Information Security Officer

Department:	IT
Reports To:	Chief/VP Information Officer
Classification:	Exempt
Pay:	Grade 14 $98,538.35 (min.) - $123,172.93 (mid.) - $147,807.52 (max.)
Type:	Full Time
Location:	Glendora, CA (Hybrid Eligible)

Purpose:

To position ACCU's physical and logical security stance to:

- Protect the personal and confidential financial information of the member.
- Safeguard both the physical and digital assets of the Credit Union from loss or corruption.
- Foster a proactive security culture to address emerging threats such as ransomware, supply chain vulnerabilities, and insider risks.

Key Responsibilities:

- Protect the personal and confidential financial information of the member.
- This role serves as the Credit Union's designated Information Security Officer, with enterprise responsibility for the Information Security Program and direct reporting access to executive leadership and the Board of Directors or a designated Board committee.
- Provides governance, oversight, and independent risk assessment while collaborating with IT and business units responsible for operational implementation.
- Safeguard both the physical and digital assets of the Credit Union from loss or corruption.
- Develop and execute information security programs to ensure ACCU maintains a strong, security-minded culture.
- Implement and execute an anti-phishing program that includes ongoing testing, training, and remediation.

- Perform internal and external vulnerability scans at regular intervals.
- Conduct workstation and server vulnerability scoring to inform vulnerability/patching priorities and efforts.
- Collaborate with IT to remediate vulnerabilities so that outstanding vulnerability metrics remain within KPI targets.
- Oversee and coordinate the annual PCI DSS self-assessment.
- Maintain and regularly update Incident Response Plans.
- Oversee physical security annual testing, including CCTV, fire alarms, glass break alarms, and ingress/egress security.
- Maintain a current and comprehensive understanding of applicable laws and regulations as they pertain to information security, cybersecurity, and physical security.
- Provide ongoing cybersecurity awareness and role-based training through a combination of live sessions and online modules.
- Research, recommend, develop, and implement new security products, services, programs, and practices in accordance with Board policy [Information Security Program].
- Provide governance and oversight of the Identity and Access Management (IAM) program, ensuring periodic user access reviews are performed by system owners and administrators.
- Research, recommend, develop, and implement computer software and hardware to enhance ACCU's security stance, loss prevention, and disaster recovery systems.
- Oversee third-party/vendor risk management, including due diligence and ongoing monitoring.
- Conduct regular risk assessments and report findings to executive leadership and the Board.
- Lead incident investigations and post-incident reviews to identify root causes and implement corrective actions.
- Coordinate the maintenance and testing of business continuity and disaster recovery plans.
- Review security architecture for new systems, applications, and projects.
- Prepare for and support regulatory exams and internal/external audits.
- Ensure information security practices support and align with BSA, AML, and OFAC compliance requirements in coordination with Compliance leadership.
- Maintain active memberships in InfraGard and FS-ISAC.
- Participate in disaster recovery and contingency exercises with key third parties on a regular basis.
- Other duties may be assigned.

Expectations:

- Adhere to the principles and requirements of all applicable laws and regulations relating to your position and ACCU employment, including but not limited to:
    - Information security and cybersecurity best practices as found in FFIEC guidelines, NCUA Reg 748 part a and b, and NIST.
    - Bank Secrecy Act (BSA)
    - Anti-terrorism procedures of the Office of Foreign Asset Control (OFAC)
    - Anti-Money Laundering (AML) provisions of the USA Patriot Act
    - PCI/DSS
- Pursue ongoing professional development through training, certifications, and industry events.
- Collaborate with IT, compliance, and other departments to ensure integrated security practices.
- Stay current with evolving regulations, standards, and best practices in information security.
- Demonstrate flexibility and responsiveness to security incidents outside standard business hours.

Qualifications and Educational Requirements:

- Four-year degree in business management, system analysis, or related field, or equivalent experience with a high degree of focus on information and physical security.
- Demonstrated verbal and written communication skills, with experience typically obtained following 5 years in a security position within a financial institution.
- Certified Information System Security Professional (CISSP) certification preferred.
- Additional certifications such as CISM, CRISC, or CISA preferred.
- Experience implementing security frameworks such as NIST CSF or ISO 27001.
- Familiarity with cloud security, SaaS/IaaS platforms, and modern endpoint protection solutions.

Disclaimer:

The above statements are intended to describe the general nature and level of work being performed by people assigned to this classification. They are not to be construed as an exhaustive list of responsibilities, duties, and skills required of personnel classification. All personnel may be required to perform duties outside of their normal responsibilities from time to time, as needed.

Pay Scale:

Our pay ranges are built to allow for candidates with various levels of skills and experience to be considered, as well as to allow room for growth and tenure achieved in this role over time. Typically, new-hire salary offers fall within the minimum to midpoint of a pay range for many candidates. Any offer extended to a candidate will be based upon their unique set of knowledge, skills, education, and experience, as well as internal equity.

ADA Compliance Statement:

In compliance with the Americans with Disabilities Act (ADA), ACCU stands ready to accommodate any qualified employee with a disability who can perform the essential duties of their position, as long as necessary accommodations for that employee's disability don't cause an undue burden to the credit union.

To apply, please visit: AmericasChristianCU.com/Apply