connections as required.

The incumbent assists in the creation of security standards for hardware and software installation. The incumbent tests, maintains, documents and modifies configurations. The incumbent works with the development and systems integration group to ensure all proprietary and third party applications are properly integrated within the ISTHA network security structure.

The incumbent documents all steps taken to modify systems and all procedures required to implement changes to the network security hardware and software, following all related Change Control policies and procedures.

#### **REQUIRMENTS:**

Bachelors degree in Computer Science or equivalent. Certification in one or more areas related to Security is required. 1-3 years experience with network administration, and general network security. Have a good understanding of TCP/IP, network protocols, VPN, IPSEC, port forwarding and networking. Must be willing to carry phone for on call support. Must be able to respond to after hour's calls and incidents. Have good people skills related to service and responsiveness. Must be able to deal with critical and industry specific pressures. Must be able to work independently and/or with minimal supervision. Must have good problem definition and problem resolution skills.

**REQUIRMENTS (continued):**

Must have previous experience in a rapid and changing business environment. Must be able to follow and understand the direction of the technology. Must have good written and verbal communication skills. Must be detail oriented, analytical and highly organized, and be able to handle a variety of tasks in an efficient manner.

**SKILLS/ABILITIES DESIRED:**

Knowledge of routing protocols such as OSPF, EIGRP, as well as switching technologies such as VLANS, trunking, etc. Have experience with FE, GE, SONET, and WAN configurations. Have hands-on knowledge of configuration of Cisco routers and switches. Skills in WAN technology; SONET, frame relay, leased lines, and virtualized networking. Familiarity with MARS security appliances. Have experience in designing, implementing, and managing Firewall logs and syslogs. Have experience in Cisco IPS monitoring and event correlation. Have knowledge in Cisco ACS and Cisco VPN. Ability to assist with incident investigation and response.

**PRINICIPAL ACCOUNTABILITIES:**

1. Review, and monitor network logging.
2. Manage Windows, Microsoft and third-party patching for all systems utilizing WSUS and other tools as appropriate.
3. Assist in troubleshooting, documenting, and correcting, network outages & security threats.
4. Participate in reviews of new and emerging technologies.
5. Respond to the needs and questions of users for general technical support, access, resources, and security.
6. Monitor computer programs that control user access to the ISTHA network.
7. Participate in validation of attacks against the network, assess overall impact, and act to eliminate identified threats.
8. Work with the development and systems integration group to ensure all proprietary and third party applications are properly integrated within the ISTHA network security structure.
9. Document all steps taken to modify systems and all procedures required to implement changes to the network security hardware and software, following all related Change Control policies and procedures.
10. Other duties as assigned.