



## INFORMATION SYSTEMS SECURITY OFFICER

FC: IC159  
PB: F  
FLSA: Exempt

PC: 890  
BU: 31(AFSCME)  
Revised: June 2015

*Class specifications are intended to present a descriptive list of the range of duties performed by employees in the class. Specifications are **not** intended to reflect all duties performed within the job.*

### **DEFINITION**

Provides complex technical and administrative support for information systems data security and disaster recovery planning; develops and implements standards and procedures that provide optimum security, protection of system access and data integrity; provides consultation, problem resolution, and training to all departments; and performs related duties as assigned.

### **CLASS CHARACTERISTICS**

This single position class serves as the in-house technical expert in the development and implementation of standards and procedures that produce optimum security and protection of access and data integrity.

### **REPORTS TO:**

This position reports to the Chief Information Officer or his/her designee..

### **EXAMPLES OF DUTIES** –*Duties may include, but are not limited to, the following:*

1. Develops and administers complex computer information security programs; ensures the protection of data against accidental or intentional unauthorized disclosure, modification or destruction.
2. Provides security and protection of system access and data integrity; selects hardware and software; monitors and resolves unauthorized access; designs and implements revisions.
3. Manages the disaster recovery program; defines recovery parameters; develops recovery plans, prepares disaster recovery planning policies, procedures and methodologies.

4. Coordinates computer security activities with user departments and information technology staff; provides training to users and information technology staff; implements projects and changes as appropriate.
5. Monitors status of database; designs and implements complex revisions to computer security software.
6. Manages the user database; defines users and level of access; adds users to systems; defines protected resources; modifies user status; disables access capabilities; reports violations.
7. Monitors and resolves issues concerning data security production problems; provides in-house complex technical consultant to resolve computer system, procedural, and policy issues to optimize provision and administration; makes recommendations on corrective actions; implements decisions.
8. Communicates with computer security professionals and vendors; researches technical journals and reference manuals; stays abreast of new trends and innovations in the field of computer security and disaster recovery planning.
9. Receives and administers on demand requests from Human Resources and from management throughout the District to technically provision, modify, or remove access to separate computer systems.
10. Maintains records; prepares periodic and special reports.
11. Installs and implements hardware and software for disaster recovery planning.
12. Provides off-hours assistance to operating staff

## **QUALIFICATIONS**

### **Knowledge of:**

- Principles and practices of computer operation, maintenance and data security systems.
- Industry standards for data security systems operations.
- Standards and procedures for computer operations and disaster recovery planning.
- A variety of operating system software, system utilities, and applicable programming languages.
- Principles of business letter writing and basic report preparation.
- Related Federal, State and local codes, laws and regulations.

### **Skill in:**

- Implementing complex data security programs.
- Analyzing and interpreting complex technical data security information.
- Utilizing a variety of computer software and programming languages.

- Assessing, troubleshooting and resolving data security problems.
- Developing security policies and procedures.
- Recommending and implementing corrective action for data security violations.
- Operating a variety of computer hardware and office equipment.
- Training staff on system data security procedures.
- Planning and organizing computer data security projects.
- Interpreting and explaining District data security policies and procedures.
- Preparing clear and concise reports, security documentation and user procedures.
- Communicating clearly and concisely, both orally and in writing.
- Establishing and maintaining effective working relationships with those contacted in the course of work.

## **MINIMUM QUALIFICATIONS**

### **Education:**

A Bachelor's degree in computer science, business administration or a closely related field from an accredited college or university.

### **Experience:**

Four (4) years of (full-time equivalent) verifiable professional experience in data security systems management.

### **Substitution:**

Additional professional experience as outlined above may be substituted for the education on a year-for-year basis. A college degree is preferred.

## **WORKING CONDITIONS**

### **Environmental Conditions:**

Office environment; computer room environment; exposure to computers.

### **Physical Conditions:**

May require maintaining physical condition necessary for sitting for prolonged periods of time.

**EEOC Code: 02**

G:\CompClas\WPFiles\ClasSpec\Group\_I\IC159-01