



INFORMATION SYSTEMS SECURITY ANALYST

SCOPE OF WORK:

Work involves the completion of technical and administrative processes to safeguard data and information system assets by identifying and resolving potential and actual security problems and threats.

DUTIES PERFORMED:

- Develop, implement, and administer standards and policies on system security, including defining access privileges and procedures.
- Conduct research and gather data to determine available security software and techniques; determine those most appropriate to the current system; recommend those to be procured and installed.
- Monitor established data security processes and maintain installed software; implement process and system improvements; provide notifications and instructions to users on changes.
- Establish and utilize procedures for monitoring utilization of systems; ensure proper backup of data.
- Conduct and/or assist users in conducting needs assessments for security systems; analyze and evaluate system needs; provide alternative procedures; recommend solutions.
- Review current security system definitions for correctness; monitor, report and investigate access to determine unauthorized access attempts; provide continuous testing of systems for situations requiring corrective action.
- Participate in vulnerability management processes, including the active identification, assessment and remediation of security weaknesses.
- Participate in or conduct informational workshops to ensure effectiveness of user procedures; update users on current technology; perform and/or assist users in performing testing of new systems; respond to inquiries relating to system security problems.
- Provide assistance to other technical and administrative staff relative to security issues.

NOTE: The duties listed are not intended to be all-inclusive. Duties assigned any individual employee are at the discretion of the appointing authority.

INFORMATION SYSTEMS SECURITY ANALYST I
GRADE L

0117

LEVEL DEFINITION:

Positions at this level perform duties in a fully qualified status and require training or orientation only in relation to new systems, methods, or technology. Duties are performed under general supervision and employees are expected to perform all duties independently except those of a very complex nature.

ADDITIONAL DUTIES PERFORMED AT THIS LEVEL:

- None.

MINIMUM QUALIFICATIONS:

Requires a bachelor's degree in a computer science field and one year of complex computer system administration work experience. Additional computer system administration experience may be substituted on a year-for-year basis for up to two years of the required education. Job specific professional certifications may be substituted for required course work on a course-by-course basis for up to one year of the required education.

Requires a demonstrated ability to communicate effectively with technical and non-technical staff. Requires knowledge of disaster recovery and business continuity planning processes.

INFORMATION SYSTEMS SECURITY ANALYST II
GRADE M

0118

LEVEL DEFINITION:

Positions at this level are considered fully qualified and individuals are generally involved in all areas of related information system security activities. Incumbents have extensive knowledge of system security standards, tools, and processes. Work involves projects with increased complexity due to large or complex systems with a variety of platforms and/or connectivity methods. Duties are performed under general supervision and employees are expected to perform all duties independently.

ADDITIONAL DUTIES PERFORMED AT THIS LEVEL:

- Participate in the establishment of information system security policies and procedures, including the development of administrative standards.
- Interpret existing system security policies and procedures; develop and implement improvements.
- Develop and provide system security awareness and education programs for technical and non-technical users.
- Perform troubleshooting activities that require high-level information system security expertise; communicate findings to others.
- May be assigned supervisory and project management responsibility.

MINIMUM QUALIFICATIONS:

Requires a bachelor's degree in a computer science field and three years of complex computer system administration work experience, including at least one year of work experience that included computer system security activities. Additional computer security system work experience may be substituted on a year-for-year basis for up to two years of the required education. Job specific professional certifications may be substituted for required course work on a course-by-course basis for up to one year of the required education.

Requires a demonstrated ability to communicate effectively with technical and non-technical staff across all levels of the organization. Requires familiarity with disaster recovery and business continuity planning processes.

INFORMATION SYSTEMS SECURITY ANALYST III
GRADE N

0119

LEVEL DEFINITION:

Positions at this level are considered technical experts and are involved in all areas of work common to system security practices across the enterprise system. Incumbents have advanced knowledge of information systems security standards, tools, and processes. Work involves projects with the highest complexity due to complex systems, a variety of platforms, and/or a variety of connectivity methods. Duties are performed under broad supervision and employees are expected to perform all duties independently.

ADDITIONAL DUTIES PERFORMED AT THIS LEVEL:

- Perform highly complex analyses and technical tasks involving assignment and coordination of measures to provide information assurance, event detection and rapid response across various environments of the State enterprise.
- Design, implement and support integration of information security solutions including security architectures, firewall administration/monitoring, integrating security products, and developing and coordinating security implementation plans.
- Guide users and technical team members in formulating security requirements, integrating security requirements into existing system architectures, developing security test plans, overseeing the execution of security testing, and providing advice on alternative approaches.
- Serve as technical lead and collaborate with system and network architects on security projects which involve a wide range of issues including secure architectures, secure electronic data traffic, network security, platform and data security and privacy.
- Provide organizational support of enterprise security architecture and design, benchmarking, technical framework and gap analysis.
- Review and contribute to the improvement and standardization of the security administration process across all business units.
- Develop and present training to technical and non-technical staff on security related technologies, initiatives, and threats.
- Lead or assist in forensic analysis, cyber-crime investigation, security incident identification, investigation, and resolution.
- May be assigned supervisory and project management responsibility.

MINIMUM QUALIFICATIONS:

Requires a bachelor's degree in a computer science field and five years of complex network or computer system administration work experience, including at least three years of work experience that involved the installation and maintenance of security requirements for complex computer systems. Requires demonstrated, advanced proficiency with security information event monitoring, intrusion detection and prevention, firewall and data encryption technologies, antivirus and malware protection, and incident response processes. Additional network or computer system administration work experience may be substituted on a year-for-year basis for up to two years of the required education. Job specific professional certifications may be substituted for required course work on a course-by-course basis for up to one year of the required education.

Requires a demonstrated ability to communicate effectively and persuasively with technical and non-technical staff across all levels of the organization. Requires strong working knowledge of disaster recovery and business continuity planning processes.

Eff. Date: 7/97

Rev: 10/97 - Re-worded minimum qualifications.

Rev: 7/12 – Conversion to Hay System

Rev: 1/15 – Revised and added second level

Rev: 4/15 – Revised and added third level