INFORMATION SECURITY ANALYST

Department	Information Technology	**Direct Care** **Non-Direct Care**	Non-Direct Care
FLSA Status	Exempt	**Exemption Type** *(HR Use Only – Check all that apply)*	☐Executive ☒Computer ☐Administrative☐Professional ☐Outside Sales
Reports to	Information Security Manager	**Supervises**	N/A
Primary Location	Corporate-Buffalo	**Employment Status**	☒Full Time ☐Part Time ☒Regular ☐Temporary
Original Date	November 2022	**Revised Date**	April 2024

JOB SUMMARY

Job summary should specify the nature and purpose of the job. Please provide one to two sentences starting with an action verb, followed by the aim of the position that identifies the primary result of the position.

The IT Information Security Analyst at Person Centered Services is a pivotal contributor in delivering comprehensive information security expertise. This role entails engaging with innovative security tools to guarantee comprehensive protection, streamline troubleshooting, ensure thorough auditing, and uphold and uphold stringent documentation standards for all security and compliance protocols.

The analyst is instrumental in bolstering the organization's technological framework, ensuring a computing environment that is not only secure and dependable but also adheres to compliance standards.

ESSENTIAL FUNCTIONS

List the essential job functions or responsibilities. Typically, most jobs have between 8 to 12 essential functions. It is critical to note that not every function of the position should be deemed as essential. Essential functions should include only those items that are "critical for getting the job done" or "accountabilities".

- Safeguard data and information systems from unauthorized access, alterations, or destruction while ensuring the confidentiality, integrity, and availability of company and partner information assets.
- Comprehend and adhere to the critical practice of protecting sensitive health information in accordance with New York State.
- Collaborate with IT Operations to implement and maintain information security systems as directed by leadership, ensuring a fortified defense against digital threats.
- Perform comprehensive assessments of the security landscape to detect and address vulnerabilities, fortifying the organization's cyber resilience across all platforms.

- Maintain comprehensive standards for intrusion detection and data loss prevention, reinforcing a proactive security stance within the organization.
- Provide expert-level information security incident response and investigative support, mitigating risks and enhancing system security.
- Review and monitor sign-in and activity logs diligently, identifying and addressing anomalies to maintain system integrity.
- Secure company data during transit and at rest, employing advanced encryption and security measures to prevent unauthorized access.
- Review permissions for enterprise information resources, ensuring strict adherence to access control policies.
- Create and disseminate security awareness training materials, fostering a culture of security mindfulness and preparedness across the organization.
- Establish industry-compliant best practices, aligning with regulatory requirements and setting the standard for information security excellence.
- Security Awareness: Conduct security awareness campaigns to educate team members, enhancing organizational resilience against social engineering.
- Provide expert-level information security incident response, investigative support, and end-user security assistance, ensuring a comprehensive security framework and user education.
- Engage in comprehensive, detailed investigations, adeptly conducting interviews and posing critical questions that contribute to the determination and resolution of cases, ensuring a well-rounded and effective investigative process.

OTHER DUTIES
List other non-essential job functions or responsibilities. May wish to include in the list "performs other duties as assigned".

- Commits to a respectful, just, and supportive environment for individuals and team members aligning with the company's commitment to diversity, equity, inclusion and belonging.
- As a leader, sets and promotes a culture focused on diversity, equity, inclusion and belonging in all business practices. This includes actively seeking, hiring, and developing talented candidates and appropriately and fairly addressing issues related to diversity, equity, and inclusion in all interactions with team members.
- Other duties as necessary or assigned.

KNOWLEDGE, SKILLS & ABILITIES
List required knowledge, skills and abilities needed for the job.

- Proficiency in Information Security standards and best practices, ensuring adherence to the highest industry benchmarks.

- Comprehensive knowledge of Information Security tools and processes, enabling effective security management and response.
- In-depth understanding of regulatory compliance and controls, including HIPAA, NIST (National Institute of Standards and Technology) 800-53, HITECH, and MCD, to maintain legal and ethical standards.
- Expertise in securing cloud-based solutions such as Microsoft Azure, and other cloud platforms, safeguarding digital assets in the cloud.
- Capability to conduct thorough assessments of risk, threats, and vulnerabilities, identifying potential security breaches before they occur.
- Self-motivation and a results-focused approach, driving initiatives to successful and timely completions.
- Critical thinking and decision-making skills, enabling swift and effective resolution of complex security challenges.
- Excellent communication skills, both written and verbal, facilitating clear and concise security directives and collaboration.
- Systematic documentation and organizational skills for management oversight and review, ensuring precision and orderliness in record-keeping and operational processes.
- Ability to develop and conduct training sessions on IT security best practices, enhancing the security competence of the organization.
- Demonstrate the ability to conduct in-depth security research and leverage that knowledge to integrate innovative tools and practices, significantly enhancing the organization's security posture. This entails keeping pace with the latest security advancements and translating those insights into strategic, actionable enhancements that bolster the organization's defenses.
- Possess the ability to author informative posts that keep the organization informed of the latest security updates, threats, and trends, contributing to a heightened awareness and proactive security culture.
- Compile concise reports highlighting the security team's metrics for management, highlighting operational efficiency and resource utilization, while ensuring compliance with security protocols and facilitating informed decision-making.
-

EDUCATION & EXPERIENCE

List required education and/or experience needed for the job.

- Bachelor's degree in information technology or Cybersecurity, or a recognized certification in an Information Security discipline **required**
- Minimum of three years' experience in IT or information/cybersecurity, with a solid foundation in Microsoft 365 and cloud computing environments. *preferred*

- Familiarity with NIST 800-53 control framework *preferred*
- Some healthcare or human service experience *preferred*

PHYSICAL REQUIREMENTS

List physical requirements of the job and indicate how often the team member is required to perform these requirements. The physical demands described here are representative of those that must be met by a team member to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Physical Activity	Frequency			
	N/A	Rarely	Occasionally	Regularly
Travel	☐	☐	☒	☐
Ambulate	☐	☐	☒	☐
Drive	☐	☐	☒	☐
Type/Keyboard	☐	☐	☐	☒
Twist/turn	☐	☐	☒	☐
Stand	☐	☐	☒	☐
Sit	☐	☐	☐	☒
Talk	☐	☐	☐	☒
Hear	☐	☐	☐	☒
Use hands and fingers	☐	☐	☐	☒
Repetitive Motion	☐	☐	☐	☒
Close vision	☐	☐	☐	☒
Peripheral Vision	☐	☐	☐	☒
Depth of Perception	☐	☐	☐	☒
Ability to see color	☐	☐	☐	☒
Lift up to 5 lbs.	☐	☐	☒	☐
Lift up to 10 lbs.	☐	☐	☒	☐
Lift up to 20 lbs.	☐	☐	☒	☐
Lift up to 50 lbs.	☐	☐	☒	☐
Lift up _____ lbs.	☐	☒	☐	☐
Carry	☐	☐	☒	☐
Reach	☐	☐	☒	☐
Push	☐	☒	☐	☐
Climb	☒	☐	☐	☐
Pull	☐	☒	☐	☐
Stoop	☐	☒	☐	☐
Kneel	☐	☒	☐	☐
Crouch	☐	☒	☐	☐
Crawl	☐	☒	☐	☐

Physical Activity				
Balancing	☐	☒	☐	☐
Other:	☐	☐	☐	☐
Other:	☐	☐	☐	☐

ENVIRONMENTAL CONDITIONS

List environmental conditions of the job and indicate how often the team member is exposed to these conditions.

Physical Activity	Frequency			
	N/A	**Rarely**	**Occasionally**	**Regularly**
Office environment	☐	☐	☐	☒
Moderate noise	☐	☐	☒	☐
Loud noise	☐	☒	☐	☐
Extremely loud noise	☒	☒	☐	☐
Confined area	☒	☐	☐	☐
Exposure to bloodborne pathogens or bodily fluids	☒	☐	☐	☐
Exposure to allergens	☒	☐	☐	☐
Exposure to chemicals	☒	☐	☐	☐
Exposure to airborne pathogens	☐	☒	☐	☐
Exposure to dim lighting	☐	☒	☐	☐
Exposure to bright lighting	☐	☐	☐	☒
Exposure to heights or high precarious places	☒	☐	☐	☐
Extreme heat/humid conditions	☒	☐	☐	☐
Outdoor conditions	☐	☒	☐	☐
Other:	☐	☐	☐	☐
Other:	☐	☐	☐	☐

I can, with or without reasonable accommodation(s), perform the essential functions of this position:

Team Member Signature: _____   Date: *Click or tap to enter a date.*

Supervisor Signature: _____   Date: *Click or tap to enter a date.*

HR Reviewed Signature: *Michelle Hoffman*   Date: 4/26/2024