Grand Bank for Savings, FSB | Member FDIC

Infrastructure Engineer

Position Summary: The Infrastructure Engineer is responsible for the day-to-day operation, maintenance, and security of the technology infrastructure that supports Grand Bank for Savings, FSB (the "Bank"). The position administers the Bank's primary and secondary data centers, the Windows Server virtual machine environment, the storage and backup platforms beneath them, and the network and firewall layer connecting them.

The Infrastructure Engineer is a hands-on, generalist engineering role within the Bank's small Information Technology department, rather than a specialized position on a larger team. The position carries primary ownership of virtualization, backup and recovery, storage, network and perimeter security, identity, and patch management; provides tier-2 and tier-3 technical escalation; supports business continuity and disaster recovery; and produces the documentation and evidence required in an environment regulated by the Office of the Comptroller of the Currency (OCC) and examined under the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook, where every change is documented, approved, and evidenced.

The successful candidate must be prepared to serve as the Bank's primary technical resource for rebuilding hypervisor hosts, tracing firewall rules, and restoring domain controllers, and must exercise sound judgment about operational risk. The position has no direct reports and is classified as exempt. The Infrastructure Engineer reports to the Bank's Chief Information Officer / Information Security Officer (CIO/ISO).

Essential Duties and Responsibilities: The essential functions include, but are not limited to, the following:

Virtualization and Compute

- Administer the Bank's VMware vSphere environment across both data centers, including host patching, cluster health, virtual machine provisioning, resource balancing, and capacity planning.
- Maintain vCenter Server, ESXi host builds, and VMware Tools currency across the virtual server environment.
- Maintain build standards and hardening baselines for current Windows Server releases and manage the server lifecycle from provisioning through decommission.

Backup, Replication, and Recovery

- Administer Veeam Backup & Replication, including job design, scale-out backup repository health, cloud capacity tier offload, and replication between the primary and secondary data centers.
- Perform and document automated restore verification and produce restore evidence for internal audit and regulatory examiners.
- Maintain and test the technical recovery procedures supporting the Bank's business continuity and disaster recovery plans.

Storage

- Administer the shared storage area network (SAN) at both data centers, including LUN and volume provisioning, multipathing, firmware currency, capacity forecasting, and performance troubleshooting.
- Coordinate storage vendor support cases and hardware replacements.

Network and Perimeter Security

- Administer enterprise next-generation firewalls, including security and NAT policy, security profiles, OS upgrades, remote-access virtual private network (VPN), and log forwarding to the security information and event management (SIEM) platform.
- Administer cloud-managed enterprise switching and wireless, including VLAN and port configuration, SSID and wireless policy, firmware management, and dashboard alerting.
- Maintain accurate network documentation, including VLAN assignments, zone definitions, and segmentation diagrams, to the standard expected by auditors and examiners.

Identity, Endpoints, and Patching

- Administer on-premises Active Directory in a hybrid configuration with Microsoft Entra ID, including Group Policy, Intune policy, Conditional Access support, and directory synchronization.
- Operate the endpoint and server patch management program on an enterprise patch management platform, including deployment rings, compliance reporting, failure triage, and exception documentation.
- Support vulnerability remediation driven by scanner findings and act on SIEM alerts in coordination with the CIO/ISO.

Governance, Support, and General Responsibilities

- Submit changes through the Bank's change management process with tested rollback plans and maintain runbooks, standards, and procedure documents.
- Provide tier-2 and tier-3 escalation for the Help Desk Associate and serve as backup coverage for tier-1 support.
- Open, manage, and close support cases with the core banking provider, Microsoft, Veeam, and hardware, network, and security vendors.
- Participate in scheduled after-hours and weekend maintenance windows and respond to critical infrastructure incidents outside business hours.
- Support internal audits, external penetration tests, and OCC examination requests with evidence and written responses.
- Comply with all departmental policies and procedures and all laws, rules, and regulations applicable to the position.
- Support special projects, technology initiatives, and enterprise projects as assigned.

Minimum Qualifications (Knowledge, Skills, and Abilities):

- Bachelor's degree in an information technology field from an accredited college or university, or equivalent practical experience.
- At least 5 years of experience administering Windows Server infrastructure in a production environment, including at least 3 years with primary ownership of virtualization, backup, and network administration.
- Demonstrated experience as a generalist infrastructure engineer in a small IT organization, or equivalent evidence of independent end-to-end ownership.
- Production administration experience with VMware vSphere, including vCenter Server, ESXi, clustering, vMotion, and host maintenance.
- Working knowledge of current versions of Veeam Backup & Replication, including job configuration, repositories, replication, and restore execution.
- Experience with shared SAN administration (iSCSI or Fibre Channel), LUN provisioning, and multipath troubleshooting.
- Working knowledge of enterprise next-generation firewall administration, including security and NAT policy, security profiles, and version upgrades.
- Experience with cloud-managed switching and wireless administration, VLAN and trunk configuration, and wireless SSID policy.

- Working knowledge of Active Directory Domain Services, DNS, DHCP, and Group Policy, as well as Microsoft Entra ID and Microsoft 365.
- Experience with patch deployment and compliance reporting using an enterprise patch management platform.
- Working knowledge of TCP/IP, routing, VLANs, network segmentation concepts, and structured packet-level troubleshooting.
- Working knowledge of Microsoft Intune and modern endpoint management.
- Ability to write clear technical documentation, including procedures, runbooks, diagrams, and change records, suitable for review by auditors and examiners, and to maintain complete and accurate records as a core part of the role.
- Sound judgment about operational risk and change impact, including an understanding that an error affecting core banking or domain controller systems may trigger incident escalation and regulatory notification obligations, and willingness to escalate rather than improvise on critical systems.
- Demonstrated ownership, with the ability to take a problem from first report through root cause to documented resolution with limited supervision.
- Ability to move effectively between storage, network, security, and endpoint issues and to manage multiple priorities in the same day.
- Strong written and verbal communication skills, including the ability to explain technical risk in plain terms to management, the IT & IS Steering Committee, and non-technical staff.
- Ability to pass a background check and satisfy bonding requirements applicable to financial institution employment.
- Reliable availability for scheduled after-hours maintenance and unscheduled incident response.

Preferred Qualifications:

- Prior experience in a bank, credit union, or other regulated financial institution, and familiarity with FFIEC IT examination expectations.
- PowerShell scripting experience for administration, reporting, and automation.
- Experience with SIEM and vulnerability management platforms.
- Experience with privileged access management tooling and just-in-time administrative access models.
- Technical certification such as VMware VCP-DCV, Microsoft Certified: Windows Server Hybrid Administrator Associate, a vendor firewall certification, Veeam VMCE, CompTIA Security+, or a GIAC equivalent.

Physical Demands and Work Environment: The following physical demands apply to this position.

While performing the duties of this position, the employee is regularly required to speak or hear. The employee is frequently required to use hands or fingers and to handle or feel objects, tools, or controls. The employee is frequently required to sit and occasionally required to stand, walk, and reach with hands and arms. The employee must occasionally lift and/or move up to 50 pounds, including lifting and racking equipment, and must be able to work in a data center environment. Specific vision abilities required by this position include close vision, distance vision, and the ability to adjust focus. The noise level in the work environment is usually low to moderate. This is an on-site position based in Hattiesburg, Mississippi, and is not structured for remote or hybrid work. The position works standard business hours plus scheduled evening and weekend maintenance windows; there is no scheduled on-call rotation, but the employee is expected to respond to critical after-hours incidents. Travel to the Bank's secondary data center is minimal, averaging approximately twice per year.

Note: This job description does not state or imply that these are the only duties to be performed. Employees must follow other job-related instructions and perform other duties requested by authorized persons. Duties and requirements may be modified to provide reasonable accommodation. This document does not create an employment contract, implied or otherwise, other than an at-will relationship.

Grand Bank offers a competitive salary along with the following benefits:

- 401(k) and Profit Sharing
- Health Insurance
- Dental Coverage Plan
- Vision Coverage Plan
- Disability Insurance
- Life Insurance
- Paid Time Off (PTO)
- Community Service PTO Match (Bank approved)
- Tuition Reimbursement

Job Type: Full-time

Location: Wilmington, DE or Hattiesburg, MS (on-site)

Pay: Based on education and experience

About Grand Bank for Savings, FSB: Grand Bank is growing rapidly and is on the fast track to becoming a leader in providing affordable, innovative financial products to customers throughout the United States. Our mission is to enhance the financial well-being of more than one million members of underserved and historically underrepresented communities nationwide by 2030. We are dedicated to breaking cycles of harmful debt, fostering savings growth, promoting homeownership, and empowering individuals and families to build generational wealth.

Chartered in 1968, Grand Bank has a rich history of thinking outside the box to offer unique products that meet the needs of our customers. We value our team members and all they bring to the table. If you are enthusiastic about delivering customer-focused solutions with a digital edge to help others build solid financial health, you will find a career full of excitement, challenge, purpose, and opportunity at Grand Bank. Grand Bank is an affirmative action and equal opportunity employer, as well as an Equal Housing Lender and Member FDIC.

We offer competitive salaries, advancement opportunities, and a comprehensive benefits package. Join our team today!

Equal Housing Lender / Member FDIC