

## **IT Manager – Job Description**

### **Description:**

The IT Manager is responsible for overseeing the daily operations, availability, and performance of the firm's technology infrastructure. Reporting to the Director of Information Technology, the IT Manager provides leadership and technical expertise across all areas of systems administration, network operations, end-user support, and IT service delivery. This role ensures that all IT systems are designed, implemented, and maintained with a focus on efficiency, reliability, scalability, and strong security practices. The IT Manager collaborates closely with business units and IT teams to support strategic initiatives, manage IT projects, supervise technical staff, and maintain a resilient, high-performing technology environment.

The IT Manager is accountable for vendor management, IT budgeting, maintaining documentation, and driving continuous improvements that enhance operational effectiveness and business productivity.

### **Key Responsibilities:**

- Oversee day-to-day IT operations, including infrastructure management, systems administration, networking, and help desk performance.
- Manage, mentor, and evaluate IT team members to ensure high-quality service delivery and professional development.
- Ensure availability, performance, and security of critical business systems, including servers, network devices, cloud services, and enterprise applications.
- Lead IT projects from planning to execution, including system upgrades, cloud migrations, hardware refresh cycles, and new technology deployments.
- Maintain and enforce IT policies, procedures, asset inventories, and standard operating documentation.
- Coordinate with vendors on procurement, licensing, maintenance contracts, and technical support escalations.
- Monitor and analyze system performance metrics to identify issues, forecast capacity needs, and recommend improvements.
- Oversee identity and access management processes, including Active Directory, Azure AD, and user lifecycle workflows.
- Collaborate with cybersecurity teams to ensure systems comply with security best practices, patch management schedules, and regulatory requirements.
- Manage backup, disaster recovery, and business continuity initiatives to minimize downtime and data loss.
- Support new employee onboarding, device imaging, and enterprise application provisioning across the firm.
- Communicate IT updates, project status, outages, and technology changes to technical and non-technical audiences.
- Ensure compliance with organizational standards and technology governance frameworks.

### **Demonstrable Requirements:**

- A four-year college degree in Information Technology, Computer Science, Information Systems, or equivalent professional experience.
- Five to seven years of experience in IT operations, systems administration, or infrastructure management, including at least two years in a leadership or supervisory role.
- Strong technical knowledge of enterprise-class technologies such as Windows Server, Active Directory, virtualization platforms (VMware/Hyper-V), networking (firewalls, routers, switches), and cloud services such as Microsoft 365 and Azure.
- Experience managing help desk operations, ticketing systems, and service level delivery.
- Proficiency with PowerShell and automation tools used for system administration and workflow optimization.
- Demonstrated expertise in system monitoring, patch management, backup administration, and disaster recovery planning.
- Working knowledge of security principles, endpoint protection, identity management, and compliance frameworks.
- Strong communication skills with the ability to convey technical concepts to non-technical stakeholders.
- Proven ability to manage multiple projects simultaneously and work autonomously in a fast-paced environment.
- Experience managing IT vendors and negotiating contracts, software licenses, and service agreements.

#### Desired Qualifications:

- One or more relevant industry certifications: ITIL, Microsoft Certified: Azure Administrator, CompTIA Network+, Security+, Cisco CCNA, or similar.
- Experience with hybrid cloud environments, mobile device management (MDM), Intune, and modern endpoint management strategies.
- Familiarity with database administration (SQL Server), application hosting, or web server management.
- Experience implementing enterprise IT governance, risk, and compliance initiatives.
- Background supporting mid-to-large organizations with distributed environments and diverse user groups.