

# Florida State Courts System

## Class Specification

**Class Title: Information Security Analyst**

**Class Code: 4250**

[Pay Grade 104](#)

### General Description

The essential function of the position within the organization is to provide technical support and analysis in the areas of security analysis, intrusion detection, incident response, and network security management. This position works independently under limited supervision.

### Examples of Work Performed

(Note: The examples of work as listed in this class specification are not necessarily descriptive of any one position in the class. The omission of specific statements does not preclude management from assigning specific duties not listed herein if such duties are a logical assignment to the position.)

Provides technical assistance with the initial set-up and secure deployment of systems which support information security including virus detection systems, firewall content filtering systems, and software license management systems.

Reviews and recommends configuration enhancements/modifications of intranets, firewalls, servers, applications, databases, desktops, laptops and other important parts of the Courts information systems infrastructure for maximum security levels.

Reviews patch levels on servers, desktops and laptops to insure they are kept current.

Assists with the development and training of a security awareness continuation training program for all Court employees.

Assists with the review of the implementation of security policies and practices for all Appellate Courts for compliance with Court Information Security Program.

Reviews log files and syslog records for suspicious activity regarding the access of court Information Services Systems resources.

Assists in supporting security initiatives with Circuit and Trial Court organizations.

Assists in developing the Security Policies to be implemented by the Court that will improve the security posture of the Court.

## **INFORMATION SECURITY ANALYST**

Assists with the selection, installation and adoption of automated tools which enforce or monitor the compliance with information security policies, procedures, and standards.

Manages the Public Key Infrastructure Used by the Court.

Evaluates information security notices issued by security vendors, government agencies, universities, professional associations, and other organizations, and as needed make recommendations to internal management to take precautionary steps. (i.e. Sans, CERT)

### **Competencies**

#### **Data Responsibility:**

Refers to information, knowledge, and conceptions obtained by observation, investigation, interpretation, visualization, and mental creation. Data are intangible and include numbers, words, symbols, ideas, concepts, and oral verbalizations.

Gathers, organizes, analyzes, examines, or evaluates data or information and may prescribe action based on these data or information.

#### **People Responsibility:**

Refers to individuals who have contact with or are influenced by the position.

Persuades or influences others in favor of a service, point of view, or course of action; may enforce laws, rules, regulations, or ordinances.

#### **Assets Responsibility:**

Refers to the responsibility for achieving economies or preventing loss within the organization.

Achieves considerable economies and/or prevents considerable losses through the management of a large division or minor department; and/or handles very large amounts of money.

#### **Mathematical Requirements:**

Deals with quantities, magnitudes, and forms and their relationships and attributes by the use of numbers and symbols.

Uses mathematics involving the practical application of fractions, percentages, ratios and proportions; or measurements, logarithmic, or geometric construction; may use algebraic solutions of equations and inequalities; descriptive statistics; deductive geometry, plane and solid, and rectangular coordinates; mathematical and classifications or schemes.

## **INFORMATION SECURITY ANALYST**

### **Communications Requirements:**

Involves the ability to read, write, and speak.

Reads journals, manuals, and professional publications; speaks informally to groups of co-workers, staff in other organizational agencies, general public, people in other organizations, and presents training; composes original reports, training and other written materials, using proper language, punctuation, grammar, and style.

### **Complexity of Work:**

Addresses the analysis, initiative, ingenuity, creativity, and concentration required by the position and the presence of any unusual pressures.

Performs work involving the application of logical principles and thinking to solve practical problems within or applying to a unit or division of the organization; requires continuous, close attention for accurate results and frequent exposure to unusual pressures.

### **Impact of Decisions:**

Refers to consequences such as damage to property, loss of data or property, exposure of the organization to legal liability, or injury or death to individuals.

The impact of errors is very serious - affects entire organization and the general public.

### **Equipment Usage:**

Refers to inanimate objects such as substances, materials, machines, tools, equipment, work aids, or products. A thing is tangible and has shape, form, and other physical characteristics.

Coordinates the handling of machines, tools, equipment or work aids involving extensive latitude for judgment regarding attainment of a standard or in selecting appropriate items.

### **Safety of Others:**

Refers to the responsibility for other people's safety, either inherent in the job or to assure the safety of the general public.

Requires some responsibility for safety and health of others and/or for occasional enforcement of the standards of public safety or health.

## INFORMATION SECURITY ANALYST

### Education and Experience Guidelines

#### **Education:**

Refers to job specific training and education that is recommended for entry into the position. Additional relevant experience may substitute for the recommended educational level on a year-for-year basis.

Bachelor's degree in engineering, computer science, management information systems or a closely related field.

#### **Experience:**

Refers to the amount of related work experience that is recommended for entry into the position that would result in reasonable expectation that the person can perform the required tasks. Additional relevant education may substitute for the recommended experience on a year-for-year basis, excluding supervisory experience.

Three years of related experience.

#### **Licenses, Certifications, and Registrations Required:**

Refers to professional, state, or federal licenses, certifications, or registrations required to enter the position.

None