Internal Audit Report 2013-04
Internal Audit - St. Louis County
St. Louis County – Staff Directory
September 18, 2013
Final Audit Report

Distribution:	**Audit Performed by:**
The Honorable Kathleen Burkett – Chairperson – County Council	Inessa V. Spring, CGAP, Staff Auditor
The Honorable Charlie A. Dooley, County Executive	David C. Makarewicz, CISA, County Auditor
St. Louis County Council Members	
Pam Reitz, Director of Administration	
Mike Duncan, Chief Information Officer	
Orville Moore, Telecommunications Manager	
Tom Arras, Public Administrator	
John Bales, Director of Aviation	**County Auditor:**
Vicky Barela, Telecommunications Specialist	David C. Makarewicz, CISA, County Auditor
Herbert Bernsen, Director – Justice Services	
Mary E. Case M.D., Chief Medical Examiner	
Mike Duncan, Chief Information Officer	
Garry W. Earls, Chief Operating Officer	
Timothy Fitch, Chief of Police	
Paul Fox, Director – Department of Judicial Administration	**Field Work:**
Genevieve M. Frank, Administrative Director – County Council	Start Date: July 16, 2013
Joan Gilmer, Clerk of the Circuit Court	Completion Date: August 23, 2013
Dolores Gunn, M.D., Director – Department of Health	Closing Date: August 27, 2013
Renee Hines-Tyce, Administrator – Department of Municipal Court	
Sheryl Hodges, D.E., P.E., L.P.G., Director of Highways and Public Works	
Rebecca Howe, Director of Procurement	
Andrea Jackson, Director – Human Services	
Mike Jones, Senior Policy Advisor	
Tom Kendrick, IT Operations Manager	
Paul T. Kreidler, Budget Director	
Eugene Leung, Director of Revenue	
Kirk McCarley, Director of Personnel	
Bob McCulloch, Prosecuting Attorney	
Loraine Miller, Administrative Assistant	
Debbie Oberlohr, Telecommunications Analyst	
Tom Ott, Acting Director of Parks and Recreation	
Glen Powers, Director of Planning	
Patricia Redington, County Counselor	
Don Rode, Chief Accounting Officer	
Michael Smiley, Emergency Management Director	
Inessa Spring, CGAP, Staff Auditor	
Jake Zimmerman, Assessor	
Kerber, Eck and Braeckel, LLP	
	Audit Report Number 2013-03

Saint Louis
COUNTY
Auditor's Office

TO: The Honorable Kathleen Burkett, Chair – County Council
The Honorable Charlie Dooley, County Executive
Pam Reitz, Director of Administration
Mike Duncan, Chief Information Officer

FROM: David Makarewicz, CISA, St. Louis County Auditor

SUBJECT: Final Audit Report
St. Louis County – Staff Directory
Audit 2013-03

DATE: September 18, 2013

EXECUTIVE SUMMARY

The St. Louis County Audit Department performed an audit of the St. Louis County Staff Directory.

The Staff Directory is a database of employees and appointees of St. Louis County, and staff within affiliated agencies. The database includes key contractors and personnel who have a relatively permanent presence within their respective departments.

To reduce duplication of effort, the Staff Directory is based on service called Active Directory. This service consists of a database, software and defined utility programs that are used together to manage a base of computer users, store their user credentials and allow these users to be authenticated to a computer system.

Active Directory is a directory service that is used extensively within Microsoft software products and operating systems. Within these systems a database provides a generic set of records with fields defined that hold information needed to establish user credentials. The database includes the defined data fields that are commonly needed by organizations to uniquely identify employees who are network users. It is a database that holds the user names, user IDs and encrypted passwords and is used to limit or grant access to a network. Additional data fields can be defined to hold identifying information that is not defined within the generic database.

As the St. Louis County data kept within Active Directory contains data that is useful for the Staff Directory, the information is keyed in one place and is used for two purposes. The user credentials are checked to authenticate users when they sign onto our network. Queries have been written that allow County employees to query the same information to find employees. It is cost effective to use information that is keyed once, and use it for two different purposes.

User credentials are also stored for programs that run on the network. Records are stored which contain a user ID and encrypted passwords, but instead of the name of a user, the records may contains the name of a program that is authorized to run on the network. These records can also contain a generic description of the purpose of a user ID (i.e. MUNIS Test User ID). These user IDs can present a risk if they a displayed or disclosed to persons other than authorized users, especially if the passwords used to secure these user IDs are simple, or easy to guess.

While the use of Active Directory for more than one purpose is cost effective, it has some limitations when used as an organization's staff directory:

1. Active Directory includes user IDs, a generic name attached to a user ID and encrypted passwords for users. While these are needed for network access, this information should generally not be made available to unauthorized individuals. The existence of user IDs and the name of user IDs used to test systems should be restricted to system administrators and those individuals who are authorized to use a particular user ID.

2. Deletion of a user's record is more problematic with Active Directory. If an employee record is deleted, the user credentials are also deleted. If user credentials are deleted, then file ownership becomes a problem. Every file stored on a network should be owned by a current user. Files can be owned by a user ID that has been deactivated or logically deleted. However, once the user ID is removed, the files are "orphaned". It becomes difficult to determine control or ownership of the files.

3. The fundamental purpose of this database is to hold user credentials such as a user name, user ID and password. There is an underlying assumption that the database is used to store information about a system user. User IDs are unique and are used as keys to specifically identify a user. The database does not work as well when used to hold information about individuals who do not have an assigned user ID and password.

4. Corruption of an Active Directory database can have a significant negative impact on an organization. A corrupt database can prevent users from logging on or greatly slow down the authentication process. It is important to have strong controls in place on the processes used to edit Active Directory.

Within St. Louis County, the Staff Directory has been used to store information about individuals in organizations that are affiliated with St. Louis County. It has been used increasingly to store information on individuals who <u>do not</u> hold a user ID as well as users who do not have as strong a tie to the County, like employees or appointed officials with assigned user IDs. For example, we noted entries for consultants and vendor representatives in the Staff Directory.
The database and Staff Directory was also used to store information on individuals such as board members, vendor representatives, individuals who work for other governmental bodies or agencies. This is a common practice for an Active Directory system, but the relationship between Active Directory and the Staff Directory system led to confusing information display. This problem was corrected by improved data filtering in the Staff Directory application.

IT staff and system administrators have experienced much more difficulty in receiving updates on information on individuals for those persons who do not work in a County facility, do not have a phone supported by the County, and do not have an email address supported by the County. The maintenance plan for the Staff Directory primarily relies upon the efforts of fifty "Telecom Coordinators". Each Telecom Coordinator" is responsible for updating staff directory records in their Department and/or Division.

Based on audit work performed in 2012, Audit noted that the percentage of incomplete records within the Staff Directory grew substantially and recognized the difficulties faced by system administrators in updating records for individuals who were not housed in County facilities. We saw a decline in the quality of the records within the Staff Directory, within audits performed in 2013. We noted an increase in misdirected calls to the County, especially for departments and divisions who had moved.

We also were advised by IT management and staff that other software tools may be much more suitable for administering this information and hosting a staff directory. The use of the current Staff Directory system has become less suitable for the needs of the County. IT Management is moving towards a migration of this data to other software, including the use of software like Sharepoint, another Microsoft product, as a better repository for the Staff Directory.

In anticipation of a near term migration, IT staff and IT-Telecom staff reviewed and updated the database in its entirety. This is a logical step that improved the quality of this database. IT also facilitates a migration of data to other software as they now have better data. Audit reviewed and monitored this work so that we could report results.

During the audit we focused on controls in these areas:
- We reviewed written Information Technology and Information Technology/Telecommunications policies.
- We reviewed written Information Technology and Information Technology/Telecommunications procedures.
- We reviewed controls over access to the network and the reliance placed on user IDs to limit or grant access.
- We checked internal and external web sites for instructions on administration of user privilege and/or administration of the Staff Directory.
- We reviewed processes used to apply updates to Active Directory.
- We checked to ensure that the information contained within Active Directory is backed up and recoverable.
- We reviewed record retention schedules.
- We reviewed written procedures for additions, changes and deletions to information within Active Directory.

With respect to the work performed by IT and IT-Telecom Staff to update the Staff Directory:

- We reviewed the Staff Directory and gathered statistics on the number of records in the Staff Directory.
- We identified problem records such as records for test users IDs, test entries and incomplete entries.
- We researched the causes of different types of errors within Staff Directory records.
- We assisted in soliciting updates to the Staff Directory directly from employee by phone and email. These updates were forwarded to IT Staff for correction.
- We reviewed procedures used to enter records into Active Directory, edit records and delete records.
- We reviewed written materials used for training. These included written procedures and presentations that were available on the intranet for use by Telecom Coordinators and IT Staff.
- We tracked certain populations of records as they were updated. For example, we validated the deletion of 222 records for terminated employees. We also found employees whose entries had been deleted, who needed to be "added back" to the Staff Directory.
- We posed questions to help IT Management and Staff formulate their future policies with respect to changes in messaging, integration of voice communications and messaging, and a lessening in reliance on older technology such as fax machines.
- We reviewed alternatives available and plan in place to migrate to a better solution for managing this data to ensure that there is a viable upgrade path and solution in place. The management of this data may require the addition of software tools to administer the data or the use of "off-the-shelf" solutions that can be adapted for use to support the Staff Directory.

RESULTS

- Based on the initial record count in May of 2013 there were 5,700 Staff Directory records. This number exceeded the count of employees by 1,700 records. A significant percentage of the records were records of terminated employees whose accounts had been disabled, but were still displayed. This was validated within recent audits. At the conclusion of the audit, the Staff Directory records count was close to 4,000 records. This is consistent with actual employee counts.

- The number of records missing two or more key data fields is now about 1%, which we believe is acceptable.

- At least 130 records for system or test user IDs were filtered out of search results. This improves data security.

- We confirmed the deletion of 222 records for employees who have terminated within the last six months.

- Telephone listings and contact listings for affiliated organizations such as the University of Missouri Extension Council are maintained on their own web sites. St. Louis County may be able to provide links to these other rosters until a new directory service can be implemented.

OPINION

Several controls were not working as intended:

- There were significant errors or omissions in more than 20% of Staff Directory records. We considered three or missing fields such as an email address, department name, or division name to be a significant error.
- Drop down lists that would normally be used to query records within certain departments and divisions did not correspond to the current organization. Fifty one of these queries produced no results.
- The organization of Telecom Coordinators tasked with supporting Staff Directory changes had grown to be too large. The Coordinators perform their tasks too infrequently to be adequately trained.
- The web site used to host documents supportive of telecommunications and messaging needed to be corrected and could be simplified.
- In the long term, we believe it will be necessary and cost effective to move the Staff Directory to a better repository and administer it with more appropriate tools. St. Louis County currently supports software that would be appropriate for a repository for the Staff Directory.
- We believe that Customer Service to County residents had been impacted because of an increase in the number of misdirected phone calls.

The findings noted during the audit were addressed by IT and IT Telecom staff. Corrective action has been taken by IT and IT-Telecom staff to correct entries in the Staff Directory:

- Their efforts to correct entries in the Staff Directory were successful.
- The quality of the data currently in the Staff Directory is much improved with the May to August 2013 timeframe.
- Current error rates are acceptable.
- The web sites used to host IT Policies have been revised and improved.
- The web sites used to host information that supports telecommunications have been revised and improved.

We have recommended:

- The web site used to host documents supportive of telecommunications and messaging need to be simplified.

CONCLUSIONS:

- Controls are in place to provide appropriate mechanisms for adding, updating and deleting user credentials.
- The recent cleanup of the Staff Directory was successful. Current error rates are acceptable.
- The quality of the data currently in the Staff Directory is much improved with the May to August 2013 timeframe.
- Additional procedures and effort is needed to address reassignment of ownership of files for terminated employees and subsequent deletion of user IDs after ownership of files is reassigned.
- The mechanisms that are currently in place and in use for adding, updating and deleting user credentials work but do not work well for managing information from affiliated organizations.
- The organization tasked with supporting Staff Directory changes is too large. The Coordinators perform their tasks too infrequently to be adequately trained. The organization tasked with supporting Staff Directory changes may need to be reduced in size or provided more training.
- The web site used to host documents supportive of telecommunications and messaging was corrected but could also be simplified. We have suggested that it be collapsed down to a core collection of policies, procedures, list of contacts and user manuals.
- In the longer term (one to two years), we believe it will be necessary and cost-effective to move the Staff Directory function to a better repository and administer it with more appropriate tools. St. Louis County currently supports software that would be appropriate for a repository, and IT management has plans to conduct such a migration.

KEY FINDINGS:

- The number of Staff Directory administrators is too large to be effective. Telecom Coordinators in many cases performs their duties so infrequently that they cannot be adequately trained.

- There were inconsistencies between lists of staff authorized to perform maintenance against Active Directory, the staff directory, personnel records and the actual privileges granted. These discrepancies were resolved.

- The web site containing procedures and instructions for Telecom Coordinators contained outdated information and dead links. The web site has been updated with newer content. The dead links are being resolved.

- The implementation of the RAVE alert system will provide proactive messaging for critical employee communications to supplement traditional methods in place. This system supports additional means for communicating with employees internally. This will help to ensure that employees will be able to receive critical communications even if their Staff Directory entries are not updated.

During this review we met with:

- Mike Duncan – Chief Information Officer,
- Tom Kendrick – IT Operations Manager,
- Orville Moore – Telecommunications Manager,
- Vickie Barela – Telecommunications Technician, and,
- Debbie Oberlohr – Telecommunications Assistant.

They were our primary contacts for the audit. We received excellent cooperation and support.

Our findings and recommendation were provided to Mike Duncan – Chief Information Officer and Orville Moore – Telecommunications Manager.

TABLE OF CONTENTS

Background and Introduction

Administration Department

The Department of Administration provides administrative services to all St. Louis County offices and departments. These services include Accounting, Budgeting, Information Technology, Personnel, Employee Benefits, Retirement, Procurement and General Services, Customer Service and Treasury. Responsibilities within those service areas include payroll, capital assets inventory, telecommunications, risk and insurance management, safety, investments, records management, mail and courier services, central receiving, satellite center administration, front desk and telephone support for the main County information telephone line and publishing employee and retirement newsletters.

The Department of Administration also prepares and publishes the annual budget and financial reports. Administration is a primary point of contact for the Civil Service Commission, Retirement Board of Trustees, Fund Investment Advisory Committee and the Employee Benefits Advisory Committee.

The 2013 budget for the Department of Administration was $15,574,504, an increase of $1.7 million or 12.3 percent. Along with increases for salaries and fringe benefits, the budget includes the following new activities:

- $360,800 to develop a supplier diversity program to encourage the participation of minority, women, and disadvantaged companies to bid on County business;
- $310,100 to expand centralized cashiering to the South County satellite office to improve customer service.
- Consolidation of Geographic Information System (GIS) functions; and,
- The addition of a computer security position to assist in managing ever increasing security risks associated with cyber-crime.

The Administration Division manages IT systems; maintains department records; assists in disaster recovery coordination and handles personnel services such as payroll, insurance benefits, recruitment, job classification and issuance of supplies. The Administration Department includes the Fiscal Management, Budget and Risk Analysis, Personnel, Procurement and Information Technology Divisions.

Information Technology (IT) Division

The Information Technology Division is responsible for information technology and telecommunications services and policies for County Government. The Chief Information Officer leads the activities of the division, which are carried through a combination division staff and contract personnel. The Chief Information Officer supervises a GIS Manager who supervises fourteen staff who support Geographic Information (digital mapping and data) systems cartographic systems. The Chief Information Officer supervises an Operations Manager who in turn supervises four other Managers or Analysts who support major enterprise information systems. The Chief Information Officer also supervises the Telecommunications Manager and functions as a liaison to the REJIS Site Manager, providing direction on REJIS services performed for the County under contract. The Telecommunications function within IT includes a Telecommunications Manager, two Telecom Technicians, and a Telecom Assistant.

Telecommunications

Staff within the Information Technology Division are tasked with providing support predominantly for telephone systems, private branch exchanges, switchboards, telephone equipment and messaging systems. Because of the overlap in policies and support responsibilities between IT and Telecommunications, it was necessary for Audit to review, at a high level, the organization and policies of the Division (Information Technology) and the Section (Telecommunications). In most cases, Policies regarding Telecommunications are defined by IT policies. A subset of these policies deal directly with Telecommunications. The Telecommunications function administers telecommunications equipment and provides support for private branch exchanges, voice mail systems, phone handsets, phone headsets and various handheld devices.

Active Directory

Active Directory is a directory service implemented by Microsoft for Windows networks. Active Directory is included within most Windows Server operating systems. It is a service that uses a particular kind of database to authenticate users when they provide their credentials (such as a user ID and password) to a network. A specialized server called a domain controller is used to host Active Directory. Domain controllers process requests to authenticate users. Domain controllers also process request for access privileges. The Domain controller enforces security policies for users and software on the network. For example, when a user logs into a computer that is part of a Windows network Active Directory checks the submitted password and determines whether the user is a current and authorized user. It also determines whether the users has special system administration privileges or is a normal system user.

Active Directory is a standard service for managing authentication and a database of user credentials that was developed by the Internet Engineering Task Force (IETF). Active Directory uses a directory technology called Lightweight Directory Access Protocol or LDAP. Active Directory was first released with Windows 2000 Server edition and revised to improve functionality in Windows Server 2003. Additional improvements were made in Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2. It is also included in Windows Server 2012.

Origin of the Staff Directory

The Staff Directory application was developed in 2003 to replace a printed employee phone directory and to provide employee location information to use in emergency situations. It is a web application (asp.net) that utilizes data from Microsoft's Active Directory user security and identity management system. It also provides a user interface for controlled access to Active Directory for administrators. The application was developed and has been maintained and updated by the REJIS application development group. The application has been included in testing by external security auditors in 2008 and 2011.

The application contains telephone contact, organization and location information for County employees. Because this application predated the MUNIS ERP system, several data items that are also maintained in MUNIS are maintained here as well.

The St. Louis County Staff Directory is a system that allows St. Louis County employees to query the database of St. Louis County users. The underlying data is the data managed by Active Directory. One database provides user credentials used to authenticate users and records that help employees enter queries to locate staff by their first name, last name, department or division. This technology was introduced with Windows 2000 Server and has been enhanced with subsequent releases of Windows Server. The application contains approximately 4,000 records, but it is queried extensively by County employees to provide contact information for staff and management within County Departments and related organizations. St. Louis County has defined four types of administrators who can enter or change data within Active Directory:

Administrator	Duties
Admin	This administrator can enter or alter data, including privileges.
Organizational Unit	This administrator can enter or alter data, for individuals within their organizational unit, which typically aligns with a Department and Division.
Phone	This administrator can modify information for a specific organization.
Telecom	This administrator can assign administrators.

If an administrator's user ID is disabled or revoked, the administrator has no privileges.

A design decision made in 2003 to make the administration of this system highly decentralized, with a large number of departmental and divisional coordinators maintaining data. The Telecommunications Section within the Information Technology Division provided high level coordination. The Personnel Division was not tasked with any role in this process, despite their status as the responsible authority for employee life cycle events for most County employees.

Current Status

Currently, St. Louis County has a group of 22 Organizational Unit (OU) Administrators, who have direct rights to Active Directory (AD) for their business units. St. Louis County also has 50 defined Telecom Coordinators have limited access via the Staff Directory administrative interface to change certain fields for their business units. In some cases the same person fulfills both roles. We also have 25 departmental personnel coordinators who enter employee information into the Munis ERP system. These personnel coordinators often overlap with the Telecom Coordinators. The creation and closing of user accounts in Active Directory is shared between OU Administrators and Enterprise IT (REJIS) staff.

Audit of Staff Directory

The Auditors met with staff and management within IT and the Telecommunications function in May of 2013 to discuss recent audit findings with the content of the Staff Directory. We had found that several persons who were designated as Telecom Coordinators performed their administration tasks so infrequently that they did not have the opportunity to become familiar with the tasks or be well trained on these tasks. Also, due to staff absence or turnover employee information was not administered or kept up-to-date. We had been reviewing the Staff Directory entries by Department, within every audit we performed. We agreed that it would be more cost effective to coordinate a review of the Staff

Directory in its entirety while IT and Telecomm staff reviewed and updated the entire database. Their review and update has yielded good results

Audit Concerns

Concerns with the current system include duplication of effort, inconsistency across departments in timeliness of maintenance, inconsistently formatted information due to "freehand" entry of data directly into AD by Organizational Unit (OU) Administrators, and potential security concerns with a homegrown application directly pulling data from Active Directory. IT and County Auditor staff reviewed the applications in May of 2013. A primary concern at that time was the inclusion of records for system or test user IDs within search results. As an interim step, additional filtering was applied by IT Staff in August 2013 to prevent display of records not related to current employees.

Changes and Future Planned Changes

In November 2013, IT will be implementing a countywide employee notification system -- a hosted service from AT&T called Rave Alert Messaging. This requires entry and maintenance of employee information in yet another system. In order to avoid duplication of effort, the IT Division's direction is to simplify and consolidate processes.

Information Technology modified Active Directory to include the Employee Identification Number (EIN). This is the key identifier in the MUNIS system for employees. IT will use extracts from MUNIS joined to Active Directory by the EIN to update location information. At the same time, employees will be directed to use the MUNIS Self-Service web site to update their personal contact information for use in employee notifications in the event of a building closing. Extracts from MUNIS and Active Directory will be loaded into the Rave system. IT has purchased an Active Directory management tool called Adaxes Active Directory Management and Automation. This tool will be used for maintenance of Active Directory. The tool has additional controls in it. It should be "safer" to use than the in-house developed applications. By relying on re-use of data in MUNIS, we reduce the amount of data entry required in Active Directory is reduced. The origination and closing of user accounts in Active Directory will now be handled primarily by Personnel staff who will have a restricted access to Active Directory via the Adaxes tool. This way one person carries out the user account life cycle at the same time that they are doing their MUNIS life-cycle data entry.

For now, the data will continue to be displayed via the Staff Directory. The application will be replaced by use of the SharePoint 2013 People Search tool, which provides comparable functionality. This transition will happen in late 2013 or early 2014. SharePoint has built-in replication with Active Directory, but provides a layer of protection, in that Active Directory is not directly accessed. The data updated in MUNIS and the Adaxes tool will feed both SharePoint and the Rave messaging system.

This will reduce or eliminate the need to have Telecom Coordinators involved in use life cycle maintenance, and allow them to be focused on telecommunications issues. The Organizational Unit (Department and/or Division) Administrators will still have business unit level rights, but they will use the Adaxes tool, which will provide structure to their access privileges.

Objectives and Scope of Audit

At the beginning of the audit, we met with management and established audit objectives. These objectives are stated in the positive. These are objectives we expect to be met or controls we would expect to find in this area. Later, in this report, we provide results of the audit, against these objectives. At the start of the audit, the objectives and the scope of the audit were as follows:

IT Policies
The Information Technology function should have written policies. Policies should be up-to-date. Written policies should represent current accepted practices. Policies should be made available to employees.

IT Procedures
The Information Technology function should have written procedures. Procedures should be complete and up-to-date. Written procedures should represent current accepted practices. Procedures should be made available to employees.

Telecommunications Policies
The Telecommunications support function should have written policies. Policies should be up-to-date. Written policies should represent current accepted practices. Policies should be made available to employees.

Telecommunications Procedures
The Telecommunications support function should have written procedures. Procedures should be up-to-date. Written procedures should represent current accepted practices. Procedures should be made available to employees.

Access Security
Access to critical data should be controlled with adequate security measures.

Web Site
Web sites (internal and external) should contain valid and correct information and be well-organized.

Active Directory Updates
Controls should be in place to limit updates to the Active Directory database that contains user credentials (user IDs and passwords) for St. Louis County network users.

Software Tools
Suitable software tools should be used for the management of data within the Active Directory database.
Suitable software tools should be used for queries generated of data from the Active Directory database.

Backup and Recovery
Data within Active Directory and the Staff Directory should be backed up and recoverable.

Record Retention
Written retention schedules should exist. Written retention schedules should be regularly reviewed and approved.

Update Procedures
Written procedures should exist that provide instruction for database update processes.

Disclosures
If data is sensitive, appropriate disclosures should be in place and displayed along with the results of queries from the data.

Compliance Testing
Results of sampling and compliance testing should demonstrate that controls are working as intended.

I. Information Technology Policies

We reviewed Information Technology policies for content and organization. Our review included these policies:

Policy Administration,
Schedule of Authorizations,
Business Records Treatment,
Email Use,
Internet Use,
Internet Publishing and Blogging,
Software Licenses,
GIS Asset Management,
Computer Equipment Maintenance,
Printer Maintenance Process,
Mobile Communications and Computing,
Disposal of Computer Equipment,
System Sourcing and Software Development,
General Information Security,
Computer and Telecom Authorization and Passwords,
Internet and Firewalls Security,
External User Network Access,
Portable Device Security,
Portable Storage Device Security,
PCI Security,
Data Centers,
Change Management,
System Interfaces,
Employee Owned Computers,
Wireless LANs,
Document Management and Imaging.

Our review included key discussions, documents, lists, agendas and reports. We noted specific reference within the Information Technology policies that were outdated.

We noted that references and links to minutes from the Information Systems Steering Committee (ISSC) meetings are posted on the IT Intranet page which span from January 2004 to September of 2010. These minutes and meeting notes need not be retained on the internet. Twenty three documents from 2004 to 2009 are likely no longer relevant and could be archived and removed from the intranet web site:

- ISSC Notes 9-11-09,
- ISSC Notes 6-02-09,
- ISSC Notes 1-21-09,
- ISSC Notes 9-18-08,
- ISSC Notes 5-19-08,
- ISSC Notes 1-17-08,
- ISSC Notes 5-24-07,
- ISSC Notes January, 2007,
- ISSC Notes September 2006,
- ISSC Notes May 2006,
- ISSC Notes January 2006,
- ISSC Notes September 2005,
- ISSC Notes June 2005,
- ISSC Notes May 2005,
- ISSC Notes January 2005,
- ISSC Notes November 2004,
- ISSC Notes September 2004,
- ISSC Notes August 2004,
- ISSC Notes July 2004,

- ISSC Notes June 2004,
- ISSC Notes May 2004,
- ISSC Notes April 2004,
- ISSC Notes March 2004,
- ISSC Notes January 2004.

This would free storage space for more relevant information.

Recommendation

1. We recommend that the Chief Information Officer consider removing archived ISSC meeting minutes from 2009 and earlier, that are currently hosted on their intranet.

Management Response

1. **We agree and have removed these from the main ISSC page.**

II. Information Technology Policy Templates

We reviewed Information Technology policies for content and organization.

We noted that the organization of the policies would be improved if the policies were placed on standard templates. These templates provide places for date of adoption, approval dates, name, subject of policy and revision dates. The templates have been adopted and are in use by other St. Louis County departments (Health, Human Services) with good results.

Recommendation

2. We recommend that the Chief Information Officer consider placing Information Technology policies and procedures on standard templates.

Management Response

2. **We agree and intend to convert the policies to the suggested template.**

III. Staff Directory – Drop Down Lists

The Staff Directory can be queried by using pre-defined drop down lists containing Department and Division names. We noted that fifty-one of these defined combinations of Department and Division yielded no results. Employees are now grouped differently. If you searched on these combinations, the search yielded no results.. No employee records were displayed:

Department	Division
Administration	Budget
Administration	ERP
Administration	Procurement and Insurance Safety
Board of Elections	Data Entry
Board of Elections	Elections Statistics
Board of Elections	Field Operations
Board of Elections	Records
Board of Elections	Teams
CASA	Administration
CASA	CASA
Health	Air Pollution
Health	CDC Clinical Lab
Health	Comm. Disease Control/Clinical Lab
Health	Environmental Protection/Env. Labs
Health	Environmental Protection/North Animal Shelter
Health	Environmental Protection/South Animal Shelter
Health	Environmental Protections/Vector Control

Health	Fiscal Services/Printshop
Health	Fiscal Services/Vital Records
Health	Health
Health	Health Services/Dental Services
Health	Health Services/Family Mental Health
Health	Health Services/Medical Records
Health	Health Services/Pharmacy
Health	Information Systems
Health	Medical Services/Pediatrics
Health	Medical Services/Women's Health
Health	Quality Control
Health	Recycling Education
Health	Research Services
Health	Research/ IT Department
Health	Research/Health Information Resources
Health	Sanitation
Health	Social Services
Health	Waste Management
Judicial Administration	Circuit Clerk/Associate Civil and Small Claims
Judicial Administration	Circuit Clerk/Circuit Civil, Equity Domestic Relations & Juvenile
Judicial Administration	Circuit Clerk/Criminal/Traffic
Judicial Administration	Circuit Clerk/Human Resources
Judicial Administration	Court En Banc/Judges
Judicial Administration	Court En Banc/Judges & Court Reporters
Judicial Administration	Probate Court/Administration
Judicial Administration	Probate Court/Certified Copies
Judicial Administration	Probate Court/Settlements
Police	Board of Police Commissioners
Police	Office of Information & Technology
Police	Special Operations/Community Action Team
Public Defender	- Blank -
REJIS	- Blank -
University of Missouri – Outreach & Extension	- Blank -
University of Missouri – Outreach & Extension	University of Missouri – Outreach and Extension

An effort was underway, during the audit, to correct these drop down lists and align them with standardized department and division names.

Recommendation

3. We recommend that the Chief Information Officer ensure that drop down boxes that are used to query the Staff Directory are replaced with amended set of Department and Division combinations.

Management Response

3. **We agree and are in the process of pruning out the obsolete drop downs. The move to the new SharePoint system should remove the need for ongoing maintenance of department/directory combinations.**

IV. Intranet Dead Links

We noted dead links on the IT Telecom intranet web. Links to documentation for the Telecom Coordinators did not work. Content needed to be updated. The web site was updated but it still contains dead links and certain key documentation was missing:

- The logo on the Telecommunications Intranet page linked to an empty page. If you click on the icon or logo in the upper right hand side of the page, you are sent to an empty page.
- The County IT Help Desk had a link to the term "Telecom Coordinator" which should display a list of the Telecom Coordinators. This was a dead link.
- A link in the Documents section to the term "Long Distance" was a dead link.
- A reference to IT policies omits the policy on PCI Security (IT Policy 09.06).
- Under "Documents – Long Distance Services", the document contained a link to Telecom Coordinators which should have displayed a list of the Telecom Coordinators. This was a dead link.

- Under “Policy 9.0 General Information Security” there were references and links to IT policies. The name of IT Policy 9.0 was incorrectly listed as Computer Telecommunications Access Identification & Authentication. Also, IT Policy 9.06 on PCI Security was missing from the list.
- Under “Rates and Pricing – Telephone Equipment Pricing” links were missing for EHS Cable for Office Pro 1 and 2 and Polycom Extension Microphones.
- Under “Rates and Pricing – Pages, the rates were from 2012. If the rate is still in effect the year could be rolled forward.
- Under “Systems & Services – Smartphone Active Sync”, there was no corresponding document.
- Under “Corporate Wireless – Verizon Business Phones & Plans”, there was a dead link.
- Under “Policies”, the links within the policies did not work.
- Under “Policy 2.0 Email Use, there was a link to a prior, outdated web page.
- Under “Policy 3.0 Internet Use, the document contained links to 2.0 Email Use. The link was broken.
- Under “Policy 9.0 Computer and Telecom Authorization”, there were links to the prior web page.
- Under “Policy 9.04 Portable Device Security” there were broken links.
- References to “Sprint/Nextel Wireless Vendor Contacts” could be shortened to “Sprint”. The company has changed their name.

These links were being corrected during the audit.

Recommendation

4. We recommend that the Chief Information Officer ensure that links to documentation for the Telecom Coordinators are repaired, including links to procedures for making changes to Active Directory and the Staff Directory.

Management Response

4. **We agree. The policy updates have been made – the telecom intranet fixes are underway.**

V. Staff Directory Updates

The update project, undertaken by IT staff was very successful:

- Based on the initial record count in May of 2013 there were 5,700 Staff Directory records. This number exceeded the count of employees by 1,700 records. A significant percentage of the records were records of terminated employees awaiting deletion. This was validated within recent audits. At the conclusion of the audit in August of 2013, the Staff Directory records count was close to 4,000 records. This is consistent with actual employee counts.
- The number of records missing two or more one key data fields is now about 1 %, which we believe is acceptable.
- At least 130 records for system or test user ID have been filtered out of search results. This improves data security.
- We confirmed the deletion of 222 records for employees who have terminated within the last six months.
- Telephone listings and contact listings for affiliated organizations such as the University of Missouri Extension Council are maintained on their own web sites. St. Louis County may be able to provide links to these other rosters until a new directory can be implemented.

Recommendation

5. We recommend that the Chief Information Officer explore the use of links to external telephone listings and contact lists maintained by other agencies or affiliated organizations.

Management Response

5. **We will review this approach when we implement the new SharePoint based system.**

VI. Organization

Organizations within St. Louis County are divided into smaller workgroups according to a well-defined structure. Departments can be divided into Divisions. Divisions may be divided into Sections. Under a Section there may be individual project defined.

This structure is well established within the Budget book and the reporting structure maintained within accounting records established in the MUNIS system.

The telecommunications support functions are described inconsistently as a Department or Division within key internal documents:

- On the Budget Office Intranet page the Telecommunications support function is defined as a Department.
- Within the 2013 Budget Book, Information Technology was described correctly as the Division:

> *"The Information Technology (IT) Division develops County IT policies and plans and manages the introduction, operation and use of information technologies, including telecommunications and Geographic Information Systems (GIS), from a countywide or enterprise perspective. Activities include developing and communicating IT strategies, policies, practices, budgets, architecture and standards. The division manages projects and issues and consults with departments to identify and address their needs. The division plans and coordinates the business telecommunications systems, facilities, operations, and projects for the County as an enterprise."*

- Telecommunications also appeared on several drop-down lists such as the main Intranet page, at the Department level.

This caused some confusion with respect to finding information grouped at the Department level that should have been placed at the Section level (Telecom) or Division/Section level (IT – Telecom). Based on the structure established within accounting records, the Telecom function is a Section.

Recommendations

6. We recommend that the Chief Information Officer ensure that inconsistencies are corrected with respect to internal references to the Telecommunications support function.

Management Responses

6. **We agree and will check for such inconsistencies.**

VII. Telecommunications Policies

Written policies that address Telecommunications Support functions are posted on an intranet site.
One of these policies has been updated recently IT Policy 9.06 PCI Security. The written policies do not have evidence of management approval.

The policies have a creation date, which corresponds to the "date of issue", however there is also a modified date, which is a more recent date.

The other policies have approval dates as follows:

Policy Number	Name	Date of Issue	Modified
Policy 01.00	Policy Administration	02/26/2003	08/20/2013
Policy 01.01	Schedule of Authorization	12/18/2003	08/20/2013
Policy 02.00	E-Mail User	04/07/2003	08/20/2013
Policy 03.00	Internet Use	04/07/2009	08/20/2013
Policy 03.01	Internet Publishing and Blogging	04/12/2006	08/20/2013
Policy 04.00	Software Licenses	10/11/2000	08/20/2013
Policy 04.01	GIS Asset Management	05/16/2006	08/20/2013
Policy 05.00	Computer Equipment Maintenance	01/01/2005	08/20/2013
Policy 05.00	Printer Maintenance Process	01/01/2005	12/27/2006
Policy 05.00	Process Diagram	10/31/2000	12/27/2006
Policy 05.00	Server Maintenance Process	01/01/2005	02/08/2010
Policy 06.00	Mobile Communications and Computing	10/15/2009	08/20/2013
Policy 07.00	Disposal of Computer Equipment	12/13/2000	08/20/2013
Policy 08.00	System Sourcing and Software Development	10/18/2001	08/20/2013

Policy 09.00	General Information Security	05/19/2008	08/20/2013
Policy 09.01	Computer and Telecom Authorization and Passwords	02/17/2005	08/20/2013
Policy 09.02	Internet and Firewall Security	11/14/2001	08/22/2013
Policy 09.03	External User Network Access	11/03/2003	02/08/2013
Policy 09.04	Portable Device Security	05/25/2005	08/20/2013
Policy 09.05	Portable Storage Device Security	03/23/2007	03/23/2007
Policy 09.06	PCI Security	09/11/2012	09/17/2012
Policy 10.00	Data Centers	01/15/2003	08/20/2013
Policy 10.01	Change Management	09/11/2008	07/17/2013
Policy 11.00	System Interfaces	01/17/2008	08/20/2013
Policy 13.00	Employee Owned Computers	07/22/2003	08/20/2013
Policy 14.00	Wireless LANs	08/21/2003	04/01/2009
Policy 15.00	Document Management and Imaging	09/29/2003	08/20/2013
Policy 16.00	Electronic Payments	10/16/2003	08/20/2013
Policy 17.00	Network Membership	11/12/2003	05/07/2010
Policy 18.00	Telecommuting	11/06/2006	04/24/2008
Policy 19.00	User Computer Mgmt Admin	07/06/2009	07/07/2009

We have recommended that these policies include a reference to existing written disaster recovery plans, or provide a high level description of critical systems and functions that may need to be recovered after a disaster. We would suggest tracking approval and modified dates rather than original issue date, as the approval date provides more information regarding the relevance of the policy.

Recommendations

7. We recommend that the Chief Information Officer review the current IT Policies and update them accordingly.

Management Responses

7. **We agree with the recommendation, while noting that disaster recovery plans will have a more limited circulation than policies which are available to all County employees.**

VIII. Telecommunications Procedures

There are written instructions for Telecom Coordinators that provide instructions for the addition of information about an employee to Active Directory (and the Staff Directory). Written procedures do not address several tasks. A few of these tasks, such as the removal of a employee from Active Directory and the Staff Directory must be performed by others (a REJIS technician), however the omission of information about these processes from the written procedures may provide the Telecom Coordinator with an incomplete understanding of the processes.

Tasks related to the reassignment of ownership of files of a former employee can be difficult in any organization.

The effect of this lack of written procedures has been an increase in the number of Active Directory and Staff Directory records for terminated and/or former employees:

- Personal computer files owned by a former employee should be archived or saved to media such as a CD or thumb drive, to ensure the files are not lost. The media should be provided to the employee's immediate supervisor. This typically requires a Help desk call so that a Help Desk technician with appropriate privileges can locate and archive the user's files.
- The ownership of personal computer files of a former employee should be re-assigned, typically to the supervisor of the former employee.
- Once the ownership of personal computer files is reassigned, a request should be forwarded to a REJIS technician so that the Active Directory entry (and the Staff Directory entry) can be deleted.

Procedures do not define the population that should be included in Active Directory or the Staff Directory. Procedures do not address acceptable omissions from the Staff Directory. For example, for security considerations, it may be acceptable to omit certain contact information for:

- Police officer depending on their assigned detail,

- Justice Services, or,
- Corrections Medical or Nursing Staff.

Recommendation

8. We recommend that the Chief Information Officer ensure that additional written procedures are provided that explain these processes:
   - archival and reassignment of ownership of a terminated user's files,
   - guidelines or rules for inclusion of information in the staff directory,
   - inclusion of links or references to external directories for affiliated agencies.

Management Response

8. **We agree that these procedures should be clarified, and we intend to do so.**

IX. Intranet Pages

We reviewed the content of intranet pages. We noted that a series of intranet pages has been hosted on subjects such as phone handsets, headphones, wireless services, and telephone service rates. IT Telecom staff have hosted documents which provide relevant information on these subjects, such as rate comparisons or owner's manuals for equipment.

We have suggested that the organization of this site be simplified through a simple list of named documents that adhere to a naming convention. If the document names are structured properly, the documents can be grouped alphabetically. This would greatly simplify the amount of web maintenance needed to add or correct web links to key documents.

For example, owner's manuals for headsets could be named for the convention: "Device, Manufacturer, Model, Document". If a convention is followed, then a document would have a name such as Headset – Motorola – Model 105C – Owners Manual". If a strict convention is followed it would be very easy to pick relevant documents from a simple one-page list.

Use of a strict naming convention could greatly simplify the effort required to find a particular document and the effort to maintain web sites were these documents are archived.

Recommendation

9. We recommend that the Chief Information Officer give consideration to use of a naming convention for documents stored and provided on their intranet page.

Management Response

9. **We will review the existing naming system to improve clarity.**

X. Record Retention Schedules

There are written record retention schedules for the Administration – IT function that describe critical records and specify retention periods. The record retention schedules are regularly reviewed and updated. They are reviewed by a Records Manager, Legal and Audit. The record retention schedule for Admin – IT does not mention Active Directory. Active Directory contains user IDs, user names and credentialing information such as encrypted passwords. It is use to store this information for 4,000 employees.

Active Directory is backed up and recoverable as part of the Microsoft network operating system.

It might also be prudent to either reference disaster recovery plans or list key facilities and systems that would need to be recovered by IT staff or IT – Telecom staff.

Recommendation

10. We recommend that the Chief Information Officer specifically mention the Active Directory database within record retention schedule and describe, at a high level, how it is backed up and recoverable.

Management Response

10. **There is a set of written backup procedures that is separate from the record retention schedule but we agree that it would be worthwhile to reference key digital resources such as Active Directory within the record retention schedule.**

XI. Centralization

Currently, St. Louis County has a defined group of 22 Organizational Unit (OU) Administrators who have direct rights to Active Directory (AD) for their business units. These are staff who help establish users IDs and privileges for employees. St. Louis County also has 50 Telecom Coordinators who have limited access via the Staff Directory administrative interface to enter certain fields in the staff directory like a phone number, phone extension fax number or street address. These staff enter the additional information that populates the Staff Directory. In some cases the same person fulfills both roles. We also have twenty-five departmental personnel coordinators who enter employee information into the MUNIS ERP system. These personnel coordinators often overlap with the Telecom Coordinators. Similar information is keyed to identify employees within the St. Louis County email system. The creation and closing of user accounts in Active Directory is shared between Organizational Unit (OU) Administrators and Enterprise IT (REJIS) staff

We have suggested that these defined roles be combined and that these informal organizations be "flattened" or performed by fewer administrators who are trained to do more than one of these tasks. The effort required to assign, re-assign and train these administrators may require more effort than the effort required to make these changes to the data.

We've review plans in place within Information Technology and believe the proposed changes may streamline this effort. Future plans require less re-keying of data and should allow individuals to update a portion of their own data.

Recommendation

11. We recommend that the Chief Information Officer review the "organizations" established to key enter employee location and identifying data and consolidate this work among fewer coordinators.

Management Response

11. **We are in agreement that the existing approach is excessively decentralized and plan to implement a more centralized method with the transition to the new SharePoint system.**

XII. Ordinance 3,107

We reviewed the ordinance that Ordinance 3,107 and Chapter 109 of the St. Louis County Code of Ordinances is in need of revision with respect to the department name, job titles, job duties and the function of the department.

For example, the ordinance refers to the division as the "Data Processing Division". The responsibilities of the current Information Technology Division extend beyond data processing and include other areas like communications, networking, security, voice and data messaging.

Recommendations

12. We recommend that the County Council consider an update to ordinances that established the Data Processing Division to reflect the department name, job titles, job duties and the function of the department as it currently exists.

Management Responses

12. **We support this idea.**

Assessment of Controls – Post Audit

At the conclusion of the audit, we assessed the effectiveness of controls based on the results of the audit:

IT Policies

The Information Technology function had written policies. We suggested specific updates to these policies. We also recommended that policies be placed on a standard template that provides standardized information about each policy, such as the adoption date, last revision date and approvals. We suggested that references to old Information Steering Committee Board meetings from 2006 and earlier be archived and deleted from the IT web site.

Written policies generally represent current accepted practices but need minor updates for things like titles.

IT Procedures

The Information Technology function had written procedures. We recommend the use of standard templates where practical. Procedures were fairly complete and up-to-date. Written procedures should represent current accepted practices, however, we have recommended and IT is implementing considerable changes to current practices. Procedures are made available to employees.

Telecommunications Policies

The Telecommunications support function has written policies. Policies are reasonably up-to-date. Written procedures should represent current accepted practices, however, we have recommended and IT is implementing considerable changes to current practices. Policies are made available to employees.

Telecommunications Procedures

The Telecommunications support function has written procedures. Procedures are reasonably up-to-date. Written procedures should represent current accepted practices however, we have recommended and IT is implementing considerable changes to current practices. Procedures are made available to employees.

Access Security

Access to critical data is controlled with adequate security measures. In the future the number of staff who can directly edit user credentials will be reduced and edits and updates to Active Directory will be performed through a utility which has additional control features.

Web Site

Web sites (internal and external) contain valid and correct information but we had concerns that the web site was overly complex.

Active Directory Updates

Controls are in place to limit updates to the Active Directory database that contains user credentials (user IDs and passwords) for St. Louis County network users. In the future, edits and updates to Active Directory will be performed by fewer individuals through a utility which has additional control features.

Software Tools

Newer and better controlled software tools are being introduced for the management of data within the Active Directory database. Queries were not functioning correctly. These queries have been repaired.

Backup and Recovery

Data within Active Directory and the Staff Directory is be backed up and recoverable.

Record Retention

Written retention schedules exist but did not include the Staff Directory nor Active Directory. Written retention schedules are regularly reviewed and approved.

Update Procedures

Written procedures exist that provide instruction for database update processes.

Disclosures

If data is sensitive, appropriate disclosures are in place and displayed along with the results of queries from the data.

Compliance Testing

Results of sampling and compliance testing demonstrated that controls were not working as intended but they were repaired and improved during the audit. Subsequent compliance testing indicated that controls had been repaired and improved greatly.