UNIFIED JUDICIAL SYSTEM
POSITION DESCRIPTION

COMPUTER SECURITY SPECIALIST

CLASS CODE: 99-31-54

POSITION PURPOSE

Defines, provides, monitors, and maintains data security measures on Unified Judicial System (UJS) networks, workstations, servers, and applications to ensure integrity of, and desired access to, UJS data.

DISTINGUISHING FEATURE

This position develops security guidelines and standards; monitors and resolves data security and cybersecurity issues; monitors and resolves virus, malware, and spyware issues; creates and maintains a disaster recovery plan; provides network and end-user technical support; and researches and evaluates hardware and software to ensure systems are secure from intrusion and remain consistently and effectively operational throughout UJS statewide.

MAJOR RESPONSIBILITIES

Note: The duties listed are typical examples of work performed by positions in this job classification. Not all duties are included, nor is the list exclusive.

1. Provides and implements data security measures on workstations, servers, and networks to ensure access is restricted to those authorized to do so and that activities are safe and data remains confidential.
   a. Monitors, tests, and installs security patches on servers and computers continually.
      i. Develops code to automate processes and update remotely.
      ii. Handles configuration changes.
   b. Maintains anti-virus, spyware, and malware software and policies for its application and implementation.
   c. Monitors unauthorized access to, and integrity of, electronic data; and immediately researches and addresses issues.

2. Develops and implements disaster recovery standards to facilitate data security in all circumstances.
   a. Creates, tests, maintains, and updates disaster recovery plans.
   b. Responds to security breaches, analyzes concerns, and determines resolutions.
   c. Establishes backup and recovery procedures for workstation and server data.
   d. Recognizes potential risks, and proactively addresses issues as soon as possible.

3. Maintains security awareness throughout UJS through information exchange and ongoing education and training.
   a. Establishes and maintains training needs.
   b. Establishes security policies and monitors compliance.
   c. Develops and coordinates security procedures, ensuring compliance with other state

agencies' procedures.

4. Provides system design and review that allows servers to function at peak performance.
   a. Designs, configures, and performs maintenance on servers including hardware, software, network connections, and security.
   b. Defines the technical resources, physical capacity (computer power and storage), networking needs, and budget impact.
   c. Schedules and manages operating system migrations.

5. Provides technical support to managers and end users; and assists and trains technicians in advanced issues to substantiate the significance of security to work integrity.
   a. Researches and evaluates new security technologies, determines whether or not they are beneficial to UJS, and makes information available to managers to support decision-making.
      i. Considers costs and budget availability.
      ii. Does the planning to determine compatibility with Bureau of Information and Technology (BIT) infrastructure.
      iii. Compiles information from vendors, BIT, etc.
   b. Evaluates hardware and software as directed.
   c. Conducts necessary research to resolve problems and issues.
   d. Sets up, installs, and configures servers and workstations.
   e. Makes sure data storage is working as designed.
   f. Works personally on potentially high-profile issues.

6. Performs other work as assigned.

SUPERVISORY FUNCTIONS

This position oversees and is accountable for UJS network and workstation data security and integrity; security patches; network disaster recovery plans; new security technology; virus, spyware, and malware issues; education, training, and policies to expand security awareness; and coordination of security procedures in UJS and with other branches of government.

ESSENTIAL FUNCTIONS REQUIRE

Evaluation and understanding of computer systems' interaction, hardware, software, and data storage capabilities; working in cramped spaces, lifting heavy equipment, and exposure to electrical hazards during installations; operating standard office equipment such as copiers, telephones, etc.; sitting for extended periods of time; working extended hours as needed; travel to meet with clients; and attendance in accordance with rules and policies. The incumbent is also required to work effectively with coworkers and the public; understand, evaluate, and analyze statistical data and draw reasonable and accurate conclusions from that data; manage stress appropriately; meet deadlines; demonstrate initiative and motivation; and communicate (verbally and in writing) complex technical concepts and ideas to non-technical individuals.

PROBLEMS AND CHALLENGES

Challenges include establishing, configuring, and maintaining measures to ensure integrity and security of electronic data on UJS computer systems 24/7/365 uptime status. This requires using a variety of methods and technology to install necessary security measures on statewide systems; and monitoring and reacting to unsolicited intrusion of, and access to, UJS data. Further challenged to develop and maintain comprehensive and intelligible documentation regarding security policy, current configurations, available technology, and recovery methods.

Problems encountered include developing code that will routinely install software updates on all workstations in UJS; keeping virus definitions up to date; running backups without overloading lines; testing new installations to identify potential problems; and daily maintenance and support of complex infrastructures.

DECISION-MAKING AUTHORITY

Decisions include priority of assigned work; suitability and feasibility of hardware and software; automation processes to convert data from one system into another; backup and recovery procedures; training and education needs for staff security awareness; solutions for security breaches; recommendations for data security measures and implementation policies and procedures; and recommendations for disaster recovery standards.

Decisions referred include priority of conflicting requests; approval of data security measures, policies, and procedures; approval of disaster recovery standards; and approval of budget requests.

CONTACT WITH OTHERS and PURPOSE

Routine contact with BIT security staff to share information and deal with issues identified by their security scans; with UJS I/T technicians to provide resolutions to advanced problems; and regarding software installations and updates, and data storage and backups.

WORKING CONDITIONS

The incumbent works in a typical office environment. Installations and repairs may require working in cramped or confined spaces, lifting heavy equipment, and exposure to electrical hazards. The incumbent may be subject to on-call or after-hours work to resolve critical system problems, as approved by the supervisor.

COMPETENCIES/QUALIFICATIONS FOR APPOINTMENT

Knowledge, Skills and Abilities:

Knowledge of:

- data security requirements and standards including installation options, access monitoring, and problem solving techniques;
- Active Directory and Group Policy objects;
- disaster recovery methods.

Ability to:

- research new technologies and advocate methods to use them and benefit UJS;

- organize and schedule large installations and upgrades;
- communicate effectively with diverse groups of users;
- create and maintain extensive, usable documentation;
- see potential issues and forestall their development.

Education:

Bachelor's degree from an accredited university or college in computer science, computer networking, computer security, or a related field.

Experience:

Two (2) years of experience providing data security support in an office network environment, or an equivalent combination of related education and experience.