HILLSBOROUGH COUNTY SHERIFF'S OFFICE
CHAD CHRONISTER, SHERIFF

Chief Technology Officer

Job Code: U8802
Pay Grade: UO
Pay Scale: $173,637.48-$293,784.70 Annually
Exempt: Yes

OVERVIEW

This is a senior management position within the Information Services Division (ISD) of the Sheriff's Office that reports to the Chief Information Officer (CIO). The Chief Technology Officer (CTO) is responsible for managing the functional/operational areas of the Information Services Division (ISD) and ensuring operations function according to pre-defined standards, policies, and processes; Service Level Agreements; Operational Level Agreements; and compliance tracking via analysis and monitoring of performance metrics implemented and collected by direct reporting sections. This role shall operate with a keen focus on transparency, operational efficiency, and quality in service delivery.

DUTIES & RESPONSIBILITIES

Duties may vary based on assignment.

- Provide executive leadership and management to the functional/operational areas of business support, criminal justice systems, field support, help desk, and infrastructure via managing, directing, and evaluating assigned staff by coordinating schedules and functions to ensure adequate coverage and control; assigning, monitoring, and reviewing work and timesheets; and evaluating performance via providing feedback, coaching, or initiating corrective action as needed, including termination.
- Evaluate and develop technology strategies, road maps, and technology investment strategies that align technology with Sheriff's Office goals, objectives, and business priorities by communicating technology strategies to external partners, management, and employees; and building relationships with vendors.
- Lead technology governance discussions via communicating the Sheriff's Office infrastructure, network, platforms, and telephony strategies to the CIO, agency leadership, and other employees; and assisting with ISD recruitment, retention, and staff development.
- Organize, prioritize, and assign the work of multiple professional level subordinates to achieve established organizational goals and objectives by ensuring that subordinates have the proper resources needed to complete the assigned work; monitoring the status of work in progress and reviewing completed work; consulting with assigned staff to assist with complex/problem situations and provide technical expertise; providing progress and activity reports to management; and assisting with the revision of standard operating procedures (SOPs) and procedure documentation as appropriate.
- Ensure adherence to all SOPs, processes, guidelines, and documentation for all security-related activities by ensuring that all defined security-related policies and procedures are adhered to; ensuring that proper tools and technologies are in place to properly protect the security of Sheriff's Office assets, technology and data, and maintain business operations continuity; and ensuring that predefined security metrics and security policies are adhered to while working with the Sheriff's Office Local Agency Security Officer (LASO) and/or Security team to respond to and resolve Sheriff's Office security incidents.
- Serve as the Escalation Point for key issues and decisions for all reporting functional/operational areas by ensuring that all IT assets (e.g., network, infrastructure, data,

applications, hardware) are properly secured and highly available, with processes implemented to manage their security and availability are up-to-date and adhered to; promoting collaboration between service management and operations areas to ensure that areas remain informed of new policies, services, security protocols, and operational events; and assisting the CIO by being an active member of ISD management and Sheriff's Office technology governance teams.

- Verify service operations against stated Service Level Agreements and Operational Level Agreements by continuously overseeing the stability and performance of the live technical environment; ensuring that a single source of consistent information on all IT services is delivered and effectively maintained; and reviewing current service performance and enterprise IT environment components to ensure IT capacity meets business needs.
- Assist in developing and administering the ISD budget by forecasting funding needs and making recommendations for functional/operational area staffing, equipment, materials, supplies, procurement, and contracting; and monitoring expenses upon budget approval to ensure compliance.
- Monitor and evaluate division contracts, services, and operations by making operational need recommendations; developing and implementing functional/operational area goals that align with Sheriff's Office and ISD goals and objectives; reviewing technical standards, operating practices, and procedures; implementing changes for improved operational efficiency; identifying strategic initiatives; developing operational work plans; and assigning projects to management staff.
- Develop and implement standards, policies, and procedures by maintaining written standards for data and work process management; documenting and reviewing procedures for specific dataset maintenance; establishing and enforcing best practices; and consulting with other managers in the design of procedures and standards.
- Maintain an awareness of new applications, technologies, technical methods, trends, and advances in the profession by reviewing professional publications, technical manuals, and web sites to increase knowledge of network operations; and attending conferences, workshops, and training sessions as appropriate.
- Process a variety of documentation associated with division operations within designated timeframes and per established procedures by receiving and reviewing various documentation (e.g., status reports, bid specifications, help desk reports, project plans) and reviewing, completing, processing, forwarding, or retaining as appropriate; preparing or completing various forms, reports, correspondence, and other documentation for the CIO and agency leadership (e.g., SOPs, procedural documentation, guidelines, employee performance reviews, personnel documentation); compiling data for further processing or use in preparation of division reports; and maintaining computerized and/or hard copy records.
- Operate or use various equipment and supplies (e.g., personal computer, word processing software, spreadsheets, databases, printer, etc.) to complete work assignments and essential job functions.
- Communicate with Sheriff's Office leadership, employees, third party vendors, and other individuals as needed to coordinate work activities, review status of work, exchange information, or resolve problems.
- Serve as acting CIO as required.
- May assist in supporting the Emergency Support Function Coordinator during emergency incidents supporting the restoration of the communications infrastructure, facilitating the recovery of systems and applications from cyber-attacks, and coordinating Sheriff’s Office communications support to response efforts during incidents.
- Effectively communicate as appropriate any information, statuses, or issues to the CIO in a timely manner to ensure that the CIO is kept informed and prepared to brief agency leadership as needed.
- Perform other related duties as required.

KNOWLEDGE & ABILITIES

- Thorough knowledge of the functions, activities, requirements, and objectives of IT functional/ operational areas to which assigned.
- Knowledge of federal, state, and local regulations pertaining to public record law, records

retention, and data security.
- Knowledge of management methods, techniques, and practices.
- Knowledge of data center environments, high availability, disaster recovery and N+1 (redundancy in place for all critical components) architectures.
- Knowledge of enterprise class data center compute devices, operating systems and the associated support and operational requirements.
- Knowledge of enterprise class storage systems and tiers, to include data protection, recovery, and optimization.
- Knowledge of virtual environments to include on-premise, hybrid and cloud (PAAS – Platform As A Service, IAAS – Infrastructure As A Service, DAAS – Desktop As A Service) and the three major cloud providers (Amazon, Google, Microsoft).
- Knowledge of enterprise networking, to include LAN (Local Area Network)/MAN (Metropolitan Area Network)/WAN (Wide Area Network), SDN (Software Defined Networking), VPN (Virtual Private Network), L2/L3 (Layer 2 / Layer 3), and wireless.
- Knowledge of perimeter defenses to include firewalls, proxies, and DMZ (De-Militarized Zone).
- Knowledge of endpoint management to include the entire network stack and both on-premise and virtual capabilities.
- Knowledge of asset management (both financial and IT).
- Knowledge of Zero Trust, NIST 800:53 (National Institute of Standards and Technology), CSF (Cyber Security Framework), CJIS (Criminal Justice Information Services) and generally accepted cybersecurity standards.
- Knowledge of end user hardware and operating systems, to include desktops, laptops, docking stations, monitors, printers, Microsoft Windows to include support and lifecycle management.
- Knowledge of government purchasing and ethical standards to include vendor interactions, purchasing contracts, and capitalization of hardware and software (GASB – Governmental Accounting Standards Board).
- Knowledge of the critical applications and services required to support a modern, large scale public safety enterprise to include dispatching, mobile terminals, record retention and employee safety mechanisms.
- Knowledge of end user support standards and processes required to adhere to user centric key performance metrics in a 24/7/365 critical environment.
- Ability to establish and maintain effective and cooperative internal and external working relationships with those contacted in the course of work.
- Ability to identify strategies and develop plans to carry out work.
- Ability to use considerable initiative, think independently, and exercise sound judgment.
- Ability to establish operation or project objectives and strategies for a functional or operational area.
- Ability to provide recommendations for improvements/efficiencies and implement recommendations.
- Ability to delegate and manage, effectively through scheduling, assigning, monitoring, reviewing, and evaluating the work of assigned staff.
- Ability to learn, understand, and implement new technology quickly and independently.
- Ability to communicate effectively, both orally and in writing, at all levels of the agency and with outside agencies.
- Ability to continuously learn and apply knowledge to work through engaging in professional skill development.
- Ability to use a computer and related software.

SKILLS

- Enterprise Architecture (EA)
- Executive Leadership
- Information Security
- Strategic Planning
- Technology Strategy Development

WORKING CONDITIONS

- Work within an office environment within a law enforcement agency.
- Stand/sit at a keyboard or workstation for prolonged periods.
- May engage in light physical exertion (e.g., lifting, carrying, pushing and/or pulling of objects and materials up to 10 pounds).
- Work standard business hours.
- May work non-standard hours including nights, weekends, and holidays.
- In the event of an emergency or disaster, may be required to respond promptly to duties and responsibilities as assigned by management chain, Division/District Commander, or the Sheriff (or their designee). Such assignments may be for before, during or after the emergency/disaster.

MINIMUM EDUCATION & EXPERIENCE

- A bachelor's degree or higher from an accredited institution of higher education with a major in Public Administration, Information Technology, Computer Science, or related field.
- Nine years of experience in IT service management and/or technical operations.
- Five years of progressive lead or managerial experience at an organization with at least 1,000 employees.

OR

- Seven years of progressive experience in a Hillsborough County Sheriff's Office Information Services Division position.
- Five years of progressive lead or managerial experience in the Hillsborough County Sheriff's Office Information Services Division and/or at an organization with at least 1,000 employees.

ADDITIONAL JOB REQUIREMENTS

- Attendance at the specified Sheriff's Office work location is required.
- Depending on assignment, employees may be required to possess a valid Florida Driver License at time of employment. Driving history will be thoroughly reviewed and may be grounds for disqualification.
- No visible tattoos on face, head, and neck. Tattoos determined to take away from the professional appearance of the Sheriff's Office must be covered with an appropriate white, black, or neutral covering.
- No illegal drug sale within lifetime.
- No illegal drug use within the past 36 months. No marijuana use within the last 12 months.
- No felony convictions within lifetime.
- No misdemeanor convictions involving perjury, false statement, or domestic violence within lifetime.
- No dishonorable discharge from any branch of the United States Armed Forces, the United States Coast Guard, National Guard, or Reserve Forces.
- Successful completion of a background investigation including criminal, reference, employment, and neighborhood checks; polygraph; medical evaluation; and drug screening.
- Live within Hillsborough County or within Citrus, Hardee, Hernando, Lake, Manatee, Pasco, Pinellas, Polk, Sarasota, or Sumter County as long as the residence is located within the 60-mile parameter of Falkenburg Road Jail at the time of appointment/employment (certified only).

The duties and responsibilities on this job description represent the essential functions that an employee must be able to satisfactorily perform with or without reasonable accommodations. Reasonable accommodations shall be made upon request to enable employees with disabilities to perform the essential functions of their job, absent undue agency hardship. The Sheriff's Office retains the right to change or assign other duties to this job as necessary.

PREFERRED QUALIFICATIONS

- Current or previous certifications in networking (Cisco, Brocade), storage (NetApp, EMC), operating systems (Microsoft, Apple, RedHat), cloud (Amazon, Google, Microsoft) or general technical knowledge (CompTIA, ISACA) and/or similar certifications.
- Experience with large public safety and/or law enforcement environments with 24/7 availability demands.
- Experience in government budget, procurement, or contract management.
- Experience managing multiple teams and/or units of highly technical, creative teams.