

WILLIAM B. FLYNN
1887 Bond Rd. SE
Darien, Georgia 31305
Cellular: (912) 432-0888
wbflynn@gmail.com

Experienced Director of Information Technology with a demonstrated history of working in the computer and network security industry. Skilled in Storage Area Network (SAN), Data Center, Cisco Meraki, Information Security, and Human Resources. Strong information technology professional with a Master of Business Administration degree with a focus on Information Technology Management.

EDUCATION

MBA, Information Technology Management

Western Governors University, Salt Lake City, Utah
Graduation Date: February 2014

BACHELOR OF SCIENCE, Information Technology Management

Western Governors University, Salt Lake City, Utah
Graduation Date: April 2012

PROFESSIONAL DEVELOPMENT

- Six Sigma Green Belt
- District Leadership I and II Supervisory Classes
- State Performance Management Program Course
- FEMA IS-00100 Introduction to the Incident Command System, (ICS 100)
- FEMA IS-00700 National Incident Management System (NIMS) an Introduction
- FEMA IS-800.A National Response Plan (NRP), An Introduction

EMPLOYMENT HISTORY

INFORMATION TECHNOLOGY DIRECTOR

Mar 2018 – Present

Southeastern Pathology Associates
Brunswick, GA

Southeastern Pathology Associates provides anatomical pathology services to patients and physicians. These pathological services are dependent upon a complex and multi-faceted enterprise network that must be reliable and responsive. The critical nature of the services provided by Southeastern Pathology Associates demands an Information Technology infrastructure that exceeds service expectations and requires reliable and expedient delivery of services.

- Negotiated services and contracts to maximize savings while delivering effective and efficient delivery of services. Never sacrificing the quality expected of Southeastern Pathology Associates. Renegotiated communications contracts and secured 25% annual savings. Secured multi-year support and maintenance contracts for over 20% savings.
- Project manager for an infrastructure revitalization that included industry leading servers, storage devices, switches and firewalls. Manage local staff and multiple contractors delivering varying services. Ensure goals and expectations are met by guiding contractors through complex project milestones and deadlines to ensure project remained on schedule and successful.

- Improved organizational security posture by replacing antiquated hardware, software, and operating systems. Improved security scores from failing to overall “A”.
- Implement and manage disaster recovery strategies. Utilized Dell’s Data Domain to create local backups and remote data recovery capabilities. Converted data center from a multi-server fragmented environment to streamlined and efficient Dell VxRail that increased reliability and stability. System performance evolved into an asset instead of liability. Company profitability increased dramatically.
- Manage, mentor, coach, and teach a newly constructed Information Technology staff. Maintain daily support responsibilities while staff develops skills and experience necessary to support the complex infrastructure of Southeastern Pathology Associates.
- Maintain positive working relationships with local and remote staffs that include physicians and other medical professionals.
- Create positive and effective working relationships with outside Information Technology departments to improve organizational dependencies such as virtual private networks and interfaces into electronic medical records and laboratory information systems.
- Manage building physical security. Upgraded security devices and cameras to improve building and personnel security. Resolved internal and external lighting issues the presented safety issues for employees.
- Manage a complex Citrix delivery platform for remote and internal employees and partners. Citrix farm includes a multi-tiered NetScaler and application server environment designed for high availability.
- Simplified a multi-host VMWare environment with varying version levels. Transformed over provisioned hardware into multi-node Dell VxRail system that is clustered for high availability and redundancy.

INFORMATION TECHNOLOGY MANAGER

Mar 2004 – Mar 2018

State of Georgia – Department of Public Health – Coastal Health District
Brunswick, GA

The Coastal Health District is an eight county, multi-site public health district interconnected with local, intrastate, and interstate networks. Responsible for the daily technical operations and functions of the Coastal Health District. Develop plans and strategies to leverage modern technologies to provide optimum service to direct and indirect customers. Develop the strategies to protect sensitive data from compromise and disasters. Ensure HIPPA and other data safeguards are implemented and enforced. Supervise the Information Technology staff. Maintain positive working relationships with county administrators, site supervisors, and program managers. Liaison with state and other District personnel to maintain focus on established and projected organizational directions. Develop plans and strategies to adjust to budget and personnel fluctuations.

- Project manager for implementation and upgrades of enterprise level applications and systems. Coordinate and manage vendors, hosting facilities, users, and staff members. Deploy client-side applications and configurations throughout the organization. Manage expectations and constraints. Flexible and adaptable to meet demands of compressed timelines.
- Project manager for Information Technology services for new construction and remodeling of offices and clinics. Negotiate contracts for broadband, telephone systems, security systems, and

all required equipment to meet organizational missions. Adapt to unpredictable challenges to timelines.

- Develop business continuity plans and disaster recovery. Migrated critical servers to cloud hosting facilities to ensure continuity during regional disasters and events. Disaster recovery includes redundant failover facilities as a safeguard against hosting facility events. Developed redundant remote connectivity procedures to account for situational restrictions.
- Develop strategies to leverage modern technologies while maintaining focus on responsibilities to budget.
- Member of Good to Great development team.
- Member of District Leadership Team.
- Member of District Health Emergency Assistance and Response Team (DHEART).
- Chair state Public Health IT Director's meetings.
- Member of the District Public Health Accreditation Board (PHAB).
- Maintain high levels of customer service through managing expectations of customers and staff.
- Create an environment of success and accomplishment through coaching and mentoring staff.
- Coordinate the deployment of the mobile disaster operations center. Ensure emergency response teams have all technological capabilities to perform mission. Service includes internet connectivity via local, cellular, and satellite providers. Deployment includes mobile servers and network equipment for continuity of services.
- Researched, installed, and administer LanSweeper network management and helpdesk system. Utilize SQL scripting to generate productivity and utilization reports.
- Researched, installed, and deployed BitDefender GravityZone Security Suite for antivirus, spyware, and malware protection.
- Researched, installed, and deployed LogMeIn Rescue and Rescue Lens for remote user support.
- Researched, installed, and deployed LastPass as enterprise password management.
- Manage the deployment of active directory infrastructure. Create and deploy group policies and application installations.
- Plan and manage upgrades of Cisco Integrated Services Routers, Cisco Meraki security devices and access points, Aruba access points, Barracuda web filters, and SonicWall security devices.
- Utilize features of Cisco Meraki security devices for intrusion prevention, intrusion detection, advance malware protection, content filtering, internet access control, and activity reporting.
- Provide support for Emergency Preparedness HAM Radio program.

- Support server operations systems Microsoft Windows Server 2016, 2012, 2008, 2003, Linux, and Unix.
- Install and manage Microsoft Hyper-V and VMware virtualized servers.
- Configure and maintain Cisco Physical Access Manager (CPAM) and Identiv Connected Physical Access Manager (ICPAM).
- Configure and maintain Cisco Unified Communications Manager.
- Configure and maintain Cisco Video Surveillance Manager.
- Support Dynamic Multipoint Virtual Private Network (DMVPN).