First Bank of Highland Park

Website Job Posting

| | | | |
|---|---|---|---|
| **Date** | 7/26/2019 | **Requisition Number** | 2019 - 27 |
| **Position** | Senior Information Security Officer | | |
| **Department** | IT | | |
| **Reports To** | Executive Vice President/Operations & IT | | |
| **Basic Function** | To research, develop, implement, test and review the Bank's IT Security infrastructure, framework and information security program in order to ensure appropriate controls are in place to protect information, prevent unauthorized access, and prevent data leaks. Work side by side with the Bank's IT Officer and BSA/IT Security Officer to manage and control the Bank's IT environment. Also, this role is part of the core IT support team responsible for overall Bank technology assets and third-party suppliers. | | |
| **Essential Duties** | • Inform bank staff about security measures and explain potential cyber threats to bank staff<br>• Strategize, evaluate and implement new software, tools and security measures to mitigate cyber risks<br>• Monitor network for vulnerabilities and threats via consistent review of internal and third-party IT service provider (ITSP) reports and close coordination with them<br>• Problem solve potential IT security issues using available tools, third part subject matter experts, and data analysis procedures<br>• Work with bank's ITSP to continually develop/manage/monitor various cybersecurity tools (i.e. SIEM; Mobile Device Management; Vulnerability Testing; Patch Management; etc.)<br>• Play active role in oversight of internal initiatives to strengthen cybersecurity controls<br>• Actively contribute to the Bank's short and long term IT strategic plan initiatives<br>• Work closely with BSA/IT Security Officer and IT Officer to run safe and sound IT infrastructure and environment both organizationally and within the IT department<br>• Review systems to identify potential security weaknesses, recommend improvements to amend vulnerabilities, implement changes and document upgrades<br>• Measure risk and play active role in management of the incident response policy, disaster recovery/business continuity plan, and related tests and exercises<br>• Coordination with various auditors and regulators to facilitate review of IT infrastructure and controls, including subsequent involvement in remediation of deficiencies identified to strengthen the IT control environment.<br>• Responsible for completion of the FFIEC Cyber Security Assessment Tool<br>• Coordinate IT security related activities including, but not limited to: FS-ISAC annual tabletop exercise; Annual Employee Security Awareness Training; etc.<br>• Work with the Bank's IT staff to support day-to-day operations, this may include desktop support, network maintenance and monitoring, end user training, third party service provider negotiations and supervision, and cross training for peer-to-peer backup of other key Bank IT skill sets.<br>• Implement and assist with drafting Bank IT security policies and procedures, contribute to updates and enhancements of policy and procedure.<br>**ADDITIONAL DUTIES**<br>• Participate in system administration duties as primary and/or backup on relevant | | |

| | |
|---|---|
| | systems<br>• Play active role in management of key vendors and contribute to the strength and success of Vendor Management program<br>• Key contributor to Active Directory review process<br>• Participate in bank staff cyber security training, monitoring and adjudication.<br>• After business hours, nights and weekend support will be occasionally required<br><br>**ATTEND MEETINGS AND MEMBER COMMITTEES**<br>• IT Steering Committee<br>• Business Continuity Disaster Recovery Committee<br>• Quarterly Officer meetings<br><br>**NONESSENTIAL DUTIES**<br>• Other duties as assigned |
| **Knowledge, Skills & Abilities** | • Tact & diplomacy in dealing with internal employees (mostly non-technical), auditors, regulators, and external vendors<br>• Ability to work with others on the IT team to support overall bank operations<br>• Detail oriented<br>• Strong knowledge of banking<br>• Strong computer background<br>• Good problem solving skills |
| **Training & Experience** | • Bachelor's degree or equivalent experience in related field<br>• Microsoft networks and active directory proficiency<br>• Previous Fiserv experience helpful<br>• Previous experience with vulnerability management<br>• 3-5 years previous banking or financial services experience<br>• 5+ years' experience in Information Systems security preferred<br>• Prior experience working with auditors, regulators helpful |
| ***To Apply: Send email with attached resume to careers@firstbankhp.com. Please reference Job Code 2019 – 27.*** | |