IT SECURITY PROFESSIONAL

*[May also apply to exempt SHRA positions in the IT Security Specialist role\*]*

*Note: This material is not intended to represent a complete position description; it is meant as a job aid to provide a foundation for completing a detailed individual description. All functions and tasks listed below will not apply to every position and this is not an exhaustive list of potential duties. Supervisors should select any of this material which applies to provide a framework for their description, then add detail, context, and other functions relevant to their specific needs. This material is also competency- and band-level neutral. In addition to functions and tasks, other considerations including but not limited to scope, organizational placement, and reporting relationship are key determining factors in position leveling.*

|  |  |
| --- | --- |
| **FUNCTIONS** | **TASKS** |
| Support | * Serves as an expert level consultant and escalation resource for peers, ITS management and other units regarding incident management, forensics, and/or critical service tickets. * Serves as a point of escalation when the most complex situations arise and participate with management in decision making regarding policy and planning relevant to policy. |
| Project Management | * Defines project timelines and deliverables, monitors progress, and recommends changes as appropriate to ensure projects are completed on time and within budget. * Coordinates and prioritizes requests for changes and enhancements in the environment based on business needs, resources, and the impact of changes on existing systems and processes. * Evaluates project issues related to scope change, resource and time constraints to provide consistent solution delivery. * Identifies project risks in advance and proactively mitigates these risks with appropriate steps. |
| Security | * Acts as team lead, subject matter expert, determiner of best approach to recover from outages and decision maker regarding technical decisions related to network firewall architecture, implementation, maintenance, change control, vendor support, disaster recovery planning, reference documentation, set and business continuity plans. * Specifies, deploys, configures, manages, and maintains a wide variety of network tools, processes, and procedures to prevent and monitor unauthorized access, misuse, modification, or denial of service against attacks on the data network and network-accessible resources. * Establishes and maintains guidelines, protocols and procedures for internally reporting, tracking, investigating, and resolving security incidents. Provides metrics to management to clarify effectiveness and efficiency of incident management function. * Acts as a technical expert regarding investigations and in the forensic analysis, malware analysis and processing of incidents to successful resolution. * Oversees the investigation and management of information security events, tracks to conclusion, takes a leadership role in recommendation meetings and manages record keeping in accord with all laws and policies. Implements forensic best practices to support the integrity of the investigations. * Directs information security policy development and implementation in accordance with business requirements, relevant laws, regulations and contracts. Creates, issues, edits, interprets, and maintains security policies, standards, protocols guidelines, processes, and procedures under delegated authority and supervision of management. |
| Consultation | * Consults with departmental computing organizations to define the correct and secure operation of information processing facilities, operating procedures, change management processes, segregation of duties, and secure coding best practices. * Acts as expert level consultant regarding backup and archiving functions, network security management, proper media handling, systems monitoring and preservation and analysis of logs. |
| Training &  Communication | * Provides training to end users on security vulnerabilities, security awareness, access, compliance programming, etc. |
| Supervision/  Management | * Provides full supervision to [define subordinate positions]; interviews and makes hiring decisions/recommendations; recommends initial pay rates and subsequent adjustments; ensures employees are trained in job responsibilities and provides for ongoing development; manages the performance review process and assigns performance ratings; addresses performance deficiencies and disciplinary issues as needed; sets work schedules and approves leave requests; etc. |
| Other Duties (5% max) | * Other duties as assigned by management to meet business needs |

\*When employees in these existing, filled positions have elected to remain SHRA