Montgomery County Government
Enterprise Architecture
Technical Architecture

Department of Technology Services
Montgomery County Government, MD

VERSION	DATE	DESCRIPTION	AUTHOR
1.0	16 March, 2011	Initial version	Mike Tarquinio, Montgomery County Government
1.1	2 January 2013	Fix links	Mike Tarquinio Montgomery County Government
1.2	29 May 2013	Add new domains, update content	Mike Tarquinio Montgomery County Government
1.3	22 March, 2016	General Updates	Mike Tarquinio Montgomery County Government
1.4	27 January, 2017	Add new domains and delete mainframe, ivr and engage	Mike Tarquinio Montgomery County Government

Table of Contents

1.0 Introduction

Montgomery County takes advantage of mature technologies in areas of data, voice and radio networking, datacenter operations and monitoring, hardware and software systems deployment, and application development. This document, prepared by the Department of Technology Services (DTS), is part of Montgomery County's Enterprise Architecture. Specifically, this document covers the Technical Architecture.

The Technical Architecture Document reflects key information around the County's Enterprise Technical Domains. It is prepared in concert with the rest of the Enterprise Architecture and the DTS Strategic Plan and is designed to support the initiatives outlined in the plan.

The County has three essential organizational resources, people, process and technology. People are the County's greatest resource, Process binds them together into a coherent workforce, and Technology is the tool.

1.1 Purpose

The purpose of this document is to document key information about the County's Enterprise Technical Domains. Specifically, it identifies the Technical building blocks that are supported in the Enterprise.

1.2 Document Format

The Montgomery County Enterprise Architecture consists of five separate sub-architectures: Business, Technical, Data, Application, and Performance. Each one of the sub-architectures is a standalone document but all five are subcomponents of the entire Enterprise Architecture.

This document addresses the Technical Architecture. It covers the supported Technical Building Blocks or domains at the Enterprise level. Each domain introduces the following topics:

Principles – explaining the purpose of the component, along with some implementation details.

Owners – identifies both the technical and business owners for the component.

Components – expanding on the operational aspects of the component by identifying preferred implementation products and staff skill-sets.

Standards and Guidelines – identifying standards and guidelines which the County follows so that it can provide quality services.

Disaster Recovery – for critical domains this section documents the domain's disaster recovery strategy.

The County has assembled information detailing its technologies and its direction. To avoid releasing potentially sensitive information the County follows a strict release process that involves review at multiple levels (See Section 10-617(g) of the Maryland Public Information Act).

The owner of all five sub-architecture documents and the rollup document is Mike Tarquinio (michael.tarquinio@montgomerycountymd.gov) the Department of Technology Service Enterprise Architect. The Department is located at the Department of Technology Services, 101 Monroe Street, 13th Floor, Rockville, Maryland 20850.

1.3 Technical Architecture Document Change Management

The Montgomery County Government Enterprise Architecture Technical Architecture document is part of the County's documented Enterprise Architecture and is published by the DTS Enterprise Architect. The Enterprise Architect is responsible for working with DTS Content Experts and department representatives (through TOMG) to document the Technical Architecture. The document adheres to stringent change management controls and follows a defined change management process.

Change requests can be initiated via DTS content experts, TOMG members, or the DTS Enterprise Architect. Contact the DTS Enterprise Architect Mike Tarquinio (michael.tarquinio@montgomerycountymd.gov) for further details.

1.4 References

1. Montgomery County Office of Management and Budget – Administrative Procedure 6-1, September 2, 2010; *Use of the County-Provided Internet, Intranet, and Electronic Mail Services*;

2. Montgomery County Office of Management and Budget – Administrative Procedure 6-6, October 20, 2003; *Information Technology Policies and Procedures*;

3. Montgomery County Office of Management and Budget – Administrative Procedure 6-7, May 4, 2005; *Information Resources Security*;

4. Montgomery County Department of Technology Services, September 2004; *Computer Security Guideline*;

5. Montgomery County Department of Technology Services, June 2016; *Enterprise Technology Strategic Plan 2016 – 2019;*

6. Montgomery County Department of Technology Services, July 19, 2007; *Enterprise Architecture Configuration Management Plan*

7. Montgomery County Government; *About County Government*; http://www.montgomerycountymd.gov/resident/about.html; page accessed 1/30/2017

8. Montgomery County Government; *The Charter and County Code*; http://www.montgomerycountymd.gov/mcg/countycode.html; page accessed 1/30/2017

9. Montgomery County Government; *Montgomery County Organization Chart*; http://www.montgomerycountymd.gov/government/orgchart.html; page accessed 1/30/2017

10. Peter Mell and Tim Grance; *The NIST Definition of Cloud Computing*; September 2011; http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf;

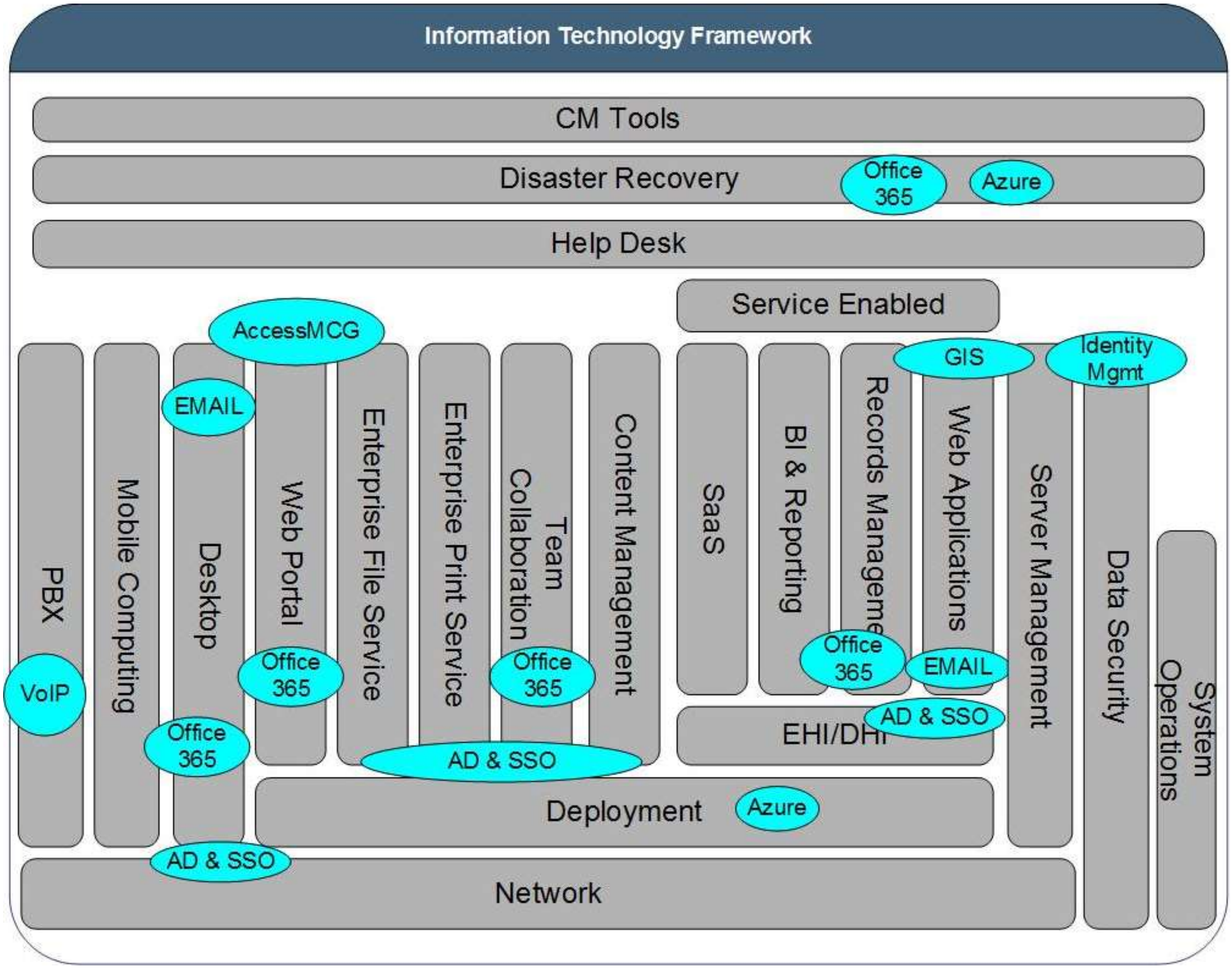
11. Montgomery County Department of Technology Services, January 2, 2013; *Montgomery County Government Enterprise Architecture Business Architecture*;

12. Montgomery County Department of Technology Services, January 2, 2013; *Montgomery County Government Enterprise Architecture*;

13. Montgomery County Department of Technology Services, January 2, 2013; *Montgomery County Government Enterprise Architecture Performance Architecture*;

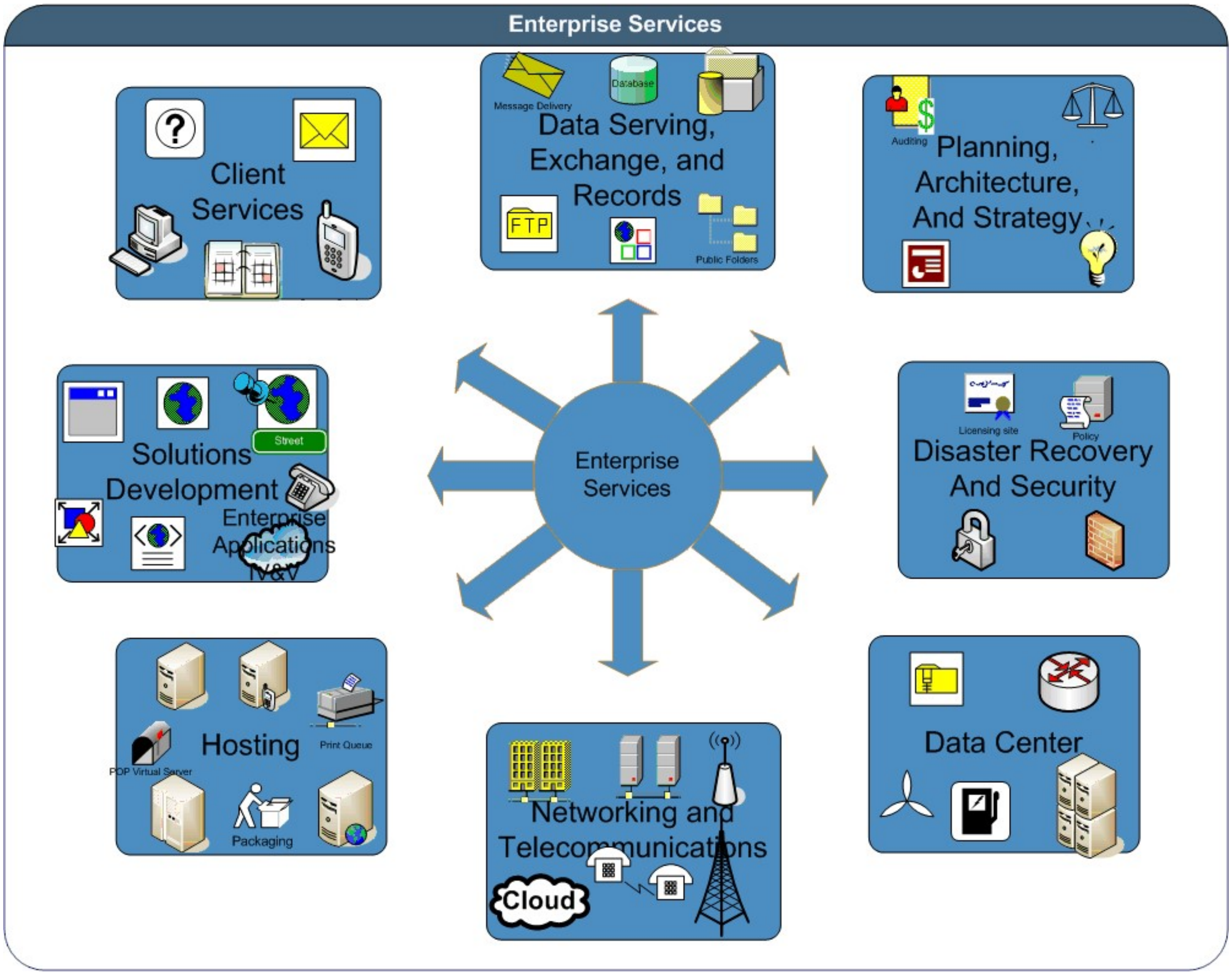
2.0 Technical Architecture Overview

The Enterprise Architecture presents well-defined, strategic standards adopted for the development and delivery of the County's information systems. It provides a cohesive blueprint to optimally design, purchase, develop, deploy and manage information systems for the County. The components of the overall infrastructure are shown in the next figure:



The Framework may be defined as a collection of interrelated component architectures or domains. The public oriented domains are offered as shared Enterprise Services to Departments, Groups, and Agencies and form a Service Catalog.

2.1 Enterprise Shared Service Catalog



Client Services

- Desktop
- Email
- Help Desk
- Team Collaboration (SharePoint)
- Mobile Computing
- Mobile Applications
- Office 365
- Office 365 Video

Disaster Recovery and Security

- Active Directory (AD)

- Security Domain
- Identity Management
- AccessMCG
- Disaster Recovery

Hosting

- Deployment
- Enterprise Hosted Infrastructure (EHI)
- Enterprise Print Service
- Software as a Service (SaaS)
- Configuration Management Tools (CM)
- Azure

Data Serving, Exchange and Records

- Enterprise File Service
- Database Hosting Infrastructure (DHI)
- dataMontgomery
- Enterprise Service Bus (ESB)
- Record and Image Management

Networking and Telecommunications

- Network
- PBX
- Cabling Requirements and Standards

Data Center

- System Operations (Enterprise Backup/Data Center Server and Appliance Hosting)

Solutions Development

- Geographic Information System (GIS)

3.0 Architecture Domains

3.1 Active Directory (AD)

Principles

The County maintains a centralized Enterprise Directory service running on Microsoft's Active Directory (AD). The Enterprise Directory Service is used to authenticate users, and to allow them into the County network. The Enterprise Directory Service contains all users within the County that have need to access IT assets. In addition to users all computers and printers that are not on a specialized domain are included and managed within the service.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

Active Directory is built around a number of Active Directory servers strategically located throughout the County government (see figure 3-1). If a failure should occur, having multiple servers increases the potential for employees to authenticate into the network. The system design allows for all servers to replicate on change, with the exception of one. The one non-synchronized server is an emergency backup copy used for recovery, and it replicates once every 24 hours.

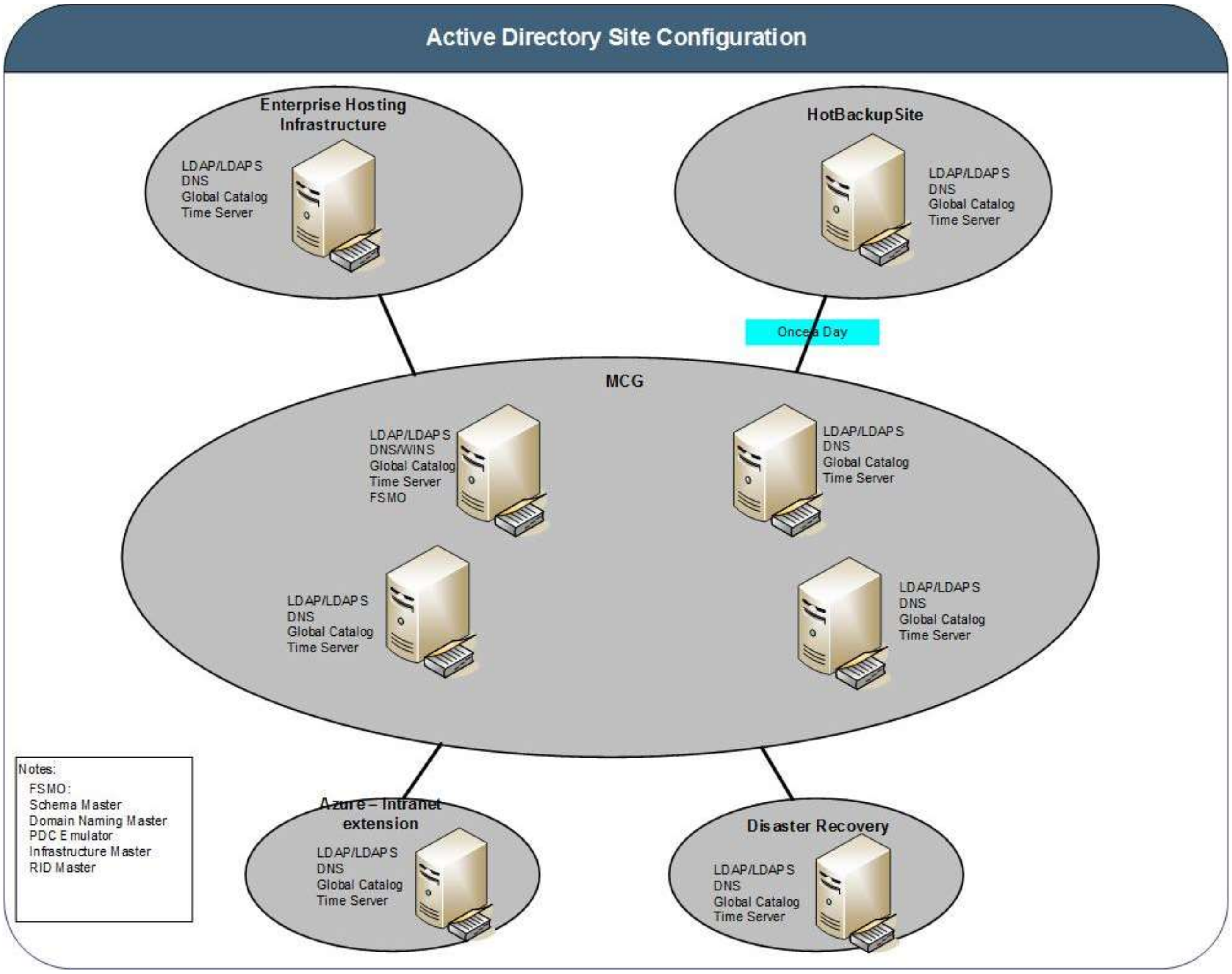


Figure 3-1 AD Site Configuration

The Department of Technology Services (DTS) manages the Enterprise Directory structure and group policies. DTS is the sole Administrator at the Enterprise level and delegates the management of select OU admin functions to department administrators. Each department's resources are defined and contained inside their own OU. Department OU Administrators have the responsibility to add, delete, and modify accounts within their OU, and to set permissions for their departmental applications.

Departmental Applications that are hosted within the DTS Enterprise Hosting Infrastructure (see Enterprise Hosting Infrastructure Domain) have permissions setup for each by DTS Administrators. DTS creates one or more Application OUs for each application and gives owning department administrators the ability to assign users to the Application OUs. When authenticating into one of these applications, the EHI frontend acts as a clearinghouse front end to AD, checking AD permissions as the user logs on.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Active Directory Domain Administration
Windows Server Administration
Understanding of Security Principles
Ability to use Magic Help Desk System
DNS, WINS and DHCP Administration

Standards and Guidelines

Special Root or Organizational Units (OU) Folders have been created to provide for additional functions in our environment, and for application SSO management. These are as follows.

Department OU Folders – Each County department is designated a specific OU folder to administer their department Users, Computers, Resources, and Groups. The names assigned are based on the standard acronyms used for each department. If the department does not have an OU Administrator, DTS assumes the responsibility.

Department Servers Folders – Each County department is designated a specific OU folder to administer their departmental servers.

Applications - OU is used for SSO. Each County SSO application is assigned a sub-folder under this OU. Groups are created and assigned rights for these applications.

Associates – OU is used for SSO and Associates. These are Non-Mail Enable Accounts (NME). The OU is made up of two sub-OUs; former County employees, and non-County or former employees who need access to SSO applications. This is for groups like the Howard County police who need access to the Auto Theft Application, employees in sister agencies, boards and committees requiring access to Financial Disclosure, or former employees needing access to benefits or deferred comp.

Computers – This is a default OU created by AD. Computers that are not pre-staged are added to the domain here. Domain admin authority is required to move these computers into their appropriate department OU.

External Contacts – This OU houses external contact information (name and external email address) in a centralized location. This allows the departments to create standard email distribution lists that include external email contacts. This process is primarily in place to overcome the limitations of Outlook for distribution lists. It is managed by the Core System's group in DTS.

Inactive – This folder has three sub-OUs; Retired, Terminated and Survivor. This folder contains former employee accounts that have been deactivated and their mailbox removed. These former employee accounts are being saved because in the near future they will need to have access to various SSO applications such as retirement and insurance benefits.

Training – OU for Admin, Power User, Svr Training. Server Admin holds user accounts which are disabled. These are accounts that probably will not be used again, but we don't want to have to recreate them. Two other OU folders contain accounts used for OU admin, Outlook, and other types of training. `

Test – This folder is kept at the root, for easier access to other departments. Usually used only by Domain Admins, it is used to test policies, or to replicate issues the users may have with external contacts, etc.

Training

All Department OU Administrators must attend the DTS OU Administrators training class prior to performance of Administration functions.

Standards

PC Policies for Improved Security & Manageability

- This policy uses AD to lockdown PCs and maintain standard configurations
- AD Policies automatically enforced through Identity Management.

The Enterprise Directory is a non-federated service

3.2 Cabling Requirements & Standards

Principles

The County's goal is to standardize its cabling infrastructure to promote faster speed, better communication, easier troubleshooting, and less need for repair. Cable installation services are offered by the County and by outside Contractors.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Network Services Team.

Components

The County's telecommunications and IT systems are interconnected by various cables. The County's cabling infrastructure contains a wide variety of cables including both electrical and optical.

Standards and Guidelines

The County Cabling standards and guidelines are for vendors and County departments which install and support the County's cabling infrastructure. As universal standards evolve, the current standards and guidelines will be updated in this document. The County maintains a standards document located at the following location on the County Internet portal -

http://www.montgomerycountymd.gov/dts/architecture/cablingDomain.html

3.3 Data Security Domain

Principles

Security is an essential part of every component in the County's IT Architecture framework with multiple domains and groups having responsibilities. The Security Domain includes not only technology but process and procedures and is present through all aspects of system acquisition and development.

The following domains have Security responsibilities:

- Active Directory – Centralized Enterprise Directory Service
- AccessMCG – Extranet and Intranet Single Sign On Services
- Identity Management – Enterprise Identity Management
- Deployment Domain – Common Enterprise Server configurations and patch management services
- Desktop Domain – Centralized desktop management with common configurations, patch management services, lockdown policy, centralized anti-virus and anti-spyware services
- Email System Services – Centralized mail service including anti-virus, anti-spyware and spam removal services
- Enterprise Hosting Infrastructure – Secure hosting infrastructure
- Help Desk Services – Centralized help desk that supports Incident Response
- Network Domain – Enterprise network that includes protected single point of access, internal and external firewalls, wireless security, and network segmentation services
- Service Enabled Domain – Use of an Enterprise Service Bus for centralized secure information transfers
- System Operations Domain – Centralized Data Center that includes redundant systems for high availability and physical security measures
- Configuration Management – Centralized Configuration Management systems for protection of project assets.
- Enterprise Server Management – 24x7 server monitoring
- Security Domain – Includes policies and procedures, risk management practices, Virtual Private Network access, and operational security monitoring including security scanning, policy enforcement, and log correlation.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS EISO Security Team
- DTS Core Systems Team
- DTS Server Team
- DTS Client Computers (DCM) Team
- DTS Network Services Team

- DTS Data Center Operations Team
- DTS Help Desk Services

Components

In addition to the Security components in use within each of the various domains mentioned in the Principles Section the following additional Security components are in use:

- Log Correlation
- Intrusion Detection
- Web Filtering
- Port and Vulnerability Scanning
- VPN
- Anti-Virus and Anti-Spyware protection
- Laptop Encryption
- Computer Security Investigations

Log Correlation

The DTS EISO Security Team maintains a centralized log correlation system that monitors critical IT Components within the County.

Intrusion Detection

The DTS EISO Security Team maintains an intrusion detection system that monitors critical parts of the County Network.

Web Filtering

The DTS EISO Security Team manages a Web Filtering system that manages employees' use of the Internet. It has the ability to block, permit, limit by time-based quota, or postpone access to individual categories by user, group, workstation, or network.

Port and Vulnerability Scanning

The DTS EISO Security Team uses various port and vulnerability scanning tools to scan the network internally and externally.

VPN

The DTS Core Team maintains a VPN solution that authenticates users, encrypts data, and provides flexible access controls for client-to-application security. With the current solution, the County can securely share critical information and applications with employees and business partners via the Internet. The VPN provides centralized access into the County network for employees and validated contractors. No other method is allowed.

Anti-Virus and Anti-Spyware Protection

The County uses centralized Anti-Virus and Anti-Spyware Protection software to provide scalable, cross-platform virus protection for workstations and network servers. County workstations and servers are currently checking for updated virus signatures every 60 minutes. This “normal conditions” deployment was architected to minimize the response time and increase the effectiveness of signature updates to all County hosts. In emergency situations signatures will be pushed out immediately to limit the County’s exposure to virus, worm, and Trojan activity.

Laptop Encryption

Because of various regulatory compliance initiatives and the due diligence obligation to the citizens of Montgomery County, the DTS Client Computers (DCM) team supports a hard disk encryption solution for mobile users. The purpose of the solution is to make all data on the hard drive unreadable should a laptop become lost or stolen. All primary County laptops must be encrypted.

Computer Security Investigations

The DTS EISO Security Team provides Computer Security Investigation services.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Network Administration – Routers, Firewall, VPN, Protocols
Network, Server and Desktop Administration. Installation and Troubleshooting.
WAN Hardware Management
IDS Administration, Penetration Testing, Vulnerability Assessment and Remediation. Forensic analysis exploitive techniques: exploit coding, virus reverse engineering and analysis, packet crafting, various injection techniques

Standards and Guidelines

Governance

- Office of Management and Budget – Administrative Procedure 6-1 *Use of County-Provided Internet, Intranet, and Electronic Mail Services*

- Office of Management and Budget – Administrative Procedure 6-6 *Information Technology Policies and Procedures*

- Office of Management and Budget – Administrative Procedure 6-7 *Information Resources Security*

- Office of Management and Budget – Administrative Procedure 8-2 *HIPAA Compliance* *and Responsibilities*

Policies

- Help Desk (see Help Desk Services Domain) provides central point of contact for incident response
- PC Policies for Improved Security & Manageability (see Active Directory and Desktop Domain sections)
- Montgomery County Government Department of Technology Services – EID Incident Response Plan; DTS EISO Security Team
- DTS EISO Security Team Risk Assessment Policy

Education

- County Security Awareness training

Incident Response

- Perceived or actual security incidents must be reported immediately to one of the following:
    - CIRT Lead/Security Official
    - DTS EISO Security Team
    - IT Help Desk at 240-777-2828
    - Department Head
    - Department IT Staff

3.4 Deployment Domain

Principles

The Deployment Domain is an Enterprise VM Guest Hosting Service that meets 4 of the 5 essential characteristics of the NIST definition of Cloud Computing [12]. The 4 supported tenants are: Broad Network Access, Resource Pooling, Rapid Elasticity, and Measured Service. The one characteristic that is not supported is On-demand Self-Service which the DTS Server Team intentionally reserves internally. The Deployment Domain is providing private cloud services to County departments and agencies.

The Domain consists of standardized server hardware, operating systems, middleware, and personnel. The DTS Server Team provides standardized VM Guest instances to requesting departments or groups. The requesting departments or groups can use the VM Guests to run their own applications. The DTS Server Team manages the VM Guests and runs them on a farm of VM Hosting machines that they solely control and administer. The resources may be in the County Data Center or in the County's Azure Cloud Service. The use of the standardized building blocks allows a standard set of services to be provided. Such services include standardized backup, monitoring, problem avoidance, dynamic configuration, and patch management.

The Deployment Domain makes use of the following Enterprise Architecture services:

- Enterprise Server Management (providing 24x7 monitoring)
- System Operations Domain (providing data center hosting services - power, air conditioning, 24x7 facilities monitoring, etc)
- System Operations Domain (weekly tape backup services)
- Microsoft Azure

The goals of the Deployment Domain are to:

- Provide robust and stable IT environments.
- Maintain a continual pool of spare server capacity, which can be used for new deployments, horizontal scaling and sparing.
- Provision new server and middleware environments in near real time.
- Research and adopt new tools and building blocks to lower Total Cost of Ownership (TCO).

Deployment Zones

When a VM Guest is configured it can be inserted into one of 3 standardized deployment zones. Each zone is tailored for a specific set of users and security rating. For example, the Enterprise Hosting Infrastructure (EHI) is for internal users. More specifically, the EHI only supports users who are in the County's Active Directory system. The Intranet zone may be in the County Data Center, the County Disaster Recovery Site or Azure. The Intranet Zone has been extended to both the Disaster Recovery Site and the County Azure instance.

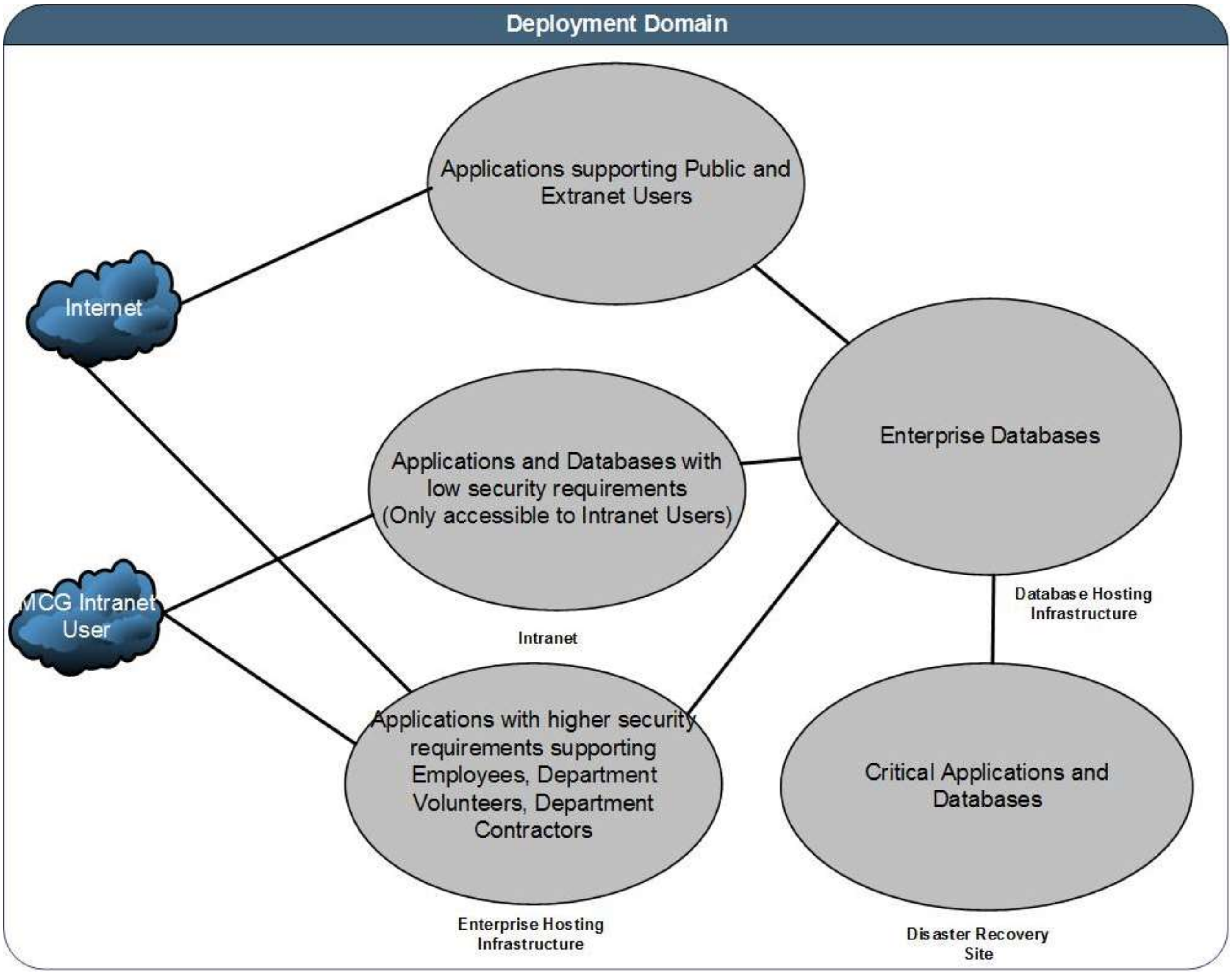

Deployment Domain
Applications supporting Public and Extranet Users
Internet
Enterprise Databases
Applications and Databases with low security requirements (Only accessible to Intranet Users)
MCG Intranet User
Database Hosting Infrastructure
Intranet
Applications with higher security requirements supporting Employees, Department Volunteers, Department Contractors
Critical Applications and Databases
Enterprise Hosting Infrastructure
Disaster Recovery Site

Figure 3-2 Deployment Zones

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Server Team

Components

Hardware

The County has standardized on Dell x64 midrange rack mount servers, which are configured at the high end of memory and disk capacity.

Hardware Capacity Planning

A sliding window of funding and replacement cycles is used for server capacity planning. New GENERATION N and N-1 servers are typically deployed as VM-HOST or DB servers. GENERATION N-2 servers released by the renewal process can become standalone servers. This process is followed a high percentage of the time for enterprise servers.

The following benefits are realized:

- Elimination of hardware selection, sizing and procurement delays
- Identical servers are purchased within a GENERATION.
- Horizontal scaling and/or VMs are used to meet processing requirements.

For example, instead of procuring 3 small servers for 3 projects, in-place capacity is used via VMs. New VM-GUESTS (for the projects) are provisioned in real-time. Project funding, from the 3 projects is lumped together to purchase a new GENERATION N server which adds back additional capacity.

Speed and ease of new server deployments

Most new servers take on the role of a VM-HOST. In just a few hours' time, these servers can be activated because only the OS, the VM engine and the utility software need to be installed. VM-GUESTS (new or existing) are then activated. Typically, this is a copy/paste operation.

Operating System, Database, and Middleware

The County stays current with Operating System and Middleware versions. The following table outlines typical versioning. Most components have service pack upgrades throughout the year with version upgrades every couple of years.

1.

FUNCTION	COMPONENT VERSION	OS VERSION
WEB/APP SERVER J2EE	JBOSS	CENTOS
Web/App Server Microsoft	ASP .NET	Windows Server

Table 5-2

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Area	Skill Set
OS	Linux (CENTOS) , Windows Server
DB	MS SQL Server, Oracle Server
Middleware	.NET AD ASP IBM MQ Series ESB (MULE) J2EE /JBOSS
Operational Support	Shell Scripting/ Perl Webmastering JUnit/HTTPUnit JMX
CM	SVN and TRAC
Cloud Services	Azure Administration
Other	Technical Project Management

Standards and Guidelines

- Current availability guideline is to keep system components available 99.5% of the time.
- DTS solely has access and manages the VM Hosting Servers.
- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates
- County has standardized on Dell x64 midrange rack mount servers, which are configured at the high end of memory and disk capacity.
- County stays current with Operating System and Middleware versions. Most components have service pack upgrades throughout the year with version upgrades every couple of years.

Disaster Recovery

The Deployment Domain involves the use of VM Guests running on VM Hosting Servers housed in the Data Centers in the System Operations Domain or Microsoft Azure. A number of disaster recovery strategies in the Deployment and System Operations Domains are employed that essentially cover the following disaster scenarios:

- server loss
- rack loss
- data center loss

The server loss and rack loss strategy has a number of mitigation strategies within the System Operations Domain. Within the Deployment Domain the mitigation strategies include:

- use of VM Guests as well as pooled VM hosting machines located in both data centers and Microsoft Azure.
- in the event of individual server or rack failure critical VM Guests will be moved to working VM hosting machines
- in the event of a data center failure critical VM Guests will be moved to working VM hosting machines in the other data center.

The design problem for the loss of one of the Data Centers is the prioritization of services that will be brought up in the working data center. See Technical Disaster Recovery section for information around prioritization of services and policies.

3.5 Desktop Domain

Principles

Desktop Computer Modernization is a centralized program for the planning, acquisition, asset management, and support services associated with desktop computers. Desktop Computer Modernization (DCM) is part of the Department of Technology Services (DTS). Under this program, the County uses its own in-house personnel for integrated desktop planning, and a single external service provider for desktop acquisition assistance, asset management, and support services. Through the implementation of DCM, the County achieves several key goals:

- Brings current technology to the desktop
- Reduces the cost of and need for support services through planning
- Provides a single source of support through a centralized single point of contact IT Help Desk
- Provides quality services to end users in an accurate, consistent, timely and professional manner
- Controls total cost of ownership.

The DCM program covers the primary seat machine for the individual worker. DCM supports based on user requirements and support considerations non-traditional as well as traditional desktops. Supported desktops include various configurations of the traditional desktop as well as laptops, netbooks, and tablets.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Client Computers (DCM) Team.

Components

Desktop Environment

The County currently has approximately 10,000 primary PCs and laptops which are located throughout the County. Existing computer equipment consists of DELL and Lenovo business class systems. The County has a 6-year replacement cycle for primary systems, subject to funding restrictions. Generally, one fifth of the County's current base of PCs is replaced each year.

External Service Provider

DCM has a single external service provider for all help desk and desktop support, asset management and computer acquisitions. DCM's current external service provider maintains a location approximately one mile from the Rockville Core which has a warehouse facility. This is also the location of the centralized IT Help Desk (see Help Desk Services section).

Asset Management

Computer hardware inventory is maintained by the external service provider in a SQL based application. The external service provider is responsible for maintaining accurate inventory reporting and continual data validation. The DCM program office staff has direct access to this database. The external service provider also makes Department inventory reports available through the intranet.

Desktop Management

DCM maintains the County's Microsoft Systems Center Configuration Manager (SCCM) Enterprise system and database. SCCM allows for a central point of desktop management, endpoint protection, software deployment, and remote control of desktops and laptops throughout the County.

Disposal of Equipment

DCM provides the County a mechanism to dispose of old computer hardware through its external service provider. Before a system can be disposed, the external service provider wipes all data from the hard drive(s) using software and procedures that meet DOD certified sanitization standards. Computer systems are then disposed or remarked in a manner that meets environmental standards. This process ensures the removal of all data from system hard drives and provides the County with the ability to maximize residual value on assets.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Project Management and Contract Administration
SCCM Administration
Endpoint Protection Administration
Wise Studio Scripting Language
SQL Administration and Maintenance
Windows Server
Microsoft Desktop OS/Platform
Dell & Lenovo Business Class Hardware
County Core Applications including MS Office, Outlook, Internet Explorer, Adobe Reader
Networking and Basic Active Directory

Standards and Guidelines

The current DCM Program Team is responsible for PC lifecycle planning and managing desktop services provided by the external service provider. The external service provider is responsible for acquisitions of new desktop equipment; imaging systems using configurations provided by

DCM staff that meet current County and Security standards; help desk and desk side services; computer maintenance and repair; and asset management.

Planning

The DCM program develops and maintains a comprehensive plan covering the life cycle of the County's PCs; integrating all aspects of desktop acquisition; help desk support; and asset disposal. The DCM program focuses on reducing the need for maintenance and other support services, while also planning for changes in technology and the IT industry. This includes developing a desktop deployment strategy and enterprise wide desktop software roll-outs (operating system upgrades, software installations, patches and new applications). The DCM Program also maintains detailed schedules identifying the PCs to be replaced, moved, installed, upgraded, disposed of, or redeployed. Planning for replacements simplifies the acquisition process by ordering in advance, minimizing disruptions to County users, providing a steady workflow, and reducing costs.

Standards

Establishes enterprise-wide standards for hardware, software, and supporting processes. DCM also standardizes on several desktop, laptop, netbook, and tablet configurations used throughout the County. A list of optional add-ons to the standard configurations is available to end-users as required.

Budgeting

Forecasts and manages desktop budget. Collects and analyzes the total cost of desktop equipment and services, reducing the total cost of ownership.

Acquisition

Functions as a single point of contact with vendors for scheduling, and obtains all desktop equipment (places orders; tracks status; approves and processes invoices).

Asset Management

Centrally manages the County’s desktop and laptop assets to maximize the return on investment. Directs the external service provider to update and maintain inventory information in the asset management database. Defines the web based reports the external service provider maintains on the intranet for Department inventory.

Contract Administration and Coordination

Oversees all DCM activities, and coordinates the resolution of escalated incidents. Monitors contract service levels in accordance with the current DCM contract. Defines and reviews monthly management reports and real-time dashboards prepared by external service provider. Contract Administration functions as a single point of contact.

Security Standards

PC Policies for Improved Security & Manageability

- This policy uses AD and SCCM to lockdown PCs and maintain standard configurations
- All County PCs must have the SCCM client installed as well as Microsoft’s Endpoint Protection.

3.6 Email System Services

Principles

The County uses Microsoft's Office 365 (see Microsoft Office 365 Domain) for its enterprise email system. This system supports Enterprise wide email functions for Montgomery County employees, contractors and volunteers. Access is supported via the Outlook desktop client, Outlook Web Access (OWA) web browser and mobile devices that support the ActiveSync protocol. Anti-Spam processing and filtering for inbound and outbound mail is currently supplied by Microsoft Office 365. Services provided to departments and groups include:

- Single Enterprise Email Domain – montgomerycountymd.gov
- Single Enterprise Calendar and Scheduling
- Single Enterprise Address List
- SMTP access for County Applications requiring outbound mail support
- Client access via:
  - Outlook desktop client (see Desktop Domain)
  - Outlook Web Access (OWA)
  - Mobile devices that support the ActiveSync protocol
- Enterprise Spam Filtering and Advanced Threat Protection
- Encrypted Email

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

An Exchange Server is configured with a virtual IP address and is used to route mail from Applications. It acts as a relay agent.

Users authenticate to Office365 via Active Directory Federation Services (ADFS) to the County's Active Directory (AD). Accounts and other Active Directory components within the Departmental organizational unit are administered by local Organizational Unit (OU) Administrators for most departments. Enterprise Administrators support the remaining departments and support all OU Administrators. User accounts are published in the Global Access List (GAL) which allows employees to easily lookup addresses, locations, departments, and phone numbers from within Outlook. Enterprise level administrators can create Contacts so that non-County partners, and contacts with non-County email addresses, can be published in the GAL allowing for membership in groups and easy emailing. The system also handles resources and conference rooms, providing scheduling services at the department and enterprise level.

Users may attach mobile devices such as the Android, iPhone, Windows mobile phones, tablets, etc through the ActiveSync protocol. Departments determine whether to issue/connect mobile devices and will be responsible for setup and providing support for the devices.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Microsoft Active Directory Administration
Microsoft Active Directory Federation Services (ADFS)
Microsoft Office 365 Administration
Magic Help Desk System
Server, Network, and Messaging Security
Windows Server Administration
Good Communication Skills
Knowledge of email processing and types of email
Knowledge of Spamming methods, and remediation
Anti-Virus Administration
Wireless Email Administration
Knowledge of Virus propagation and methods of prevention and removal
Knowledge of eMessaging Standards and enforcement methodologies
Anti-Spam Server Administration Skills
Knowledge of the Outlook Client and features

Standards and Guidelines

Availability/Uptime: The system is designed to be available 24/7.

A single enterprise email address standard:

FirstName.LastName@montgomerycountymd.gov

There is an eight character minimum. Those accounts with less than eight characters will receive x(s) to meet this requirement. To eliminate duplication, FirstName and the addition of middle initial can be used.

Specific naming conventions have been defined for Distribution Groups, Resources, Rooms, Non-Fixed resources

Shared mailboxes are defined at the enterprise level, and managed at the OU level

USERID/Mailbox policies

Deletion

Enterprise Core Systems team will monitor the use of mailboxes, and departments will be notified of mailboxes not accessed in last 60-90 days. After 90 days not being accessed, mailboxes will be deleted.

Each Dept/OU Administrator must establish an internal procedure to remove mail boxes. When an employee is terminated, the AD accounts must be deactivated **ON THE SAME DAY.**

If a department needs a mailbox, it must be copied to a PST file and saved separately.

If a department needs to temporarily access a de-activated account, the password must be reset to limit potentially damaging access by the former employee.

Once the department is finished with the employee account and it has been de-activated, the account must be deleted (as in the case of a temp, intern or contractor account) or moved to the AD Root folder INACTIVE folder (as in the case of a Retired or Terminated account).

Mail

Duplicate email addresses cannot exist.

Resources can be mailbox enabled.

Department distribution groups should use an Access Control List (ACL) to limit other department's access. Options should be set to "disallow with exception".

Shared resources must use a mail enabled security group to govern access. Security group should be created by the department in their OU and be sent with the request to create the new email resource.

Global Distribution groups will be created by the Core Systems team at the enterprise level.

Users are limited to sending emails to a maximum of 2000 recipients unless special permissions are granted.

Address List

Global Addresses

All users, groups, contacts, conference resources & public folders

Department address list

All employees

Department employees

Personal Address Books (PAB)
Not supported at the enterprise level

Individual Mailboxes

Individually deleted Mailboxes and items (messages) can be recovered up to 30 days after deletion. For recovery instructions contact the Help Desk.

All messages (including attachments) are limited in size to approximately 35 MB.

Email Administration is done centrally via the Department of Technology Services Core

Team.

- requests for new mailboxes should come through help desk tickets
- requests to delete mailboxes should come through help desk ticket

The County relies on Microsoft's cloud service to maintain service availability.

SMTP access for County Applications supported through an SMTP gateway for mail enabled applications and devices

No POP or IMAP protocol support.

Disaster Recovery

See Microsoft Office 365 Domain.

3.7 Enterprise Hosting Infrastructure Platform

Principles

The Enterprise Hosting Infrastructure (EHI) is the framework the County uses to deploy its enterprise applications. The County's EHI goals are to integrate business processes across the County by integrating and extending existing web applications. The County benefits from EHI because it promotes enterprise-wide data standardization, reuse, interoperability, and information management across applications and agencies. Reducing cost and development time, EHI facilitates common solutions for business processes, lower operational costs, increased business productivity, and better utilization of resources.

EHI encompasses most components of the County's IT Framework with Figure 3-3 demonstrating those components.

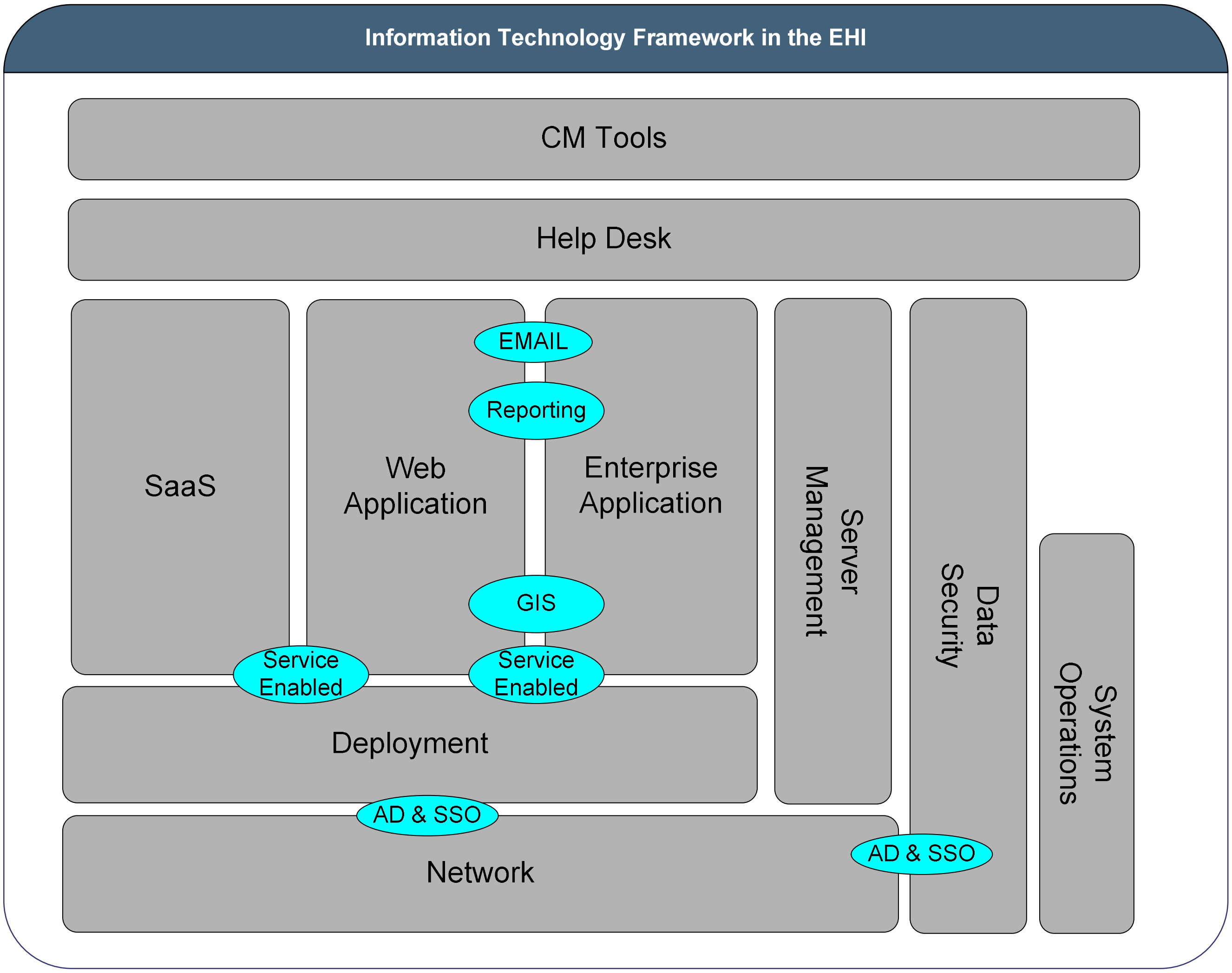


Figure 3-3 Enterprise Hosting Infrastructure Components

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Server Team
- DTS Enterprise Services Architect

Components

Architecture Overview

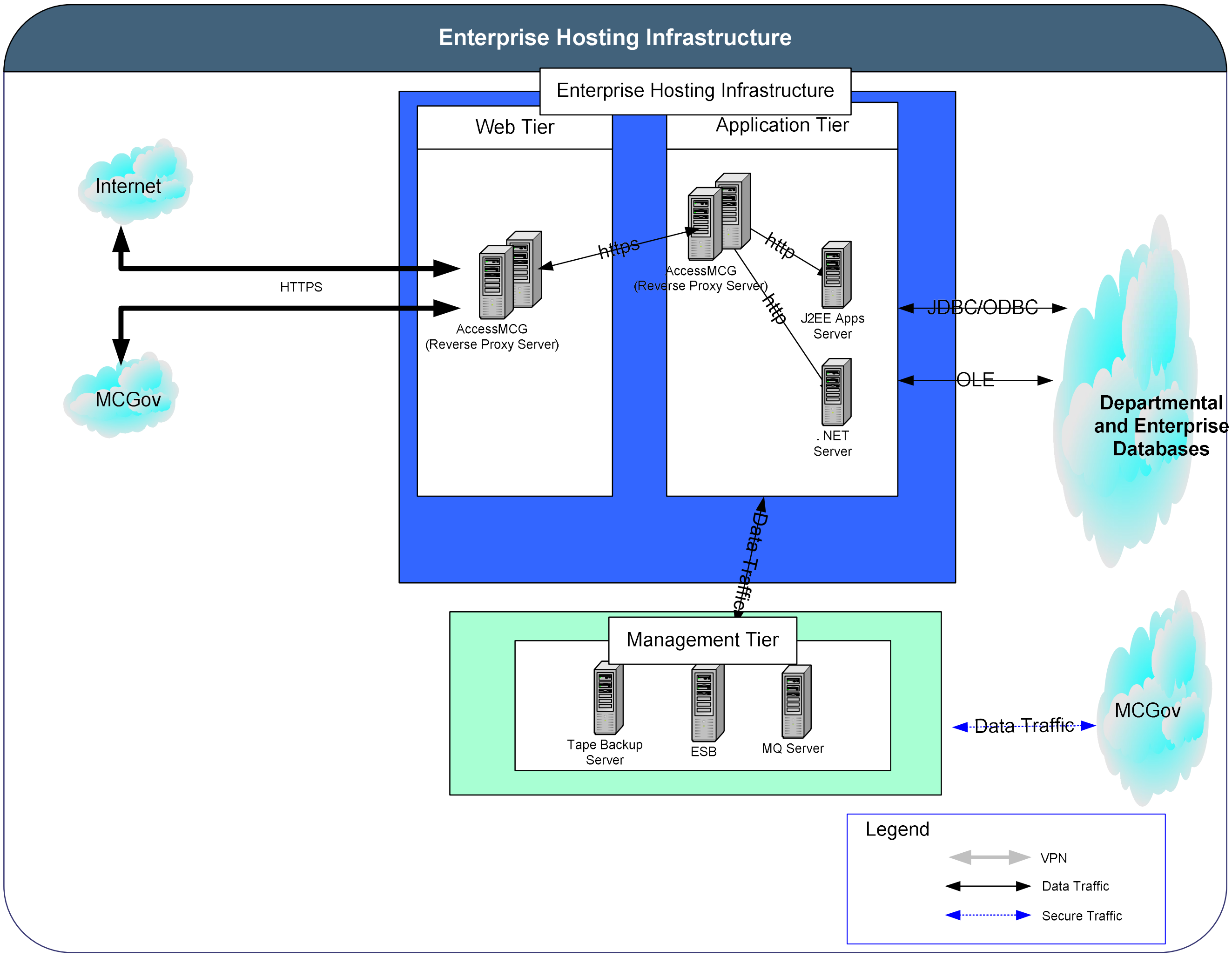
In general, the EHI architecture is based on three layers of application deployment:

- the first layer incorporates security and Single Sign On (SSO) components for the application
- the second layer incorporates the presentation and business logic of the application
- the third layer incorporates the data model of the application

Only the first layer is located in the Web Tier. The Web Tier serves as the gatekeeper for client access to Web Applications that serve Internal County Users as defined in Active Directory.

The second layer is located in the Application Tier. It is the location for the Application Servers.

The third tier is the database tier and is supported through individual departmental database servers as well as Enterprise Database Servers hosted in the Database Hosting Infrastructure (see Database Hosting Infrastructure Platform). All traffic between the Web tier to the Application Tier is encrypted with certificate Secure Socket Layer (SSL). All Web traffic (from the internet and the intranet) designated to the application server in the Application Tier will be routed thru the Web Tier. The following paragraphs describe the components that make up the platform architecture.



Active Directory

Microsoft Active Directory is the master user registry for all county employees and for all applications hosted in the EHI (see Active Directory section). All LDAP traffic from the Web and Application tiers is encrypted (LDAPS) and accesses one of the Active Directory controllers. Active Directory also provides the primary DNS service for the Application tier of servers.

AccessMCG Reverse Proxy Servers

The EHI uses the AccessMCG Domain's reverse proxy servers to maintain a directory of user roles that have permission to access specific applications. AccessMCG intercepts all application access by a user and ensures that they are properly authenticated. In addition, it allows users to sign on one time and access multiple applications. AccessMCG checks against Active Directory one time to confirm or "validate" an individual's roles or permissions to application(s). This function is known as Single Sign On (SSO).

Application Server

JBOSS is used to serve the County's J2EE applications. All JBOSS servers are located inside the Application tier. Microsoft.Net servers are also hosted inside the application tier to support County .Net and ASP applications. The AcccessMCG server in the Application tier directly accesses the HTTP services of the Application servers. Beside the standard J2EE and .Net applications, other commercial off-the-shelf COTS applications are hosted in the Application Tier, for which AccessMCG provides the SSO integration.

Enterprise Service Bus (ESB)

The Enterprise Service Bus (see Service Enabled Domain section) provides secure methods of transferring data between different platforms across different Tiers.

Servers located in the EHI Application tier can use the ESB to securely interface with servers outside the EHI platform.

The ESB is also used for secure file transfers into and out of the County.

Database Server

The database servers are located outside the EHI as either Departmental Database Servers or as Enterprise Database Servers that are hosted in the Database Hosting Infrastructure (see Database Hosting Infrastructure Platform section). The County supports both Oracle and Microsoft SQL servers under the DHI architecture. Application servers can access the database servers directly thru JDBC/ODBC/OLE.

Platform Choice

Hardware

All servers are Intel based and manufactured by Dell Computers. The hardware sizing is based on the County standard as outlined in the Deployment domain (see Deployment Domain section).

Operating System

Virtual Machine technology is used in the platform architecture. Server virtualization increases the efficiency and effectiveness of deploying and developing new technology. It aides' server consolidation and capacity optimization by utilizing excess hardware capacity. The ease of cloning of the entire virtual system provides easy backup and restore capability. This is an important operational practice for the high performance and high availability of applications within the EHI.

The Operating Systems supported on the servers are:

- CentOS
- Microsoft Windows Server

CentOS is an Open Source OS which uses the Red Hat Linux kernel and hence is an “identical twin” of Red Hat Linux.

Services

Time Service

Time services are supplied through two time servers. Windows machines are synchronized through the Active Directory Domain controllers. UNIX machines are synchronized through the County UNIX time server.

Backup Service

The EHI uses the backup services of the System Operations Domain. Once a week each VM Guest has a snapshot taken of its image. That image is then backed up through System Operations Domain services.

Refer to the System Operations Domain Server Backup and Recovery Section for details on retention and backup times.

Antivirus Service

Antivirus service is provided on the Windows Machines. Virus signatures are automatically synchronized from the County Central Antivirus server.

SMTP Service

Email services are provided through access to one of the County Exchange Servers (see Email System Services section).

Storage Service

Storage is provided through Direct Access Storage (DAS) Shelves on a per server basis.

Directory and User Registry (LDAP Server) Services

Directory and User Registry services are supported through Active Directory. For LDAP, only the LDAPS protocol is supported.

Certificate Server

Certificate services are provided through a Microsoft Windows Certificate Server and issues certificates based on the MCGOV root certificate.

Network

The EHI uses the Network Domain’s Firewalls and Switches (see Network Domain section).

The EHI is separated from both the Intranet and the Internet through one or more stateful firewalls. In addition, firewalls are also used to separate tiers internally within the EHI.

Security

AccessMCG

A set of AccessMCG (see AccessMCG Domain section) reverse proxy servers are located inside the web and application tiers to receive encrypted traffic (SSL) from the intranet and the internet. The AccessMCG server within the Web tier will authenticate the user with the LDAP server in an encrypted form (LDAPS). In turn, it will pass the traffic to an AccessMCG server (identified by the part of the web URL called junction) inside the Application tier thru an SSL channel. The AccessMCG server inside the Application tier passes the traffic in non-SSL fashion to the application server to process. The application server then returns the response data back to the Web tier AccessMCG server through the same SSL channel.

The AccessMCG to AccessMCG junction optimizes the traffic inside the Application tier while providing security to the Application tier.

Application Principles

The general principles that an application must follow are:

- Access to the Application's Application Server must pass through the Web Tier and the AccessMCG Servers
- Client access is via HTTPS only
- Access can be from the Internet or MCGov Intranet
- The ESB is used for non-client inbound and outbound traffic between the EHI and the MCGov Intranet with all traffic being point to point
- inactive session timeout
- Firewall is a stateful firewall
- Application access must be through the stateful sessions maintained by AccessMCG

Standards

EHI Hosting Agreement

A requesting team or department must read and agree to the EHI Hosting Agreement. The EHI Hosting agreement lists roles and responsibilities for the service.

Administration Policies

- No access to resources other than by DTS employees performing administration services
- Monthly patching of Operating System and middleware software
- Virus updates every 10 minutes
- Weekly VM Guest backups
- Active Directory Group Policies (DTS Server Team Administrators are the only persons allowed to administer the machine and processes)

- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates
- Each ESB integration has its requirements documented, implementation documented and data transfers audit logged.
- Each Application has a standard Help Desk Incident Script. Custom scripts can be created based on the Applications need.
- Each Application must use Active Directory Authentication
- Highly Recommended that each application use Active Directory Authorization

Application Policies

The following are standards and guidelines the County has set forth for its EHI Applications.

- Performance Guideline – The County expects a turnaround time for Enterprise Applications in 3 seconds or less
- Availability Guideline – The County expects an Enterprise Application be available no less than 99.5% of the time.
- ADA compliant – The County expects an Enterprise Application to be ADA compliant.
- HIPAA compliant – The County expects an Enterprise Application that handles HIPAA covered data to comply with the HIPAA Privacy Rule and the HIPAA Security Rule.
- Each Application will use Active Directory Authentication. Applications are strongly recommended to use Active Directory Authorization. Applications are provided with one or more Application Groups to manage Authentication. J2EE applications are provided with a library that validates authentication against the groups. .Net applications are provided with a similar design pattern. The County has standards for Java files to have the following package structure:

  gov.montgomerycountymd.<<dept>>.<<application>>.<<module>>

  where

  dept will be the short name of the department that owns the application
  application will be the short name of the application itself
  module will be the implementation section

- The County has standards for .NET namespace:

  gov.montgomerycountymd.<<dept>>.<<application>>.<<module>>

  where

  dept will be the short name of the department that owns the application
  application will be the short name of the application itself
  module will be the implementation section.

Quality of Service

- Multiple deployment environments have been set up for application deployment and testing:

  Development – AccessMCG junctions are directed to a developer(s) machine

Test/Staging – A separate environment for Test and Staging

Production – A separate environment for Production

- There is an ACL (Access Control) rule defined for Production AccessMCG in such a way that test Active Directory accounts can NOT access the Production applications.
- The Active Directory Application Authorization Model allows the delegation of application administration to different application administrators in the County.
- Heart Beat uses same SSO access paths to SSO application to provide continual monitoring.
- Using VM and Microsoft disk mirroring, servers in EHI can be easily restored and tested with updates or patches.
- AccessMCG provides standard SSL protection (FIPS 140-2 certified) for the County's existing applications.

Physical Security

The networking switches and firewalls as well as the hosts that support the Production EHI are all located within one of the Department of Technology Services Data Centers (see Systems Operation Domain section).

Help Desk Support

A key component of the EHI is the Help Desk (see Help Desk Services section). It provides a single point of contact for the users of applications hosted within the EHI. The Help Desk resolves problems or, as needed, routes problems to the EHI administrators.

As part of the intake process for a new EHI application a support plan is developed with the help desk. The support plan includes information such as:

- Identifying the business system owner
- Identifying the EHI Administrator contacts
- Identifying common problems and their resolution that a level 1 support person can handle
- Identifying the contact for level 2 problems

Server Administration

Administration of the EHI Servers is performed by the DTS Server Team (see Enterprise Server Management section)

Deployment Model

A J2EE application must be packaged into an EAR (Enterprise Archive) file for deployment. Even if the application contains only the Web components (a collection of Web Archive WAR) files), it should be packaged into an EAR file.

Applications may not package the libraries' JARs for the County's standard components, such as Oracle, LDAP, and WebSphere. The County should have full flexibility to deploy upgrades for its standard libraries without altering the applications.

Every J2EE Web component should be self-contained. All the required libraries should reside within the WAR package. Similarly, every other component (such as EJBs) should be self-contained within EAR package.

Every application may accompany a folder with subfolders for configs, scripts, and properties files.

Every application package must accompany a Configuration document. This document should clearly explain the prerequisites and steps for installing the application. The document must include:

- List of files in the package
- List of configuration options and description of each
- List and description of 3rd party dependencies
- List of log files, their location, and description

The County encourages programmers and analysts to include a troubleshooting section in their Installation and Configuration documents to help avoid known mistakes. The County also encourages programmers and analysts to include a health-check section to check the health of the application after installation or after a restart.

The County encourages applications to write log error condition messages in the standard format. The document may indicate the format and the expected error messages. All applications shall support multiple log levels which can be modified without re-starting.

3.8 Geographic Information Systems Domain

Principles

The County has designed and implemented a Geographic Information System (GIS) to deliver geospatial data to spatially enabled desktops, Web-based applications, and location services. The system generates both soft and hard copy and Web-based cartographic/mapping presentations enabling data analysis and decision support services. The County has dedicated resources to create, maintain, manage, and store geo-spatial data.

The County has two definitions of spatially enabled services. One is a service capable of integrating spatial data with other business data across multiple, heterogeneous data sources. The other is a service supporting abstract data types (images, text, and spatial data) spatial operators, functions, and spatial locator indexes. The County implements Environmental Systems Research Institute's (ESRI) GIS data models and ArcGIS suite of software.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS GIS Team.

Components

The GIS configuration is designed to be flexible, fast, scalable, reliable, manageable, and secure in order to satisfy the needs of a wide variety of users and customers. Casual users typically use GIS services delivered by Web and desktop applications to perform basic tasks such as generating maps and travel directions or finding a map feature such as a place of interest. Intermediate users perform basic mapping functions in addition to inputting data and performing basic geo-spatial analysis (queries, geo-coding, buffering, overlay, etc.). Casual and intermediate users use Web browsers to access customized *ArcIMS* or *ArcGIS* Server map and image services/viewers, as well as ArcView, ArcReader, or ArcExplorer (free viewer) software products. Advanced users use GIS and cartographic software products such as ArcGIS (one of the three tiers), ArcSDE/Oracle, ArcView , and Adobe Illustrator and Photoshop (used for mapping) to produce, maintain, manage, analyze, and map geo-spatial data sets. Advanced users also use GIS software products to create customized applications on both the desktop (Arc Macro Language, Avenue, Visual Basic, and Visual Basic for Applications) and the Web (Active Server Pages, XML, HTML, JavaScript, and Perl). Recent experiments with GoogleMaps has also shown great potential for presenting County's geo-spatial data in a vivid way.

System requirements (provided by ESRI), and customer requirements dictate the County's GIS design. Figure 3-5 and Table 3-6 provide an overview of the GIS system and Web architectural designs.

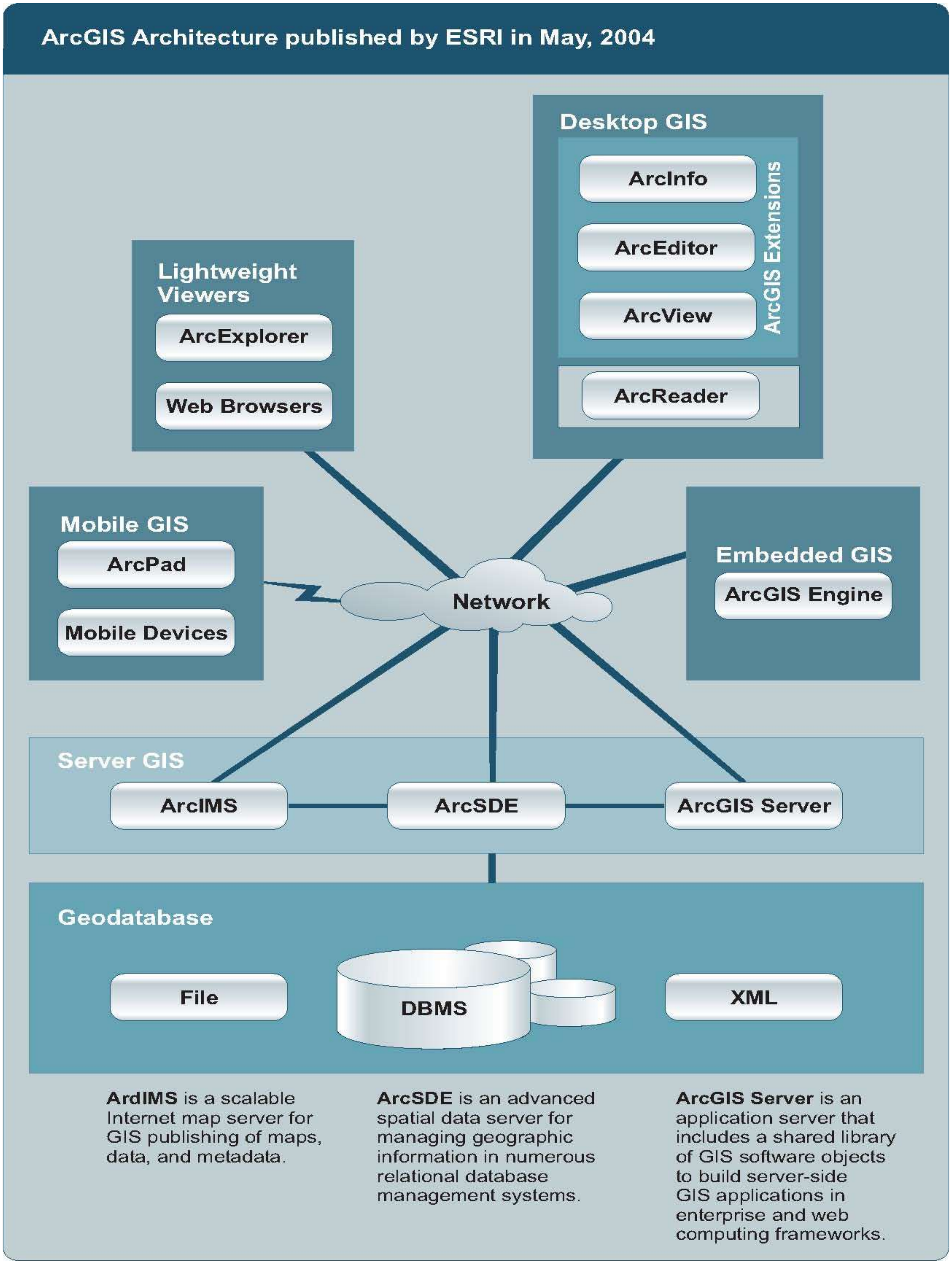

ArcGIS Architecture published by ESRI in May, 2004
Desktop GIS
ArcInfo
ArcEditor
ArcView
ArcGIS Extensions
ArcReader
Lightweight Viewers
ArcExplorer
Web Browsers
Mobile GIS
ArcPad
Mobile Devices
Network
Embedded GIS
ArcGIS Engine
Server GIS
ArcIMS
ArcSDE
ArcGIS Server
Geodatabase
File
DBMS
XML
ArdIMS is a scalable Internet map server for GIS publishing of maps, data, and metadata.
ArcSDE is an advanced spatial data server for managing geographic information in numerous relational database management systems.
ArcGIS Server is an application server that includes a shared library of GIS software objects to build server-side GIS applications in enterprise and web computing frameworks.

Figure 3-5 ArcGIS Architecture [1]

[1] ArcGIS Architecture, Published by ESRI, May 2004

Table 3-6 below identifies the GIS software that has been installed in the County. These versions of ArcGIS software, ArcSDE middleware, and Oracle databases have helped to centralize the GIS data layers to the new ArcGIS Geo-data model.

GIS Software Components		
New Version		**Platform**
Enterprise GIS	Server-side Geo-processing environment - ArcGIS Engine: with embeddable GIS components ("Maps for Apps")	Intel PC MS Windows
ArcGIS Tiers	ArcInfo ArcEditor ArcView ArcReader (free)	Intel PC MS Windows
ArcGIS Extensions	ArcGIS Business Analyst (at DED) ArcGIS Spatial Analyst ArcGIS 3D Analyst ArcGIS Geostatistical Analyst ArcGIS Survey Analyst ArcGIS Tracking Analyst ArcGIS Publisher ArcGIS StreetMap ArcGIS Schematics ArcScan for ArcGIS ArcPress for ArcGIS MrSID Encoder for ArcGIS	
Free ArcGIS Add-Ons	Tablet PC Support for ArcGIS ArcMap GPS Support Districting for ArcGIS	
Mobile GIS	ArcPAD ArcPAD Developer Tool Kit	Pocket PC Windows CE
Database	ArcSDE – middleware Oracle (licensed separately from Oracle Corp.)	Oracle
Web GIS	ArcIMS - RouteServer ArcGIS Server ArcExplorer (free)	Wintel Server

Table 3-6 GIS Software Components

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
ArcGIS software – core modules
ArcGIS Extensions
Geo-database data model, ArcSDE and Oracle
ArcIMS, ArcExplorer, and ArcGIS Server
Visual Basic for Applications
Develop Geo-processing Scripts Using Python
Utilizing ArcObjects for application development
XML, ASP
J2EE, JavaScript

Standards and Guidelines

GIS Servers

- Administrator privileges are limited to DTS employees performing administration services
- Monthly patching of GIS Servers Operating System and middleware software
- Virus signature updates every 10 minutes
- Read only access provided to other departments to use ArcGIS
- DTS backs up Enterprise GIS Servers for disaster recovery purposes. DTS' current recovery process is to restore servers in the event of system crashes, facility loss, or some other disaster. To support the current model, the GIS Domain uses the backup services of the System Operations Domain (see System Operation Domain section). Refer to that domain for backup retention times.

GIS Data

- Some departments maintain their own department specific GIS maps and data layers but send their data to the DTS GIS team to keep in the County Central Repository
- Street Addressing standard
- Centerlines, districts, buildings, and places of interest maintenance procedures
- Secure Web application requests and approval forms
- GIS data requests form
- All County employees having access to the Enterprise computing resource can access all commonly available GIS data layers.

- County GIS data, hardware, and software are for business use only.
- DTS' GIS coordinates the distribution of the County's GIS data to outside entities. Consultants performing contracted County projects can be supplied needed GIS data free of charge. This data is sold to outside entities and transferred electronically or by CD/DVD media.

3.9 Help Desk Services

Principles

The IT Help Desk provides a single point-of-contact, centralized support to County employees and contractors using the County's IT Infrastructure. The IT Help Desk resolves problems or, as needed, routes problems to other support organizations to assure that they are resolved properly.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Client Computers (DCM) Team.

Components

The County uses Remedyforce, a cloud based service management system from BMC Software, to manage problem identification, analysis, and resolution. As it is currently implemented, Remedyforce is used by the County for service management, asset management, self-service ticketing, and reporting.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Remedyforce
Customer Service
Problem Analysis & Resolution
MS Office Products
MS Windows OS/Platform
Networking

Standards and Guidelines

Level 1 Support - The IT Help Desk will provide support for all IT requests it receives by attempting to resolve the problem immediately over the telephone. Level 1 includes support for standard desktop PC hardware, software, and operating systems. The IT Help Desk shall support new, standard software whenever adopted by the County. The IT Help Desk shall also be available for support and service requests received via e-mail and self-service requests created in the Self-Help Information Portal (SHIP).

The responsibilities of Level 1 Analysts are to receive trouble calls, enter the calls into the Remedyforce System, document the problem, and perform remote troubleshooting. If the problem does not pertain to the desktop PC environment the call will be transferred to the appropriate support organization within the County's IT Help Desk. The Level 1 Analyst coordinates the problem resolution process with other IT support resources, and communicates the status of the problem to the end-user. To ensure user satisfaction, the Service Desk Express system will automatically notify the client via email when the problem has been resolved.

When it is unable to resolve a trouble report remotely, Level 1 will escalate the resolution process to Level 2. Level 2 personnel will inform Level 1 personnel of the status of the problem and the actions being taken to resolve it. The responsibility to coordinate problem resolution, and to document the status of problems, remains with Level 1. This is facilitated by the communication capabilities of the Remedyforce System.

Level 2 Support - If the call cannot be resolved by Level 1 support, the request will escalate to Level 2 Support, which provides Senior IT Help Desk Analysts, Hardware Technicians and Maintenance Technicians. The IT Help Desk will dispatch technicians, as needed, to provide desk-side assistance. Upon escalation to a Level 2 request, the IT Help Desk shall immediately assign an appropriate technician. This technician will call the user to acknowledge receipt of the request, analyze the problem and attempt to initiate resolution over the telephone. Level 2 support personnel shall have advanced skills on the standard County's PC hardware and software. Should further support be required, the call will then be transferred to other support organizations in the County's IT Help Desk.

Problem Escalation - If the problem has not been solved by Level 1 or Level 2 support, it will escalate to the IT Help Desk Support Manager for resolution. Unresolved issues will escalate to the Desktop Computer Modernization (DCM) Program Office. The IT Help Desk generates monthly trend analysis reports. These trend analysis reports help to identify repeat problems, which might indicate systemic issues beyond the scope of the problem reported.

Service Levels - Service level indicators for the IT Help Desk are established in the DCM Contract and are used to show performance level. The service level indicators established are the Minimum Acceptable Level (required) and the Incentive Level (incentive goals).

Phone Number

Help desk phone number is 240-777-2828.

3.10 Network Domain

Principles

The County built and manages its own network called FiberNet. FiberNet is a County wide electro-optical communication network with the capacity to support Voice, public-safety, traffic management, data, Internet access, wireless networking (including public Wifi) and video transmissions among Montgomery County Government (MCG), Montgomery County Public Schools (MCPS), Montgomery College (MC), Maryland National Capital Park and Planning Commission (M-NCPPC), Housing Opportunities Commission (HOC) and Washington Suburban Sanitary Commission (WSSC) facilities. FiberNet is the communications backbone for the Public Safety Radio and Public Safety Mobile Data Systems (collectively, Public Safety Communications System (PSCS), and future technology implementations (including 800 MHz IP public safety radio). FiberNet's outside physical plant has a practically unlimited useful life. Upgrades and replacements to electronic components in the core and at user sites will be required periodically throughout the service life.

There are currently two generations of FiberNet in active service with a 3rd generation in planning. The 3 generations of FiberNet are called FiberNet I, II, and soon to be FiberNet III. FiberNet I is a legacy network still used to support specific public safety and traffic communications. It is in the process of being retired. FiberNet II is currently used to support all County communications services including 311, e-mail, Internet, and local cable channel video. FiberNet III is in the pilot and planning phase. FiberNet III's goal is to significantly increase bandwidth and services for agency needs. The first step toward FiberNet III is the introduction of dense wave division multiplexing (DWDM) into the infrastructure. DWDM enables FiberNet to provide high speed point-to-point links for specific applications like Public Safety Radio, Internet II and virtual data center operation. DWDM solutions are currently being piloted for Montgomery College, WSSC, and Montgomery County E911. DWDM does not scale to the number of FiberNet sites and is not a viable contender to replace FiberNet II. We believe FiberNet III will be a next generation MPLS/VPN based infrastructure capable of serving 10 Gig client sites over multiple 100 Gig backbone links.

FiberNet II is a robust and resilient service provider class metro-Ethernet network composed of over 500 miles of optical fiber plant, ATM and Ethernet switches, routers using one and ten Gigabit Ethernet (GbE) links. These technologies are combined to deliver connectivity solutions that are efficient, bandwidth-rich, and economically justifiable. The first principles of engineering design are performance, security, reliability and availability, and these principles dominate FiberNet's daily operation. Cost recognition, reduction and containment are the economic principles that guide the operation of the network. FiberNet is monitored and evaluated against these principles and improved accordingly.

FiberNet is a multi-agency telecommunications resource that is subject to inter-agency governance. FiberNet's strategic planning, budgeting and operational oversight is a matter of concern and involvement by the County Council which created the Information Technology Planning and Coordinating Committee (ITPCC) and its subgroups. This governance structure manages the direction of FiberNet, approves budgets and oversees the stewardship of DTS in operating the network.

In 2016 the Department of Technology Services opened a Network Operations Center to support FiberNet. It is staffed 24x7x52 and formalized the support structure for FiberNet. FiberNet has grown to be a critical County resource that is used around the clock. The NOC was necessary to support those services.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the Network Services Team.

Components

FiberNet is a standard-based infrastructure implementing IETF, IEEE and ITU-T protocols on hardware and software products from Aruba, Cisco, GDC Communications, 3Com and other major equipment manufacturers. Standards implemented within the County's network infrastructure are shown in Table 3.12. Element managers and network management system tools (NMS) help maintain control of the network by tracking utilization, reporting faults, and maintaining configurations. NMS products currently in use or planned to be used are Cisco Works, IBM Netcool, Statseeker, and TIVOLI Network Manager.

FiberNet III

FiberNet is continuing to expand and take on new services. To handle the future growth and new services FiberNet is currently in the planning stages for its next generation architecture.

Part of that next generation architecture involves the County moving to convert the current backbone to use Dense Wavelength Division Multiplexing (DWDM). By using DWDM it greatly expands the capacity of FiberNet and gives the County greater flexibility for the architecture. For example, DWDM is being added to the core hubs which allows the County to create point to point connections through the network. At the same time the current FiberNet II network will move to ride on top of the DWDM connected hubs.

FiberNet II

With FiberNet II Montgomery County adopted a service provider network model and moved to metro-Ethernet and Multi-Protocol Label Switching (MPLS). In doing so, they have been able to offer virtual private network (VPN) solutions based on logical network separation at the IP layer. A major advantage of this combination of technologies is the easy segmentation of networks so that departmental isolation is based on security requirements and business needs. For Montgomery County Government, key workgroups and departments will be given their own virtual private network with common and shared services being accessed via a stateful firewall. The service provider model enhances FiberNet's ability to provide secure network services to critical Public Safety and Health departments in the County government. It is designed to better respond to Compliance Initiatives as well as improve survivability from network attacks.

Figure 3.8 depicts the general design of FiberNet II.

FiberNet II Core

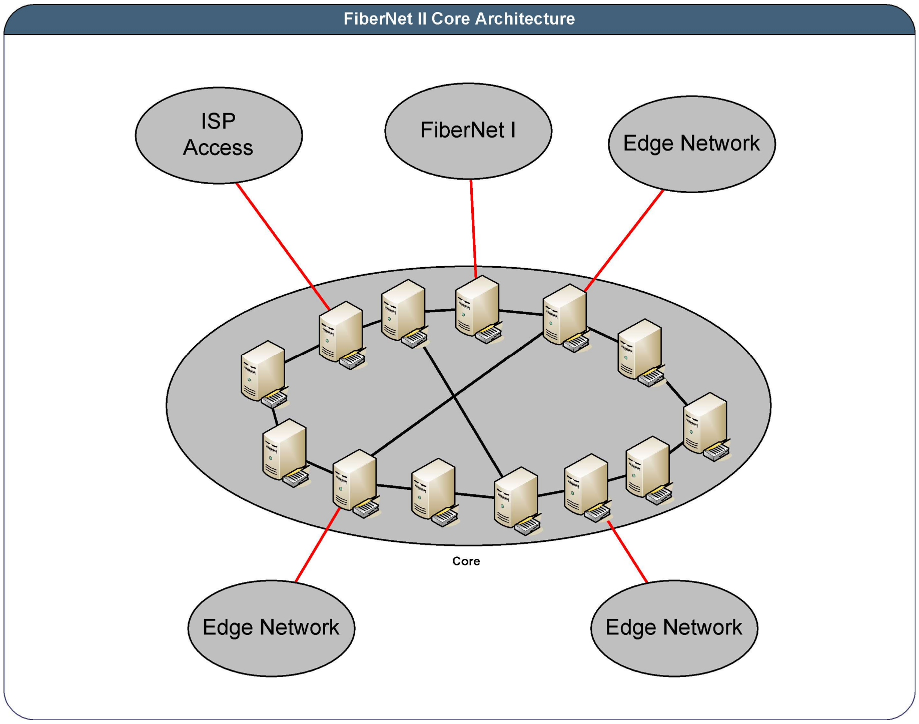


Figure 3.8

The core of FiberNet II is built around a number of 6509 CISCO Routers in a partially meshed configuration where on average every node on the backbone is connected to three neighbor nodes. These form the backbone of the County's MPLS/VPN infrastructure. Customer edge networks are attached to one of the core routers over a fiber optic or frame-relay link.

FiberNet II Edge Architecture

FiberNet II departmental edge networks are based around Passive Optical Networking (PON), Ethernet and wireless technology. In older and rental buildings employees in County offices attach to a local area network through either 802.11 wireless access or direct access to a local Ethernet switch. The County uses CISCO switches and routers to build out their local area networks. Switches are VLAN capable. Where necessary, MPLS capable routers provide the ability to segregate collocated departments and workgroups that will be mapped into departmental IP networks. The edge networks are connected to one of the backbone routers in the core network.

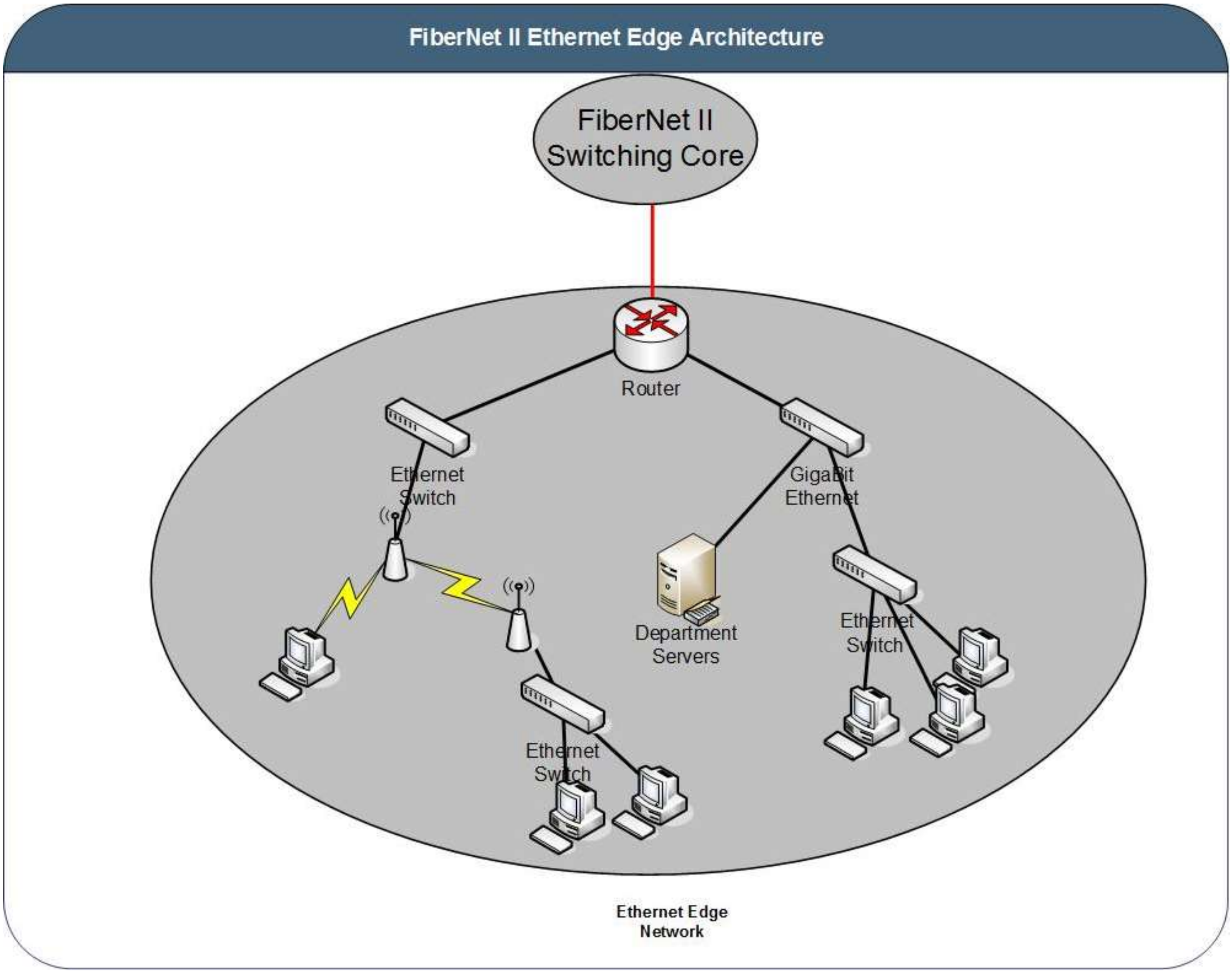


Figure 3.9

With future buildings that have compatible wiring the County will selectively use Passive Optical Networking for Local Area Network (LAN) access. With PON, buildings are wired with fiber that runs from a building head-end device called an Optical Line Terminal to each of the offices. The PON technology uses a point to multipoint design to multiplex data streams to end points called Optical Network Terminals (ONT). The OLT interfaces on the trunk side with a traditional distribution switch and then radiates-out and receives back from hundreds of ONTs multiplexed light streams carrying IT traffic. Each ONT is connected to an optical splitter that is in turn connected to the OLT. All connections use a single strand of Single Mode optical fiber. The splitter optically breaks the downstream light into as many as 32 individual streams carrying traffic to each ONT and then recombines the return traffic sending it up stream back to the OLT and then into the County network. At each ONT the County may connect as many as 24 personal computers, telephones, WiFi Access Points, CATV devices, CCTV cameras or other IT devices. This reduces the costs of the Local Area Network because routers and switches are not required on each floor. The devices will still be on an Ethernet network attaching to the ONTs through their standard Ethernet connections but the Ethernet layer 2 packets will ride over the PON network to the OLT which will be connected to a building distribution switch and thence into the MCGOV network.

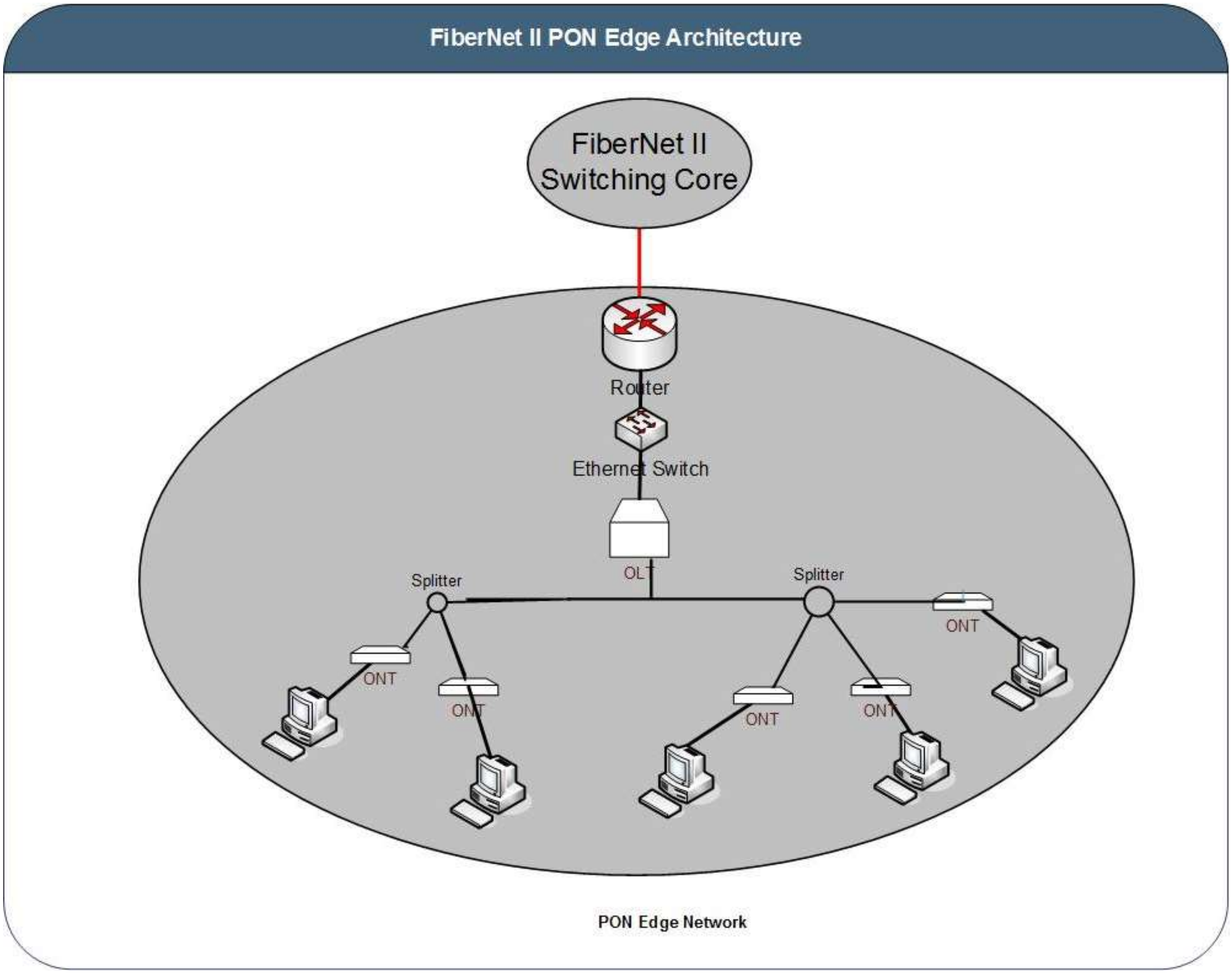
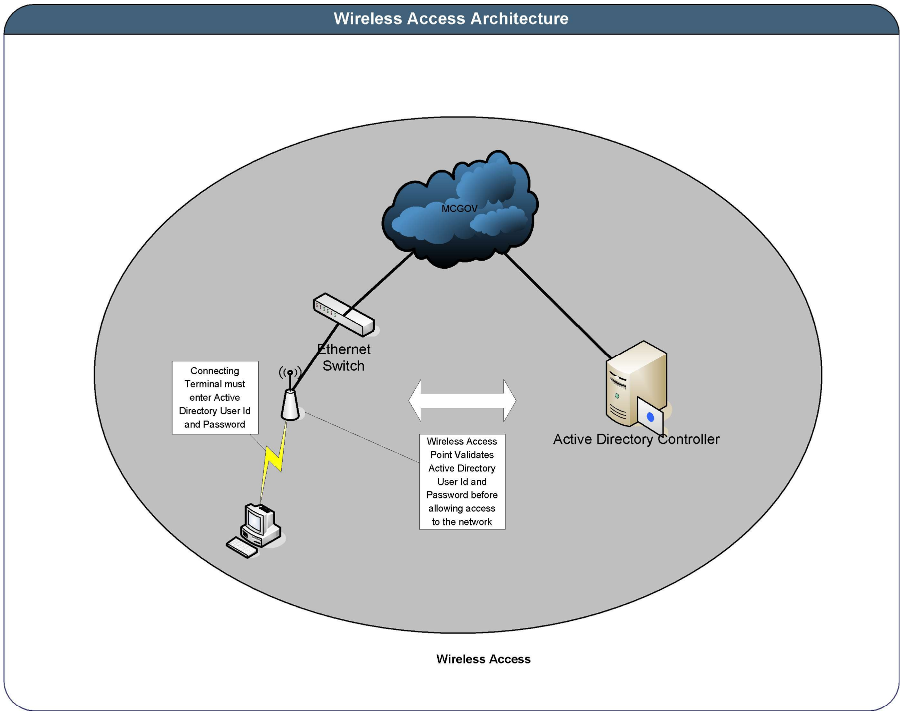

FiberNet II PON Edge Architecture
FiberNet II Switching Core
Router
Ethernet Switch
OLT
Splitter
Splitter
ONT
ONT
ONT
ONT
ONT
PON Edge Network

Figure 3.10

FiberNet Wireless Access Architecture



Connecting Terminal must enter Active Directory User Id and Password

Wireless Access Point Validates Active Directory User Id and Password before allowing access to the network

Figure 3.10

In addition to wired technology the County has deployed a large WiFi network. Wireless access is provided in many places via 802.11 b/g/n/ac Aruba access points. The Aruba access points can expose a number of secure and guest interfaces. The secure access interfaces will use the WPA2 and PEAP authentication method. When a wireless user connects to the access point through the secure interface the WPA2 protocol is supporting an encrypted transport to the access point. The access point will allow only the WPA2 traffic to pass through the access point and will prevent all other traffic until the user is authenticated.

The user's Active Directory userid and password are passed through the protocol to the access point that passes it to the Wireless Management Server. The Wireless Management Server is configured to perform an LDAP request to the Active Directory server to authenticate.

In addition to the secure interfaces that provide access to the MCG Intranet and other internal networks the access points are providing a MCGuest interface. The MCGuest interface is an open interface and is designed to support mobile device access. The network provides access to the users to the Internet and to the MCG VPN.

FiberNet ISP Access Architecture

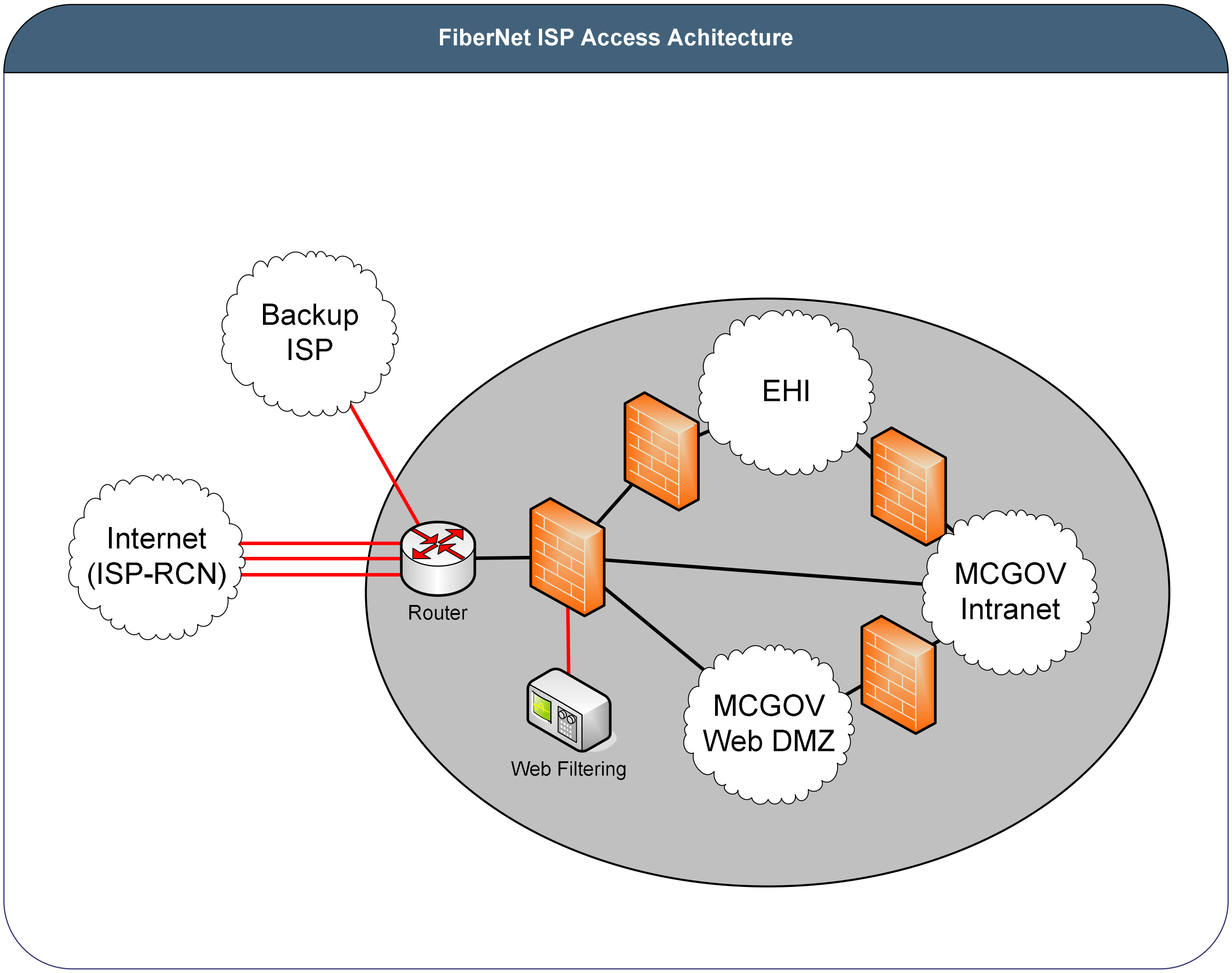


Figure 3.11

Internet access is provided by two ISPs over multiple T3 circuits that are multi-homed into the County network for load-sharing, redundancy and resiliency. All traffic that enters and exits the County passes through a stateful firewall. Outbound HTTP traffic is filtered through the DTS EISO Security Team's Web Filtering system (See Security Domain section).

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Link Layer Protocols including wireless
Routing & Switching

Perimeter & Internal Security
Network Management
Project Management
Optical Plant Design and Networking
Customer Satisfaction & Support
Network Design
NOC Operation

Standards and Guidelines

The County will introduce additional or new standards-based technologies, as these are required. Cost justification of technology is of paramount importance in our decision-making process. New technologies must meet the County's architecture goals and must make sense economically. See Table 3-12 for Primary Standards

Table 3-12

IETF Standard/Protocol	**Title/Name**	**Comment**
RFC 768	UDP	User Datagram Protocol
RFC 791	IP	Including IP routing processes
RFC 792	ICMP	
RFC 793	TCP	Transmission Control Protocol
RFC 826	ARP	Address Resolution Protocol
RFC 1918	Address Allocation for Private Internet Space	Network Address Translation is used to permit RFC 1918 address to communicate over the Internet.
RFC 2131	DHCP	IP address management
RFC 2362	PIM/SM	Multicasting
RFC 2390	Reverse ARP	Reverse Address Resolution Protocol
RFC 2571 through RFC 2580, inclusive	SNMP	Network Management
RFC 2547bis	MPLS/VPN	MultiProtocol Label Switching/Virtual Private Networks
RFC 4851	EAP-FAST	802.11 security protocol developed by Cisco Systems and made available to the general public in RFC4851
IEEE Standard/Protocol	Title/Name	Comment
802.1D	Spanning Tree Protocol	
802.1P	Prioritization	
802.1Q	VLAN	
802.3	CSMA/CD	
802.3AD	Link aggregation	Trunking
802.3U	MAC 100 Base-T	Fast Ethernet (100 Mbs)

802.3X	Flow Control	
802.3FX	Fast Ethernet over single mode optical fiber	
802.3Z	MAC Gigabit Ethernet	
802.5	Token Ring	Being replaced with Ethernet
802.11B/G/N	Wireless LAN	
802.1W	Rapid Spanning Tree	
802.1X	Port Based Network Access Control	One of the elements supporting Extensible Authentication Protocol (EAP) used to implement 802.11 security.
ITU-T & ATM Forum	Title/Name	Comment
AAL1	Circuit Emulation Services	Used for TDM based services
AAL2/3	Variable Bit Rate	Voice – G711, etc
AAL5	Unspecified Bit Rate	Data
PVS & SPVC	Permanent & Switched Virtual Circuits	
PON	Passive Optical Networking	
DWDM	Dense Wavelength Division Multiplexing	

Performance

Network performance is monitored continuously in the optical core, and at the client edge. Network Services has developed an integrated Network Management System using standard based tools like HP Network Node Manager, Statseeker and IBM Netcool. Network devices are configured to send SNMP traps when faults or changes in the network occur. These are parsed, filtered and forward to the Data Center and Network Services team for evaluation and resolution. This system is under constant development and improvement.

Capacity planning is performed periodically to determine whether a traffic bottleneck is causing congestion in the network. Statseeker is used to track bandwidth utilization and system availability. Reports are reviewed on a weekly basis to look for developing problems and to analyze problems as these are reported.

In general, site to site response times across FiberNet vary depending upon the time of day, inherent delay, and latency in the traveled circuit. Observed ping response times between sites on the fiber-optic network range between 1 to 3 milliseconds (ms). Adding frame-relay to the traveled circuit adds another 3 to 4 milliseconds, and adding a wireless link adds another 1 to 4 milliseconds. During normal network operation, ping response times are usually below 11 milliseconds, from edge to edge. Network throughput is governed by the most restrictive carrier link in the circuit. FiberNet uses circuits ranging from 10 gigabit/second to 10 megabits/second for Ethernet links and 1.544 megabits/second for frame-relay. Contention and congestion affect throughput and must be considered when designing applications. Each media and every component in FiberNet is shared by every active application traveling a particular communication channel.

Reliability

At the physical layer, reliability has been achieved with redundant components like multiple switches and power supplies, multiple and diverse fiber paths, and uninterruptible power supplies (including dedicated generators) within the supporting infrastructure. FiberNet uses a partially meshed backbone design with every FiberNet Hub having at least two diverse links (east-west) attaching to its nearest neighbor. In most cases, there are three links. On FiberNet, the same partially meshed backbone provides protection from backbone link failures. FiberNet is fundamentally a Layer 3 network topology. Fault recovery is performed in the routing plane of the network.

The County maintains an inventory of spare equipment. Equipment from this inventory is used to quickly replace failures at edge sites and in the core. FiberNet/WAN was designed to transport public safety applications. For this reason, redundancy, robustness, proactive monitoring, and management have been design requirements from the beginning. The core and the customer edge sites are monitored 24 hours per day, 7 days per week. Field engineering is available within a two-hour response time, and all outages are treated as major outages. Service Level Agreements stipulate an eight-hour time frame for repairs to electrical component faults. Fiber repair times are more problematic due to external forces like hurricanes, snow storms, thunder storms and accidents. Our experience has been favorable; these types of failures and long-lived outages have been rare.

Availability

The County tracks availability statistics for FiberNet's backbone, and user sites separately. Average availability over the most recent quarter has been 100% for FiberNet's backbone and 99.9% for all user site outages. Public safety and other important sites which operate on a 24 hour, 7 days per week basis receive 2-hour on-site response times with 8 hours as the targeted time to repair for equipment related faults. Most user-site outages are related to local power failures and the recovery there from. Such outages do not reflect upon the stability and reliability of FiberNet core; rather these indicate the assessed criticality of the user site. Sites are not public safety sites or other critical sites, and do not operate on a 24 hour per day, 7 days per week schedule. These are sites closed on the weekends and after 6:00 PM, forcing repairs efforts to wait until the site is accessible.

Security

Although security is addressed as a separate topic within this document, it is also a design goal within the network infrastructure. FiberNet's circuits are inherently secure. Desktop and server connectivity is provided through switches. The County does not use shared media hubs to deliver services. This design principal mitigates the risk of network sniffing and man-in-the-middle attacks. FiberNet is also concerned about the security and survival of its physical infrastructure. FiberNet has added and will continue to add external physical security, fire suppression, environmental monitoring, and control systems to this infrastructure.

Management systems and protocols are often a security risk in a large network. The management core for FiberNet is not accessible from the County network and the Internet. Network Services maintains a logically separated NMS network to monitor the networking infrastructure. There is no dial-in capability within the WAN.

Internal security for the network is provided by several firewalls that provide "security in-depth" for the County's IT assets. Internet access is mediated by high-availability firewalls that screen all traffic. Additionally, dedicated internal firewalls segregate special purpose networks from the main County network.

Wireless access to the County network is protected using the WPA2 and PEAP authentication method.

Wireless Access

The Network Services team must specify and install all wireless access points attached to the County's networking infrastructure. Wireless access points must follow the County's architecture and standards. Fundamentally this means using WPA2 and PEAP for authenticating to the County Active Directory.

Internet Access

The Network Services is responsible for protecting the perimeter of the County's network as well as providing security in depth; where it is required. Concerning Internet access, Montgomery County Governmental access to the Internet must pass through designated border routers and firewalls maintained by DTS. Any Internet connection that is not maintained by DTS is considered to connect to a foreign network. The Internet attaching network will not be permitted to connect directly to the County's network. Each of these networks will connect to the County network only through a stateful firewall that is maintained by Network Services.

New Applications or Services

New applications or services must use IP based communications for their Network Protocols, conform to industry best practices and comply with the County's Security Policy as well as legal mandates and contractual obligations entered into by Montgomery County Government, e.g. PCI.

Disaster Recovery

The Network Domain is the most basic IT Service within the County. Almost all Enterprise Services depend on the Network in one form or another. Several disaster recovery strategies are employed in the Network Domain to avoid and recover from failure such as:

- Staffing of a Network Operations Center 24x7x52
- Multi-homed ISP connections - in the event of one ISP failure the other will take the load.
- FiberNet is designed with a partially meshed backbone which provides protection from backbone link failures.
  - FiberNet is fundamentally a Layer 3 network topology.
  - Fault recovery is performed in the routing plane of the network.
  - FiberNet does not have a single point of failure.
- The County maintains an inventory of spare equipment. Equipment from this inventory is used to quickly replace failures at edge sites and in the core.
- Core and customer edge sites are monitored 24 hours per day, 7 days per week. Field engineering is available within a two-hour response time, and all outages are treated as major outages. Service Level Agreements stipulate an eight-hour period for repairs to electrical component faults.

3.11 PBX Network Domain

Principles

The PBX Network Domain provides advanced voice services for most of the County Executive Branch Departments. The DTS PBX Telephone Services team provides the following services:

- Legacy Voice Services
- VoIP Services
- Voice Mail
- Management of the connection and agreement with the County ILEC
- Maintenance of the County Phone Directory – both online and printed
- Maintenance of the County's 311 connection with the various Telecommunications providers servicing in the County
- Maintenance of the endpoint switches with select departments including MC311
- Maintenance of a backup switch for critical phone numbers

The County maintains a modern Avaya Communication Manager that leverages the Network Domain (see Network Domain section) to provide the above services. Communications Manager is a highly reliable and scalable system that provides access between voice and data endpoints.

The DTS PBX Telephone Services team supports both legacy voice and newer VoIP services. New installations are now being installed as VoIP services. The Communication Manager system supports both the old legacy voice and the newer VoIP services, enabling the County to continue to leverage its investment and allocate funds for new locations and new applications.

Select departments such as MC311 have their own Avaya endpoint switch. The PBX Network team supports the endpoint switches and their connection to the main Avaya Switch.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS PBX Telephone Services Team.

Components

The Avaya Communication Manager is a highly reliable and scalable system that supports digital voice, video and data communications and is designed to meet the County's information movement and management requirements, both today and in the future.

The platform provides an open architecture; conforming to QSIG, TCP/IP, ISDN BRI, TAPI, TSAPI, JTAPI, ASAI, LDAP, H.323, and H.248 standards. This translates into better integration and an increased number of high quality applications.

Avaya Communication Manager combines the legacy architecture of its predecessor, Definity ECS, with the IP Telephony Standard H.323 Media Server/Media Gateway architecture. This enables the County to leverage its current infrastructure and minimize capital outlays. With Communication Manager, Definity ECS Expansion Port Networks (EPNs) become Media Gateways that communicate with new S8720 Media Servers via IP addresses. The existing cabinets and cards continue to provide service, enabling the County to continue to support legacy requirements for as long as needed. New media gateways are added as either chassis based G650s or H.248 switches that have call processing elements built in. IP endpoints can be supported from either the legacy gateways or the newer H.248 gateways. All the capabilities and features that previously existed in the system carry forward to the new gateways. And new features and capabilities are now available to existing users as well.

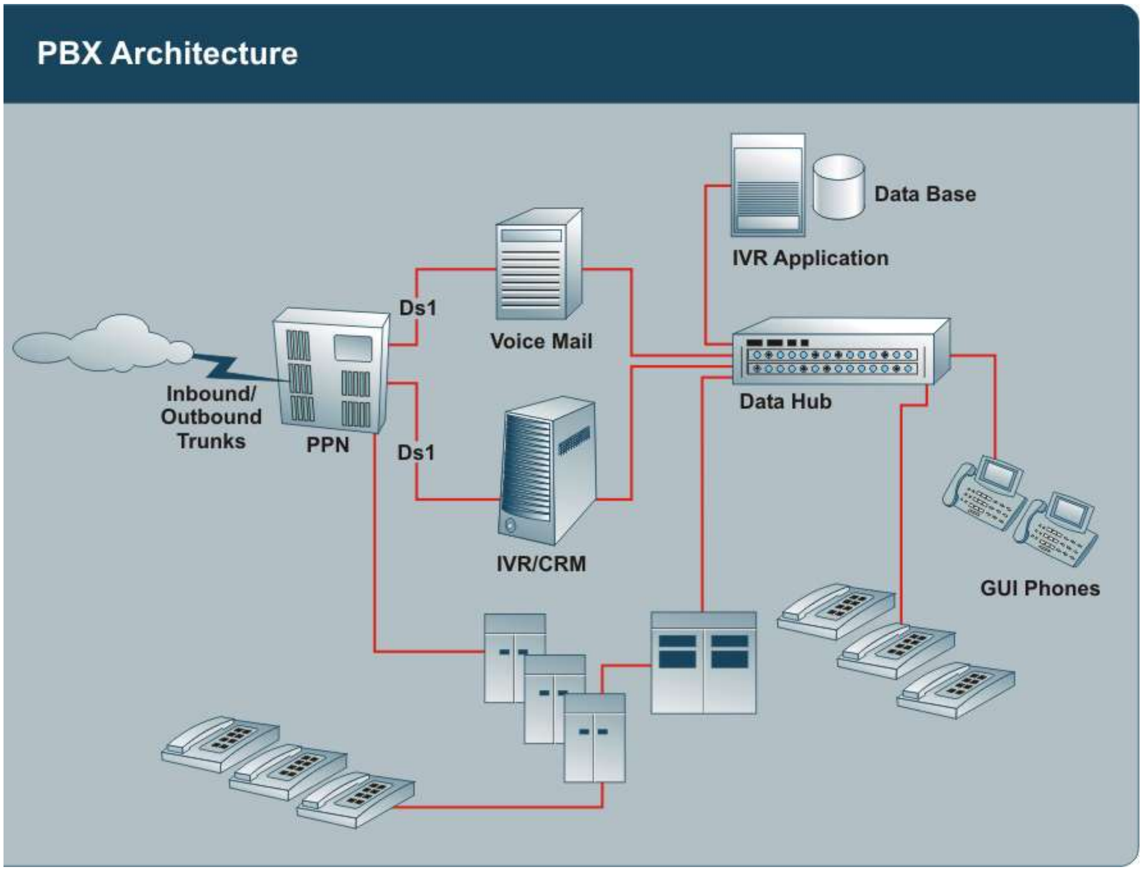


Figure 3-13 PBX Network Domain

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
PBX System Administration programming
Network wiring techniques
Call Center Vector programming
PBX network Design and Installation
VoIP

Standards and Guidelines

- The County conforms to security standards for G3r systems as outlined in the Avaya Toll Fraud and Security Handbook [2]
- All new endpoints are added as VoIP
- Critical Phone numbers are identified through department's telephone services administrators. The PBX Network team uses a backup switch during critical failures and during switch maintenance to keep these numbers operational.

Disaster Recovery

The PBX Network team has several Disaster Recovery solutions in place. The first solution relies on 24x7 monitoring support from Avaya and maintenance by the DTS PBX Team of an On-Call PBX Administrator who is informed of any outages by Avaya. The On-Call PBX Administrator determines the severity of the outage and manages the resolution of the issue.

To maintain availability of critical telephone numbers the PBX Network Team has a backup switch that can support the critical phone numbers during periods of switch maintenance or critical failures.

Finally, departments like MC311 who have their own endpoint switch are connected to the main County PBX switch. Disaster recovery support can be provided on a case by case basis with the department whereby the failure of the endpoint switch or the main County switch can be recovered through the other switch. In the case of VOIP phones the phones can be configured to failover to the other switch for services during a failover. Ability to dial out is maintained with the ability to accept incoming calls requiring additional support which is again provided on a case by case basis.

[2] Avaya Inc., *Avaya Toll Fraud Security Handbook*, May 2003

3.12 Record and Document Management Domain

Principles

The Record and Document Management Domain is Montgomery County’s integrated, comprehensive enterprise approach to centrally administer and manage all County electronic records.

The Records Management function for Montgomery County is the responsibility of the Department of General Services (DGS), Division of Real Estate Management Services Section. They own the responsibility for Records Management in the County which includes both physical and electronic records. They define the policy the County will follow, enforce the policy, provide education on the policy, define the tools (warehouse and IT) that will be used to implement the policy, etc.

Records Management is a management discipline that is responsible for the control of official records. It is a methodology for defining important records, their safe storage, how they can be used, how long they must be retained, and when they can be destroyed. A data retention policy is an important aspect to the Records Management function.

The DTS Core Systems team supports their IT Requirements by maintaining a Document Management/Imaging solution. The solution accommodates records from virtually any source, including scanned documents, electronic files (e.g. Microsoft Word, PDF, JPEG, etc), e-mails and attachments, COLD reports and other business applications.

The Document Management/Imaging function is integrated with Records Management which manages the life cycle of the records. The records are kept in the system during the active period when records have the operational value. The inactive records are archived for records management in accordance with the retention policy.

DTS will maintain a Record and Document Management section on the DTS departmental homepage on the Intranet Portal. The Record and Document Management section will contain information about the service as well as an intake form and a roles and responsibility document. Finally, it will contain a directory listing for the electronic Records and Document management sites.

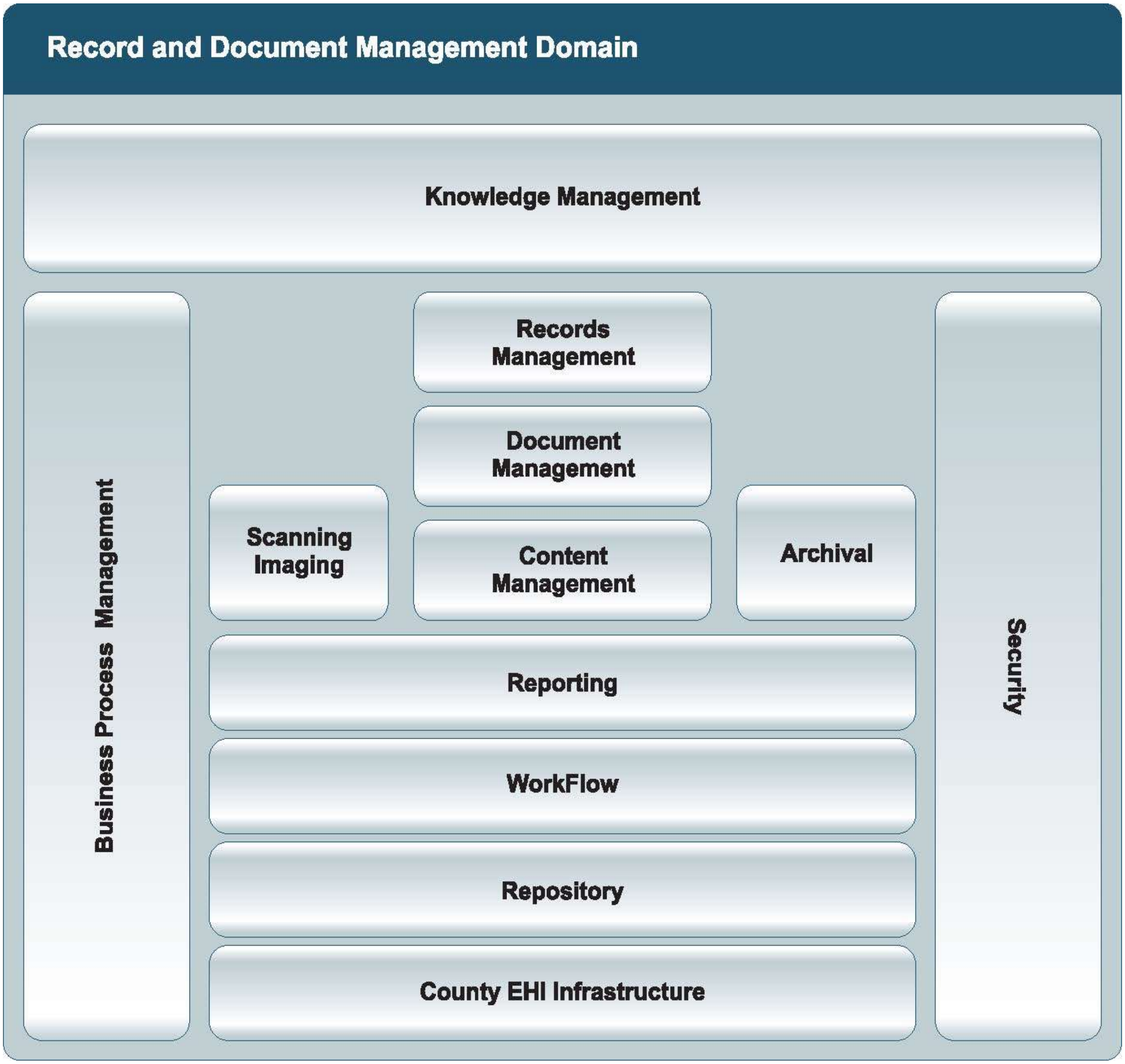


Figure 3-14 Records and Documents Management

Owners

Business Owner

The business owner for this Domain is DGS's Division of Operations Support Services Section.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

The DTS Core Systems Team supports the ZyImage Enterprise Web Server for storage of electronic records and documents.   The ZyImage Enterprise platform provides functions for office workers to capture, manage, publish, share, and archive information throughout its entire lifecycle in a single document repository. It is designed for performance, flexibility, and reliability.

The ZyImage system leverages the other Architecture domains including the Deployment Domain, Network Domain, Help Desk, Active Directory, Service Enabled Domain, Enterprise Server Management and System Operations Domain.

When groups are given access to the system their area and content are restricted to an Active Directory group that is under the control of their Department. The owning Department controls membership within that Active Directory group.

The platform has an open architecture, conforming to standards like ODBC, LDAP, Active Directory, TCP/IP, XML, COLD, .NET, and NARA/ERA and offers a robust fuzzy search and retrieval engine. System integration can be done through common gateway interface (cgi) coding to integrate with Microsoft office applications and web applications, or ZyImage Application Integrator. ZyImage accommodates records from virtually any source, including scanned documents, electronic files (e.g. Microsoft Word, PDF, JPEG, etc), e-mails and attachments, COLD reports and other business applications and synchronizes with databases like Oracle, SQL and Access.

The following modules are major ZyImage elements working together to support the enterprise document management and records management need:

- Zyscan converts paper documents and existing image formats into searchable online information. By digitizing the paper documents into electronic format, records become searchable.

- ZyIndex converts and manages scanned and electronic information. This module has a timer program to index all data collection. It also creates web clients for different applications.

- ZyCold automatically converts digital spool files into ZyImage searchable files, and adds key fields for key-field search and full-text retrieval.

- ZyImage for Forms interprets all common types of characters in paper forms, whether they are machine-print (OCR), isolated handprint (ICR), alpha and numeric mark sense (OMR) or bar codes.

- Records Management and Archival plug-ins enable storage of documents into a data repository from County standard desktop applications such as Microsoft Outlook, Microsoft Word, Microsoft Excel, Microsoft Internet Explorer and Adobe Acrobat.

- ZyFind allows searching, finding and organizing the documents in the data repository.

- ZyPublish copies data onto a CD or a DVD, and makes the data searchable.

- ZyImage webserver allows users to share indexes and data over the intranet. Using the browser, authorized users can search information.

- Records Management converts ZyImage into a record-management system and allows users to manage and search records.

- Document Management adds the additional functions of version control and check-in/check-out, to enable multiple users to work on the same set of documents. This module integrates with Microsoft Office XP applications.

- Workflow allows users to route documents through an organization, according to a specific pre-defined path.

- Audit Trail stores all user activities (such as searching, viewing and editing documents and opening, deleting, and building indexes) in an XML file.

- Advanced Security modules provide document-level security options. The document groups are based on the contents of key fields and protect documents from unauthorized access. The system looks up users in Active Directory and set security rights for specific functions such as building, deleting, and creating indexes and editing, deleting and merging documents.

- Bates Stamping module provides every document and page a unique identifier which can be placed on the original images during the ZyFind export or printing process.

- XML Wrapper modules generate a universal key field structure over scanned paper and electronic file formats. This module connects electronic files to an XML file containing key-field information.

- Application integration enables ZyImage integration with other systems. This module will enable the County to integrate with other business applications.

- ZyAlert modules enable selective dissemination of information. It automatically detects relevant information in huge indexes and sends notification when the requested information is found. This module acts as an information agent which searches the data at set times, based on user profile.

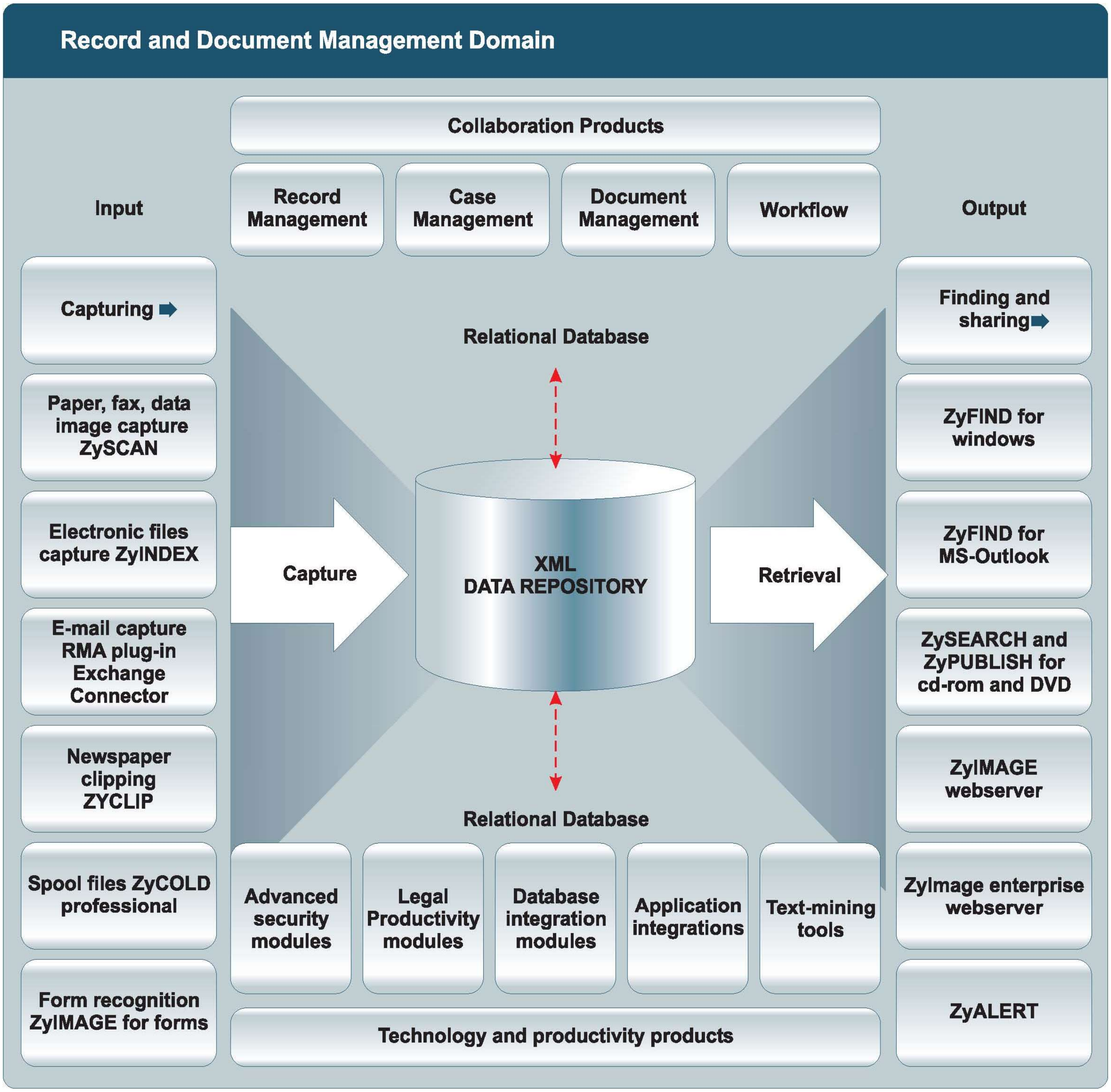

Record and Document Management Domain
Collaboration Products
Input
Record Management
Case Management
Document Management
Workflow
Output
Capturing
Paper, fax, data image capture ZySCAN
Electronic files capture ZyINDEX
E-mail capture RMA plug-in Exchange Connector
Newspaper clipping ZYCLIP
Spool files ZyCOLD professional
Form recognition ZyIMAGE for forms
Relational Database
Capture
XML DATA REPOSITORY
Retrieval
Relational Database
Finding and sharing
ZyFIND for windows
ZyFIND for MS-Outlook
ZySEARCH and ZyPUBLISH for cd-rom and DVD
ZyIMAGE webserver
ZyImage enterprise webserver
ZyALERT
Advanced security modules
Legal Productivity modules
Database integration modules
Application integrations
Text-mining tools
Technology and productivity products

Figure 3-15 Record and Document Management Domain

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Microsoft Windows Operating system knowledge and experience
Microsoft Windows Applications
Data Base Management - Oracle and Microsoft SQL knowledge and experience

Records Management
Visual Basic
Networking
Active Directory
HTML, XHTML
XML, XSLT
Java
ASP.Net
SOAP

Standards and Guidelines

The County needs to comply with the rules and regulations of Montgomery County, the State of Maryland, and the Federal Government. Some of the standards that must be taken into account are HIPAA, Sarbanes-Oxley and COMAR 14.18.02 to 14.18.05 to ensure that vital records needed for business purpose are retained, organized, protected and searchable. The following guidelines should be applied to a document before it enters records management**.**

- Inventory the records (the official documentation of business activities)
- Categorize the records generated. State laws allow records to be grouped into categories (contracts, personnel records, etc.).
- Prepare the metadata, or taxonomy so that the records can be searched
- Consider the format of the electronic data
- Identify the employees responsible for maintaining the record
- Preserve the data and determine how long specific types of records should be maintained.
- Manage hardcopy and electronic documents (including computer generated documents and email)
- Give instructions for disposal of certain records, and update the retention schedule
- Establish procedures for ensuring compliance with the policy
- Enable historical preservation of the County records if it is required
- During litigation:
    - Provide documents and preserve evidence to support positions in litigation
    - Suspend the destruction schedule
- Permit the disposition, discard unnecessary records, and reduce storage costs.
- Comply with federal laws and state-specific requirements
    - COMAR (Code of Maryland Regulations 14:18:04 Electronic Records)
    - HIPAA (Health Insurance Portability and Accountability Act)
    - MPIA (Maryland Public Information Act)
    - NARA/ERA (National Archives and Records Administration/Electronic Records Archives)

Collaboration Agreement

- A requesting team or department must read and agree to the Record and Document Management Agreement. The Record and Document Management agreement lists roles and responsibilities for the service.

Records Management Administrative Procedure

Montgomery County Office of Management and Budget – Administrative Procedure 6-3, September 8, 1975; *Records Management Addendum*;

3.13 Reporting Domain

Principles

The County has two Enterprise Reporting packages with one being Crystal and the other Oracle's OBIEE.

The County uses the Crystal Reports package to meet its diverse non-ERP Enterprise Reporting requirements. The County uses Crystal Reports outside ERP because it offers distinct capabilities and optimizes the use of software licenses.

The County uses OBIEE for its Oracle based ERP suite of products and for its ERP domain data warehouse.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are the:

- DTS Core Systems Team (Crystal)
- DTS ERP Project Team (OBIEE)

Components

Crystal Reports

Crystal Reports is used to develop reports to various data sources, including On-Line Transaction Processing (OLTP) systems. Crystal Reports is comprised of the Crystal Reports Designer (CR) and Crystal Enterprise Server (CE). CR is used for report development and is a package which installs on the developer's desktop. Its design allows for control over data access and presentation and offers a variety of formula functions, operators report formatting, complex logic, and data selection. Once developed, the report is then made available or "published" to the CE server.

The CE server is a web-enabled server, which runs on the Windows operating system. Connectivity to all data sources is through Open Data Base Connectivity (ODBC). Current data sources are Oracle, MS Access, PC-based DB2, and MS SQL Server. Other standard data sources are supported. The County is licensed for unlimited connections, and currently hosts 1,500 clients and 2,400 reports. Access by other non-County government entities is provided. The CE server is very scalable, and allows for specific growth options as required.

Clients access the published reports through a desktop client browser from the CE server. Additionally, several applications have been developed in-house which call CR reports directly from the server, bypassing all direct user input. J2EE is the standard application development platform. CE supports Single Sign On by authenticating users with the County's Active Directory (AD). Security for report access is based on individual accounts and AD group membership. Enhanced security is available and can be applied to users, groups, or reports.

Once a report request has been processed on the CE server, the report can be accessed using the following methods:

- Web browser
- PDF (Adobe Acrobat)
- Excel
- Word

Additionally, reports can be scheduled to run once or on a schedule. Users can view the latest or a previous "instance" of a report. Reports can be deposited to file shares or sent as an email attachment in the desired format. Report parameters can be entered via custom application interfaces or directly by the user. Reports can be integrated and are viewable from within an application.

OBIEE

OBIEE is Oracle's strategic reporting platform and as such the County is using OBIEE to perform reporting across the ERP's Oracle suite of products and the ERP data warehouse. OBIEE is different architecturally than Crystal in that report writers do not generally have direct access to the data source. Instead, OBIEE supports a modeling paradigm where a logical data model is developed against the data source. This modelling is currently supported by developers in the ERP project team. Once a model is developed and validated with the data owner it is published to report writers who then can develop reports and dashboards against the published data models. OBIEE supports authorization and the reports can be role based limited.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Crystal Reports Designer
Windows Server Administration
Crystal Enterprise Server Administration
OBIEE Administration

Printer Administration
Network concepts and administration
ODBC configuration management
Active Directory concepts and administration
Relational Data Base concepts
Desktop configuration for Crystal clients
Troubleshooting skills
DBA knowledge and administration

Standards and Guidelines

Crystal

Reports must be tested using Crystal Reports from the developer, then tested using Crystal Reports on the CE server, and then tested in “published” form.

Access to reports must follow security guidelines. Applications which call published Crystal Reports from the CE server should be developed using J2EE. This will provide for secure transmission of the user name, password, and report contents over the intranet and internet.

Direct access to the CE server via a Web browser requires AD authentication. For example, to access published Crystal Reports, the requestor must have a user account in Active Directory.

There are two kinds of accounts that access Crystal reports, those which are imported from AD and those which are created on the Crystal Enterprise server. The accounts created on the Crystal Enterprise server are not authenticated with AD, and they do not support Single Sign On (SSO). Applications that directly call reports from the CE server use these accounts. This assumes that acceptable security is provided from the application for intranet-only applications. If it is not provided, the application should be developed using J2EE.

Large additions (more than 50 reports), or major applications that rely heavily on Crystal will be examined for their effects on resources. This will be done to ensure satisfactory performance for existing and new application users. The number of reports, their complexity, frequency of generation, and average and maximum concurrent users will be reviewed. From this, the County may determine the potential effects of change on the CE servers.

OBIEE

The ERP technical team is the sole creator of the logical data models.

Report writers are given access to the logical data models to create dashboards or reports

OBIEE supports role based authorization that is provisioned from the Identity Management System (See Identity Management Domain)

3.14 Service Enabled Domain

Principles

The Service Enabled Domain promotes the development of robust, scalable, and flexible services for business integration with the County infrastructure. The goal is to achieve a cooperative and secure service and data sharing environment, and to avoid data replication

The County recognizes the importance of developing Services capable of integration with internal and external systems. These Services will be designed and implemented, based on events and messages. An event-based, messaging model will help avoid stovepipes (rigid, self-contained functionally organized service solutions for each department, not acting as a single-entity).   To do this, the County hosts a healthy mix of services. Some have been developed in-house, and some are COTS (Commercial Off-The-Shelf) solutions. Each application will document and publish well-defined interfaces to the protocols identified in this section.

An events-based messaging service will foster the maturation of service implementations based on Service Oriented Architecture (SOA). The County encourages the use of XML to define event messages, Web Services technologies for integrating .NET and J2EE services and Enterprise Java Bean (EJB) for integrating J2EE services. The following table lists the County's supported protocols.

Protocols
Message Q
Enterprise Java Bean (EJB)
Java Messaging Services (JMS)
Service Oriented Access Protocol (SOAP)
Secure Hypertext Transfer Protocol (HTTPS)
Web Services Description Language (WSDL)
Universal Description Discovery and Integration (UDDI)
Representational State Transfer (REST)

Table 3-17 Service Enabled Domain Protocols

Enterprise Service Bus (ESB)

The County has deployed and maintains a distributed event services environment for communications between peer Services. This event service environment uses the SOA architecture pattern called Enterprise Service Bus (ESB). ESB is a specific server implementation of Service Enabled Domain services. ESB provides the feature capabilities listed in table 3-18.

Features
Protocol Switching
Message Routing
Message Transforms

Message Transports
Message Security
Message Aggregation/Splitting

Table 3-18 ESB Feature Capabilities

ESB provides a rich, event-based messaging infrastructure that aids the implementation of complex Service Enabled Domain Services and client consumers. Figure 3-19 shows a modular overview of the ESB.

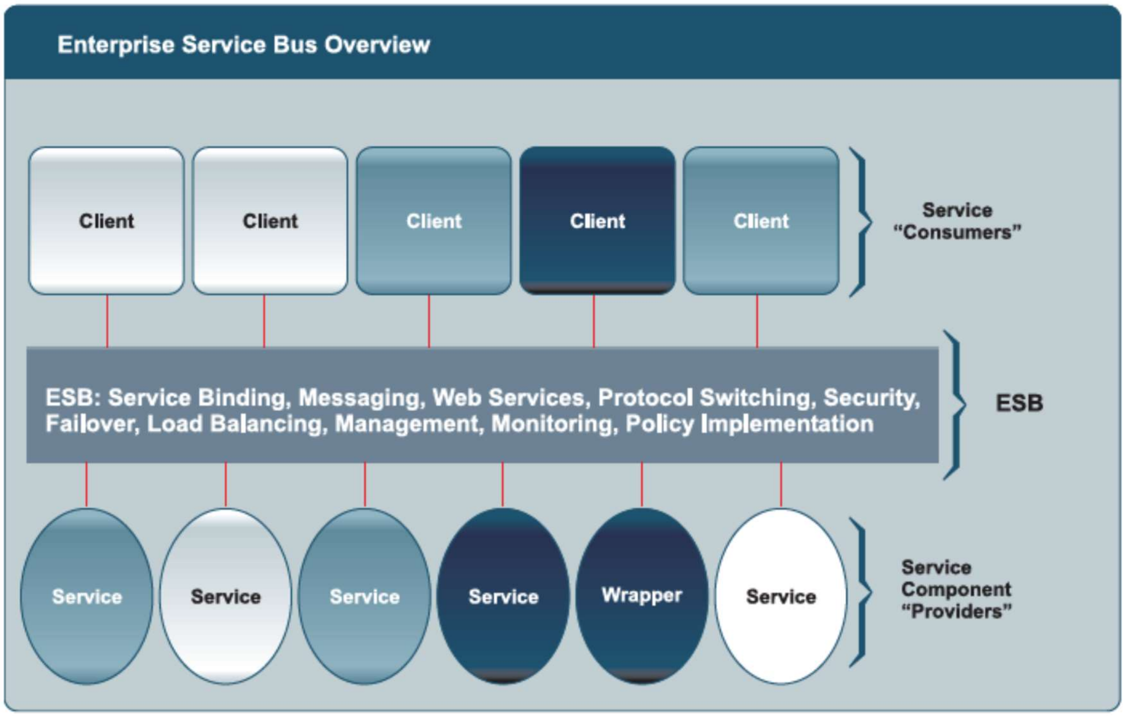

Enterprise Service Bus Overview
Client
Client
Client
Client
Client
Service "Consumers"
ESB: Service Binding, Messaging, Web Services, Protocol Switching, Security, Failover, Load Balancing, Management, Monitoring, Policy Implementation
ESB
Service
Service
Service
Service
Wrapper
Service
Service Component "Providers"

Figure 3-19 Enterprise Service Bus Overview

Compared to a home-grown Service Enabled Domain hosting environment, the standards-based ESB provides extreme flexibility for future integrations and extensibility.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Enterprise Services Architect.

Components

The County will deploy a distributed environment for communications between peer Services. With the development of a robust collection of Business Objects, their Service Interfaces and bindings will expose functions to other applications. Figure 3-20 shows an integration scenario for Services using ESB.

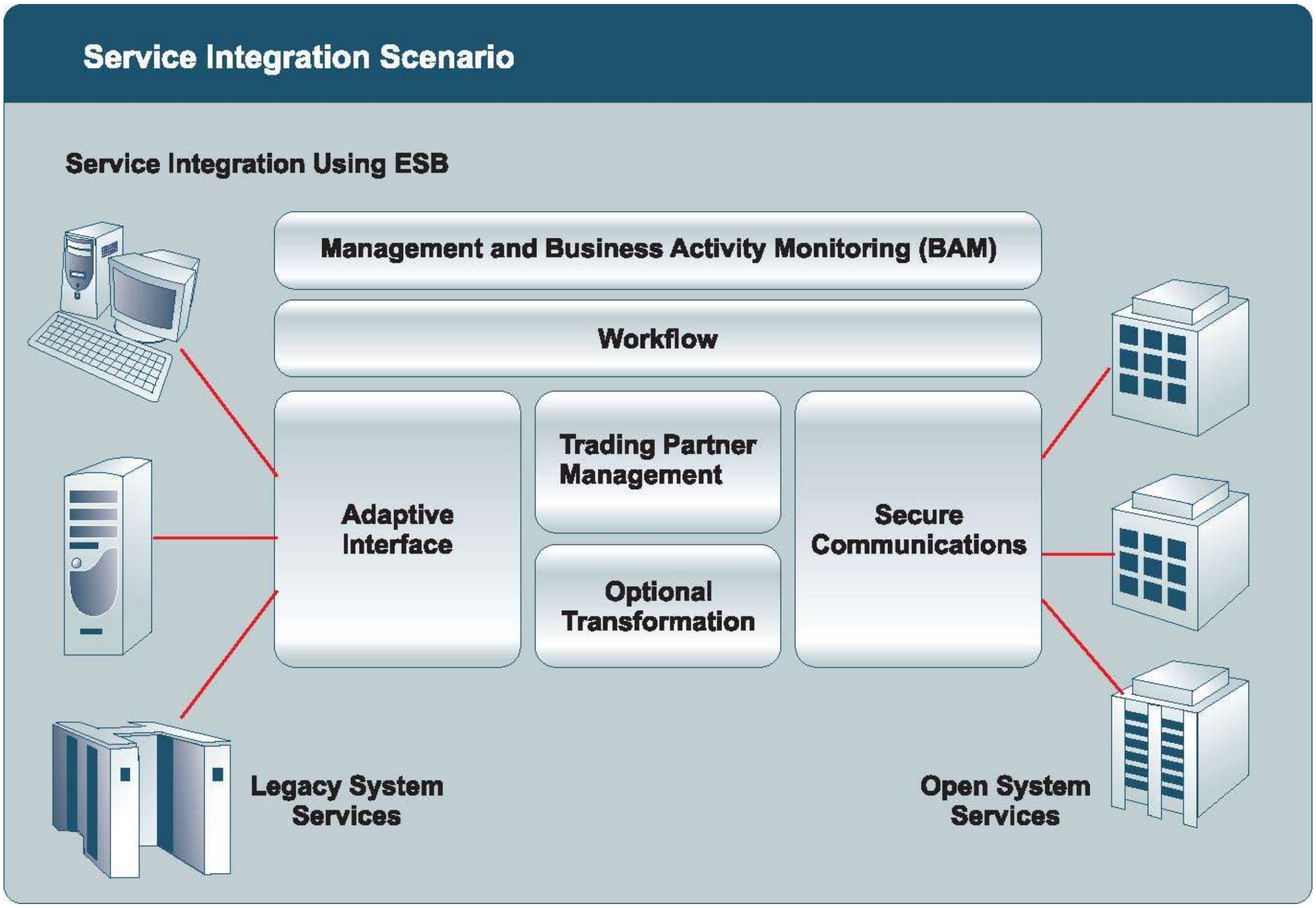

Service Integration Scenario
Service Integration Using ESB
Management and Business Activity Monitoring (BAM)
Workflow
Adaptive Interface
Trading Partner Management
Optional Transformation
Secure Communications
Legacy System Services
Open System Services

Figure 3-20 Service Integration Scenario

As Figure 3-20 shows, the County encourages the development of wrapper services for legacy system services. This is to enable legacy implementations to participate in event-based Service Enabled Domain.

The County encourages Service providers and consumers to document the message structure, format, data requirements, and security requirements. It also encourages documentation of the event generation, flow, security, and other SLA requirements. For secure communications, the County is using messaging protocols such as HTTPS (for Web services, and normal web calls) and JMS on WebSphere MQ (channels secured as needed). Business Objects may be implemented as EJB, Message Driven Beans or Java objects.

To accommodate diverse technologies, the County recognizes the value of a Service Oriented Domain, and plans to develop an infrastructure to support Web Services . The County encourages Services to be implemented to comply with industry-published standards and specifications like the Web Services – Interoperability Basic Profile (WS-I BP), which minimally includes vendor-neutral components such as SOAP, WSDL, UDDI and XML and XML Schema.

Security issues are associated with Web Services and other messaging services, and the County will proceed with caution as the technology matures. The County strongly recommends encryption of data in transmission. Upon review of a service and the content of its messages, the County may mandate data encryption. The ESB platform which the County hosts contains a standard set of data encryption capabilities, such as PGP. The County will reserve the right to review the publication of Services (via JNDI or UDDI) both within and outside its Intranet boundaries. Data transmissions to and from systems external to the County will be reviewed and approved on a case-by-case basis.

The County will encourage data transmission in XML format (where the technology permits), particularly in domains where industry standards exist. The County views XML as the interoperability "glue" that allows systems being developed to communicate with each other. It paves the way for future expanded collaboration. This XML data transmission architecture is technology independent, therefore it will work with both J2EE and .NET protocols. Also, XML data transmission architecture on an ESB platform provides a seamless mechanism to transform message data for the requirements of other services and consumer clients. The following Figure 3-21 demonstrates the County's Service Enabled Domain.

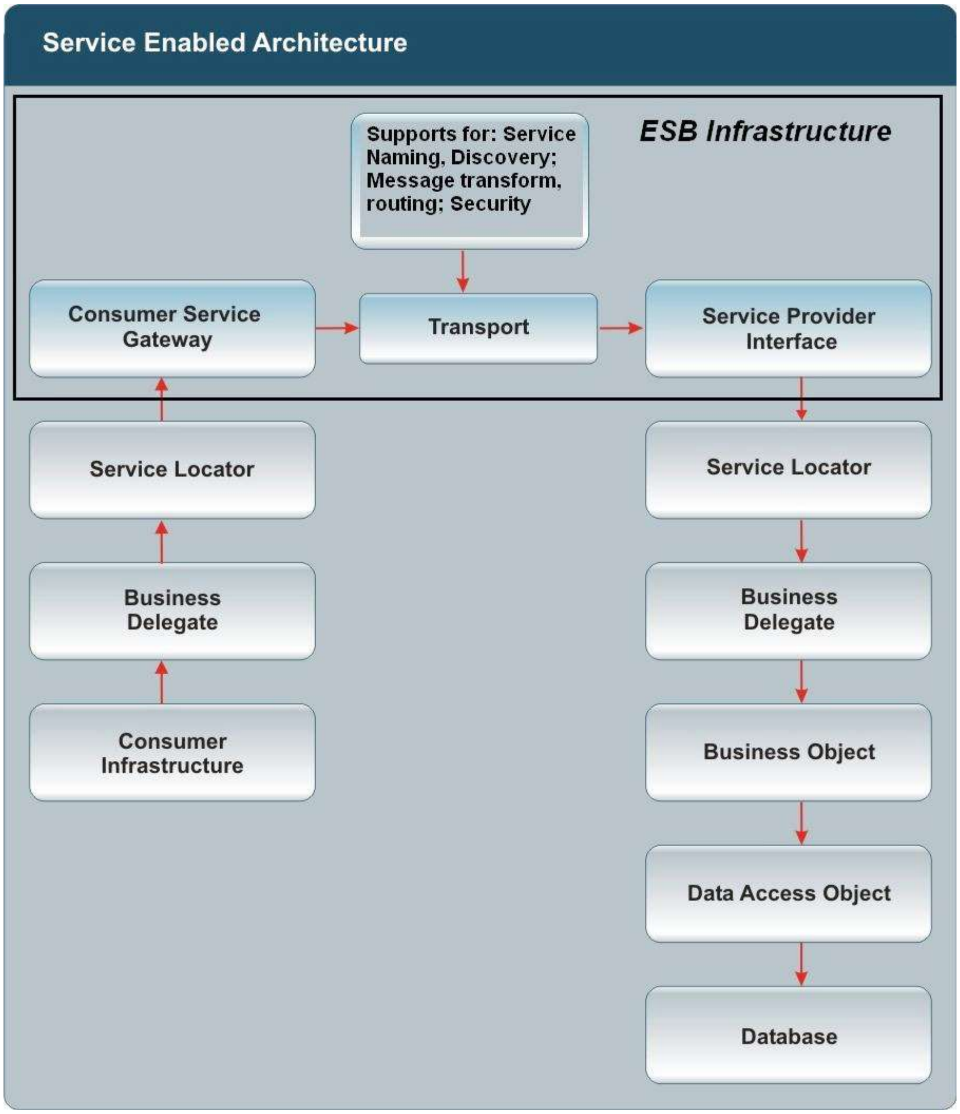


Figure 3-21 Service Enabled Domain

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
WebSphere MQ
Java Message Service (JMS)
Enterprise Service Bus (ESB)
Web Services
Enterprise Java Beans (EJB)
Simple Object Access Protocol (SOAP)
Representational State Transfer (REST)
XML
XSL Transformations (XSLT)

Standards and Guidelines

The County has standards for Java files to have the following package structure:

gov.montgomerycountymd.<<dept>>.<<application>>.<<module>>

where

dept will be the short name of the department that owns the application
application will be the short name of the application itself
module will be the implementation section.

The County has standards for .NET namespace:

gov.montgomerycountymd.<<dept>>.<<application>>.<<module>>

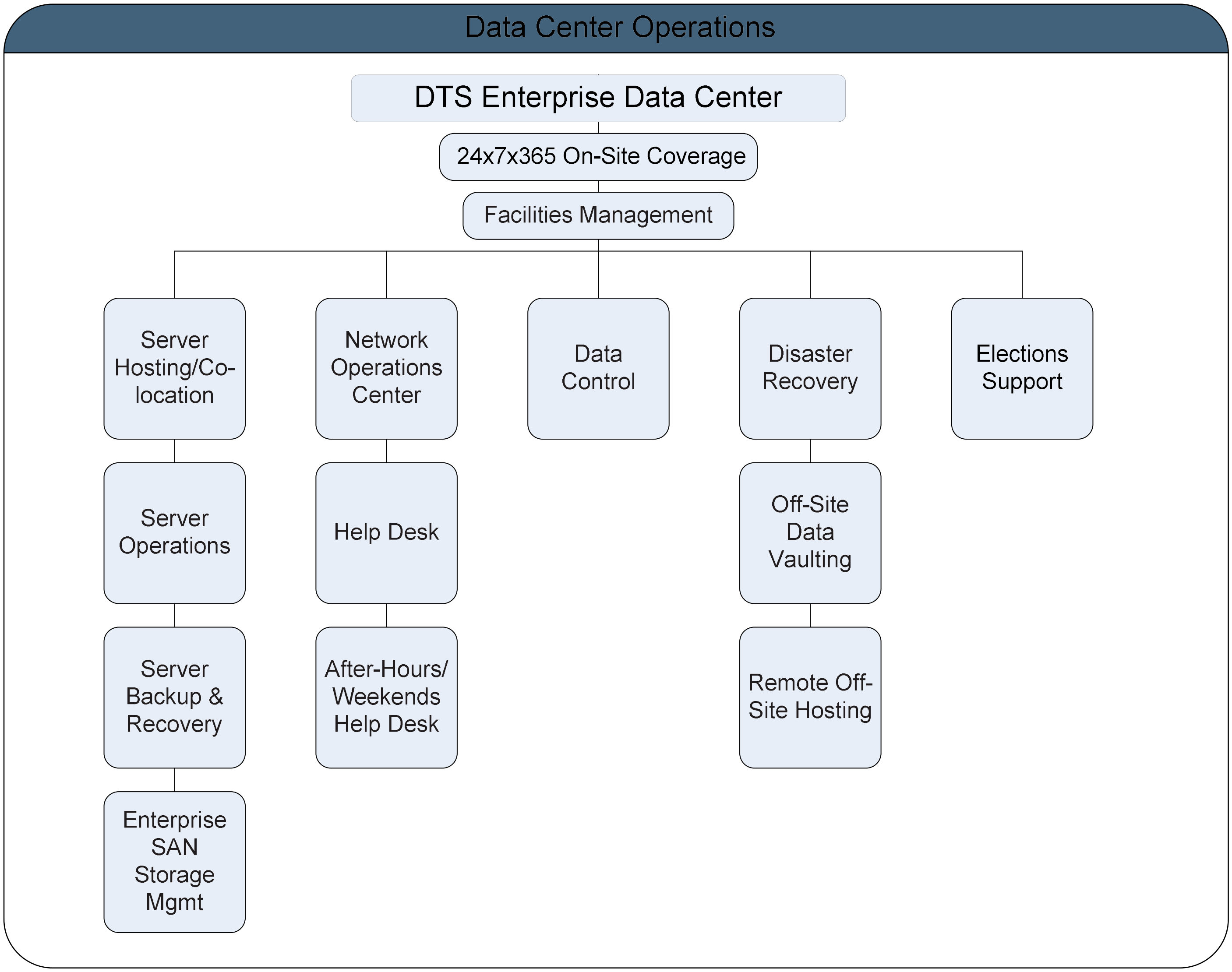
where

dept will be the short name of the department that owns the application
application will be the short name of the application itself
module will be the implementation section.

3.15 System Operations Domain

Principles

Data Center Operations provides first-line operational and virtual support and security (24-hours per day, 7-days a week) for mission critical servers and main network hubs that reside in the County's Enterprise Data Centers. Major support services provided by the team include server and Storage Area Network (SAN) operations, server backup/recovery, server hosting and system/network monitoring (NOC), and Data Production Control. Data Center Operations coordinates the Disaster Recovery plans and test exercises for several of the County's mission-critical systems. Operations protects the secured Data Center environments around the clock from power outages with UPS units and diesel generators. A constant climate controlled environment for the Data Centers is provided as well as fire protection and suppression systems. All hardware equipment is housed on a raised floor.



Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Data Center Operations Team.

Components

Data Center Operations Services:

Server Hosting/Co-location:

Server hosting and co-location services for Dell Intel and various appliances from DTS and other County Departments/Agencies. The County's main Network Hubs and voicemail system are located in the Data Centers. Physical security provided by card access only entry and closed-circuit video surveillance. 24x7 conditioned power uptime provided by a UPS unit connected to a diesel generator supplied by underground fuel tanks. All equipment is housed on a 12" raised floor and all rack cabinets are equipped with dual PDUs for power redundancy, and KVM over IP console switches for remote access. For network connectivity, each rack connects to a Cisco switch configurable for accessing any segment on the County's network. Backup & monitoring is provided 24x7 for all equipment housed in the Data Centers.

Server Backup and Recovery:

The Data Center Operations team uses Symantec Veritas NetBackup v6.1. There is one NetBackup Master server that houses the main tape catalog and is where master scheduling and control is done. Communicating with the NetBackup Master are Multiple Media Backup servers with either LTO-2 or LTO-3 tape libraries attached to them. The Media Backup servers are located closer to the data that is going to be backed up and is where the data is physically backed up to.

Oracle database backups are exported to a file, which is then automatically picked-up by the nightly backups. Veritas's NetBackup Oracle and RMAN database agent is used for online backups of the Oracle databases. The Oracle database servers are connected to the Nexsan ATABeast or SATABeast disk arrays for disk-to-disk backups, which are also backed-up by the Veritas tape backup server.

Symantec Veritas Backup Exec v10 is also used for backups on various Windows based systems.

Backups are performed every day according to the following schedule:

- Daily (Incremental) - Monday thru Friday
- Weekly (Full) - Saturday
- Off-site (Full) - Sunday
- Monthly (Full) - 1st Saturday of each month

Server Backup Reporting provided by Aptare's StorageConsole v6.05

Monthly auditing of the server backups are performed by Operations and various server support teams.

Backup Retention Schedule

Backup	Retention Time
Daily	21 days (3 weeks)
Off-site (Full)	21 days (3 weeks)
Monthly (1st Weekend)	91 days (13 weeks)

Enterprise SAN Storage Management:

SAN Storage/Fabric Management & Operations of the County's Enterprise Dell/EMC CX500 Storage Area Network connected to a Connectix 1600 Fiber Channel Switch. Nexsan ATA/SATABeast SAN used for server hosting services and D2D backups and VTL (Virtual Tape Library) connected to QLogic 5202 Fiber Channel Switches. QLogic 2354 Host Bus Adapters (HBA) used by clients connecting to the various SAN configurations. SRM tool by Aptare is used for reporting purposes.

Network Operations Center (NOC):

Server, System & Network Monitoring of all systems located in the Enterprise Data Centers and various mission critical systems Countywide. CiscoWorks & WhatsUp Gold monitoring software used. Operations performs the coordination between Verizon & AMS for completing the trouble tickets on data circuits or switches involved.

Off-Site Data Vaulting:

Daily off-site data storage vaulting of backup tape cartridges to the County's offsite data storage vendor, Monday – Friday. Emergency 2-hour tape callback available upon special request.

Facilities Management:

Data Center Infrastructure Management and monitoring. Includes electrical power, UPS, air-conditioners (cooling) and fire suppression system management. Card Access entry system and CCTV used for maintaining security of the Data Centers 24x7. Electrical branch circuit and room temperature monitoring is performed by Intellipool Network Monitor.

Hardware Used	**Software Used**
Dell Power Edge 2850 Dell Power Edge 1855 Blades	Microsoft Server, Redhat Linux

Dell PV132T LTO-2 Tape Library Dell PV136T LTO-3 Tape Library Dell MLM6010 LTO-3 Tape Library FalconStor VTL	Ipswitch WhatsUp Gold Aptare StorageConsole Falconstor IpStor
Dell/EMC CX500 Disk Array/SAN Dell/EMC B162 Fiber Switch Nexsan ATA/SATAT Beast Disk Array/SAN QLogic 5202 Fiber Switch	Veritas NetBackup Enterprise v. 6.1 Veritas NetBackup Oracle/RMAN Agent Veritas Bare Metal Restore v. 6.1 Veritas Backup Exec v10

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Microsoft Windows and Redhat Linux System Administration
Hardware Management and Troubleshooting
Veritas NetBackup Enterprise Administration and Setup
Veritas Backup Exec Administration and Setup
FalconStor IpStor Administration and Setup
SAN Administration and Setup
Veritas Bare Metal Restore Administration and Setup
Help Desk & Customer Service Skills
Basic Networking Skills

Standards and Guidelines

For the Microsoft Windows, Linux, and Sun Solaris platforms, the County’s software standard for server backups is Veritas NetBackup Enterprise v. 6.1, and Veritas Backup Exec v. 10 as needed. LTO Tape Libraries containing 2 tape cartridge drives are attached to the backup servers. All server backup tapes are rotated off-site daily.

3.16 Team Collaboration

Principles

The County uses Microsoft's Office 365 (see Microsoft Office 365 Domain) for its Team Collaboration Services. This system supports the following collaboration opportunities for a group, project team, and department:

- OneDrive (Personal File Services)
- SharePoint (Group/Department Collaboration)
- Skype for Business (Conferencing)
- Office 365 Video

OneDrive

Every user with a County email address has access to Microsoft's OneDrive as part of the Office 365 service. Their OneDrive space is for storing their own user's files and can be used for limited sharing as well. Users are responsible for sharing their data and must not share sensitive data through anonymous links.

SharePoint Services

The SharePoint Service provides an easy to use online meeting space for internal County teams. Team members can come to a team portal and collaborate on projects using their desktop browsers. The collaboration service provides some of the following abilities to a team:

- Announcements
- Meeting Agendas
- Document Sharing
- Calendar
- Tasks
- Discussion Board
- Linking Ability

Every department has been allocated a departmental collaboration site for internal collaboration within their department. Access to the department site is by default limited to the department.

The Intranet Portal has also been implemented via SharePoint with each department having their own site that is linked into the main Intranet Portal. Access to these sites is open to everyone on the Intranet.

Skype for Business

Every user with a County email address has access to Microsoft's Skype for Business as part of the Office 365 service. Skype for Business supports user conferencing through video, audio, and messaging. The Skype for Business client has been installed on all Client Machines.

Office 365 Video

Office 365 Video allows the County to include Video services for our internal County Collaboration. It is like YouTube except the video and channels can be limited to only internal County Users

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Microsoft Office 365 Administration
Team Collaboration

Standards and Guidelines

- See Microsoft Office 365 Domain.
- Outage and maintenance reports through HelpIT updates
- Availability/Uptime
    - The system is designed to be available 24/7.

Disaster Recovery

See Microsoft Office 365 Domain.

3.17 Configuration Management (CM) Tools

Principles

The Configuration Management Tools Service provides the following functions to a team:

- Version Control Code Repository
- Version Control Document Repository
- Requirements Tracking
- Bug Tracking
- Issues Tracking

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Server Team.

Components

The County uses two Open Source tools to provide the above services. The Version Control functions are provided through the Open Source Subversion Tool. The Requirements Tracking, Bug Tracking, Issue Tracking and the rest of the Application Lifecycle Management functions are provided through the Open Source Trac Tool.

The Subversion Tool is an Open Source follow on to the CVS product. It contains most of CVS's features and many enhancements. Requesting teams will be provided with a subversion project for their use.

The Trac Tool is an Open Source tool that provides requirement, issue and bug tracking to a development/deployment project. Also, the Trac tool provides such project management features as Milestone tracking, Version Timeline tracking, Regression test reports and Custom reports. It can have an interface to a Subversion project where code checkins can be linked to bug reports (and vice versa).

When a team requests one of the above services DTS allocates an area on the Enterprise CM Tools server. DTS maintains the overall CM Tools server providing proactive server management and backup facilities. When a team requests one of the new services it is set up by the DTS CM Tools Administrator. The team must designate their own CM Tools Site Administrator, who will be responsible for the content and administrative duties for the site, including:

- adding and deleting users (Users must be County Active Directory members)
- management of the content

DTS will maintain a CM Tools section on the DTS departmental homepage on the Intranet Portal. The CM Tools section will contain information about the services as well as a directory of all CM Tools sites.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Subversion
Trac
Linux
Apache/SQLite

Standards and Guidelines

CM Tools Intake Form

A requesting team or department must fill out a CM Tools Service Request Form. The form must contain:

- type of tool – repository and/or tracking
- site description
- owning department
- administrator name
- group members (for initial AD group population)
- estimated project completion date

Collaboration Agreement

A requesting team or department must read and agree to the CM Tools Collaboration Agreement. The CM Tools Collaboration Agreement lists roles and responsibilities for the service.

3.18 Enterprise Server Management

Principles

The Enterprise Server Management Service provides the following functions for management of both physical and virtualized Enterprise Servers:

- Availability Monitoring
- Inventory Management
- Configuration Auditing
- Performance Monitoring
- Event Management
- Historical Data Tracking and Reporting
- Incident Alerts and Escalations

Owners

Business Owner

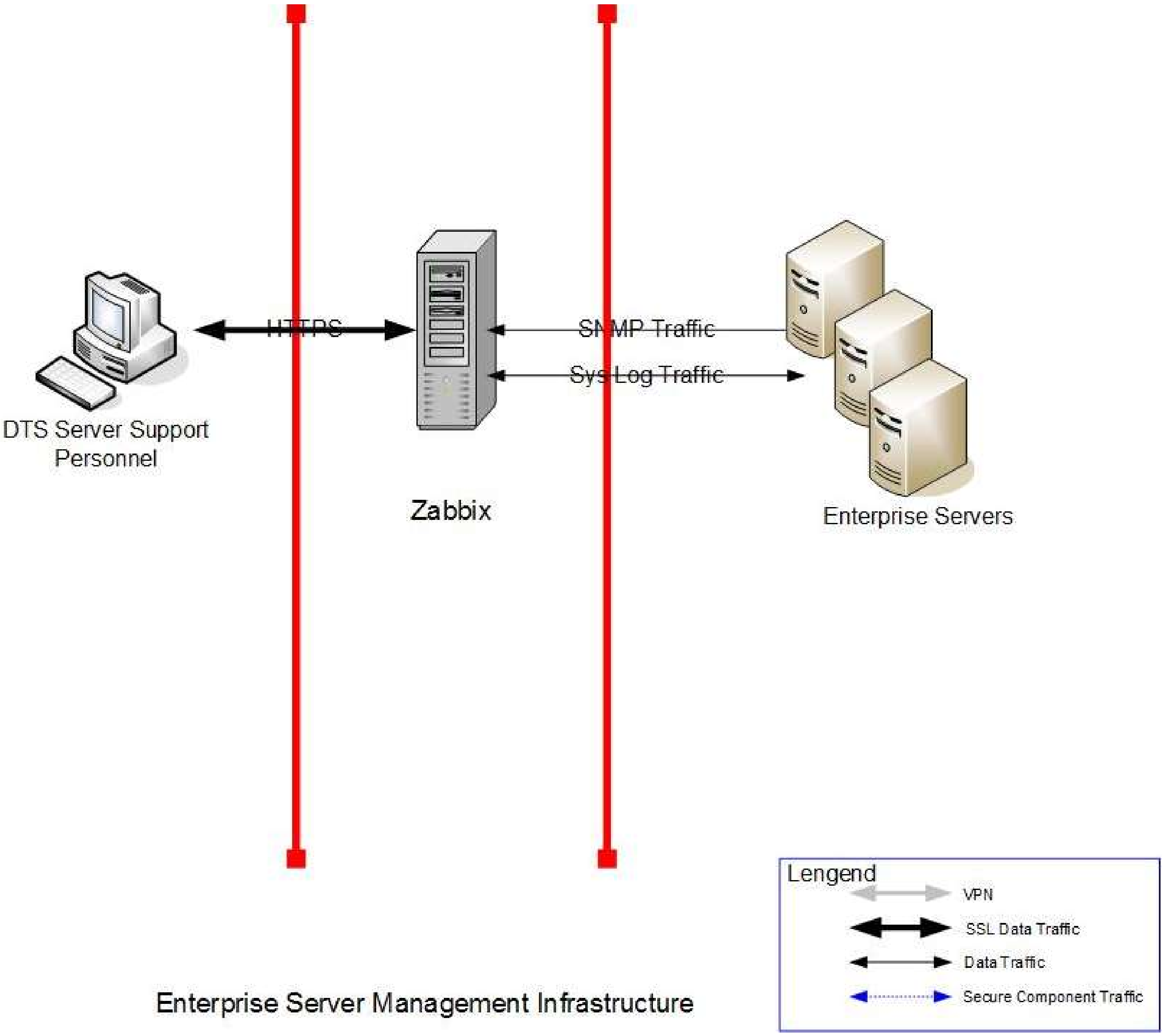
The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Server Team.

Components

Architecture Overview



Description

The County uses the Open Source Zabbix tool to provide the Enterprise Server Management Service functions to Enterprise Servers.

The DTS Server team runs an instance of Zabbix that has access to the Enterprise Servers that the DTS

Server Team manages. All physical and virtualized instances are modeled and monitored through the service.

Zabbix can support both agent based and a SNMP polling model. Server based machines will have the Zabbix agent installed on their system. SNMP will be reserved for devices that cannot support the agent.

The Zabbix server is protected by a firewall with access to the server restricted to DTS personnel.

Functions

The DTS Server team uses Zabbix as its primary Enterprise Server Management tool. It uses:

- the monitoring and alert functionality through the use of the Zabbix console during business hours. Server team members respond to system alerts that identify performance and system issues
- the ITIL CMDB standard inventory capability of Zabbix for rich modeling of the servers and their Patch Management and Update process
- the performance monitoring capabilities for proactive alerts and capacity planning exercises
- the email notification capability to alert DTS Server Team Members performing off hours support of critical alert errors such as “System Down”
- various real-time and historical reports

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
SNMP, SysLog
Zabbix, Python

Standards and Guidelines

- All EHI physical and virtualized server instances are monitored.
- All MCGOV Internet and Intranet Portal Servers are monitored
- Only DTS Support personnel have access to the Zabbix Server (SSO Integrated)
- SNMP probes in monitored physical and virtual Server instances are configured as Read Only. They respond ONLY to the Zabbix server. SysLog probes also respond ONLY to the Zabbix server

3.19 Software as a Service (SaaS)

Principles

The SaaS Domain supports the use of externally hosted applications by Montgomery County. This service provides support that solves the common issues around using an externally hosted application. The common issues that are addressed within the SaaS support are related to:

- Identity
- Security
- Single Sign On Integration (Internal SSO redirection, Open Source SAML, OAUTH, Microsoft ADFS)

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Enterprise Services Architect.

Components

The supported service makes use of the following components:

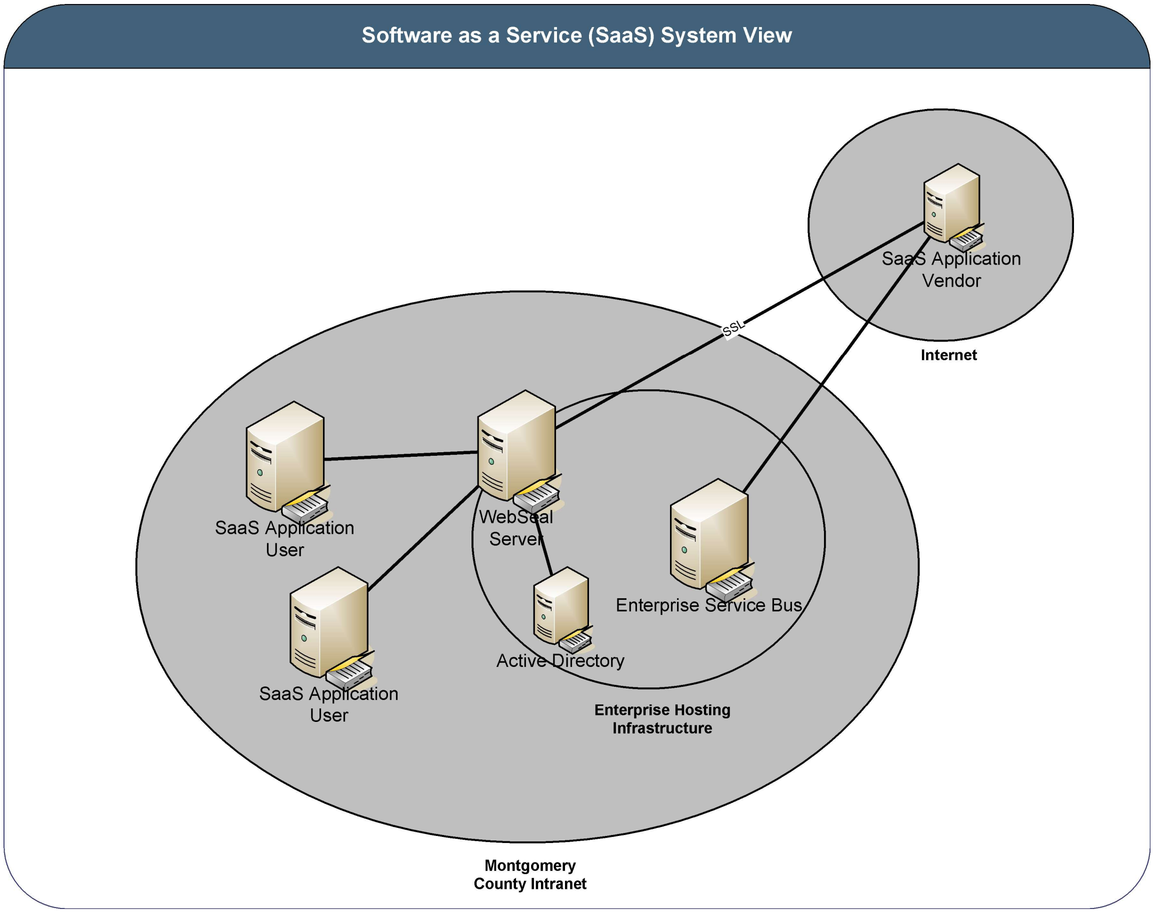
- Active Directory (AD) Services Domain
- Enterprise Hosting Infrastructure Domain
- Services Enabled Domain (ESB)
- Microsoft ADFS
- Open Source SAML
- Open Source OAUTH

Identity Management can be supported through one of four methods:

- Internal SSO Redirection
- MS ADFS
- Open Source SAML
- Open Source OAUTH

Which option that is selected depends on the cloud service and the method that the cloud service aligns with best.

Internal SSO Redirection



The Internal SSO Redirection uses the Enterprise Hosting Infrastructure (EHI) Domain. The EHI is used as a front end to the externally hosted application. Once the user signs on through the normal County single sign on challenge an encrypted tunnel is opened out to the hosted application provider. This support allows Departments to restrict access to the externally hosted application through the County Active Directory Domain. Users can be assigned to use the SaaS Application by the owning department through Active Directory.

MS ADFS and Open Source SAML

The County supports SAML service through either Microsoft ADFS infrastructure or through an Open Source implementation of SAML.

Enterprise Service Bus

Integration Services support centers around the use of the Services Enabled Domain. The County's Enterprise Service Bus is used to securely pull data from the externally hosted application back into County systems or push the data to the externally hosted application from the County systems.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Active Directory Domain Administration
Windows Server Administration
SAML
OAuth
ADFS
Understanding of Security Principles
Enterprise Service Bus (ESB)
Web Services

Standards and Guidelines

SaaS Application Administrator

When a department requests the new service, it must designate their own SaaS Application Administrator, who will be responsible for the content and administrative duties for the externally hosted application, including:

- adding and deleting users
- being the coordinator and document/security key-owner of integration implementation(s)
- being the primary contact to the SaaS Application vendor
- management of the content

SaaS Intake Form

A requesting team or department must fill out a SaaS Service Request Form. The form must contain:

- name of the externally hosted application
- description of the externally hosted application
- vendor information on the externally hosted application
- owning department
- administrator name
- group members (for initial AD group population)
- description of data that must be retrieved from the externally hosted application back into the County
- destination where the retrieved data should go
- estimated retirement date for the application

Collaboration Agreement

A requesting team or department must read and agree to the SaaS Agreement. The SaaS agreement lists roles and responsibilities for the service.

The SaaS Application vendor must support an encrypted SSL tunnel from the County to the application.

The SaaS Application vendor must support static IP Addressing to it's service.

The SaaS Application vendor must refuse connections to the SaaS Application from sources other than the encrypted SSL tunnel from the County

If data within the SaaS Application is needed by the Department the SaaS Application must support retrieval of the data by the County Enterprise Service Bus.

If data that needs to be retrieved by the Department has a high confidentiality or integrity requirement than the SaaS Application must support encryption of the data and key based access to the data.

Recommendations

County Attorney's Office list of issues that need to be considered when procuring a cloud solution (not meant as an exhaustive list but as a starting point)

DTS recommends a Cost Benefit Analysis that includes the full life cycle of the solution and data

Owning departments are still responsible for County Discovery, Records Management, and Security and Privacy Policies

3.20 Database Hosting Infrastructure Platform

Principles

The Database Hosting Infrastructure (DHI) is the framework the County uses to deploy its enterprise databases. The County's DHI goals are to host Enterprise Databases in a standardized secure environment in a cost-effective manner. The County benefits from DHI because its data is housed in a centralized manner that supports a centralized Data Architecture. Databases are documented with identified owners. Cost is reduced because the Data Owners benefit from the shared services offered by the Enterprise. The Shared Services not only includes the Database Servers but support services such as monitoring and backup.

DHI encompasses multiple components of the County's IT Framework: Deployment Domain, Network Domain, Security Domain, Help Desk, Active Directory, and System Operations Domain.

When a new Database is targeted to be hosted in the DHI an intake form is filled out for the database. The intake form contains information about the database with one aspect of the information being the NIST Confidentiality, Integrity and Availability requirements for the application.

Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of confidentiality is the unauthorized disclosure of information.

Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of integrity is the unauthorized modification or destruction of information.

Availability

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of availability is the disruption of access to or use of information of an information system.

The County database standard supports both Oracle and Microsoft SQL Servers.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

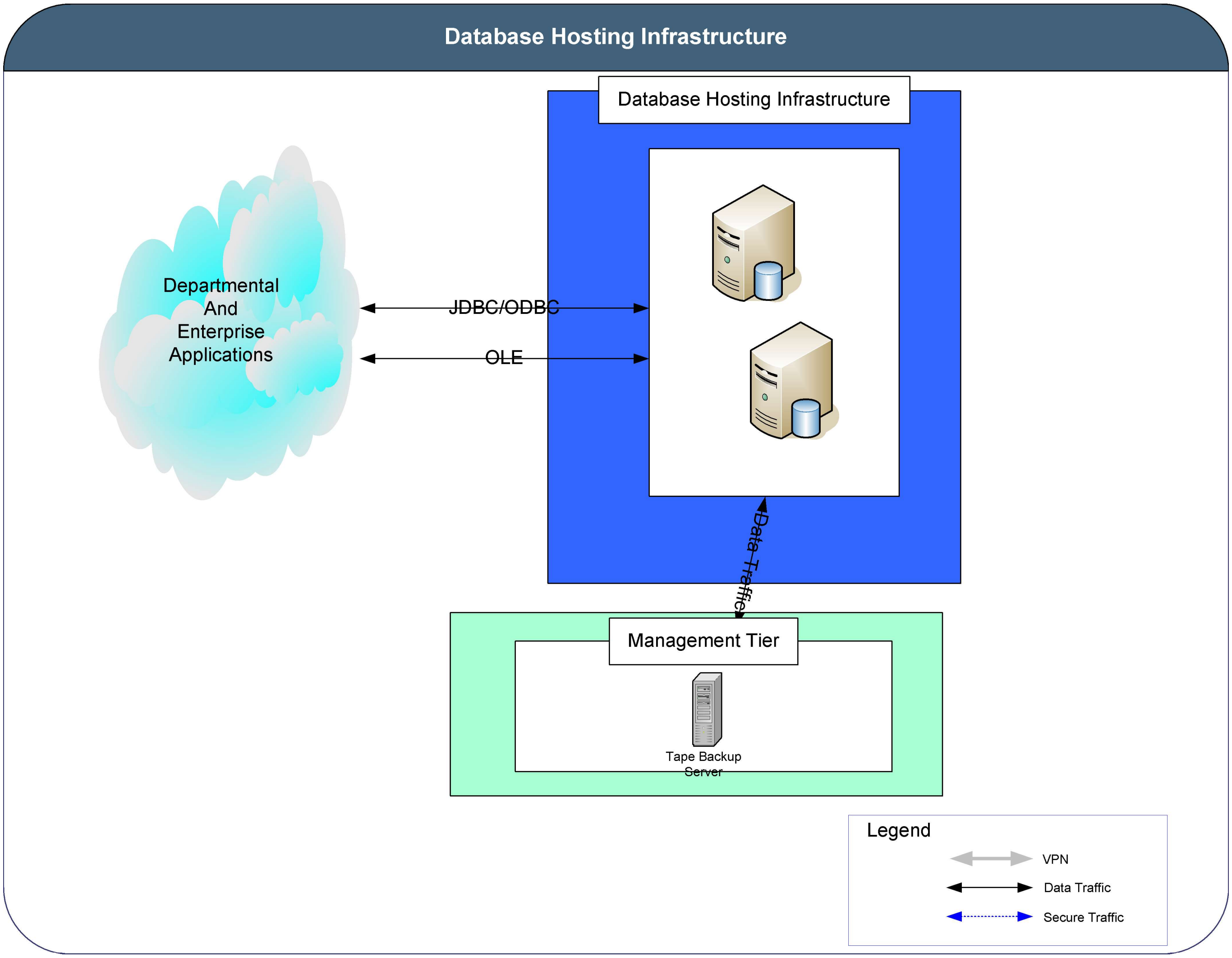
The technical owner for this Domain is:

- DTS Server Team

Components

Architecture Overview

In general, the DHI architecture is based on creating a security zone for just the Enterprise Databases. Access to the database servers is via ODBC/JDBC access only. It is a shared database server environment where multiple databases are hosted on the Enterprise Database Servers. Administrative access is kept within DTS with DTS delegating privileges to change and modify a user's database contents only. DTS does not give access at the database level or higher.


Database Hosting Infrastructure
Database Hosting Infrastructure
Departmental And Enterprise Applications
JDBC/ODBC
OLE
Data Traffic
Management Tier
Tape Backup Server
Legend
VPN
Data Traffic
Secure Traffic

Active Directory

Microsoft Active Directory is the master user registry for all County employees and for all applications hosted in the EHI (see Active Directory (AD) Domain). All LDAP traffic from the Web, Application, and Database tiers is encrypted (LDAPS) and accesses one of the Active Directory controllers. Active Directory also provides the primary DNS service for both Application and Database tiers of servers.

Database Server

The County supports both Oracle and Microsoft SQL servers under the DHI architecture. Users or Applications can access the database servers thru JDBC/ODBC/OLE.

Platform Choice

Hardware

All servers are Intel based and manufactured by Dell Computers. The hardware sizing is based on the County standard as outlined in the Deployment domain.

Operating System

Production Database Servers are all physical servers. Virtual Machines are not used.

The Operating Systems supported on the servers are:

- CentOS
- Microsoft Windows.

CentOS is an Open Source OS which uses the Red Hat Linux kernel and hence is an “identical twin” of Red Hat Linux.

The supported Microsoft Operating System is Windows Server.

Services

Backup Service

The DHI uses the backup services of the System Operations Domain.

Antivirus Service

Antivirus service is provided on the Windows Machines. Virus signatures are automatically synchronized from the County Central Antivirus server.

Network

The DHI uses the Network Domain’s Firewalls and Switches.

The DHI is separated from the Intranet through a stateful firewall. Internet access is not supported.

Security

Database Principles

The general principles that a database must follow are:

- Access to the Database must be through ODBC/JDBC only.
- Access to the Database from the Internet is not allowed.
- DTS solely has access and manages the production database servers.
- DTS delegates privileges to change and modify the database contents. DTS does not give access at the database level or higher.
- inactive session timeout
- Firewall is a stateful firewall

Standards

DHI Hosting Agreement

A requesting team or department must read and agree to the DHI Hosting Agreement. The DHI Hosting agreement lists roles and responsibilities for the database.

Administration Policies

- No access to the database servers other than by DTS employees performing administration services
- Monthly patching of Operating System and middleware software
- Virus updates every 10 minutes
- Daily backups
- Active Directory Group Policies (DTS Server Team Administrators are the only persons allowed to administer the machine and processes)
- Quarterly review of the Firewall Rules
- Quarterly review by Stakeholders of their database intake information
- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates

Physical Security

The networking switches and firewalls as well as the hosts that support the Production DHI are all located within one of the Department of Technology Services Data Centers (see Systems Operation Domain).

Disaster Recovery

The DHI Domain involves the use of physical Deployment Domain Servers housed in the Data Centers in the System Operations Domain. DTS employs a number of disaster recovery strategies in the Deployment and System Operations Domains that essentially cover the following disaster scenarios:

- server loss
- rack loss
- data center loss

The server loss and rack loss strategy has a number of mitigation strategies within the System Operations Domain. Within the DHI Domain the mitigation strategies include:

- use of physical database server machines located in both data centers.
- in the event of individual server or rack failure critical databases will be moved to working database server machines
- in the event of a data center failure critical databases will be moved to working database servers in the other data center.

The design problem for the loss of one of the Data Centers is the prioritization of services that will be brought up in the working data center. See the Disaster Recovery Domain for information around prioritization of services and policies.

Help Desk Support

A key component of the DHI is the Help Desk (see Help Desk Services Domain). It provides a single point of contact for the users of databases hosted within the DHI. The Help Desk resolves problems or, as needed, routes problems to the DHI administrators.

As part of the intake process for a new DHI database a support plan is developed with the help desk. The support plan includes information such as:

- Identifying the business system owner
- Identifying the DHI Administrator contacts
- Identifying common problems and their resolution that a level 1 support person can handle
- Identifying the contact for level 2 problems

Server Administration

Administration of the DHI Servers is performed by the DTS Server Team (See Enterprise Server Management Domain)

3.21 Technical Disaster Recovery

Principles

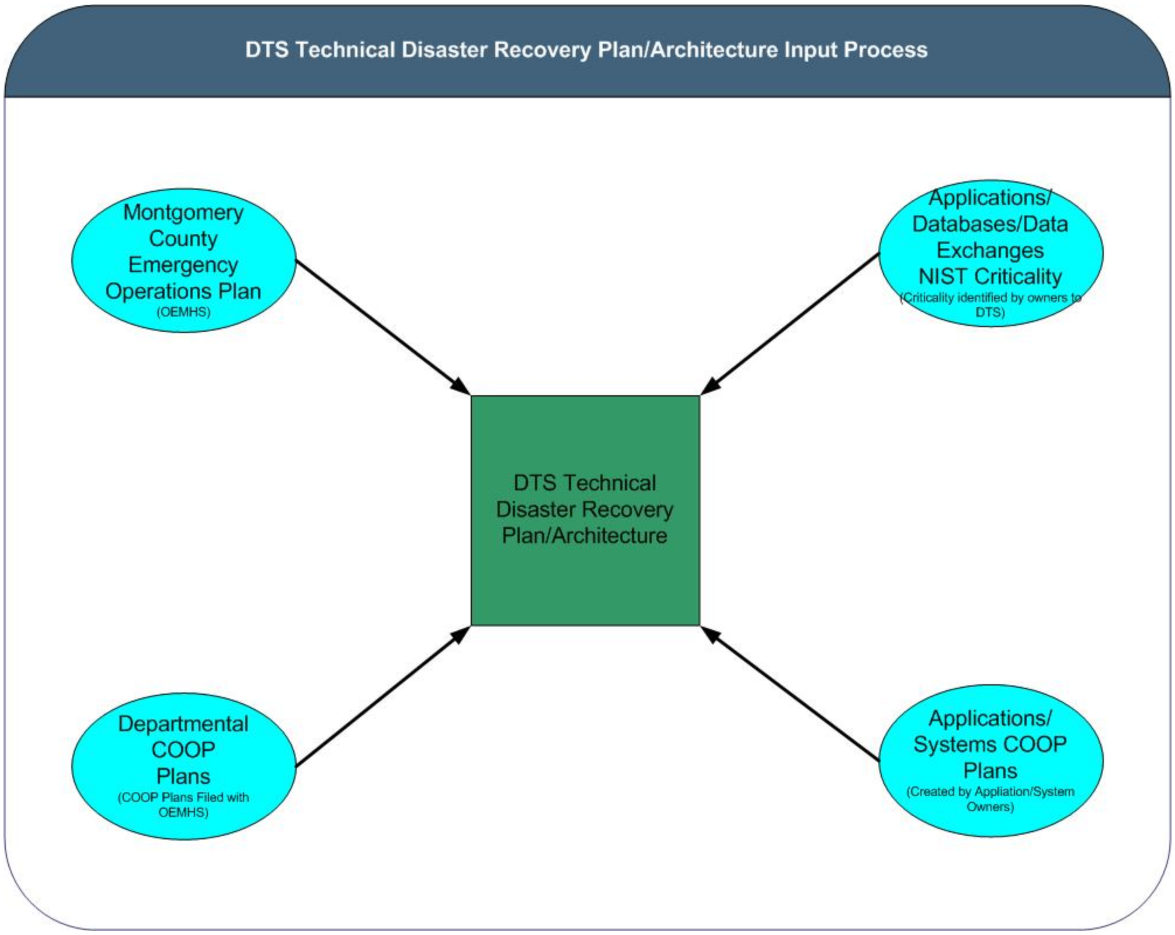
Disaster recovery is a complex undertaking that has both functional and technical components. It is strongly tied to COOP (process owned by OEMHS) and requires an iterative design approach with the business. It is not cost effective for the technical team to design a fully redundant Technical Disaster Recovery Plan and Architecture. A fully redundant plan requires a one for one replication of all services that must be maintained and regularly exercised by both functional and technical personnel.

The Technical Disaster Recovery Plan and Architecture must work closely with the business to classify all business functions for criticality of operation. Questions that the business should ask itself are:

- How critical is the service?
- How long can it be down?
- Can data be lost? If so, how much?
- How much are you willing to pay? Initial expense? Yearly expense? Support extra functional and technical head count to regularly exercise and update the plan?

An effective Disaster Recovery plan must include use cases to help design and assess the Disaster Recovery plan. The use cases or scenarios help bound the problem and test the design.

The following graphic details the inputs to the Technical Disaster Recovery Plan and Architecture:


DTS Technical Disaster Recovery Plan/Architecture Input Process
Montgomery County Emergency Operations Plan
(OEMHS)
Applications/ Databases/Data Exchanges NIST Criticality
(Criticality identified by owners to DTS)
DTS Technical Disaster Recovery Plan/Architecture
Departmental COOP Plans
(COOP Plans Filed with OEMHS)
Applications/ Systems COOP Plans
(Created by Appliation/System Owners)

Disaster Recovery Strategy

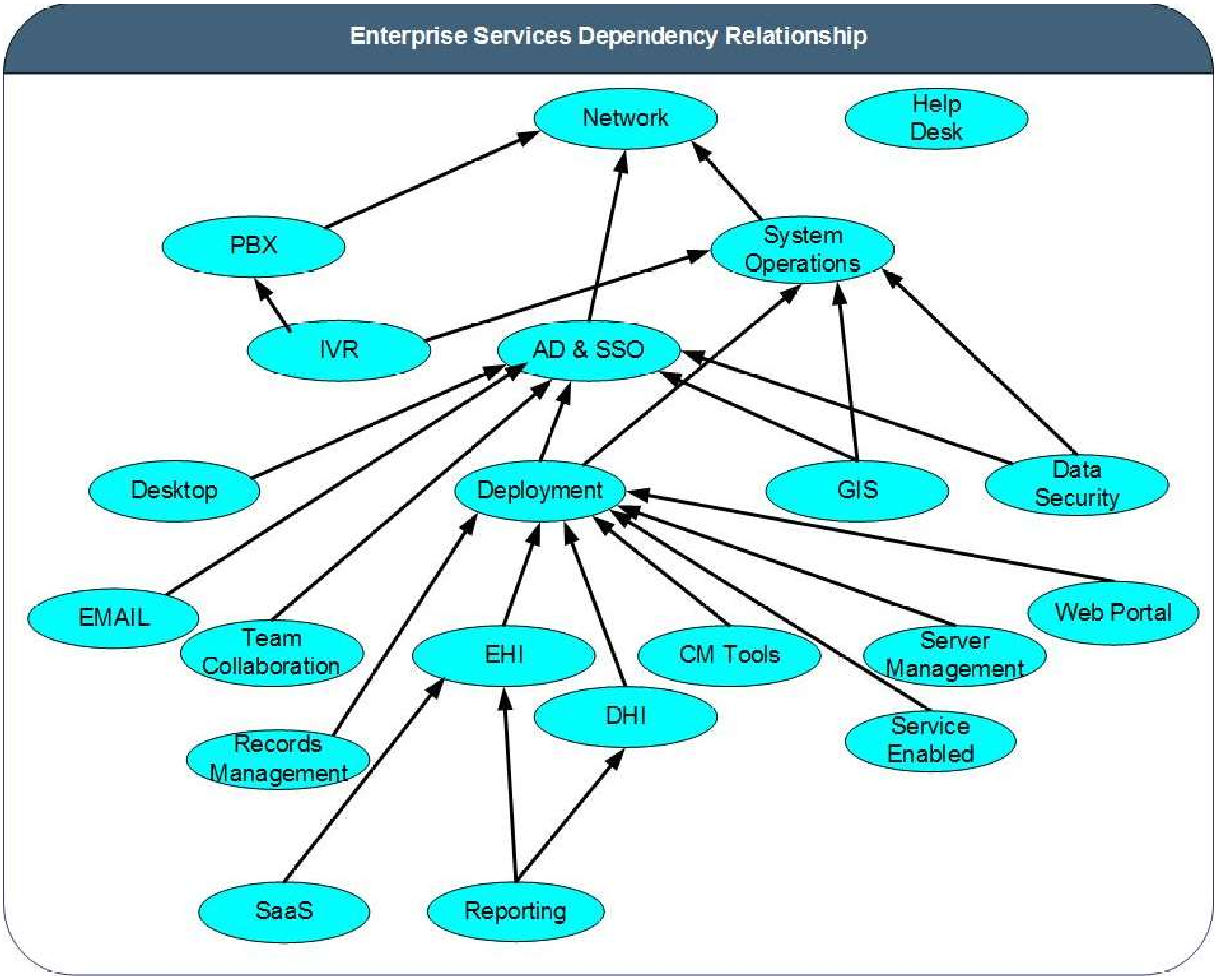
Technical Disaster Recovery is viewed from two perspectives. The first perspective involves the Enterprise Shared Services that are supplied to departments and agencies. The second involves the Enterprise and Departmental Services (applications, databases, and data exchanges) that are being hosted on the shared services infrastructures:

- Deployment Domain - VM Guests provided to departments
- EHI Domain - Enterprise Application Hosting
- DHI Domain - Enterprise Database Hosting
- Services Domain - Enterprise Service Bus (ESB) data exchanges

Enterprise Shared Services

The Department of Technology Services (DTS) offers a number of Enterprise Shared Services. Each one of the services is ranked in importance and the service includes as part of their Domain Architecture a section on Disaster Recovery that documents the processes and strategy for the service.

The Enterprise Services are built to work with each other and have the following dependency relationships:



DTS Hosting for Enterprise and Departmental Services

This section covers the hosted applications, databases, and data exchanges in the EHI, DHI, and the ESB.

EHI, DHI, and ESB

Applications, Databases, and Data Exchanges in the EHI, DHI, and ESB ultimately make use of the Deployment Domain. The Deployment Domain involves the use of VM Guests running on VM Hosting Servers housed in the Data Centers in the System Operations Domain. DTS employs a number of disaster recovery strategies in the Deployment, Network and System Operations Domains that essentially cover the following disaster scenarios:

- server loss
- rack loss
- data center loss

The design problem for any of the three scenarios is the loss of VM Hosting Server capacity and the prioritization of services that will be brought up on the working VM Hosting Servers.

DTS will bring up services on the available capacity following the documented prioritization from highest to lowest **until capacity is exhausted**.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Server Team
- DTS Data Center Management Team
- DTS Core Team
- DTS Networking Team
- DTS PBX Team

Components

Architecture Overview

In general, the Technical Disaster Recovery Domain is based on the Disaster Recovery Sections in each of the component domains. The Disaster Recovery domain is essentially providing the overall guidance, governance, and the process.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
COOP Planning
Disaster Recovery Planning
Technical Services Redundancy
Technical Services Failover
Ability to use Magic Help Desk System

Standards and Guidelines

- Enterprise Services Domain's Disaster Recovery Components (see Disaster Recovery section in each service)

- Hosted Applications(EHI) , Databases(DHI) , Data exchanges (ESB) NIST Classification determines priority
- CIO assigns overall priority for both Enterprise Services and Hosted Services
- DTS declares the DR event
- DTS starts recovering services starting with the highest ranked services first
- Critical Departmental and Enterprise Solution COOP/Disaster Recovery plans
- Outage reports through HelpIT updates
- Data Center Recovery Plan
- Solution Level Disaster Recovery Services Agreement - A team or department that is requesting Solution Level Disaster Recovery Services must read and agree to the Disaster Recovery Service Level Agreement. The Disaster Recovery agreement lists roles and responsibilities for administering the service.
- Solution Level Disaster Recovery Services - Solutions and/or applications often use many interfaces and exchanges and require careful coordination. The Departmental or Enterprise Owners for an application should write a COOP/Disaster Recovery Plan for the application and work with DTS to provide a higher level of Disaster Recovery Services.

3.22 Enterprise File Services Domain

Principles

The County maintains a centralized Shared Enterprise File Service for use by Departments. A Department can request space on the Enterprise File Server(s) that are centrally managed by DTS. The Enterprise File Service is implemented on Microsoft File Servers and makes use of the Active Directory Domain for security. A requesting Department is assigned a directory on the File Server and their administrator is assigned Administrator privileges for the directory. The Administrator has the ability to manage access and file privileges (ie Read/Write/etc).

Services provided to departments include:

- Centrally Managed Enterprise Shared File Service
- Ability to limit access to groups and individuals
- Ability to assign file permissions to groups and individuals
- Daily backups via the Enterprise System Operations Domain

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

The Enterprise File Service is implemented on Microsoft Enterprise Servers within the Deployment Domain. The Enterprise File Service is using the hosting and backup services of the System Operations Domain and is monitored and managed through the Enterprise Server Management Domain.

Requesting departments are assigned a Disk Space Quota that they are charged for and that DTS manages and monitors.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Active Directory Domain Administration
Windows Server Administration
Understanding of Security Principles

Ability to use Help Desk System

Standards and Guidelines

Enterprise File Service Hosting Agreement

A requesting team or department must read and agree to the Enterprise File Service Hosting Agreement. The Enterprise File Service Hosting agreement lists roles and responsibilities for the service.

Administration Policies

- Root Access and Administrator privileges are limited to DTS employees performing administration services
- Monthly patching of Operating System and middleware software
- Virus updates every 10 minutes
- Daily backups
- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates
- Highly Recommended that each Administrator use Active Directory Groups for Authorization
- DTS Enterprise File Service Administrators will monitor capacity and notify departments when allocations are reaching maximum limits.
- Departments incur yearly charge backs for various disk quotas.

Disaster Recovery

DTS backs up Enterprise File Servers for disaster recovery purposes. DTS' current recovery process is to restore servers in the event of system crashes, facility loss, or some other disaster. To support the current model, Enterprise Backup tapes (see System Operation Domain) are retained 3 weeks. The Monthly (1st Weekend) backup is retained 13 weeks.

DTS will restore individual files from specific Enterprise file server backup tapes upon request.

3.23 Enterprise Print Services Domain

Principles

The County maintains a centralized Shared Enterprise Print Server for use by Departments. A Department can purchase a compatible printer either directly or through the DCM contract (see Desktop Domain) and have its profile and driver hosted on the Enterprise Print Server(s) that are centrally managed by DTS. The Enterprise Print Service is implemented on Microsoft Servers and makes use of the Active Directory Domain as a directory service. A requesting Department will work with DTS to load their driver and profile on the Print Server. DTS will monitor and manage the centralized print queue. The owning department manages and maintains the printer.

Services provided to departments include:

- Centrally Managed Enterprise Shared Print Service
- Printers listed in a Directory Service (Active Directory)
- Central location for profiles and print drivers
- Authorized usage management
- Simple, local installation by end-user
- Printer firmware, driver updates
- Debug printer problems, interface with vendor
- Provide fax, imaging services
- Printer model compatibility with County's print server architecture

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

The Enterprise Print Service is implemented on Microsoft Enterprise Servers within the Deployment Domain. The Enterprise Print Service is using the hosting and backup services of the System Operations Domain and is monitored and managed through the Enterprise Server Management Domain.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Active Directory Domain Administration
Windows Server Administration
Understanding of Security Principles
Understanding of Microsoft-based Enterprise printing
Ability to use Help Desk System

Standards and Guidelines

Enterprise Print Service Hosting Agreement

A requesting team or department must read and agree to the Enterprise Print Service Hosting Agreement. The Enterprise Print Service Hosting agreement lists roles and responsibilities for the service.

Administration Policies

- Administrator privileges are limited to DTS employees performing administration services
- Monthly patching of Operating System and middleware software
- Virus updates every 10 minutes
- Daily backups
- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates

Disaster Recovery

DTS backs up Enterprise Print Servers for disaster recovery purposes. DTS' current recovery process is to restore servers in the event of system crashes, facility loss, or some other disaster. To support the current model, Enterprise Backup tapes (see System Operation Domain) are retained 3 weeks. The Monthly (1st Weekend) backup is retained 13 weeks.

3.24 Web Portal Domain

The Montgomery County Web Portal Domain supports both an Internet and Intranet Portal.

The County Internet Portal (http://www.montgomerycountymd.gov) is the main Internet (public internet and mobile access) entry point for County electronic government (eGovernment) services and is run on County Internet Web Servers.

The County Intranet Portal (http://mcgov.sharepoint.com) provides eGovernment services for County employees and associates (contractors, volunteers, partners, etc.) and is implemented on the County's Office 365 SharePoint Service (see Microsoft Office 365 Domain).

Montgomery County takes a decentralized approach to managing its Web Portals. A small number of staff within the Department of Technology Services (DTS) and the Public Information Office (PIO), called the Core Web Portal Team, is responsible for designing, developing, testing, and maintaining Web Portal master templates, navigation menus / flows, and styles to support a robust information architecture and to maintain a web site continuity (County Brand), while providing greater flexibility, with regard to look and feel, and space "real estate".

The Core Web Portal Team also reviews and recommends Internet and Intranet policies, standards, and practices to the Web Portal Change Control Board and the Oversight Committee for their approval.

DTS maintains the Intranet and Internet (MCGOV) Web Portal Domains including County Web and Application Servers, Office 365 SharePoint Administration, and Map Servers. In addition, DTS provides Internet Server load balancing, incident response, and middleware support. Furthermore, DTS enforces access to the Web Portal Domains. File transfer access (read/write) permissions to the Internet Web Portal is available through the Content Management System or CMS (see Content Management System Domain) for web content and through JFM and/or an equivalent DTS approved tool for web applications.

Owners

Business Owner

The business owner for this Domain is both the Public Information Office (Internet) and the Department of Technology Services (Intranet).

Technical Owner

The technical owners for this Domain are:

- DTS Web and Mobile Application Team
- DTS Server Team
- Public Information Office

Standards and Guidelines

- **Social Media**

Administrative Procedure 6-8, Social Media

- **Performance Guideline**
  - The County expects a turnaround time for Web content in 3 seconds or less
- **Availability Guideline**
  - The County expects Web content to be available no less than 99.5% of the time
- **Web Accessibility Policies and Guidelines**
- **Web Application Security Best Practices Guide**
- **Web Content Search and Discovery Guide**
- **Web Portal Application Design and Development Guide**
- **Web Portal Communications Guide**
- **Web Portal Link Policy**
- **Web Portal Domain Name Policy**
- **Web Portal Reporting Guide**
- **Web Portal Shortcut Policy**
- **Web Portal Sites User Terms and Conditions**
- **Web Portal Privacy Policy**

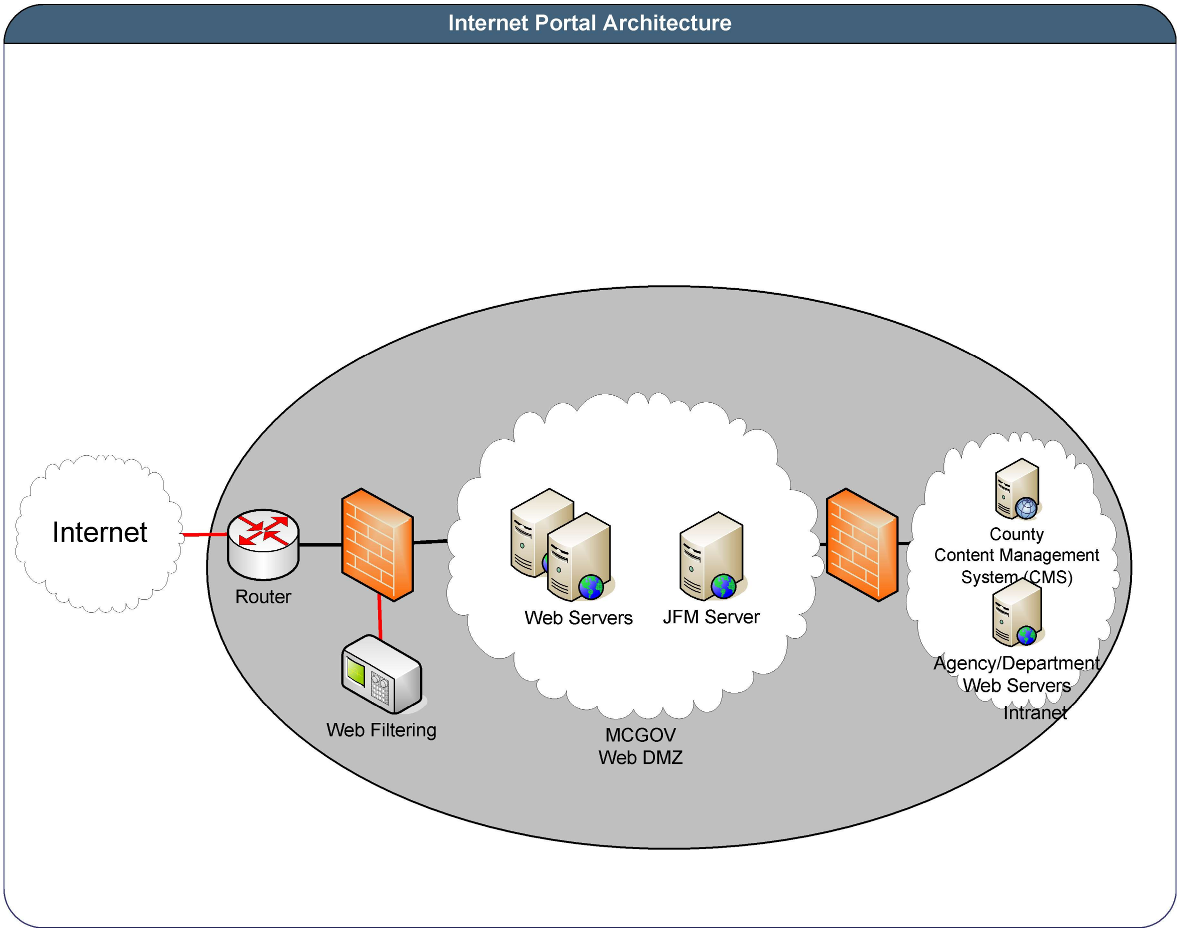
Internet (MCGOV) Web Portal Domain

Principles

The audience for the Internet Portal includes, but is not limited to the following:

- County Residents and Visitors
- Other Government entities
- Business owners and operators
- Job seekers
- Other constituents

Components



Web Servers

The MCGOV DMZ consists of several Web Servers and includes links to publicly available applications running within the Enterprise Hosting Infrastructure (EHI) (See Enterprise Hosting Infrastructure Domain). The Web Servers within the MCGOV DMZ are running Microsoft IIS Server and follow the Deployment Domain (see Deployment Domain).

MCGOV – Internet Portal Server (http://www.montgomerycountymd.gov)

The Internet Portal is used as the primary platform to deploy web content and applications to the public. A well-defined Internet Portal directory structure was created in a manner to enable application developers and content contributors to efficiently store and publish applications and content in addition to sharing common files. Responsive (mobile-friendly) master web templates, which are used to provide web site design continuity (same look and feel) and flexibility (templates can be quickly altered to affect thousands of web pages), are stored in the County web site's root directory.

Responsive master templates are available to County application developers in ASP.NET format. The proper use of the master web templates by County application developers are enforced by the Web Portal Governance policies and guidelines. In addition, County Internet policies such as, the Privacy Policy, User Rights, Accessibility, Social Media, and Language Translations are provided in the footer of master templates. The Internet Web Portal also provides a Secure Socket Layer (SSL) certificate for applications that require transmission encryption. Port 80 is the default open port using Hyper Text Transfer Protocol (HTTP). File transfer access (read/write) permissions to the Server is available through the Enterprise Service Bus (ESB) from the County Content Management System (CMS) for web content and through JFM for web applications.

MCGOV – Internet Application Servers

The Internet Application Server supports the storing and serving of ASP.NET web applications. The Servers currently run Microsoft IIS along with various ASP.NET Frameworks and consists of a directory structure that is like that of the Internet Portal Server. Application Server hosted applications are typically encrypted using Secure Socket Layer (SSL) certificate, thereby minimizing the risk in having Internet data transmissions intercepted or corrupted by unknown third party entities or hackers. Port 80 is the default open port using Hyper Text Transfer Protocol (HTTP). JFM can be used to deploy or update web application files.

Agency/Department Web Servers

Departments like Department of Permitting Services (permittingservices.montgomerycountymd.gov) and the Department of Technology Services (gis.montgomerycountymd.gov) have their own MCGOV Web Servers. These departments typically have staff or contractors to maintain and manage their servers, content, and applications. However, even though their applications and content are not hosted on the primary County Internet Server, the departments are expected to follow and adhere to County Web Portal Governance policies and standards.

Java File Manager (JFM) Server

The JFM Server provides file transfer access to the Web Servers. Department users who have a special need to update their application content on the Web Servers can be provided access. They are provided access to their application folders on the Web Server and are restricted by privilege level to only their folders.

Google Site Search – Will be discontinued in December 2017

The Google Site Search service provides sophisticated text-matching techniques to enable County Internet Portal visitors to quickly search and locate relevant web content by keyword or phrase.

County web site search forms, available in almost all County web pages, use Google Site Search technology to find relevant non-excluded content daily throughout the year.

Google Site Search department-specific search filters, refinements, and content weighing are available to County departments as well through Google Site Search.

Content Management System

The Core Portal Team is responsible for designing, developing, testing, and maintaining a content management system (CMS) that enables designated non-technical web content contributors and administrators, dispersed throughout the County Government's departments and associated agencies, to create, maintain, and manage County Internet (publicly accessible) web content in a secure and organized fashion with minimal training and simple, yet effective workflows. The CMS integrates with Internet web content templates and leverages existing County information technology resources.

Intranet Portal

Principles

The function of the Intranet portal is to support:

- Employee communications
- Employee services
- Departmental pages

The audience for the Intranet portal includes:

- Employees, Paid Interns, Temporary Workers (Active)
- Associates (Active)
  - Contractors
  - Partners - affiliated company/business user accounts, partners to the County
  - Volunteers - Volunteers, unpaid Interns

Components

The Intranet Web Portal is now supported in Office 365 via SharePoint Services (see Microsoft Office 365 Domain). Each department has been given their own site that is linked into the main Intranet Portal. Access to these sites is open to everyone on the Intranet.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Content Management
Web Development
User Interface Design
Office 365 SharePoint Administration
Office 365 SharePoint Development
Training Skills
Technical Writing

3.25 Mobile Computing Domain

Principles

The Mobile Computing Domain provides support for Mobile Client devices such as smart phones, netbooks, and tablets. It is an extension of the Desktop (DCM), Network, and Data Security domains.

With the advance in intelligence of non-traditional mobile computing devices the County has found the need to support these devices for County Mobile User populations and as secondary devices.

The user populations for this domain are expected to include:

- traditional seat machine for mobile users where the seat machine is a device such as a tablet or netbook
- secondary or user owned personal devices employed as productivity aids

Support comes in two categories that correspond to:

- behind the fire-wall devices
- outside the fire-wall devices

Mobile device support that is behind the firewall is for County owned devices that can meet County Security and management policies. This support means that they can access the internal County wireless network through the Wireless Access security protocol (see Network Domain for details). The Mobile Device is considered a County Device that is owned by the County and is centrally managed in an inventory system, has a standard image, can be managed through a remote login service, and is using the Enterprise Virus Protection Services (see Data Security Domain for details). Devices such as these are acting as seat machines and are supported through the help desk and DCM replacement schedule like a DCM desktop or laptop.

Mobile device support that is outside the firewall can include County Owned devices purchased through the DCM contract as well as personal devices. These devices operate outside the internal County network. For these devices, the County offers limited County Application support that includes Internet access for applications like:

- MCTime (timesheet)
- County Email and Calendaring (see Email System Services Domain)
- ERP Employee self-service

The device must support the Application's Web Browser Requirements.

Additionally, the County VPN offers limited support for mobiles that can allow them to log in to the internal County network and access certain behind the fire-wall services.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Client Computers (DCM) Team
- DTS Core Team (VPN)
- Network Team

Components

Mobile Device

The mobile device can be any mobile device that meets VPN access requirements or the browser requirements of the externally offered applications.

County owned devices are possible either as a seat machine offered through the County DCM contract or as a departmental purchased system that can be bought through the DCM contract but is not a seat machine.

Network Access

All personal and non-centrally managed devices must access County Services outside the internal County network. The Network Team is planning to upgrade current County wireless access points to support both internal County network access as well as external access. External access will tunnel the device out to the County External Firewall where they can access County Internet based services or use the VPN to access the internal County network.

Application Support

The County Email and Calendaring system (see Email System Services) supports Internet access via OWA as well as ActiveSync. Other application owners can choose to make their application available externally by hosting them in the Enterprise Hosting Infrastructure (see Enterprise Hosting Infrastructure Domain). These applications can support mobile devices if the mobile device browser can meet the EHI and Application minimum requirements.

Security (VPN)

The DTS Core Team maintains a VPN (see Data Security Domain for details) and is the primary solution for external users to gain access to the County internal network. Users must be approved for the VPN and use a device that is supported by the VPN. Upon login all devices are checked for up to date Operating Systems and for certain class of machines for up to date Virus checking software and definitions.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Desktop Computer Management
Tablet, Netbook, and Smartphone administration
Virtual Private Networking Administration
Network Access Point Administration
Enterprise Application development and support.

Standards and Guidelines

- Service Level Agreement (SLA) for Mobile Device Support under Desktop Computer Modernization (DCM) Program
    - SLA for departments using mobile devices

- Office of Management and Budget – Administrative Procedure 6-1 *Use of County-Provided Internet, Intranet, and Electronic Mail Services*

- Office of Management and Budget – Administrative Procedure 6-6 *Information Technology Policies and Procedures*

- Office of Management and Budget – Administrative Procedure 6-7 *Information Resources Security*

- Office of Management and Budget – Administrative Procedure 8-2 *HIPAA Compliance and Responsibilities*

3.26 Mobile Application Domain

Principles

With the recent emergence of the mobile market a new channel for constituent support services has developed. This channel supports both smart phones and tablets and has come about because these devices have a rich set of capabilities which include features such as high speed data connections, location services, modern browsers, and advanced application development support.

The Mobile Application Domain provides support for constituents to access the following categories of County services on mobile devices:

- Publishing of Information
- Service requests

The domain makes use of the following other Enterprise Services Domains: Open Data, Web Portal, and Service Enabled.

Publishing of Information

This category is broad but is essentially giving constituents access to information that is held within the County. Examples of information can be:

- Department of Recreation Seasonal Class Schedule
- List of libraries
- Library service hours
- Ride On bus schedule
- Traffic conditions
- List of specials in the liquor stores

Each of the above examples is publishing some information that is held inside the County and has timeliness associated with it. For example, the list of specials in the liquor stores might only be valid for the weekend while the list of Recreation classes might be for 3 months.

Service Requests

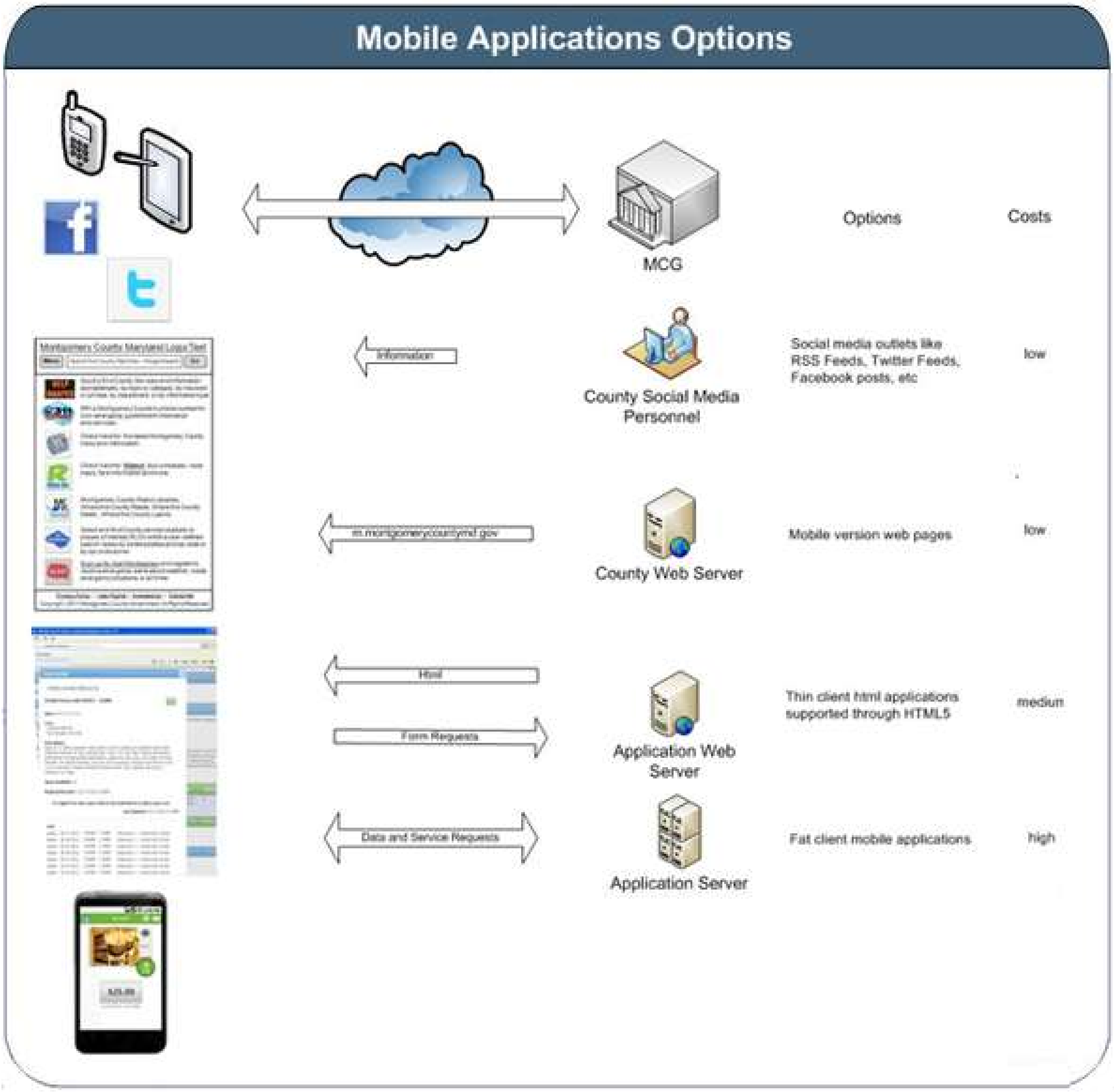
This category is also broad but is essentially a constituent making some sort of request for a County Service. Examples are

- Request a trash pick up
- Reserve a book in the library
- Request my current tax assessment
- Reserve a community room

- Sign up for a recreation class
- Order a case of liquor
- Find when the next Ride On bus is going to arrive at my stop

These requests involve a near real time interaction with an internal County application and have higher architecture requirements than information publishing. Each interaction requires a carefully designed interface that protects the internal system from adverse effects from the external clients.

Delivery Options



Options	Costs
Social media outlets like RSS Feeds, Twitter Feeds, Facebook posts, etc	low
Mobile version web pages	low
Thin client html applications supported through HTML5	medium
Fat client mobile applications	high

Social Media Outlets

Most smart devices have mobile specific applications that support social media. County posting of information through the outlets is a cost-effective way to reach citizens with information.

Mobile Version Web Pages

A tried and true method for publishing information to mobile devices has been through the use of mobile web pages. These pages are essentially basic html web pages that are tailored for the reduced screen and device capabilities of mobile devices. This is a very cost effective method to reach citizens with the County's current web portal domain supporting new mobile style sheets.

Thin Client Html Applications

The more advanced mobile platforms like Android and Apple's IOS support feature rich web browsers. These browsers are advancing rapidly in their support for HTML 5 and its application like capabilities. These capabilities support application like features through served up web pages that does not tie the County to device specific development platforms.

Fat Client Mobile Applications

The major mobile device platforms like Android, Blackberry, Windows, and Apple's IOS all offer Fat Client Development environments and delivery platforms. This allows the delivery of specialized fat client style applications. Each development platform has their architecture and requires a new program to provide the same functionality. To provide a mobile application in this format is to develop a specialized application for each environment. This is not unlike the application development model that fell out of favor in the 90s when applications were written for only specific platforms. A rich set of services can be provided but at a high cost.

Design Guide

If social applications or mobile web pages do not support the business need, the following development options exist (in order of preference):

1. Publish data on the Montgomery County Open Data platform (http://data.montgomerycountymd.gov) and allow the private sector or other parties including County constituents to develop independent applications of interest.

2. Develop or contract for HTML5 based App (thin client, server based) that either links to or is embedded in the County's Mobile Portal or MC311 Mobile App.

3. Create industry standard open APIs like Open311 (http://open311.org) and leverage commercial solutions that call those APIs.

4. Purchase a mobile App module/option from the business system application vendor.

5. Develop or Contract for custom App (fat client, device based)

Departments should look at the above options and start with the least expensive delivery method. All of the previous 5 options must go through the DTS CIO Approval Process. The process analyzes the request through a scorecard method with areas like cost benefit, alignment with the County Executives mission, project risks, duplication of enterprise processes like MC311, architecture risks, and security risks all being analyzed and scored. The CIO must approve of any request.

Options 2, 3, 4, and 5 require custom development and require review and architecture support for connectivity with systems and databases within the County.

Options 2, 3, 4, and 5 require use of the County's Mobile Application Contract Template as well as review of the contract by the County Attorney's Office.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS PMO (IT Review)
- DTS Server Team (App Store)
- County Attorney's Office (Contract Review)

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Contracting
Cost benefit analysis

Standards and Guidelines

- Mobile Applications (Apps) Policy
- IT Review Process
- Mobile Application Contract Templates and Guidance
- Mobile Application Style Guidelines

3.27 dataMontgomery Domain

Principles

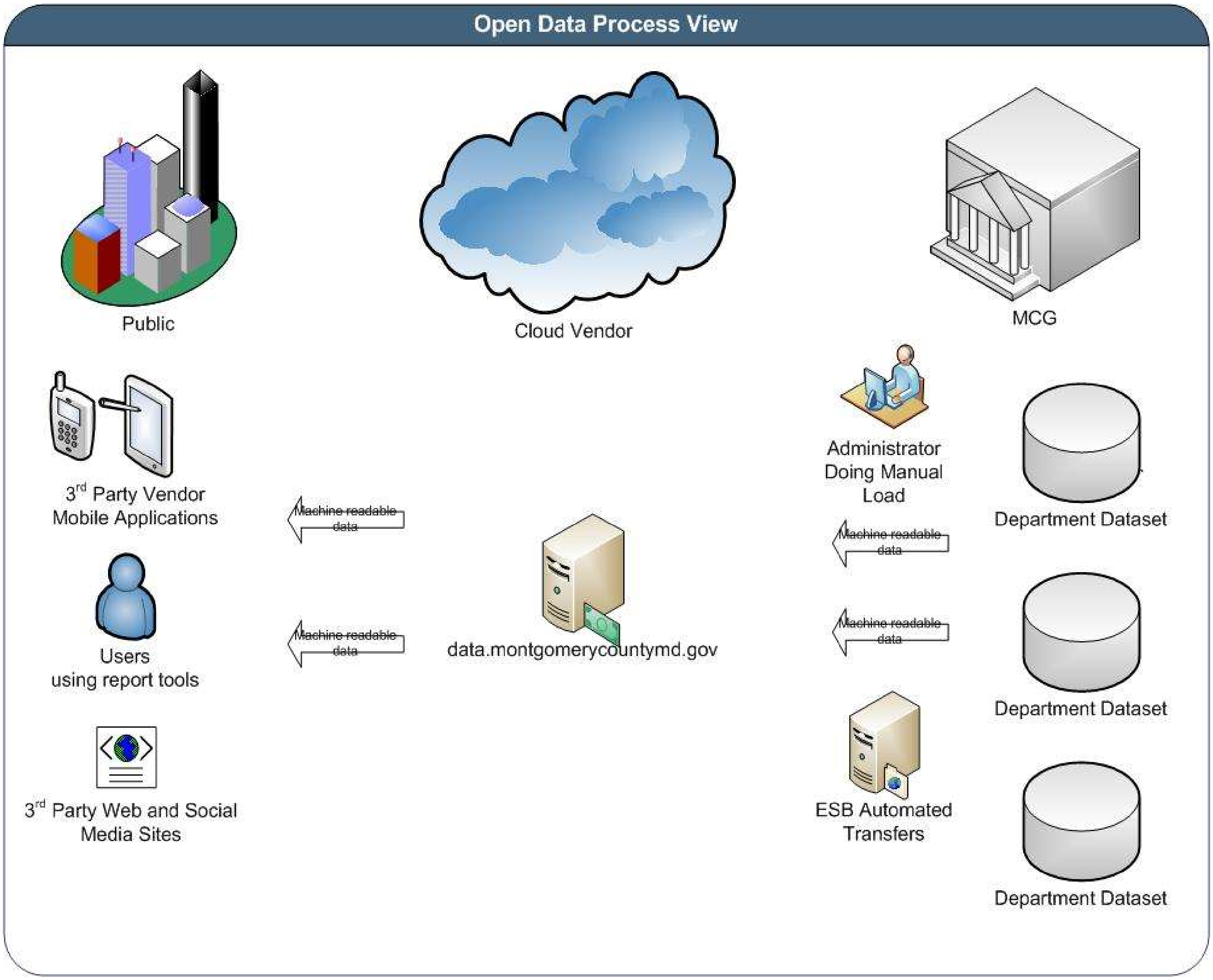
The dataMontgomery Domain provides support for increased public access to high value, non-sensitive, programmable ready Montgomery County Government datasets. Data is one of the most valuable assets for the County and the dataMontgomery Domain is the County Enterprise Strategy for publishing data to the public. It provides a central repository and standard set of tools where the public can go to retrieve published County Data Sets.

This Domain provides the following benefits:

- Supports the County Mission Statement “A Responsive and Accountable County Government”
- Keeps the public informed
- Reduces publishing costs by providing a centralized mechanism and repository for publishing County data
- Leverages private sector resources, initiative, and creativity for development of mobile and Web Applications that make use of the data
- Can improve data quality through more people looking at the data
- Can avoid the expense of some MPIA requests by already publishing the data
- Provides a standard set of tools for updating and retrieving the data
- Provides analytical functions that provide feedback on the value of the data
- Is a cloud based solution that reduces the cost of providing data access via many departments and their systems
- Provides a safe mechanism to share data by decoupling access from internal systems

Guiding principles for the domain are:

- **Complete** - All public data is made available. Public data is data that is not subject to valid privacy, security, or privilege limitations.
- **Timely** - Data is made available as quickly as necessary to preserve the value of the data.
- **Non-discriminatory** - Data is available to anyone, with no requirement of registration.
- **License-free –** Data is not subject to any copyright, patent, trademark, or trade secret regulation. Reasonable privacy, security, and privilege restrictions may be allowed.
- **Primary** – Data is as collected at the source, with the highest possible level of granularity, not in aggregate or modified forms.
- **Accessible** – Data is presented in a meaningful way.
- **Machine Process able** – Data can be processed.
- **Non-proprietary** – Data is available in a format over which no entity has exclusive control.


Open Data Process View
Public
Cloud Vendor
MCG
3rd Party Vendor Mobile Applications
Machine readable data
Users using report tools
Machine readable data
3rd Party Web and Social Media Sites
data.montgomerycountymd.gov
Administrator Doing Manual Load
Machine readable data
Machine readable data
ESB Automated Transfers
Department Dataset
Department Dataset
Department Dataset

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS PMO
- DTS Server Team (ESB Exchanges)

Components

Socrata

The Department of Technology Services has contracted with a 3rd party cloud solution provider to support the County's dataMontgomery site. The site called http://data.montgomerycountymd.gov hosts the identified data sets.

Enterprise Service Bus

To support the domain DTS can use the Enterprise Service Bus (see Service Enabled Domain) to update data on the site via a recurring schedule. For one time uploads the data will be given to the DTS administrator and they will upload data to the site.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Project Management
Data Formats and Conversions
Data Governance
Cloud Administration

Standards and Guidelines

- dataMontgomery Data Governance Document

  - Includes governance body, guiding principles, responsibilities, approval process, risks, sign offs, etc

- The Department Of Technology Services will centrally administer the dataMontgomery site

- Office of Management and Budget – Administrative Procedure 6-7 *Information Resources Security*
- Office of Management and Budget – Administrative Procedure 8-2 *HIPAA Compliance and Responsibilities*

- Montgomery County Government Technical Standards Manual for Publishing a Public Data Set

3.28 Content Management System (CMS) Domain

Principles

The County CMS Server is the County's primary web content management system and repository. The CMS enables non-technical web content contributors or editors and publishers (approvers), dispersed throughout the County's departments and associated agencies, to create, maintain, and manage web content in a secure and organized fashion with minimal training and simple, yet effective workflows.

The CMS supports a rich set of markup language file formats, documents, and image file support and provides an easy to use WYSWIG interface for content creation. The CMS supports a workflow between content creators and approvers. When a content creator is satisfied with a file it can be marked for approval. When the reviewer accepts the file, it is published (uploaded) to the Web Portal.

The Content Management System contains the approved County templates and style sheets from which content creators generate their content. The master style sheets and templates are maintained by the Office of Public Information and DTS.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS ADT Team (Content and Standards)
- DTS Server Team (Server)

Components

County Content Management System Server

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Content Management
Web Development
User Interface Design

Standards and Guidelines

Content Management Plan

Departments who are maintaining content on County Web Portals should create a Content Management Plan.

Site Administrator

Departments must designate a department staff person or Site Administrator to create and oversee content management for the department. They should establish and enforce the department content management plan.

Site Administrators are responsible for:

- adding, removing or inactivating CMS accounts for their staff
- ensuring that users have satisfied the required CMS training criteria
- being the primary contact for customer support issues, optimizing web content discovery, and for receiving web site reports
- validating content quality and accuracy and that it follows all County standards.

Training

New users are required to take a County CMS Course before being granted access.

Web Portal Content Management Guide

3.29 AccessMCG Domain

Principles

The County supports both internal and extranet Single Sign On (SSO) Services. Single Sign On (SSO) services are an enterprise strategy designed to minimize administration and user authentication stress, improve security, eliminate multiple userids and multiple passwords.

The internal Single Sign On service looks to the County's Active Directory Service (see Active Directory Domain) and supports the internal user population. It provides Single Sign On services to applications who service the internal County user population or more specifically the user population defined in the County Active Directory Service. With the internal SSO service, users are able to log on to the network, and log into specific SSO configured applications as the need arises. For example, once the user is logged into the network, the user is not required to log into Exchange to access the County's email system. The internal applications are supported through an internal ePortal (http://www.montgomerycountymd.gov/eportal). The user logs into the ePortal where they are provided with the list of applications to which they have been granted access.

The extranet Single Sign On service supports the non-internal user population. The intended range of users are people who have some relationship or business with the County but are not employees. Examples could be retirees, volunteer fire fighters, vendors, etc. Users can self-register creating an account that includes information such as their contact information and challenge strings for password resets. The user can then request access to a particular Extranet SSO enabled application. When the user makes the request, the request is routed through a work flow to the business owner of the application. The business owner for the application must grant access before a user can access the application. The Extranet Applications are supported through an external ePortal (http://www.montgomerycountymd.gov/AccessMCG). The user logs into the ePortal where they are provided with the list of Extranet applications to which they have been granted access.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Server Team

Components

Both the Extranet SSO and Internal SSO is supported through the openAM Open Source Product.

The Department of Technology Services (DTS) manages both Single Sign On Services and is the sole Administrator at the Enterprise level.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Active Directory Domain Administration
Windows Server Administration
openAM Architecture and Administration
Understanding of Security Principles
Ability to use Help Desk System

Standards and Guidelines

- The Extranet SSO looks to the Identity Management Domain for user authentication
- The Internet SSO looks to the Enterprise Active Directory Domain for user authentication
- The DTS Server Team is the sole administrator for both domains
- The DTS Server Team can support multiple options for Applications that are integrating with either Single Sign On implementation. Options include SAML, JAAS, and various .Net integration methods.

3.30 Identity Management Domain

Principles

The Identity Management Domain supports the provisioning of the IT Systems of the County. It is a central repository of people objects and the attributes that define them. It supports objects such as:

- Employees
- Retirees
- Contractors
- Volunteers

The system may receive people from systems of record like ERP for employee and retiree objects or from self-registration systems that require approval. Any person that is required to provision an internal County resource is a candidate for inclusion in the Identity Management System.

The Identity Management Domain offers its provisioning services to resources such as County Applications and Processes. A Resource Owner can request that their system be supported within the domain. They will engage with the DTS Server team to define what attributes or groups that their resource requires association with a user. The DTS Server team will implement those groups and attributes and add them into the system. Those groups and/or attributes can then be associated to a user but only with the approval of the requesting resource owner. A workflow can be setup to implement the business rules associated with the resource. The Resource Owner will be part of the workflow and can approve or reject requests.

The Identity Management System can be set up to be the master provisioning source for a system. It can remove any authorizations or attributes that are not in the Identity Management System.

Owners

Business Owner

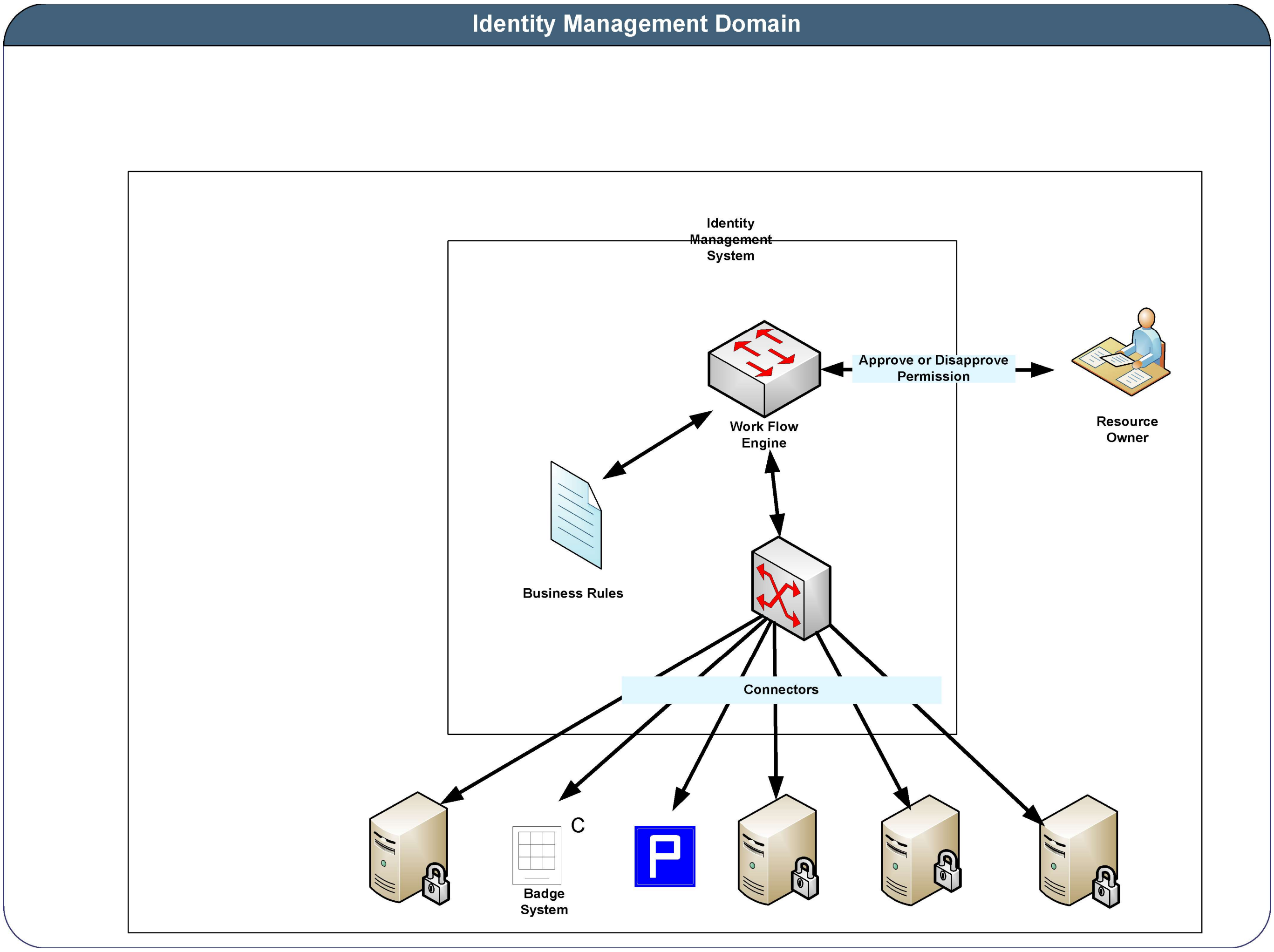
The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Server Team

Components


Identity Management Domain
Identity Management System
Approve or Disapprove Permission
Work Flow Engine
Resource Owner
Business Rules
Connectors
C
Badge System

Velo

The County uses the open source product called Velo. Velo is a provisioning product that can support work flows and has a connector architecture for talking to different systems.

Velo can provision not only the user for authentication but for authorization. Role(s) will be associated to each user. The individual provisioned systems will need to map the Velo roles to their authorization structure.

Connectors

Velo supports a connector paradigm where adapters are built to communicate with the target systems to be provisioned. The adapter could be as simple as sending an email to the administrator of the target system up to a programmable connection between the two systems through some sort of interface such as SOAP.

Work Flow

Velo has its own customizable work flow capability. The Resource Owner will define the work flows that need to be followed in the provisioning and deprovisioning process.

Business Rules

Velo supports the definition of business rules around the provisioning process. The business rules are configurable and defined by the Resource Owner.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
J2EE Software Development
Configuration Management
Performance and Concurrency Testing
JDBC, RDBMS
Velo Administration

Standards and Guidelines

- Service level agreements defining roles and responsibilities

3.31 Business Intelligence/Data Warehousing

Principles

The Business Intelligence/Data Warehouse domain supports the following functions:

- Building a data warehouse
- Building a data store
- Performing an Extract, Transform, and Load (ETL) operation
- Performing data cleansing services
- Writing reports and dashboards against a data warehouse or data store

The domain is supported through two toolsets with one being the Oracle OBIEE/ODI suite and the other being through the open source Pentaho suite. The preferred toolset due to cost considerations is the Pentaho suite.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Server Team

Components

Oracle

ODI

- Oracle ETL tool used to move data between disparate systems

OBIEE

- Oracle Enterprise reporting and analysis tool

Pentaho

Report Writer

- Pentaho report writing tool

Kettle

- Pentaho ETL tool

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Data Warehouse Design
Dashboard and Report Creation
ETL design
JDBC, RDBMS
OBIEE
Pentaho

Standards and Guidelines

- Service level agreements defining roles and responsibilities

3.32 Microsoft Office 365

Principles

The County is using Microsoft's Office 365 cloud service to support a number of the County's Enterprise Technology Services. Specifically, the County is using the Microsoft Government cloud service that comes with higher levels of security and privacy. The higher levels of security are delivered in a separate Microsoft Government Cloud and is specified in their contract with the County.

Key services that are being supported in Microsoft Office 365 are:

- Email
- Enterprise Spam Filtering
- Calendaring
- Collaboration
- OneDrive (personal File Services)
- SharePoint (Group/Department Collaboration)
- Lync (Conferencing)
- Office Productivity (Word, Excel, PowerPoint)

The Department of Technology services is funding the G3 level of the service for all County employees, volunteers, and contractors. Limited use accounts and accounts that are accessed on shared machines may be limited to the G1 level of service. The service is subscription based and requires a yearly subscription fee.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Core Team

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Microsoft Office 365 Administration
Microsoft Office 365 Troubleshooting
Active Directory Administration
Microsoft Office Client Software

Standards and Guidelines

- DTS Core team is the central administrator
- Microsoft Office 365 Services will be made as accessible as possible.

Disaster Recovery

The Microsoft Cloud Service offers a high level of service and we expect higher availability then our previous on premise support. The County does maintain a Single Sign on infrastructure within the County that supports identity management and must be touched before users can use the service. That infrastructure was built with redundant servers and network paths.

3.33 Microsoft Office 365 Video

Principles

The County uses the Microsoft's Office 365 cloud service for its Video Portal Collaboration Service. This system allows the County to include Video services for our internal County Collaboration. It is like YouTube except the video and channels can be limited to only internal County Users.

Benefits for the Video Service include:

- Easily consumable Video through a Modern Portal
- Supported on Mobile Devices
- Integrated within Office 365 and works with other Office 365 Collaboration Services
- Has built in security and is easy to manage
- Can be limited to our internal users

The Video Portal is an easy to use online Video Portal for internal County teams. County Users can come to the Video portal and see videos that are published in Department and Group assigned Channels. The Video service provides some of the following abilities to a team:

- Easy to create Channel
- Access to the channel can be limited to a user group
- Group can manage who can see and edit the videos

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Core Team

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Microsoft Office 365 Administration
Microsoft Office 365 Troubleshooting

Active Directory Administration
Microsoft Office Client Software

Standards and Guidelines

- DTS Core team is the central administrator
- Microsoft Office 365 Services will be made as accessible as possible.
- Departments and Groups can request a channel be created for them.
- Each channel must have an administrator
- The Department/Group is responsible for the management and security of the channel.
- Outage and maintenance reports through HelpIT updates
- Availability/Uptime
  - The system is designed to be available 24/7.

Disaster Recovery

The Microsoft Cloud Service offers a high level of service and we expect higher availability then our previous on premise support. The County does maintain a Single Sign on infrastructure within the County that supports identity management and must be touched before users can use the service. That infrastructure was built with redundant servers and network paths.

3.34 Microsoft Azure

Principles

The County has added Microsoft's Azure Cloud Services into the County's Enterprise Architecture. Specifically, the County is using the Microsoft Government Azure Cloud Service that comes with higher levels of security and privacy. The higher levels of security are delivered in a separate Microsoft Government Cloud and is specified in their contract with the County. Azure is Microsoft's Cloud Hosting environment that has many offerings within it with services in PaaS, SaaS, and IaaS categories.

In the short term the County will expands its Intranet to include a section of network addresses in Azure and will include access to the County's Active Directory. The initial use of Azure is likely to be in Disaster Recovery, Backup and Cloud Storage.

In the long term Azure may be used to support a number of the County's Enterprise Service Domains such as:

- Active Directory
- Web Portal
- Enterprise File Service
- SaaS
- Disaster Recovery
- Backup
- Records Management
- Deployment
- Database Hosting

The service is subscription based and requires a yearly subscription fee. The County will look at moving select Enterprise IT Services into Azure on a case by case basis and as Cost Benefit Analysis justifies.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Core Team

- DTS Server Team

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Microsoft Azure Administration
Microsoft Azure Troubleshooting
Active Directory Administration

Standards and Guidelines

- DTS Core team is the central administrator
- If a Departmental Solution is placed into Azure the cost of the solution will be charged back to the Department.
- The County Intranet has been extended to the Azure Cloud and includes access to the County's Active Directory
- Department solutions and projects will be tied to and part of a Department or Project resource group. All parts of the solution such as VM guests and storage will be part of the Resource Group. Each element of the solution will have a department tag associated with the resource. The department tag is used for tracking and chargeback calculation.
- DTS will cover the funding of the Core Services such as the network, VPN connection and Active Directory controller
- When a Virtual Machine is supplied to a project or department and they are given local administrator rights to the box the administrator must not try and change IP addresses. It will corrupt their box
- Resources that are provisioned on the Intranet in Azure will have their public Internet IP Addresses removed. They must be accessed and administered through the Intranet and the point to point VPN connection like on premise resources.
- A Point to Point VPN connection is established with the Intranet zone in Azure. The connection is limited to 200 megabytes per second.

- IaaS resources that are configured for a department or project exist on the County Intranet and must follow all current policies. For example, the department or project must keep the resource patched and have Sophos Virus Scanning software installed.
- Azure includes charges for outbound network traffic from Azure. All solutions must minimize such traffic. Traffic inbound to Azure and traffic between resources in Azure are free.
- All services will be configured in the new Azure Administrator Portal. The classic Portal will be avoided.

Disaster Recovery

The Microsoft Cloud Service offers a high level of service and we expect higher availability then our previous on premise support. The County does maintain a Single Sign on infrastructure within the County that supports identity management and must be touched before users can use the service. That infrastructure was built with redundant servers and network paths.