OptiFunder

VP Information Technology

About OptiFunder

OptiFunder is fast growing FinTech company and the pioneer of the Warehouse Lending Management System for mortgage bankers. We provide a portfolio of technology solutions to help lenders originate more loans, reduce origination costs, and increase operational efficiency across the mortgage lifecycle. By joining OptiFunder, you'll become part of a forward-thinking company that is transforming the way our customers embrace technology to enhance their business and the bottom line. One of the fastest growing fintech companies, we offer the excitement of a rapidly growing technology disruptor with the stability of a seasoned management team and some of the brightest minds in mortgage banking and best talent around. Visit www.OptiFunder.com to learn more. To Apply: careers@optifunder.com

Job Description

Under the general direction of CTO, the VP of Information Technology is responsible for the design, development, and implementation of the company's comprehensive information security, compliance, and privacy programs. The role will provide leadership in developing strategies that include all software products, hosted infrastructure and all internal risk and controls. The VP of Information Technology oversees day-to-day operations of the company's IT infrastructure and cybersecurity assurance and ensures information is used in accordance with its intended purpose; is protected from from external or internal threats; and assures that the company complies with statutory and regulatory requirements regarding information access, security, and privacy.

Essential Functions

- Develop, design, direct and manage the company's GCP, Info Sec, and Compliance domains
- Develop and implement an ongoing risk assessment program targeting information security and privacy matters; recommend methods for vulnerability detection and remediation and oversee vulnerability testing.
- Coordinate the development of institutional information security policies, standards, and procedures. Work with key groups in the development of such policies.
- Ensure that the companies' policies support compliance with external requirements.
- Oversee the dissemination of policies, standards and procedures to the employees and onboarding clients.
- Coordinate the development and delivery of an education and training program on information security and privacy matters for employees, other authorized users, and clients.
- Keep current and advise management with federal banking information security policies and regulations.
- Prepare and submit required reports to onboarding clients, auditors, and agencies.

- Develop and implement an incident Reporting and Response System to react and trace security breach attempts, incidents, respond to alleged policy violations, or complaints from external parties.
- Serve as the official contact point for information security, privacy, and client communication, including relationships with law enforcement entities.
- Represent company on Information-Security matters; serve as the company's point of contact for external auditors and agencies, survey requests, on security/privacy matters.
- Keep abreast of latest security and privacy legislation, regulations, advisories, alerts, and vulnerabilities pertaining to the company and its mission.
- Build and manage Information Security team
- Other duties as assigned

Skills and Experience

- Well spoken, with strong interpersonal, writing, listening, change agent, educator, and risk management consulting skills.
- Comprehensive understanding of information security administration, architecture, process, procedures, controls, and how they are implemented into policy and practices.
- Information security knowledge and skills across policies and procedures, security information systems and applications, security awareness, and compliance requirements.
- Strong deductive reasoning skills. Ability to draw conclusions from careful analysis of data. Ability to discern and communicate the impact and repercussions of policy and/or technology decisions.
- Experience implementing and maintaining security for cloud-based systems and application in GCP, network security, email security, server, and computer security.
- 2 or more years architecting, implementing, and supporting GCP infrastructure and topologies
- In-depth hands-on work experience with implementations of Google Cloud Platform (GCP) especially in areas such as: IAM, secrets manager, VPC, SSH, loan balancers, firewalls, VMs, Cloud functions, Cloud Run, Cloud SQL, Cloud Scheduler, Buckets, Big Query, Postgres
- Experience migrating and deploying GCP cloud-based solutions, particularly using containerized services with docker, yamls
- Experience with Anti-virus, anti-malware, anti-spam defense systems, with knowledge of Crowdstrike
- Experiencing hardening email systems, servers, PCs, and Macs. Setting up SSL, DKIM, DMARC, SPFs, etc.
- OWASP10 expertise, penetration testing and manual testing abilities
- Compliance expertise with knowledge of SOC2, NYDFS requirements

- Advanced working knowledge of Windows operating systems
- Demonstrated ability to interpret and communicate technical security concepts to a broad range of technical and non-technical audiences.

5+ years of relevant professional system engineering or administration experience, with significant exposure to a variety of technologies

LOCATION St. Louis, MO or remote
Job Type: Full-time

We are an equal opportunity employer. All qualified applicants will receive consideration for employment without regard to any protected class status.