Job Title: **INFORMATION SECURITY ARCHITECT**

**SUMMARY**
Responsible for the development of Information Security architecture. Leads teams in the design of architecture components to support Information Security and business requirements. Creates a balanced Information Security architecture that considers people, process, technology and risk.

**ESSENTIAL FUNCTIONS**
- Acts as highest level Information Security technical expert, addressing problems of infrastructure, systems/applications integration, compatibility and multiple platforms.
- Develops business, information and technical architectures that are aligned with IT strategies and principles.
- Identifies and implements process improvements in the architecture and/or infrastructure of existing systems in regards to Information Security.
- Contributes towards the execution and maintenance of an Information Security risk acceptance process.
- Develops and documents Information Security policies and standards.
- Documents information security architecture design and analysis work in accordance with IT standards. Identifies the organizational and financial impact of information security architecture initiatives.
- Ensures delivery of scalable Information Security architecture compatible with business needs across applications, technologies and facilities.
- Promotes the enterprise architecture process, its outcome and ongoing results by mentoring IT staff.
- Leads the evaluation and selection of technology solutions in support of information security and business requirements.
- Performs gap analysis and develops optimized road maps to support strategic initiatives.
- Communicates highly technical aspects of architecture and integration effectively in a customer consulting setting.
- Establishes guidelines for reporting procedures. Consults with application or infrastructure development projects to ensure compliance with information security standards and policies.
- Leads architecture projects and teams to formulate and document architecture standards and strategy.
- Analyzes Information Security industry and market trends, and communicates their potential impact on the enterprise.
- Facilitates meetings and engages teams to participate and reach sound business and technical decisions by a consensus process.
- Maintains satisfactory attendance, to include timeliness.
• Responsible for understanding and complying with applicable quality, environmental and safety regulatory considerations. If accountable for the work of others, responsible for ensuring their understanding and compliance.
• This job description reflects management's assignment of essential functions; it does not prescribe or restrict the tasks that may be assigned.

SUPERVISORY RESPONSIBILITIES
Participates in the review and evaluation of personnel performance. Acts as senior-level mentor to technical staff and experienced management.

QUALIFICATIONS
To perform this job successfully, an individual must be able to perform each essential duty satisfactorily. The requirements listed below are representative of the knowledge, skill, and ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

MINIMUM QUALIFICATIONS
• High school diploma or State-issued equivalency certificate.
• Bachelor's degree in Information Security, Cybersecurity, Computer Science, Business Administration, MIS, Mathematics, or Engineering plus 8 years of experience spanning at least two IT disciplines, including Information Security, technical architecture, network management, application development, middleware, database management, business intelligence or operations reflecting increasing levels of responsibility; or 12 years of experience spanning at least two IT disciplines, including technical architecture, network management, application development, middleware, database management, business intelligence or operations reflecting increasing levels of responsibility.

PREFERRED QUALIFICATIONS
• Master’s degree in Computer Science, Business Administration, MIS, Mathematics, or Engineering.
• Experience with creation of Information Security policies and standards.
• Experience with design and execution of Information Security risk acceptance process.
• Experience with report creation using security analytics toolsets.
• Competency with IT-GRC tools (i.e. Archer, RiskVision, Metricstream, ServiceNow, etc.)
• Experience with creating assessment programs/campaigns within a GRC platform that allow for automation of control testing, and flexible workflows to support various business processes.
• Experience with securing and risk assessing SAP environments.
• Working knowledge of major security frameworks and control methodologies such as NIST, COBIT, ISO27001, etc.
- Experience with network switching, infrastructure security, virtualization, Linux/Unix, virtualization technology, storage area network/network attached storage, and similar IT infrastructure components
- Experience with MS Word, MS Excel and MS PowerPoint.
- Understanding of web servers and applications, Java application servers and applications, EAI, SOA and LDAP directory technologies.
- Exposure to multiple, diverse technologies and processing environments
- Knowledge of all components of an enterprise technical architecture
- Knowledge of business process re-engineering principles and processes
- Strong understanding of network architecture and application development methodologies
- Experience reading, analyzing, and interpreting common scientific and technical journals, financial reports, and legal documents.
- Understanding of emerging technologies, development platforms and hardware platforms.
- Experience responding to common inquiries or complaints from customers, regulatory agencies, or members of the business community.
- Experience effectively presenting information to top management, public groups, IT stakeholders, and internal/external auditors.
- Possesses a passion for Information Security and its impact on the enterprise, customers and consumers along with a breadth of experience that can balance business, application and operational requirements.
- Strong understanding of systems and “systems thinking” with the ability to make trade-off decisions to accomplish system-wide goals.
- Excellent written and verbal communication skills.
- Excellent planning and organizational skills.
- Comprehends the functions and capabilities of new technologies.
- Skilled in balancing long-term and short-term perspectives of challenging situations.
- Skilled in translating business needs into Information Security architecture requirements.
- Skilled in applying multiple technical solutions to business problems.
- Remains unbiased toward any specific technology or vendor choice.
- Excellent analytical and technical skills.
- Strong leadership skills.
- Skilled in navigating complex political situations to ensure successful change management.
- Exceptional interpersonal skills, including teamwork, facilitation and negotiation.
- Demonstrates strong technical thinking and developed high credibility with the technical community. Recognized by the IT community as someone who solves complex technology related business problems.

PHYSICAL DEMANDS
The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is frequently required to sit. The employee is occasionally required to stand and walk.

WORK ENVIRONMENT
The work environment characteristics described here are representative of those an employee encounters while performing the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

The noise level in the work environment is usually moderate.