

Chief Information Officer / Chief Technology Officer (CIO/CTO)

Location: Laurel, Maryland (Hybrid)

Schedule: Full-time

Position Summary

Market USA Federal Credit Union, a \$140 million, Great Place to Work-Certified credit union located in Laurel, Maryland, is seeking an innovative and strategic Chief Information Officer / Chief Technology Officer (CIO/CTO) to lead the organization's technology vision, cybersecurity initiatives, digital transformation efforts, and information systems strategy.

As a member of the executive leadership team, the CIO/CTO will oversee all aspects of information technology, cybersecurity, digital banking, data governance, business continuity planning, vendor management, and emerging technologies. This position will play a critical role in advancing the credit union's technology roadmap, enhancing member experience, improving operational efficiency, and supporting long-term organizational growth.

The ideal candidate will possess a strong combination of strategic leadership, cybersecurity expertise, technology management experience, and a passion for innovation.

Key Responsibilities

Strategic Technology Leadership

- Develop and execute a comprehensive technology strategy aligned with the credit union's strategic objectives.
- Advise executive leadership and the Board of Directors on technology trends, cybersecurity risks, and strategic technology investment opportunities.
- Lead digital transformation initiatives that enhance member service and operational effectiveness.
- Drive the adoption of emerging technologies, including artificial intelligence, automation, cloud services, and advanced analytics.

Information Technology Management

- Direct all aspects of technology infrastructure, network operations, telecommunications, systems administration, and end-user support.
- Ensure the reliability, scalability, security, and performance of all technology systems.

- Oversee core processing platforms, digital banking applications, and integrated third-party technologies.
- Establish and maintain technology standards, policies, and procedures.

Cybersecurity & Information Security

- Provide executive oversight for the credit union's cybersecurity and information security programs.
- Ensure compliance with NCUA regulations, FFIEC guidance, GLBA requirements, and applicable federal and state laws.
- Lead cybersecurity risk assessments, incident response activities, vulnerability management efforts, and third-party security reviews.
- Promote an organization-wide culture of cybersecurity awareness and information protection.

Digital Banking & Innovation

- Oversee digital banking platforms, online and mobile banking services, digital account opening, and payment solutions.
- Identify opportunities to improve member experience through technology innovation and process automation.
- Evaluate and implement emerging technologies that support growth, efficiency, and member engagement.

Data Governance & Analytics

- Establish enterprise-wide data governance standards and best practices.
- Promote the use of business intelligence and analytics in strategic decision-making.
- Ensure data quality, security, retention, and regulatory compliance across the organization.

Vendor & Project Management

- Manage strategic technology vendor relationships and contract negotiations.
- Oversee technology project portfolios and ensure successful implementation within budget and on schedule.
- Conduct due diligence, risk assessments, and performance monitoring of technology vendors.
- Manage departmental operating and capital budgets.

Business Continuity & Disaster Recovery

- Direct the credit union's business continuity and disaster recovery programs.
- Ensure technology recovery capabilities are tested, maintained, and aligned with organizational requirements.
- Coordinate technology recovery efforts during incidents and business disruptions.

Team Leadership

- Recruit, develop, and retain high-performing technology professionals.
- Foster a culture of innovation, collaboration, accountability, and continuous improvement.
- Provide leadership, coaching, mentoring, and professional development opportunities to the Business Systems Manager, Senior Network & Systems Administrator, and indirect reports, as appropriate.

Regulatory Compliance & Governance

- Support internal and external audits, regulatory examinations, and risk assessments.
- Maintain policies related to information technology, cybersecurity, vendor management, and business continuity.
- Present technology and cybersecurity updates to senior leadership, committees, and the Board of Directors.
- Lead technology-related oversight functions and enterprise technology risk initiatives.

Qualifications

Experience

- Minimum of five (5) years of progressively responsible experience in information technology leadership, cybersecurity, or related executive technology roles.
- Financial institution experience preferred.
- Experience leading technology strategy, cybersecurity programs, vendor management, and digital transformation initiatives.

- Experience providing strategic oversight and technical guidance for Microsoft 365 environments, including Exchange Online, SharePoint, Teams, OneDrive, Intune, Entra ID (Azure Active Directory), and security/compliance services.
- Experience providing strategic oversight and technical guidance for Active Directory and identity management solutions, including authentication, authorization, single sign-on, and Group Policy administration.
- Experience providing strategic oversight and technical guidance for Windows desktop and server environments, including endpoint management, patch management, operating system lifecycle management, and infrastructure modernization.
- Experience providing strategic oversight and technical guidance for Linux operating systems and enterprise applications in production environments.
- Experience providing strategic oversight and technical guidance for managing enterprise networking infrastructure, including LAN, WAN, wireless networks, VPNs, SD-WAN, and telecommunications systems.
- Experience providing strategic oversight and technical guidance for firewall technologies, intrusion prevention systems, network security controls, and perimeter security architectures.
- Experience providing strategic oversight and technical guidance for VMware virtualization environments, including high availability, disaster recovery, storage integration, and capacity planning.
- Experience providing strategic oversight and technical guidance for DNS, DHCP, certificate services, and core network infrastructure components.
- Experience leading the evaluation, implementation, integration, and ongoing management of automation solutions using scripting, orchestration tools, robotic process automation (RPA), workflow technologies, and third-party vendors to improve operational efficiency.
- Experience working with SQL databases, including query development, reporting, data integration, performance optimization, and business intelligence solutions.
- Experience leading service desk and technical support operations, including ITIL-based service management practices, SLA management, and customer service excellence.
- Experience implementing and managing encryption technologies, key management solutions, data protection controls, and secure communications platforms.

- Experience managing enterprise database environments, including administration, backup and recovery, performance monitoring, security, and data governance initiatives.

Education

- Bachelor's degree in Information Technology, Computer Science, Information Systems, Cybersecurity, Business Administration, or a related field.
- In lieu of degree, an equivalent combination of education, certifications, and directly related experience may be considered.

Preferred Certifications

- Certified Information Systems Security Professional (CISSP)
 - Certified Information Systems Auditor (CISA)
 - Certified Information Security Manager (CISM)
 - Certified Chief Information Security Officer (CCISO)
 - Certified Cloud Security Professional (CCSP)
 - ITIL 4 or 5 Managing Professional or ITIL Strategic Leader
 - Project Management Professional (PMP)
-

Knowledge, Skills & Abilities

- Strong knowledge of information technology infrastructure, networking, cloud computing, cybersecurity, and application systems.
- Understanding of credit union and financial institution technologies and regulatory requirements.
- Strong leadership, project management, and vendor management skills.
- Excellent written, verbal, and presentation communication abilities.
- Ability to influence strategic decisions and build strong relationships across all organizational levels.
- Strong analytical and problem-solving skills with a commitment to innovation and continuous improvement.
- Advanced knowledge of Microsoft 365 administration, security, compliance, collaboration, and productivity platforms.

- Strong understanding of Active Directory
- Knowledge of Entra ID (Azure Active Directory), identity governance, access management, and authentication technologies.
- Comprehensive knowledge of Windows desktop and server operating systems, endpoint management, virtualization, and systems architecture.
- Working knowledge of Linux operating systems, server administration, and enterprise application hosting.
- Advanced understanding of network architecture, routing, switching, wireless technologies, VPNs, DNS, DHCP, and telecommunications systems.
- Expertise in firewall administration, network segmentation, intrusion prevention, security monitoring, and cybersecurity best practices.
- Strong knowledge of VMware virtualization technologies, virtual infrastructure design, capacity planning, business continuity, and disaster recovery.
- Experience with website technologies, content management systems, web hosting, SSL certificate administration, and web security principles.
- Strong knowledge of automation technologies, scripting languages, workflow orchestration, and process improvement methodologies.
- Proficiency in SQL reporting and analytics.
- Knowledge of IT service management frameworks such as ITIL, including incident, problem, change, and asset management processes.
- Thorough understanding of encryption technologies, key management practices, data loss prevention, and information security controls.
- Strong knowledge of relational database management systems, database architecture, backup and recovery strategies, and data governance principles.
- Understanding of cloud computing platforms, hybrid infrastructure architectures, SaaS solutions, and cloud security frameworks.

Additional Comments

- This position is hybrid eligible and based in Laurel, Maryland. The hybrid schedule provides flexibility to work remotely, with some mandatory onsite workdays based on organizational and leadership needs.

Compensation

Salary Range: \$105,455 – \$162,000 annually. Compensation is commensurate with experience and qualifications.

About Market USA Federal Credit Union

Market USA FCU is a certified Great Place to Work employer. Founded in 1953, the credit union is focused on improving the financial lives of its members. Market USA FCU offers competitive salaries and a comprehensive benefit package including medical and dental insurance, generous paid time off, an employee assistance program, casual back-office dress, back-office pet policy, hybrid work model, employee banking benefits, an employer matching 401(k) plan, life insurance, long term disability and career advancement opportunities. For more information on Market USA, please visit our website at www.marketusafcu.com.

Equal Opportunity Employer

Market USA Federal Credit Union is an Equal Opportunity Employer.

How to Apply

Interested candidates should send a resume and salary requirements to jobs@marketusafcu.com and reference CIO/CTO position in the subject line.