



State of Montana

**Department of Public Health and
Human Services**

Information Technology Plan 2016



Healthy People. Healthy Communities.

Department of Public Health & Human Services

Table of Contents

1. EXECUTIVE SUMMARY	3
2. ENVIRONMENT, SUCCESS, AND CAPABILITIES.....	5
3. IT CONTRIBUTIONS AND STRATEGIES	8
4. IT PRINCIPLES	10
5. IT GOVERNANCE	13
6. IT FINANCIAL MANAGEMENT.....	14
7. IT SERVICES AND PROCESSES	16
8. IT INFRASTRUCTURE, STAFFING AND RESOURCES	20
9. IT RISKS AND ISSUES	22
10. IT GOALS AND OBJECTIVES	23
11. IT PROJECTS	26
12. SECURITY AND BUSINESS CONTINUITY PROGRAMS.....	29
13. PLANNED IT EXPENDITURES	33
14. ADMINISTRATIVE INFORMATION.....	34
15. ACRONYMS AND DEFINITIONS.....	35

1. Executive Summary

Montana has three basic business drivers that shape the State's programs and Information Technology (IT) strategies: jobs, education, and effective/efficient government. The Department of Public Health and Human Services' (DPHHS) mission is to improve and protect the health, well-being, and self-reliance of all Montanans. To fulfill that mission, the department has made significant investments in information technology. Our systems and the data they manage are mission critical for the programs they support. Responsibility for these systems lies within the Technology Services Division (TSD), which oversees system development, maintenance, and operations. TSD also oversees IT system procurement, project management, and data center and telecommunications services.

The department strives to manage its systems as an overall integrated portfolio. System life-cycle management is key in keeping up with fundamental technology changes like web services, enterprise-service architecture and cloud-based systems. Several of the department's largest and most complicated systems have reached end-of-life and are scheduled to be replaced or in the midst of being replaced. The department is going through a modernization effort with the goal of being off the State of Montana mainframe system. According to a report by the Department of Administration – State Information Technology Services Division (SITSD), DPHHS will be sole customer of the State Mainframe at the end of calendar year 2019.

The system replacement efforts focus on the next generation of IT systems. The new generation of department systems will:

- Improve the integration of services to customers that use more than one of the department's programs.
- Improve the quality, integrity, reliability, and security of data used to administer the department's programs and provide benefits to customers.
- Increase the value and lower the risk of the department's investment in information technology by providing components to be shared and reused by many systems.
- Provide access to mobile technology solutions for both citizens and employees.

The system modernization efforts incorporate technologies such as a business rules engine, web services, mobile technology solutions, and Service-Oriented Architecture (SOA) into the design for replacing the legacy human service systems. The goal of the replacement effort is to foster holistic service delivery where programs collaborate with each other in meeting the needs of individuals and families.

Our plan includes goals and objectives that directly support the department's strategic goals and objectives and the goals in the State IT Plan published by the State Chief Information Officer (CIO). The DPHHS IT Plan supports department-wide initiatives to enhance the service levels of all its programs by establishing an enterprise-based environment. This will increase the efficiency of service delivery by facilitating information sharing while maintaining the data, functionality, and confidentiality unique to

each program. All of the initiatives presented in this plan are designed to ensure that the department is able to accomplish its mission to promote the health and welfare of the citizens of Montana.

TSD has adopted the values statement identified in the State IT Plan. The values are:

Integrity – Do what is right, legally and morally

Honesty – Communicate and act truthfully

Accountability – Take responsibility for actions

Stewardship – Properly utilize the resources of the state

Respect – Treat people with dignity and value them as individuals

2. Environment, Success, and Capabilities

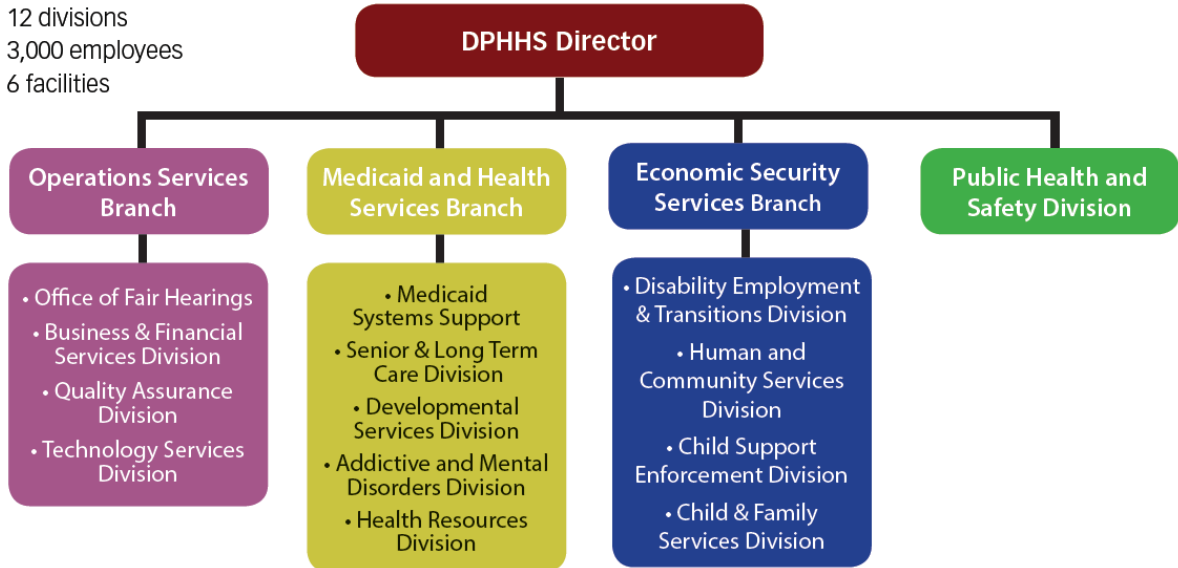
The Department of Public Health and Human Services is a diverse state department that provides services for people all over Montana. It is the largest department in state government with over 3,000 employees, a nearly \$3.8 billion dollar annual budget and almost 2,500 contractual agreements with partners in every community across the state including eight tribal governments. The department's mission is to improve and protect the health, well-being and self-reliance of all Montanans. Montana's small population, scattered over an immense area, poses challenges in delivering information technology services. We make a big difference in thousands of Montanans' lives, families and communities every day.

The department has three branches: Operations Services; Medicaid and Health Services; and Economic Security Services. Each branch has several divisions under its umbrella. The department has a total of 12 divisions. In turn, each division oversees numerous bureaus, programs, services, grants, and facilities. The Public Health and Safety Division is unique in the organizational structure as it is directly attached to the Director's Office. The other functions that reside within the Director's Office include the Office of Legal Affairs, Human Resources, Public Information, Government Support, and the Prevention Resource Center.

The Technology Services Division is part of the Operational Services Branch and manages IT system development and maintenance, IT procurement, IT projects, data center, and telecommunications services.

How DPHHS is organized

- 3 branches
- 12 divisions
- 3,000 employees
- 6 facilities



Funding

The department derives its funding from three major streams: federal funds, state general funds, and state special revenues. Below is a breakdown of where the department received its funding for the 2017 Biennium:

Source	Amount	Percent
Federal Funds	\$2.6 billion	70 percent
State General Funds	\$837 million	22 percent
State Special Revenue	\$307 million	8 percent
Total Funding -	\$3.8 billion	

The department has some of the most complex and resource-intensive IT systems in the State. It is a primary user of the State of Montana Mainframe with the state’s child welfare system (CAPS) and the child support enforcement system (SEARCHS) operating there, as well as the Medicaid programs Supplemental Nutrition Assistance Program (SNAP), and the Temporary Assistance for Needy Families (TANF) eligibility system called TEAMS. This system is currently in archive mode for records retention for TANF cases. A small amount of funding was provided in HB2 by the 2015 legislature to start the replacement of CAPS. The first phase is focused on case management, investigations, and centralized intake areas. Funds for planning to develop an RFP for SEARCHS replacement were not obtained in the 2015 Legislature, therefore the department will be proposing funding to start the replacement of SEARCHS in a small, component based method like the CAPS replacement, or potentially porting the existing code from the Mainframe to a more modern infrastructure.

The department also has over 185 separate IT systems and applications supporting its programs. These applications include such areas as health facility licensing, laboratory management, case management, accounts receivable, disability determination, and vital records. One of the goals of the department is to manage all these applications as a portfolio with a defined system lifecycle. A large number of applications desperately need upgrading to the most recent versions of web services and databases. In addition, a number of systems need redesign and replacement to fit with new program business and security requirements.

The department serves Montanans from border-to-border. Our programs aim to increase Montanans self-reliance, success, and connect them to community resources. The key business drivers for the department are to serve citizens effectively and efficiently, improve the delivery of children and adult mental health services, create a strong statewide system of early childhood services, strengthen effective health and human services programs, and provide through Medicaid health care coverage for eligible Montanans. A number of department initiatives around holistic family-based services require the exchange of information between systems. The department is working toward a fully realized enterprise system architecture that allows for easy data interchange over a defined application called a “service bus” (see Section 4 for more information).

The department has over 100 separate locations across the state including six major facilities with one of those facilities closing. TSD manages over 3,000 personal computers in addition to 400 tablets and various mobile devices. Network bandwidth at affordable prices to the remote locations is a key driver of technology adoption. A reliable high-speed network allows the department to implement such things as a video learning system, remote desktop management tools, phone systems, desktop video conferencing, document imaging, electronic health records, and remote medical imaging.

Other business drivers for the department are various federal and state rules and regulations. The key technology regulations are ones associated with HIPAA, IRS Publication 1075 (security), and National Institute of Standards and Technology (NIST) security standards and guidelines. The department has implemented a NIST-based security framework, which requires a significant amount of staff work to ensure compliance. For more information about the department’s security program, see section 12 of this document.

State
Objectives

Education
Increase post-secondary education levels

Jobs
Increase employment and compensation levels

Efficient and Effective Government
Minimize government expenditures and increase the value and impact of state delivered services

DPHHS Business
requirements

To improve and protect the health, well-being and self reliance of all Montanans.

All Montanans are healthy and safe from injury and have access to high-quality health care.

All Montanans, including the elderly and those with disabilities, have the tools they need to be as self-sufficient as possible.

All children are wanted, safe and living in healthy families.

DPHHS IT Business
requirements

Provide efficient and effective IT services

Manage system data protection and security

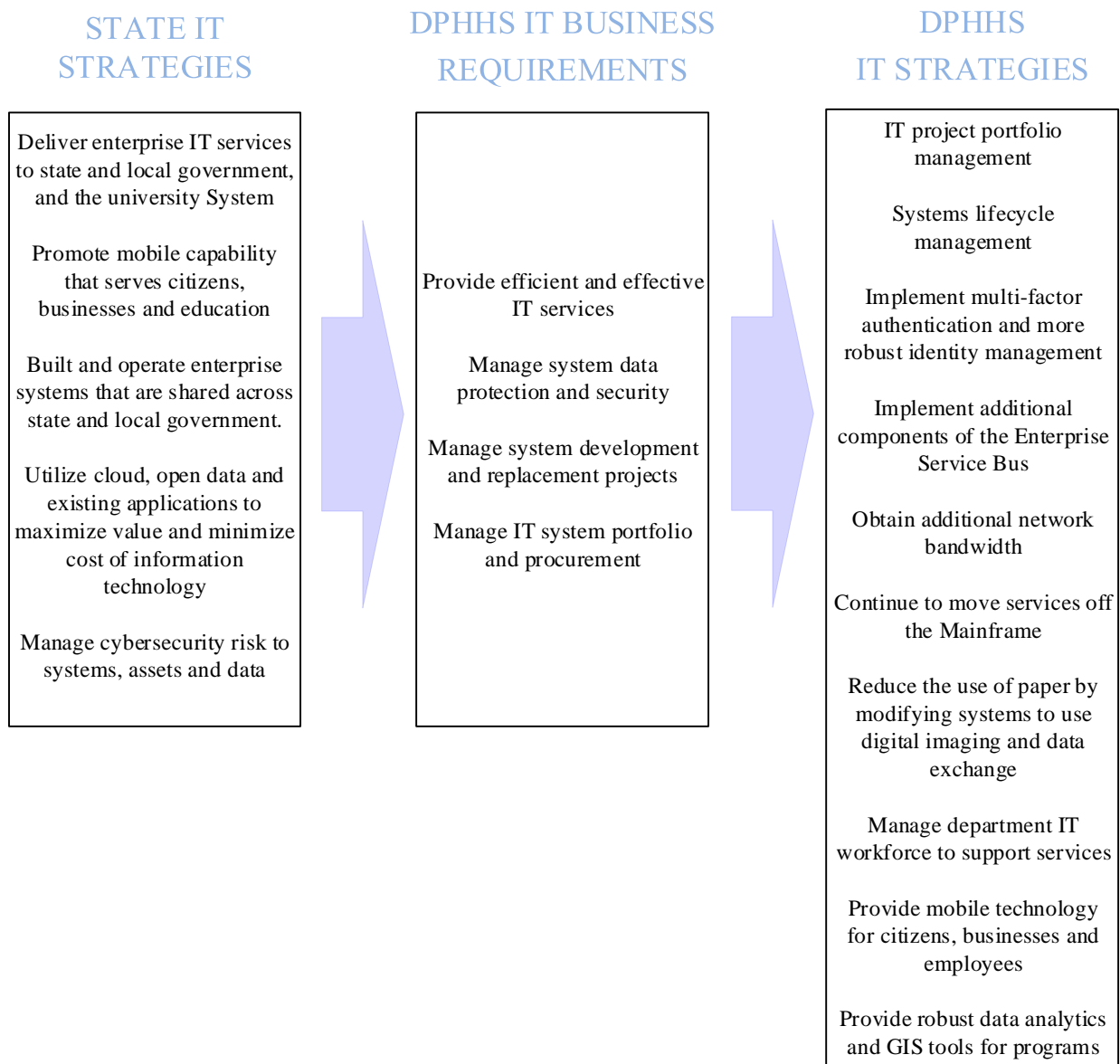
Manage system development and replacement projects

Manage IT system portfolio and procurement

3. IT Contributions and Strategies

The department’s IT business strategy is to support the state’s three primary strategies and the department’s mission to improve and protect the health, well-being, and self-reliance of all Montanans. Not all IT programs and projects will address all three state business strategies, but all IT projects will support at least one strategy and the department’s mission. Most IT projects and systems focus on efficient and effective government to support the department’s mission.

TSD obtains a wide variety of IT services and applications from providers for the department. These services may be developed and operated by internal staff resources, the State Information Technology Services Division (SITSD), or external contractors such as cloud providers. The department’s IT strategies are:



- IT Project Portfolio management consists of managing all IT projects, in total, within the department in a deliberate manner. Allocation of scarce resources and setting of priorities are done collaboratively across the department where overall objectives are considered and managed.
- IT Systems Lifecycle management consists of inventorying all systems within the department and then managing the operations and regular replacement of those systems in a coordinated fashion.
- The department is implementing multi-factor authentication (MFA) for desktop systems. It is also implementing MFA for those applications that have protected personnel information or other data.
- The department is obtaining additional network bandwidth as funds permit to enable key technological innovations that improve efficiency and effectiveness.
- The department will move legacy services off the State of Montana Mainframe.
- The department will continue to enhance its enterprise services bus by adding additional reusable components.
- The department will continue to modify existing systems and develop new systems to use digital imaging and electronic data exchange.
- The department will actively manage its IT workforce to provide clear career development paths for staff.
- The department will actively pursue mobile technology to enable citizens, businesses, and employees to interact with systems using mobile devices.
- The department will employ best-of-breed Business Intelligence (BI) reporting and analytics tools as well as Geographical Information System (GIS) tools to deliver timely, actionable insights to our programs, management, citizens and legislators.

4. IT Principles

The department's IT principles govern activities and decisions made in choosing what to implement as services and how to implement those services. The principles form the basis for specific policies and actions taken by the department. The following principles build on the principles outlined in the State's strategic plan:

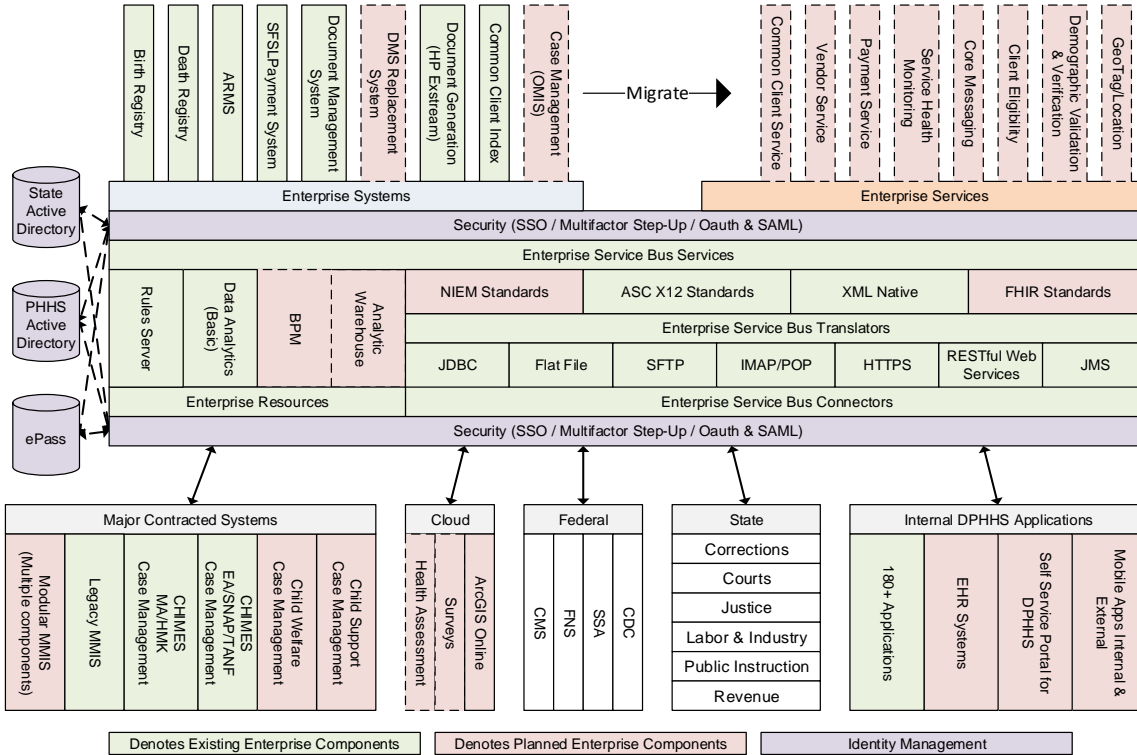
- Resources and funding are allocated to the IT projects that contribute the greatest net value and benefits to the department's clients and operations.
- Reuse of systems and electronic sharing of data will minimize unwarranted duplication of systems and services.
- IT resources are used in an organized, deliberative, and cost-effective manner.
- Systems will provide citizens easy access to services and their data.
- Data about citizens and clients will be protected and the risks of improper disclosure of data will be mitigated.
- External providers of IT services will be used where it makes fiscal and managerial sense.
- The full lifecycle of systems, including the strategy for retirement and replacement of systems, will be managed.
- The department will actively encourage the elimination of paper processes. Paper will be replaced by electronic data exchange and, where necessary, digital imaging of documents.
- New systems will be built on modern web-based service-oriented architectures. Old client-server and Mainframe systems will be actively decommissioned and replaced.
- New systems will be built with interfaces and appropriate geo-tagging of data to be used with GIS systems.
- Systems will be made accessible to mobile devices and mobile applications where appropriate.
- Systems will be designed and implemented according to the Medicaid Information Technology Architecture (MITA) principles where appropriate.
- The Information Technology Infrastructure Library (ITIL) 2011 edition framework of Information Technology Service Management (ITSM) principles will be used to manage delivery of IT services to users and clients.
- Systems and services will follow security controls based on the federal National Institute of Standards and Technology (NIST) security standards.
- Principles in the "*A Guide to the Project Management Body of Knowledge (PMBOK)*" from the Project Management Institute (PMI) will be followed for managing projects.
- The Department's overall portfolio of IT projects will be managed using PMI's "*Standard for Portfolio Management*" guide.

DPHHS Enterprise SOA and Enterprise Service Bus

The department is moving away from monolithic and outdated legacy systems toward a vision of web-based, people-friendly, and interoperable systems. Enterprise Service Oriented Architecture (SOA) is the centerpiece of this shift from the present to the future. This architecture will allow separate, standalone systems to communicate using exposed, shared services through a common shared architecture and service bus. Users will be able to seamlessly access data from multiple systems, and errors associated with redundant data entry will be reduced. Enterprise SOA is reshaping and improving the way the department serves Montanans and does business.

“Enterprise Service Bus Vision”

Version: 20160310



The department employs SOA for system interoperability that takes advantage of Commercial Off-The-Shelf (COTS) products and allows for the reuse of system components across business functions as services. SOA is an approach to loosely coupled, protocol independent, standards-based distributed computing where software resources expose their functionality as services and are available across the network. The department has implemented a data exchange service bus that provides interoperability that makes use of multiple industry standards, including ASC X12, HL7 (V 3), XML, XSLT, WS-I, WSDL, SOAP, UDDI, and WS-BPEL. The department’s current and future system replacement projects will be required to align with these standards. The department will also require third-party contractors to exchange data with the department via web services using the appropriate standards like ASC X12.

The department also plans to collect and store data from multiple systems for the purpose of decision support. The department is working on an enterprise data warehouse and data marts that will allow data mining and analytics. This service is essential in the assessment of program performance and efficacy, particularly for evaluating the impact and correlation of services from multiple programs and agencies over time, as it affects a single client or a population. Accordingly, internally and externally hosted systems will have the capability to transmit data to a data warehouse and other databases within the department using the department’s Enterprise Data Exchange. A data mart and basic data analytics service has been implemented as part of the department’s enterprise services.

Finally, for future healthcare systems, the department follows the federal guidance on the Medicaid Information Technology Architecture (MITA) principles that are associated with high-quality software systems (e.g., scalability, adaptability, secureability, availability, manageability, and interoperability) as

the basis for the system architecture. To this end, the department is currently replacing its legacy Medicaid Management Information System (MMIS) with one that is fully aligned with the MITA standards and the new CMS Modular rules and guidance. The department intends to continue to adhere to the MITA roadmap for controlled and strategic transformation for all programs and systems where appropriate.

5. IT Governance

The department's IT governance rests with the department CIO with oversight from the branch managers and the department director. Planning and coordination of IT projects are managed as a partnership between the individual divisions and TSD. The department's division administrators have significant input and control over IT decisions in their respective areas. The shared vision of a single connected enterprise helps to resolve conflict and competing program priorities.

IT projects and system requests are managed via fiscal procurement controls including the department's procurement API request process. The need for a new IT system or service is typically identified at the business level. A business case for the new service is presented through either the EPP process or the procurement process. Both these processes require a description of the business need, the proposed solution and budget information. This information is used within these two processes to determine whether to move forward with the new service. The department has developed a basic IT project portfolio with associated governance based on the Project Management Institute's "*the Standard for Portfolio Management*" framework. The department has not implemented a department-wide formal IT project portfolio management at this time.

The department CIO recommends IT policy to the department director for adoption by the department. Policy and standards enforcement is done via the management chain including the department director, as necessary. A cloud-based policy management tool is used to manage policies. Relevant policies are communicated to staff via multiple methods and are available via the cloud-based tool.

The CIO has authority to manage the provision of IT services and programs to the department both internally and from external partners such as SITSD. The CIO signs all IT contracts for the department. The Compliance and Security Office of TSD manages IT contracts while the Project Management Bureau (PMB) manages large system projects and associated contractors.

The Network and Communications Bureau (NCB) manages desktop systems and network services. NCB operates the department's Technology Service Center (TSC / help desk), which provides end-user support for the department. PMB manages change control for large contracted systems such as CHIMES. The Information Systems Bureau (ISB) manages change control for internally developed and managed applications. Change control communication is coordinated via the TSC.

One of the objectives of the department is to continue to implement the Information Technology Infrastructure Library (ITIL) 2011 edition framework for IT Service Management. ITIL is helping the department better manage and operate its complex IT systems.

6. IT Financial Management

Funding for the department IT services and TSD is a combination of general, state special revenue, and federal funds. The funds are appropriated via the General Appropriations Act (HB 2) for on-going IT services, and the Long Range Information Technology Act (HB 10) for development, implementation, and replacement of large systems. The projected IT budget for TSD for SFY 2016 including Long Range IT projects is \$47.7 million. This amount includes \$6.2 million for personal services for IT staff positions. The overall department's projected spending on IT for SFY 2016 is \$52.4 million. The table below summarizes the budget categories for TSD.

<u>Expense Category</u>	-	<u>FY2016</u>	<u>FY2017</u>	<u>FY2018</u>	<u>FY2019</u>	<u>FY2020</u>	<u>FY2021</u>
Personal Services		5,831,177	6,006,112	6,186,296	6,186,296	6,186,296	6,186,296
Operating Expenses		18,745,531.12	22,873,935	23,509,830	24,163,404	24,163,404	24,163,404
Initiatives		27,837,075	25,000,975	38,552,134	37,371,049	30,119,301	30,449,019
Other expenditures							
Totals		52,413,783	53,881,022	68,248,260	67,720,748	60,469,000	60,798,718

The department takes advantage of federal funding opportunities where state general fund or state special revenue fund dollars can be matched with federal dollars. Recently the department used a waiver to OMB A-87 to use Medicaid 90/10 matching funds to implement various system infrastructure components, including the Enterprise Service bus. A large amount of the department's IT budget is derived from federal sources at 90/10, 75/25, or 50/50 match rates.

Controls on the fiscal management for IT systems funding are various cost allocation plans that follow various federal program rules for allocating federal funds. The Children, Families, Health, and Human Services Committee and the Legislative Finance Committee regularly review the department's budget information. The department is also required to report fiscal information monthly, quarterly and annually to federal funding partners including ACF, FNS, and CMS. Federal Advance Planning Document (APD) reporting for IT systems development and implementation is required and submitted on a regular basis. The department follows various standard internal fiscal controls as established by GAAP, GASB, and the Montana Operations Manual. The department also follows federal and state fiscal statute and regulations and various federal policy directives such as A-133 and OMB A-87.

Federal Advance Planning Documents (APD)

Some of our federal partners require APDs for systems that meet specific criteria set by each federal agency. The APD process is a series of successive steps through which State agencies obtain Federal prior approval of and Federal financial participation (FFP) in IT system projects. The APD process includes the following:

Planning Advanced Planning Documents (PAPD) requests funding for planning activities; specifies the nature of the IT system project; investigates the feasibility, system alternatives, requirements, and resources needed to move forward with the system development.

Implementation Advanced Planning Documents (IAPD) addresses system analysis, design, development, integration, testing, and deployment; completes the planning phase; requests funding for enhancements to ongoing operations; and obtains approval to conduct implementation activities.

Operational Advanced Planning Document (OAPD) provide a short summary of the activities, method of acquisition, and annual budget for operations and software maintenance.

Annual Advanced Planning Document Updates (APDU) can consist of planning, implementation, or operational. It is an update to an ongoing project and is required annually when planning or implementation activities occur for more than one year.

Advanced Planning Document Updates, As-Needed (APDU As-Needed) can consist of planning, implementation, or operational. An APDU As-Needed may be needed for unexpected project changes that significantly affect project cost and outcomes.

Each federal agency has slightly different criteria for APDs that change over time due to changes in Federal rules. The department must submit the APDs to the Federal partners to obtain, or maintain, FFP. In addition to the APDs, the APD process also requires federal partner approval of RFPs, contracts, and contract amendments that meet the criteria for APD requirements.

The expected APDs for the next biennium include:

- Eligibility and Enrollment (EE) Operational Advanced Planning Document Update (OAPDU)
- SEARCHS OAPDU
- Child and Adult Protective Services Annual APDU
- EE APDU
- Health Information Technology (HIT) APDU
- WIC EBT APDU
- SNAP EBT APDU
- EE As-Needed APDU
- SEARCHS Planning APDU (PAPD)
- MMIS Annual APDU
- MMIS Modularity PAPD
- MMIS Pharmacy System Annual APDU

7. IT Services and Processes

The department operates, maintains, and/or uses over 185 separate systems and supports users at over 100 locations. The department also uses various services provided by SITSD like the Exchange email system, datacenter, mid-tier server hosting, and the Mainframe. The following is a list and short description of some of our major line of business IT systems:

- Montana Medicaid Information System (MMIS) – This system accepts, processes, and pays the Medicaid, CHIP, and Montana Mental Health Service claims for the State. It is a hosted legacy solution and is operated by Xerox. The department has ended the DDI contract with Xerox for a replacement system. The department did implement a new Xerox Pharmacy Benefit program. Xerox continues to run the legacy MMIS system and provides fiscal agent services for Medicaid.
- CHIMES – This system is the combined eligibility management system for Medicaid, SNAP, TANF, and the Healthy Montana Kids (HMK). HMK is also known as the Children’s Health Insurance Plan (CHIP). CHIMES is actually composed of three separate components (SNAP, TANF, and MA/HMK) that work together as a single system.
- Enterprise Service Bus (ESB) – This platform federates various systems allows data exchange between systems for Department. It was implemented in conjunction with the CHIMES system and continues to support the CHIMES Enterprise Architecture (CHIMES – EA). The Enterprise service bus has been expanded and upgraded to serve as an Enterprise Data Exchange (EDX) for department systems.
- SFSL (Shared Fiscal Services Layer) – This system is a shared component of the enterprise services bus and serves as the department’s payment engine and interfaces with SABHRS. Currently, CHIMES is the only system that uses this enterprise component to process payments, however, it will be used by other systems as they are reconfigured to use the SFSL services.
- ARMS (Accounts Receivable Management System) – As a sibling to SFSL, ARMS supports receivables business processes for the department. As a pair, SFSL and ARMS are the systems that respectively provide accounts payable and accounts receivable to the department.
- DMS (Document Management System) – This is a document management imaging system built as a set of web services that are part of the DPHHS enterprise architecture. It is primarily used by the Public Assistance Bureau for centralized scanning of documents and forms from clients. The DMS system is scheduled to be replaced by an Enterprise Content Management (ECM) system hosted by SITSD. That system is based on ECM software from Perceptive.
- CAPS – This is the case management system for Child Welfare. It is a Mainframe system and part of it is being partially redesigned and replaced during 2016. Additional work is anticipated to continue during the 2017 biennium.
- SEARCHS – This is the case management system for Child Support Enforcement. It is a Mainframe system and is proposed for redesign/re-platform and partial replacement in 2017.
- Open Scan – This is the document imaging and management system used by Child Support Enforcement to track receipt and disbursement of child support payments. It interfaces with the SEARCHS system and is scheduled for replacement at the same time as SEARCHS. It is very likely that Open Scan will be replaced by the Perceptive ECM system hosted by SITSD.
- MT Access – Montana Access is the Electronic Benefits Transfer (EBT) system for the state. Clients are issued plastic mag-stripe cards which they can use to access their SNAP and TANF benefits at various retailers and ATMs across the state. For example, a SNAP client can purchase groceries at a supermarket using the card. MT Access was scheduled for replacement in 2015 but JP Morgan, who was the winning bidder, walked away from the contract in January of 2014. The department awarded a new contract to Solutran. It is anticipated that the new EBT system that

will also include electronic WIC (Women, Infant, and Children) benefits will be implemented in early 2017.

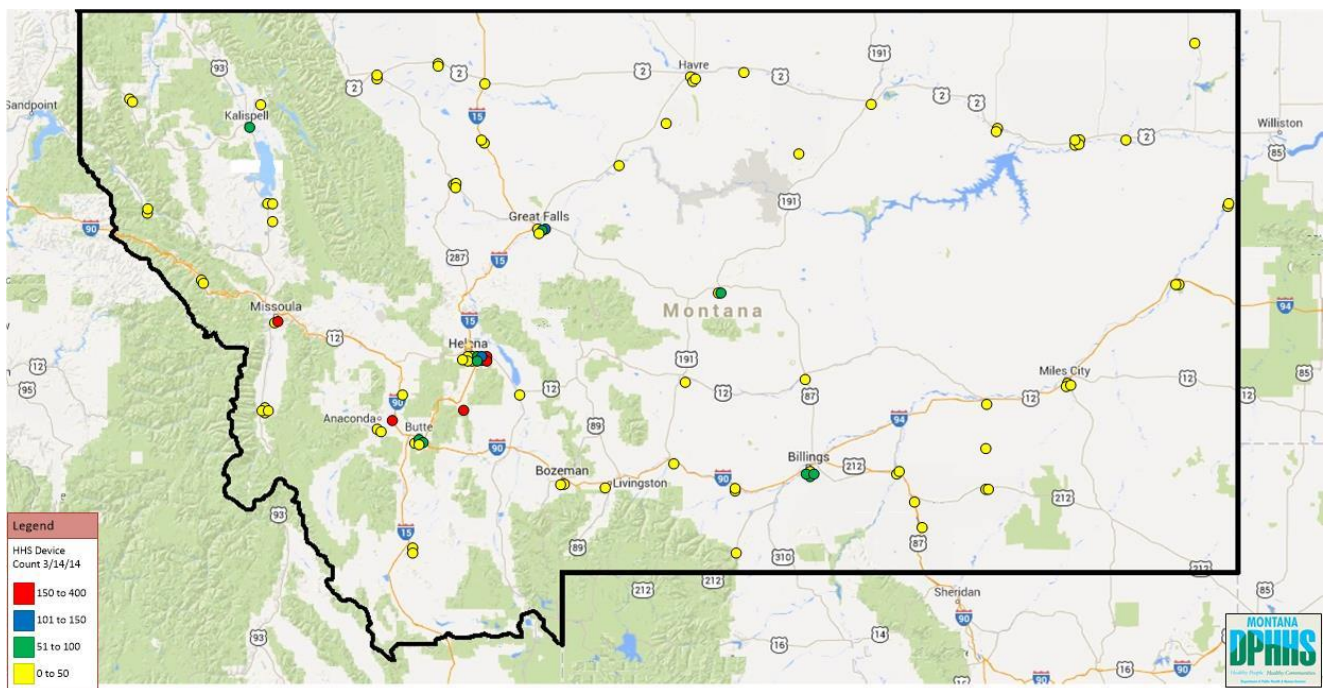
- CCUBS (Child Care under the Big Sky) – This system supports Montana’s child care program. Primary functions include child care licensing, provider inspection, family eligibility determination for subsidy and payment processes, federal error rates, quality assessment, quality improvement, and contract management.
- AWACS (Agency Wide Accounting System) – AWACS is a collection of functionality at the core of many DPHHS applications systems. AWACS provides a common financial application interface and services for generating payment and journal transaction in SABHRS. This system will gradually be replaced by SFSL.
- TIER – This system is used to manage a selection of electronic health records for the Montana State Hospital. The system is proposed for replacement by a more functional department-wide set of electronic health records systems.
- IMMTRAX (Montana Immunization Tracking System) – This system is used to register and track child immunization records across the state.
- CDS (Central Database System) – This system is used by the Human Resource Development Councils (HRDCs) to enter client services they provide as well as for all aspects of managing the Low Income Energy Assistance Program (LIEAP), Weatherization, Energy Share, and Energy Audit Programs. The CDS is comprised of these components:
 - Central Information System (CIS) / Data Warehouse (DWH)
 - Low Income Energy Assistance Program (LIEAP)
 - Energy Share, Energy Audit (EA) and Energy Audit Mobile
 - Homeless Management Information System (HMIS)
 - CDS LIEAP SNAP Web Service
 - Energy Education System (EES)
- MSPIRIT – This is Montana’s implementation of the consortium-based SPIRIT system and is used to manage the Woman, Infant, and Child (WIC) program.
- MICRS (Management Information and Cost Recovery System) - MICRS tracks all beds, medication, and services for clients in the departments facilities and bills the various payers such as Medicaid, Medicare, private insurance, and/or the client.
- SAMS (Substance Abuse Management System) – This system is for tracking substance abuse treatments and outcomes for Federal reporting and provider payment.
- Statewide Trauma Data System – This is a web-based system used by hospitals to report data to the State about ER visits.
- HIRMS (Health Information and Resource Management System) – This system manages emergency medical services licensing, EMS Service Patient records and data, registration of community AED program, registration of healthcare providers for disaster response, and other hospital information on trauma patients.
- Copia & Harvest – These systems are management systems for the State Public Health Laboratory.
- Vital Stats – This is an old system used to manage and record birth, death, and marriage records. This system is proposed for redesign and replacement in 2017.
- Moodle – This system is used to manage and provide training videos and coursework to Department staff.
- Microsoft System Center 2012 – This system is comprised of three different components that manage desktop systems, servers, and the service desk ticketing system. This is a COTS product from Microsoft obtained via the Microsoft Enterprise Agreement (EA).
- Microsoft SharePoint 2010 – SharePoint is a COTS product that is used for the department-wide workgroup collaboration portal.

- Citrix NetScaler and Application Server – These systems are used to provide remote application access, remote desktop access, and desktop virtualization services.

TSD also provides multiple internal services for the department. Below is a short description of the services provided by each area:

Technology Services Center (TSC)

The TSC provides technical support and resources for over 3,000 department employees and 5,000 non-employees, professional service providers, and internet users that use or interact with the department’s services. Services are provided to users at over 100 locations (see map below). These services include help desk, basic desktop and application support, mainframe support, and mid-tier server operations support for the department. Approximately 3,100 incidents are opened per month at the TSC. It is the goal of the TSC to resolve as many customer incidents as possible during the initial call. The first call resolution rate of the TSC is currently 76%.



2014

Desktop Administration and Management

Network and Communications Support (NCS) uses Microsoft System Center Configuration Manager (SCCM) to remotely administer computers, deploy operating systems, software applications, and software updates. SCCM is used to monitor and remediate computers for compliance settings and inventories hardware and software installed on computers and servers.

Microsoft System Center Service Manger is used to manage incidents and service requests called into the Technology Services Center by end-users. It provides NCS with processes for incident and problem resolution, change control, and asset lifecycle management.

Microsoft System Center Operations Manager is used to monitor services, devices, and operations for many of the server systems. Operations Manager helps to gain rapid insight into the state of the server environment and the services running across different systems. We are able to monitor system state,

server health, and performance as well as alerts generated for availability, performance, configuration, and security situations.

The Network Security Unit (NSU) provides operational security services such as monitoring and alerting. NSU also responds to all access requests and works with the data owner to appropriately grant and rescind access to department systems.

Computer Application System Development and Support

The Application Development and Support Sections (ADSS) develop, enhance, and maintain applications that support the department's business functions with a primary focus on business critical services. This focus includes defining enterprise architecture to provide common business services across multiple divisions. ADSS supports two separate development technologies, Oracle Forms and Java, both being typically connected to an Oracle database. Most ADSS applications use Oracle Forms. New work uses Java and Mulesoft. ADSS is actively working to define enterprise-class services that will reduce the size and scope of new or replacement applications.

Computer Application and Database Hosting

The Database and Web Group (DAWG) Section provides Oracle Database Hosting and Web/Application Server Hosting. Servers are either AIX or Linux and are primarily virtualized. They reside in the State of Montana Data Centers in Helena and Miles City. The DAWG purchases, configures, and manages database and web/application servers. Database hosting is primarily done in an Oracle environment. Web/Application servers include Oracle Application Server (Weblogic), Tomcat, JBoss, and Apache. Hosting services include production support of online and batch processing, and 7x24 on-call support for applications that require it.

Project Management

The Project Management Bureau (PMB) is the IT Project Management Office (PMO) for the department. The PMO provides centralized and coordinated management of large information technology projects. PMB is responsible for ensuring the success of system development projects by staffing them with qualified professionals. Maintenance and operations services are provided for selected existing large systems. The PMB identifies, develops, and enforces project management methodology, practices, and guidelines. They also act as a centralized clearinghouse for project policies, procedures, templates, and other project tools.

Information Security

The department has developed a NIST-based information security program. For more information, see section 12.

IT Procurement and Contract Oversight

All IT procurements go through the division. TSD assists the programs to select the appropriate method of procurement, complete the procurement documents, and obtain the necessary approvals. TSD works with the department's procurement office or the State Procurement Bureau to move the procurement through the appropriate process including RFPs. TSD will facilitate, scribe, and participate in the scoring of RFPs or Contractor Engagement Proposals (CEP). Once an IT service/product is procured, the TSD finalizes the contractual document with the vendor, the program, legal staff and management. Operational IT contract management is also maintained in TSD.

8. IT Infrastructure, Staffing, and Resources

Infrastructure

The department uses both internal and external infrastructure resources to operate its IT systems. There are department-owned servers and data storage equipment in the State of Montana Helena Data Center and the Miles City Data Center. The department uses Miles City for backup and disaster recovery. DPHHS has moved to primarily use servers and storage hosted by SITSD at the Helena data center.

SITSD provides a large number of hosted services that the department rely on including email, phone service, network connectivity, server hosting, and disk storage. SITSD provides the hosting service for CHIMES and several other main line-of-business systems for the department, including the State Mainframe system. Internally developed and managed department systems are typically hosted on TSD-managed server infrastructure. The underlying server infrastructure that TSD manages is obtained as hosted services from SITSD.

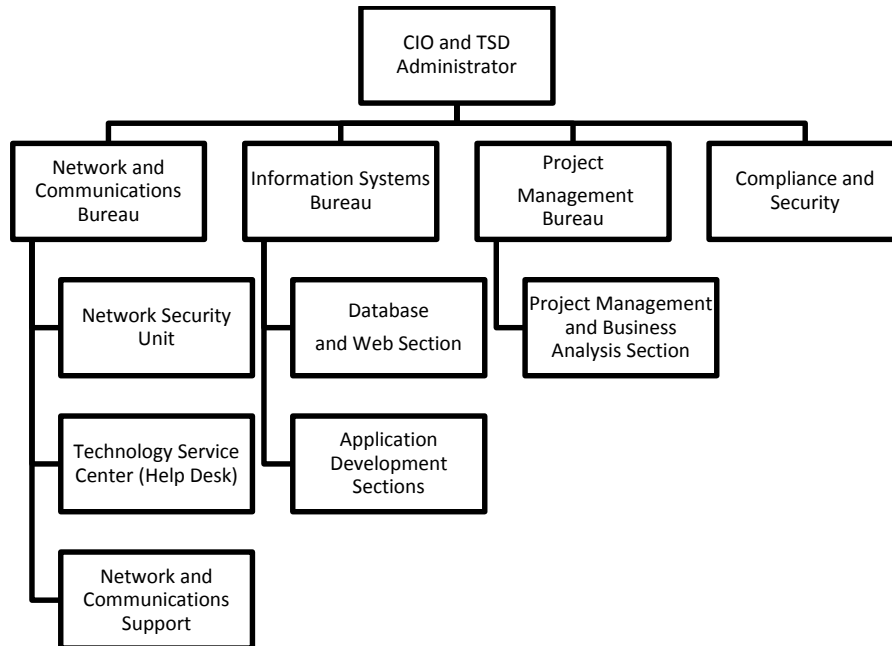
The department uses the SummitNet network provided by SITSD to connect its remote locations. A large number of department office locations have local file servers. However, as good quality, affordable, high-speed network connections become available, those file servers are being decommissioned and services are being provided from the Helena Data Center.

The department does use various external vendor-hosted systems including the Medicaid claims system which is hosted by Xerox and an electronic benefits system that is partially hosted by Northrop Grumman. The department continues to look for opportunities to use cloud services as appropriate.

Staffing

TSD has approximately 62.60 FTE's, including 5.00 HB2 modified FTE's, that are organized into four functional bureaus. The Network and Communications Bureau (NCB) is responsible for desktop LAN administration, the technology service center (help desk), security operations, and Microsoft Windows-based support systems. The Information System Bureau (ISB) is responsible for internal application development, maintenance and operations, database administration, and system administration for the departments Oracle web and database servers. The Project Management Bureau (PMB) is responsible for IT project management, IT systems business analysis, and contractor management and maintenance for large IT systems. The Compliance and Security Office (CSO) is responsible for security policy and compliance, IT security and system audits, IT contract management, and IT procurement management.

Technology Services Division Functional Organization Chart



Vendor Partners and Resources

TSD spends a substantial amount of its budget on contracted vendors that manage, support, and maintain its systems. A large amount of the funds go to several large system integrators such as Deloitte and Northrop Grumman. The department is heavily invested with Microsoft, Oracle, IBM, Dell, Commvault, and Citrix. The department follows state software standards and uses Microsoft's Office products on the desktop. The department has a large investment in Oracle forms and web applications and Oracle databases. Recently the department decided to outsource its hosting of Microsoft SQL databases and a large number of Oracle databases to SITSD. The department uses Citrix to provide remote desktop applications and virtualize desktops to selected users.

9. IT Risks and Issues

The following table contains the major risks to the department's IT strategy. Major risks meet one of two criteria.

- Risks with a probability of medium or high with an impact of high.
- Risks with a probability of high with an impact of medium or high.

Mitigation strategies are the pro-active actions that the department uses to lessen the probability of the risk occurring and minimizing the impact of the risk.

Primary Risk	Probability	Impact	Mitigation Strategy
Staff retirements	High	Medium	The department will develop a succession planning program that creates a list of staff eligible to retire and forecast an estimated retirement date and replacement plan when possible. Positions/skills rated as critical will have individual plans for skills transfer, replacement, documented procedures, etc. for mitigating the impact.
Security breach	Medium	High	The department has an active security program including, but not limited to, periodic third-party security assessments, staff training and awareness, data encryption, and security policies.
Resources to adequately manage security planning and risk management	High	High	The department will request additional staffing and resources to manage risk along with prioritizing projects.
Difficulty of hiring qualified technical staff	High	High	Increase pay for positions most affected by this issue.
Lack of funding to retire Mainframe systems	Medium	High	The department will develop a specific care and maintenance plan to reduce the likelihood of being affected by staffing shortages with contractors and SITSD. The department will also revise plans for discontinuing mainframe services.
Inability to secure sufficient funding for some projects	Medium	High	Continue with current operations and plan to renew request at next opportunity. Manage and set expectations for program needs and requirements.
Staff resources stretched thin between multiple Department IT priorities	High	Medium	Use project portfolio management to prioritize projects and requests. Look for additional resources both internally and externally.

10. IT Goals and Objectives

IT Goal 1

Use information technology to support and enhance department program service delivery and increase efficiencies.

Information technology is an essential tool used to support and improve the department's program service delivery. The department will continue to look for ways in which information technology can add value to its business functions. Examples include document management, document imaging, system integration, web-based applications, internet portals, and public/provider access.

Benefits: Increased efficiency and effectiveness in performing the department's business functions.

Objective 1-1: Start to replace the legacy State Automated Child Welfare Information System (CAPS) and the legacy Child Support Enforcement System (SEARCHS) which have reached end-of-life.

Objective 1-2: Continue activities to migrate, replace, or discontinue all other secondary Mainframe systems. (Note - the mainframe is still used as a file transfer platform for various Federal interfaces).

Objective 1-3: Implement electronic health records systems and replace legacy EHR systems for the department's facilities.

Objective 1-4: Replace the Document Management System (DMS) with the new Enterprise Content Management system from SITSD.

Objective 1-5: Continue to expand the use of eGovernment services for client interactions including reporting of benefits.

Objective 1-6: Extend and enhance the framework of the self-service client portal for the department.

Objective 1-7: Implement and manage secondary IT systems and programs as required by the department.

Objective 1-8: Implement mobile technology applications for citizen and employee access to systems. Enhance existing systems to provide mobile device access where possible.

IT Goal 2

Ensure that information technology resources are efficient, responsive, cost-effective, and available when needed.

The department must acquire and maintain the adequate number, type, and quality of IT resources needed to support its systems. IT resources including staff, hardware and software tools, must be maintained at the appropriate levels to adequately provide this support. IT resources must be responsive and provide the required availability and redundancy in a cost-effective manner.

Benefits: Increased efficiency, cost-effectiveness, responsiveness, and availability and redundancy of IT resources to support the department's business functions.

Objective 2-1: Continue to implement an enterprise ITSM governance structure based on the ITIL 2011 framework.

Objective 2-2: Continue to implement IT project portfolio management based on PMBOK framework.

Objective 2-3: Continue to maintain and enhance an Information System Inventory of all department systems that includes information necessary for system life cycle planning and management.

Objective 2-4: Implement a division wide career ladder system for workforce development following a successful pilot of the system with ISB.

Objective 2-5: Implement increased network bandwidth in various locations across the state.

Objective 2-6: Request sufficient staffing resources to accomplish the department's IT objectives.

IT Goal 3

Implement a modern enterprise architecture that supports interoperability and sharing of data and functionality.

Create an Enterprise Architecture plan that leverages State (conceptual Architecture Plan) and federal (Medicaid Information Technology Architecture) guidelines and initiatives that will allow systems to maximize their functionality and increase efficiencies and effectiveness.

Benefits: Increase the value of the department's investment in information technology by defining an Enterprise Architecture that allows systems to maximize their function and data through re-use and sharing.

Objective 3-1: Continue to integrate the Enterprise Service Bus and web services into more Department systems.

Objective 3-2: Enhance the capabilities and system coverage of the Department's business intelligence tool, Pentaho.

Objective 3-3: Implement additional functionality and components of the Enterprise Service Bus and Enterprise Data Exchange.

IT Goal 4

Maintain and operate a National Institutes of Standards and Technology (NIST) Based Security Program.

The department's systems and data are a critical and valuable resource that is required for the continued success of program business functions. Access to this data and these systems must be appropriate,

allowing access only for those with a legitimate need-to-know. Data must be available but protected from both deliberate and accidental theft or destruction.

Benefits: Ensuring the confidentiality, integrity and availability of data allows the department to provide services to Montana citizens.

Objective 4-1: Continue to implement NIST-based security controls to ensure the security, privacy, availability, and integrity of data and systems.

Objective 4-2: Update and promulgate Information Security Policies that comply with the NIST cyber-security framework.

Objective 4-3: Continue the implementation of multi-factor authentication on systems that contain protected, sensitive, or private information.

Objective 4-4: Continue the implementation of additional encryption for those systems that contain protected, sensitive, or private information.

Objective 4-5: Continue to implement enterprise security information and event management for department systems as appropriate.

Objective 4-6: Continue to implement and develop a NIST based risk management system for system lifecycle management.

11. IT Projects <NOTE: This section will be submitted later in the budgeting process>

The department is moving to replace several of its largest systems in a methodical way following system development lifecycle concepts. As systems age they eventually require replacement or significant redesign to meet new business processes or technology. The department desires to manage these systems as a portfolio with a planned cycle of development, operations, and replacement. The portfolio concept also allows the department to manage the resource demands on staff and funding. Another key portfolio concept is doing sufficient advanced planning and analysis of business processes and requirements before a system needs to be replaced. As the date for system replacement or redesign approaches, there has to be a significant effort to do that analysis of requirements and business process and be ready to procure a new system.

A project timeline showing some of the major current and upcoming IT projects for the department is below:

Major IT Projects Timeline



Design, Development and Implementation Projects:

Previously funded:

Item	Description
Project name	
Project/program purpose and objectives	
Estimated start date	
Estimated cost	
Funding source - 1	
Funding source - 2	
Funding source - 3	
Funding source - 4	
Annual Costs upon completion	

System Maintenance and Operations

Previously funded:

Item	Description
Project name	
Project/program purpose and objectives	
Estimated start date	
Estimated cost	
Funding source - 1	
Funding source - 2	
Funding source - 3	
Funding source - 4	
Annual Costs upon completion	

New funding requests:

Item	Description
Project name	
Project/program purpose and objectives	
Estimated start date	
Estimated cost	
Funding source - 1	
Funding source - 2	
Funding source - 3	
Funding source - 4	
Annual Costs upon completion	

12. Security and Business Continuity Programs

Security Program Description:

With the adoption of the National Institute of Standards and Technology (NIST) Special Publication 800 series as guides for establishing appropriate security procedures, the department has implemented an information security management program that is compliant with §2-15-114, MCA and State Information Technology Systems Division *Information Security Programs* policy. The program is in alignment with the State of Information Technology Service's direction for an enterprise approach to protect sensitive and critical information being housed and shared on State and/or external/commercial information assets or systems.

As described in NIST SP 800-39, the department has developed and adopted the Information Risk Management Strategy to guide the department through information security lifecycle architecture with application of risk management. This structure provides a programmatic approach to reducing the level of risk to an acceptable level, while ensuring legal and regulatory mandates are met in accordance with MCA §2-15-114.

The department's information security management program is challenged with limited resources, staff, and funding. While alternatives are reviewed and mitigation efforts are implemented, the level of acceptable risk is constantly challenged by the ever-changing technology and associated risks from growing attacks and social structure changes.

The information security management program consists of the following components:

- Defined Roles and Responsibilities
- Security Awareness and Training Program
- Security Planning
- Risk Management
- Authorization and Certification

Roles and Responsibilities

SITSD has released an enterprise level Information Security Policy that the department has adopted. Appendix B of that policy is a security roles and responsibilities document. The department had previously created a roles and responsibilities document that defines the security roles throughout the agency. The department will align their roles and responsibilities with the SITSD enterprise policy.

Security Awareness and Training Program

The department has created a NIST compliant Security Awareness and Training Program. NIST SP 800-50 provides guidance for the department. Security awareness and training is focused on the department's entire user population. The awareness and training program is crucial in that it is the vehicle for communicating security requirements. The department continues to improve, develop, and implement the awareness and training program. Most training is conducted during the month of October, which is cyber security month.

The program includes:

- Cyber security month training – posters, emails, newsletters, computer pop-ups, etc.
- Newsletters – SITSD provides newsletters throughout the year. The department has developed and implemented a process to consistently utilize and disseminate these newsletters.
- New Employee Orientation – information security is part of new employee orientation.

- Securing the Human (STH) – The department is participating in this online training mandated by the Governor.

One of the primary information security focuses of the next biennium is to continue to develop a more robust awareness and training program. The department has refined the list of employees receiving the STH training. The STH training is tracked from year to year. Challenges faced include determining how to get security awareness and training to employees who have limited access to computers (i.e., direct care staff in institutions).

Security Planning

Using NIST SP 800-18 as a guideline the department has established an Enterprise System Security Plan for securing all systems. The Enterprise Security Plan provides an overview of the security requirements for the systems and describes the controls planned for meeting those requirements. This plan also defines the responsibilities and expected behavior of all individuals who access systems. The department has developed a prioritized list of systems for completion of system security plans. All new systems will have an individualized security plan.

The objective of system security planning is to improve protection of information system resources. The purpose of a system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. This plan delineates responsibilities and expected behavior of all individuals who access the system. The plan documents the structured process of planning adequate, cost-effective security protection for a system. The plan also establishes and documents the security controls and forms the basis for the authorization. The department uses NIST SP 800-53 and NIST SP 800-53A to select appropriate privacy and security controls for its systems.

Security Policies

The department has adopted the enterprise Information Security Policy drafted by SITSD. With the adoption of this policy individual security control family policies (as discussed in the last plan) are not necessary. The information security policy addresses all of the security families.

The department has implemented the PolicyTech application, which is a policy and procedure management application. PolicyTech allows for authoring, approving, distributing, and reviewing of policies and procedures. The department will be using the e-Learning platform Moodle for attestation of reading policies.

Risk Management

The department utilizes NIST SP 800-39, NIST SP 800-37 and NIST SP 800-30 as guidelines to assist in performing risk management. Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. The objective of performing risk management is to enable the department to accomplish its mission by:

- Better securing the IT systems that store, process, or transmit department information
- Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget
- Assisting the management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management

Risk assessment is used to determine the extent of the potential threat and the risk associated with an IT system throughout its System Development Life Cycle. This process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk is a function of the likelihood of a given threat-source is exploiting a particular potential vulnerability, and the resulting impact of that adverse event. The department has developed a robust risk management process with templates and guides. A risk management team is currently updating and developing SSPs and conducting risk assessments on all DPHHS systems. The risk management team currently consists of two full-time Security Analysts and three additional resources contracted to assist with the risk assessments. The department is in the process of hiring one more full-time Security Analyst.

The Risk Management team works with data owners and system owners to complete the System Security Plan. Once this plan is completed a risk assessment is conducted. During the risk assessment implementation of the moderate security controls is assessed, using a SSP Workbook. Based on the findings of the risk assessment a Plan of Action and Milestone (POAM) document is created. This POAM is used by the department to determine a plan of action to correct the findings. Following the creation of the POAM a Risk Assessment Executive Summary is drafted. These four documents (the SSP, the SSP workbook, the POAMs, and the RA Executive Summary) are submitted to the Department CIO who reviews it and determines whether or not to grant the Authority to Operate (ATO).

The data owner, system owner, and department manager will respond to any identified risk. Risk response identifies, evaluates, decides on, and implements appropriate courses of action to accept, avoid, mitigate, share, or transfer risk to organizational operations and assets, individuals, and other organizations resulting from the operation and use of information systems.

The department has developed, and will continue to refine, a prioritized list of systems needing risk assessment. The department does not have the staff necessary to quickly conduct risk assessments on all systems.

Authorization/Certification

Based on all the information from the security planning and risk management, the authorizing official must make decisions on whether or not the information systems are initially authorized to operate within the designated environments of operation or continue to receive authorization to operate on an ongoing basis. The risk management process, with guidance from the security team and the various architectural considerations supporting the mission/business processes, informs the ongoing risk-based decisions.

Affordable Care Act (ACA) Security Reporting

The department was required to submit a System Security Plan (SSP) before implementing the changes required by ACA. From this SSP a Plan of Action and Milestones (POAM) was developed. The POAM is required to be updated and reported to CMS quarterly. The SSP is updated and submitted to CMS on a regular basis. The Authority to Connect to the Federal Hub that was granted by CMS in 2013 must be renewed in 2016. The department is working towards this renewal. CMS has also released the Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.0.

Internal Revenue Services (IRS) Safeguard Reporting

The IRS revised their Publication 1075, which directs safeguarding requirements for any system receiving IRS data. Under these revised guidelines, we are required to submit annual reports. Additionally, every three years the IRS does an in-person safeguard assessment. That assessment results in a Corrective Action Plan (CAP), which must be updated and submitted to the IRS on a semi-annual basis. The IRS plans to conduct a safeguard assessment in Montana April 26-28, 2016.

Federal Agreements

The department has several data and security agreements with different federal agencies. These agreements must be updated and re-signed on either an annual or a longer basis, depending on the agreements terms.

Continuity of Operations (COOP) Capability Program Description:

The department continues to work toward completion of continuity of operations plans. COOP provides the structure to facilitate response and recovery capabilities to ensure the continued performance of identified State Essential Functions. The state uses the Living Disaster Recovery Planning System (LDRPS) to accomplish this goal. Phase I of the plan, including identification of units, business service processes, and delegation of authority was completed May 2015. Phase II assigns resources to the business processes and compiles essential records and documents. Phase II is underway and estimated to end December 2017. LDRPS is not a standalone process; the information under this structure often exists in the Records Management Program and associates with Information Security Management Program requirements.

In addition to completing the COOP requirements there are also several other areas of emergency preparedness that are being worked on simultaneously. These other areas involve the development of business processes or activity plans such as Emergency Action Plans (EAP), Information System Contingency Plan (ISCP), Communications Plans, Incident Management Plans, and more.

13. Planned IT Expenditures

	FY2014	FY2015	FY2016	FY2017	FY2018	FY2019
IT personal services	\$ 6,128,242	\$ 6,096,797	\$ 6,328,260	\$ 6,831,594	\$ 6,870,250	\$ 6,916,383
IT operating expenses	\$ 11,700,876	\$ 12,385,485	\$ 12,628,496	\$ 12,768,674	\$ 12,876,964	\$ 12,986,968
IT initiatives	\$ 38,731,504	\$ 56,826,506	\$ 63,488,769	\$ 44,712,857	\$ 54,982,702	\$ 60,442,472
Other						
Total	\$ 56,560,622	\$ 75,308,788	\$ 82,445,524	\$ 64,313,125	\$ 74,729,916	\$ 80,345,823

14. Administrative Information

IT strategy, plan owner, and IT contact:

Stuart Fuller, Department CIO and TSD Administrator, 406-444-2794, sfuller@mt.gov

Alternate IT contacts:

Dan Forbes, ISB Bureau Chief, 406-444-1794, dforbes@mt.gov

Harold Bruce, PMB Bureau Chief, 406-444-0639, hbruce@mt.gov

Chris Gleason, NCB Bureau Chief, 406-444-1922, cgleason@mt.gov

Information Security Manager:

Jackie Thiel, CSO, 406-444-6983, jthiel@mt.gov

15. Acronyms and Definitions

<u>Acronym</u>	<u>Definition</u>
ADSS	Application Development and Support Section
APD	Advance Planning Document
APDU	Annual Advanced Planning Document Updates
AWACS	Agency Wide Accounting System
CAPS	Child and Adult Protective Services
CCUBS	Child Care Under The Big Sky
CDS	Central Database System
CEP	Contractor Engagement Proposals
CHIMES	Current Medicaid, SNAP and TANF eligibility system
CHIP	Children's Health Insurance Plan
CIO	Chief Information Officer
CIS	Central Information System
DMS	Centers for Medicaid and Medicare Services
COOP	Continuity of Operations Capability Program
COTS	Commercial Off-The-Shelf
CSO	Compliance and Security Office
DAWG	Database and Web Group
DMS	Document Management System
DTP	Disability Transitions Program
DWH	Data Warehouse
EA	Enterprise Architecture
EAP	Emergency Action Plan
EBT	Electronic Benefits Transfer
EES	Energy Education System
ESB	Enterprise Service Bus
FFP	Federal Financial Participation
FRAAP	Facilitated Risk Analysis Assessment Process
GIS	Geographical Information System
EHR	Electronic Health Records
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIRMS	Health Information and Resource Management System
HIT	Health Information Technology
HMIS	Homeless Management Information System
HMK	Healthy Montana Kids
IAPD	Implementation Advanced Planning Documents
IMMTRAX	Montana Immunization Tracking System
ISB	Information Systems Bureau
ISCP	Information System Contingency Plan
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management

JIRA	Commercial Software Product for Tracking Bugs and Issues
LIEAP	Low Income Energy Assistance Program
LRIT	Long Range Information Technology
MA	Medicaid
MACWIS	Montana Automated Child Welfare Information System
MHSP	Mental Health Services Plan
MICRS	Management Information and Cost Recovery System
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MSAMS	Montana Safety Assessment Management System
MSPIRIT	Woman, Infant and Child Management Program
NCB	Network and Communications Bureau
NIST	National Institute of Standards and Technology
OPM	Operation Protect Montana
PAPD	Planning Advanced Planning Documents
PMB	Project Management Bureau
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
POAM	Plan of Action and Milestones
RFP	Request for Proposal
SAMS	Substance Abuse Management System
SEARCHS	System for Enforcement and Recovery of Child Support
SIEM	Security Information and Event Management
SFSL	Shared Fiscal Services Layer
SITSD	State Information Technology Services Division
SNAP	Supplemental Nutrition Assistance Program
SOA	Service-Oriented Architecture
SSP	System Security Plan
TANF	Temporary Assistance for Needy Families
TEAMS	Former Medicaid, SNAP and TANF Eligibility System
TSC	Technology Services Center
TSD	Technology Services Division
VOIP	Voice Over Internet Protocol