HIGHLAND COUNTY CLERK OF COURTS

JOB DESCRIPTION

JOB TITLE: **IT Security Analyst**

CLASS:

DEPARTMENT: Information Technology

GENERAL DESCRIPTION:

The IT Security Analyst performs two core functions for the enterprise. The first is the day-to-day operations of the in-place security solutions while the second is the identification, investigation and resolution of security breaches detected by those systems. Secondary tasks may include involvement in the implementation of new security solutions, participation in the creation and or maintenance of policies, standards, baselines, guidelines and procedures as well as conducting vulnerability audits and assessments. The IT Security Analyst is expected to be fully aware of the enterprise's security goals as established by its stated policies, procedures and guidelines and to actively work towards upholding those goals.

ESSENTIAL JOB FUNCTION:

Strategy & Planning

- Participate in the planning and design of enterprise security architecture, under the direction of the IT Security Manager, where appropriate.
- Participate in the creation of enterprise security documents (policies, standards, baselines, guidelines and procedures) under the direction of the IT Security Manager, where appropriate.
- Participate in the planning and design of an enterprise Business Continuity Plan and Disaster Recovery Plan, under the direction of the IT Security Manager, where appropriate.

Acquisition & Deployment

- Maintain up-to-date detailed knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attack and threat vectors.
- Recommend additional security solutions or enhancements to existing security solutions to improve overall enterprise security.
- Perform the deployment, integration and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating practices/procedures generically, and the enterprise's security documents specifically.

Operational Management

- Maintain up-to-date baselines for the secure configuration and operations of all in-place devices, whether they be under direct control (i.e., security tools) or not (i.e., workstations, servers, network devices, etc.).
- Maintain operational configurations of all in-place security solutions as per the established baselines.
- Monitor all in-place security solutions for efficient and appropriate operations.

- Review logs and reports of all in-place devices, whether they be under direct control (i.e., security tools) or not (i.e., workstations, servers, network devices, etc.). Interpret the implications of that activity and devise plans for appropriate resolution.
- Participate in investigations into problematic activity.
- Participate in the design and execution of vulnerability assessments, penetration tests and security audits.
- Provide on-call support for end users for all in-place security solutions.

{These essential job functions are not to be construed as a complete statement of all duties performed. Employees will be required to perform other job related marginal duties as required.}

MINIMUM QUALIFICATION:

Formal Education & Certification

- College diploma or university degree in the field of computer science and/or 2 years equivalent work experience.
- One or more of the following certifications:
    - CompTIA Security+
    - GIAC Information Security Fundamentals
    - Microsoft Certified Systems Administrator: Security
    - Associate of (ISC)

Knowledge & Experience

- Extensive experience with intrusion detection and Internet architecture.
- Experience of five (5) or more years.
- Working technical knowledge of firewall theory and configuration.
- Strong understanding of IP, TCP/IP, and other network administration protocols.
- Strong understanding of necessary procedures to maintain security in domain structures, user authentication, and digital signatures.
- Must be able to weigh business needs against security concerns and articulate issues to management.

Personal Attributes

- Proven analytical and problem-solving abilities.
- Ability to effectively prioritize and execute tasks in a high-pressure environment.
- Good written, oral, and interpersonal communication skills.
- Ability to conduct research into IT security issues and products as required.
- Ability to present ideas in business-friendly and user-friendly language.
- Highly self-motivated and directed.
- Keen attention to detail.
- Team-oriented and skilled in working within a collaborative environment.

ENVIROMENTAL CONDITIONS:

Office environment.

Reasonable accommodations will be made for otherwise qualified individuals with a disability.

APPROVED:_____

NAME **TITLE** **DATE**