Washington State Department of Social & Health Services

Transforming lives

Administrative Policy No. 15.25

Subject:	DSHS Information Technology Governance
Information Contact:	DSHS Chief Information Officer MS 45880 / (360) 902-7652
Authorizing Source:	DSHS Secretary Washington State Office of the Chief Information Officer
Effective Date:	October 1, 2016
Revised:	New
Approved By:	original signed by Dana Phelps Assistant Secretary, Services and Enterprise Support

Purpose

This policy establishes the information technology (IT) governance principles, processes and foundation for effective and secure information technology across the Department of Social and Health Services (DSHS). The intent is to ensure alignment with the Department's strategic direction and compliance with applicable laws, regulations, contractual obligations, and DSHS and statewide information technologies, information security, and privacy policies and standards.

Background

IT governance is key to IT-related decision-making throughout the Department. It includes:

- Utilization of IT systems and/or components that enable end-to-end business processes that coordinate the activities of the Department over time and across administration boundaries;
- IT investments that effectively deliver strategic business value year after year.

Continuous review and improvement processes to ensure IT investments are efficiently made and optimally managed. These processes are repeatable, predictable, and scalable to meet business needs.

IT governance encompasses IT systems and assets, the overall IT infrastructure, and communications to support the Department's strategic direction by improving overall management processes. IT governance provides a process to set priorities and select solutions based on business needs.

- Business defines its needs.

    - Business processes or issues are identified that require information technology solutions.
    - A business case is developed to clearly identify business requirements.
- IT recommends solutions that meet business needs.
    - Employing efficiency and optimization principles, and using the business case, IT recommends one or more solutions to meet the identified business requirements.
- IT governance throughout the Department provides processes to set priorities and select appropriate IT investments in alignment with the Department's strategic direction and in compliance with applicable laws, regulations, contractual obligations, and DSHS and statewide information technologies, information security, and privacy policies and standards.
    - Business needs, budget and resources are prioritized, and selected IT investments move forward with appropriate management and oversight.

Scope

This policy applies to all DSHS organizational units.

Additional Guidance

- DSHS Administrative Policies
    - No. 5.01 Privacy Policy – Safeguarding Confidential Information
    - No. 15-10 Information and Technology Security
    - No. 15-20 Exceptions to Policy for Information Technology
    - No. 15-21 Information Technology Standards Compliance
    - No. 15-22 Information Technology Portfolio Management
    - No. 15-23 Information Technology Project Management
- DSHS IT Standards Manual
- DSHS Information Security Manual
- Washington State Office of the Chief Information Officer Policies

Definitions

Administration – An organization within the Department of Social and Health Services that is governed by an assistant secretary. Administrations may have a designated Chief Information Officer/Information Technology Director and an IT Security Administrator. Administrations may serve one or more line of business, and all DSHS entities are governed by an administration.

Administration Chief Information Officer/IT Director – The individual within an administration responsible for recommending, implementing and managing information technologies that support the DSHS administration's business goals.

Asset – In the context of this policy, asset refers to IT investments owned or procured by DSHS, such as systems, hardware, software, equipment, services, contracts, and data contained or managed in said items.

Business Owner/Steward – Person responsible for business decisions related to IT systems or applications.

Client – A person who is currently receiving, has received in the past, or is applying for services or benefits from DSHS. This term includes, but is not limited to, consumers, recipients, applicants, residents of DSHS facilities or institutions, patients, parents and children involved with child welfare services, juveniles involved with the juvenile justice system, and parents receiving support enforcement services.

Confidentiality – A set of rules or a promise that limits access to or places restrictions on use or disclosure of certain types of information.

Customer – Internal or external DSHS IT service recipient.

Department – The Department of Social and Health Services.

Disaster Recovery – The documentation, plans, policies, and procedures that are required to restore normal operation to a state agency impacted by man-made or natural outages or disasters.

DSHS Cabinet – The leadership group comprised of the DSHS Secretary and assistant secretaries.

DSHS Chief Information Officer (CIO) – The individual in the DSHS Enterprise Technology Division with executive authority who serves as the Department's principal advisor on the effective application of information technology to meet business needs.

DSHS Chief Information Security Officer (CISO) – The individual in the DSHS Enterprise Technology Division responsible for the administration of the DSHS Information Security program.

DSHS Enterprise Technology Division (ET) – Serves as the primary provider for Department-wide information technology services such as network infrastructure, telephone and voice, information security, enterprise architecture, and information technology governance support.

DSHS Privacy Officer – The person designated by the DSHS Secretary or the DSHS Secretary's designee to oversee the Department's Privacy Program, which is responsible for carrying out Department-adopted policies and procedures related to the privacy and security of confidential information.

DSHS Secretary – The highest ranking DSHS executive and chair of the DSHS Cabinet. Serves as the final escalation point for decisions that cannot be resolved at the Cabinet level, and is responsible for final decisions.

Enterprise Technology Steering Committee (ETSC) – A group chaired by the DSHS Chief Information Officer and comprised of the DSHS administrations' CIOs/IT directors, and Enterprise Technology office chiefs.

Federated Model – A model for IT governance that combines the best features of centralized and decentralized models. The **centralized model** leverages economies of scale and emphasizes efficiency and cost control over line of business responsiveness. The **decentralized model** provides greater business ownership and responsiveness, but with less integration and fewer shared resources, likely resulting in higher costs. The **federated model** provides for common applications and pools infrastructure resources to reduce costs, while lines of business maintain control of their respective applications.

Governance – The processes, groups and activities associated with decision making and the exercising of authority.

Information Security – The practice of defending both paper and electronic information from unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction.

IT and Security Customer Review Board (CRB) – A Department-level group comprised of DSHS technical subject matter experts from each administration that represents the voice of the customer and provides advice on industry trends, business priorities, and strategic direction in the areas of application development, technology and security.

IT Investment – An organizational investment employing or producing information technology or IT-related assets. Each investment has or will incur costs for the investment, has expected or realized benefits arising from the investment, has a schedule of project activities and deadlines, and has or will incur risks associated with engaging in the investment. A "major IT project" (also referred to as a "major IT investment") is any project assessed as a risk level 2 or level 3 investment using the Severity and Risk Assessment process defined by the Washington State Office of the Chief Information Officer (OCIO) in OCIO 121 – Procedures, Appendix A: Severity and Risk Assessment.

IT Investment Planning – A systematic process for linking each agency's investment in IT to its business strategies, objectives, programs, and processes.

IT Portfolio – The application of systematic management of IT investments, projects, applications, systems, and assets within the Department.

Lines of Business – The various types of businesses managed within DSHS administrations.

Portfolio and Project Management Program Review Board (PRB) – A Department-level group comprised of DSHS IT portfolio and project management subject matter experts from each administration that represents the voice of the customer and provides advice on industry trends, business priorities, and strategic direction in the areas of IT portfolio management and project management.

Project – A temporary undertaking to create a unique product, service or result.

Project Management – The application of knowledge, skills, tools, and techniques to project activities to meet the project requirements and objectives.
Security Design Review – A process within a project or work effort through which a mature design is evaluated against state, federal, and Department requirements to identify and attempt to mitigate potential security issues before the product of the project or work effort is implemented.

Severity and Risk Review – An assessment review conducted on IT investments to identify the level of severity and risk of the investment. The level of overall risk determines the required level of oversight by DSHS and by the Washington State Office of the Chief Information Officer.

Wide Area Network (WAN) – The Department's telecommunications and computer network that extends across Washington State.

Policy Requirements

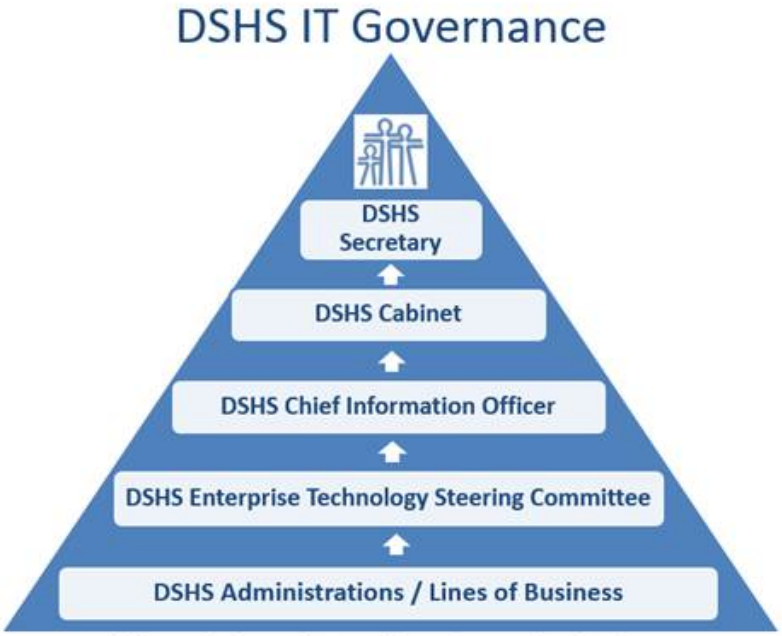
DSHS will use IT governance to align IT-related decision making with the mission, vision, values, strategic direction, and priorities set by the DSHS Secretary and assistant secretaries. These governance principles and processes provide the foundation for information technology across the Department, and ensure compliance with applicable laws, regulations, contractual obligations and statewide information technologies policies and standards.

Principles

The Department embraces the following principles in the provision of information technology services:

- We keep our focus on the customer and collaborate to meet client needs.
- We secure information technology and protect the privacy and confidentiality of data.
- We ensure fiscal responsibility for information technology financial management.
- We foster collaboration across the Department and embrace a federated model for its lines of business.
- We commit to open and effective communication, transparency and information sharing.

Business-Driven Information Technology Governance Process



Administrations are the foundation of the DSHS IT governance structure. The lines of business represented within the administrations are our connection to our clients and our staff must be enabled to respond to client needs quickly and efficiently.

IT governance is meant to simplify and streamline processes related to information technology, information security, and privacy to ensure responsiveness in providing services to our clients.

IT governance enables administrations to manage applications that support client services while balancing the Department's responsibility to provide oversight, manage risk, and adhere to applicable rules and requirements implemented at the federal and state levels. As such, DSHS information technology, information security, and privacy policies, standards, and processes need to clearly reflect and define this balance.

Administrations are responsible for maintaining their new and existing IT systems and applications, and ensuring they comply with all applicable rules and regulations as well as DSHS information technology, information security, and privacy policies and standards. Significant enhancements to existing IT systems are considered new IT investments requiring oversight level assessments.

Business areas within the administrations are responsible for identifying business needs or issues that appear to have an IT component, or require an IT enhancement or solution.

The overall IT governance process requires the following steps to ensure investments in business-responsive IT solutions that further the mission of the Department and comply with appropriate rules and regulations.

1. The business representative(s), assigned by and representing an interest of the administration, creates a business case for their leadership that clearly defines the business need or issue, as well as the scope, which includes whether the need or issue is limited to a business unit or program or impacts multiple divisions within the administration, multiple administrations and/or other agencies or external entities.

2. The business representative(s) meet(s) with the administration's CIO or IT director, or a designee, to review the business case and identify possible IT solutions responsive to the business need.
    a. If the response requires technology new to the administration, but not new to the Department, the administration's IT and Security Customer Review Board representative may bring questions to the Customer Review Board for discussion and guidance.
    b. If the investment requires technology new to the Department, the administration's CIO or IT director will bring the topic to the Enterprise Technology Steering Committee for discussion and direction. If the ETSC determines there is potential benefit for the Department, then the ETSC may recommend making it a Department-wide investment and managing it as such. If not, then the administration will manage the investment internally and share with the ETSC any enterprise-applicable knowledge obtained.

3. If an IT investment is required, it must be assessed for severity and risk, using the DSHS IT informal and formal assessment processes outlined in DSHS IT Standard: 12.3. – Informal IT Investment Assessments and DSHS IT Standard: 12.4. – Formal IT Investment Assessments, to determine the level of oversight required for the proposed investment/project per OCIO Policy121 - IT Investments - Approval and Oversight.

4. If the IT investment/project involves multiple administrations or external agencies/entities, it may be sponsored and managed by the involved administration(s) or by the DSHS Enterprise Technology Division as an enterprise-wide IT investment.

5. The DSHS CIO will raise awareness for all enterprise-wide IT investments to the DSHS Cabinet to ensure alignment with the DSHS strategic direction.

6. Once an IT investment has been approved, the administrations are required to:
    a. Work with DSHS contracts staff to assess the procurement requirements for the investment and ensure the IT investment is procured in accordance with state laws and policies.
    b. Ensure all IT investments/projects are managed in accordance with OCIO Policy 131 - Managing Information Technology Projects and all applicable DSHS IT policies and standards.

c. Ensure the IT investment/project and any resulting IT solutions comply with all applicable rules and regulations, and DSHS IT, information security, and privacy policies and standards.

Roles and Responsibilities

All of the following roles are responsible for adhering to the IT principles outlined in this policy when provisioning IT services including, but not limited to, development of IT systems, purchases of IT hardware, software or services, operation and maintenance of existing IT systems, and ensuring privacy and information security.

1. **DSHS Secretary**
   a. The DSHS Secretary delegates to the DSHS CIO the following IT responsibilities defined in OCIO Policy 121 – IT Investments – Approval and Oversight:
      - Planning, management and use of IT systems, telecommunications, equipment, software, and services of their respective agencies.
      - Ensuring the Department follows the processes delineated by the OCIO.
      - Responding to OCIO and Technology Services Board recommendations as needed.
      - Understanding conditions requiring OCIO approval of investments.
      - Ensuring all applicable laws, rules, policies, and standards governing IT are followed.
   b. The DSHS Secretary is responsible for making the final decision when the DSHS Cabinet is unable to come to agreement on IT decisions.

2. **DSHS Cabinet**
   a. Is comprised of the Department Secretary (chair) and the assistant secretaries from each DSHS administration.
   b. Serves as the escalation path for IT decisions that cannot be resolved at the Enterprise Technology Steering Committee level.
   c. Is the final arbiter of IT resource allocation decisions.

3. **DSHS Chief Information Officer**
   a. Develops and manages DSHS enterprise technology policies, standards, architectures, and infrastructure in alignment with the Department's strategic direction.
   b. Ensures proper management of information systems and solutions within DSHS by providing executive-level management advice and consultation on policy and program implications involving information technology.
   c. Works closely with the Department's operating executives and staff in developing a comprehensive IT strategic plan to meet the priority strategic needs of the Department with a focus on measureable results and accountability.
   d. Manages the DSHS IT portfolio used in establishing technology priorities and strategies to align with business priorities.
   e. Manages the DSHS relationship with the Washington State Office of the Chief Information Officer, and acts as a key liaison to Consolidated Technology

Services (CTS)/Washington Technology Solutions (WaTech), the Department of Enterprise Services (DES), other state agencies, and the Legislature.

f. Has the delegated authority to grant exceptions to DSHS IT policies, standards and processes as defined in DSHS Administrative Policy No. 15.20 – Exceptions to Policy for Information Technology.
g. Provides oversight and management of the services offered by and the activities conducted within the DSHS Enterprise Technology Division.
h. Chairs the Enterprise Technology Steering Committee.

4. DSHS Enterprise Technology Steering Committee

a. Is comprised of the DSHS CIO (chair), administration CIO(s) and IT directors, the DSHS Chief Information Security Officer and the DSHS Enterprise Technology Division Office Chiefs (Infrastructure, Technology/Strategy and Support Services), as defined in the ETSC charter.
b. Serves as the decision-making body and escalation path for IT issues that cross administrations or external agencies.
    i. If resolution is not obtained by the Enterprise Technology Steering Committee for an issue, it is referred to the DSHS Cabinet.
    ii. If issue resolution is not obtained from the DSHS Cabinet, it is referred to the DSHS Secretary.
c. Establishes and enforces DSHS IT governance policy and IT standards.
d. Establishes advisory customer and program review boards to provide venues for Department subject matter experts to advise the Enterprise Technology Steering Committee decision-making processes, designates administration representatives to serve as technical subject matter experts on the IT and Security Customer Review Board and the Portfolio and Project Management Program Review Board (CRB/PRB), and assigns work efforts to these review boards as required.
e. Collaborates with the DSHS CIO to create an overall DSHS IT strategic plan for the entire enterprise.
f. Collaborates with other members of the Enterprise Technology Steering Committee on behalf of the best interests of DSHS clients, and escalates disagreements between ETSC members, the DSHS CIO and/or the DSHS Enterprise Technology Division, to the DSHS Cabinet and the DSHS Secretary for resolution.

5. DSHS Chief Information Security Officer

Establishes and enforces the DSHS Information Security program, including information security, privacy (in collaboration with DSHS Privacy Officer) and disaster recovery planning.

6. DSHS Privacy Officer

Collaborates with the DSHS Information Security Office to ensure Department adherence to data privacy requirements.

7. Department-Level IT and Security Customer Review Board and Portfolio and Project Management Program Review Board

a. Are comprised of representatives with subject matter expertise from each administration, as designated by members of the Enterprise Technology Steering Committee in collaboration with their respective administration's leadership.
b. Perform advisory functions [without decision-making authority] as requested by the Enterprise Technology Steering Committee and DSHS administration lines of business.
c. Provide DSHS administration lines of business with access to Department technical subject matter experts.
d. Collaborate with the Enterprise Technology Steering Committee and other administrations on development of Customer Review Board/Program Review Board meeting agendas.
e. Review Customer Review Board/Program Review Board documents prior to meetings, collaborate with other members, and staff within their respective administration on behalf of DSHS clients, and make recommendations to the Enterprise Technology Steering Committee to inform decision-making.
f. Assess and recommend to the Enterprise Technology Steering Committee development of models, and implementation of principles, policies, and standards related to the management of information security and common technologies within DSHS.
g. Keep respective Enterprise Technology Steering Committee members and administration lines of business apprised of IT initiative status and issues as appropriate between Customer Review Board/Program Review Board meetings, with timely communication prior to Enterprise Technology Steering Committee meetings.

8. **Administrations/DSHS Lines of Business**
   a. Develop appropriately resourced IT initiatives and appropriately managed IT assets (including data) to meet their business needs.
   b. Ensure IT systems/applications have a business owner/steward who has responsibility and accountability for ensuring the system/application meets the business needs and priorities, and a technical owner/steward who ensures business and technical priorities are implemented as determined through IT governance processes.
   c. Provide business representatives to create business cases that clearly define the business need or issue as well as the scope, including whether it is limited to a business unit or program, or it impacts multiple divisions within the administration, multiple administrations and/or other agencies or outside entities.
   d. Ensure that the administration's CIO or IT director, or a designee, reviews the business case and identifies possible IT responses to the need.
   e. Ensure all IT investments/projects are assessed to determine required level of oversight.
   f. Ensure all IT investments/projects are managed in accordance with OCIO Policy 131 - Managing Information Technology Projects and all applicable DSHS IT policies and standards.
   g. Ensure all IT investments/projects that require the purchase of IT hardware, software or services are procured in compliance with Chapter 39.26 RCW –

Procurement of Goods and Services, as well as all DES and DSHS procurement and contracts policies.

h. Ensure IT investments/projects and any resulting IT solutions comply with all applicable rules and regulations, and DSHS IT, information security, and privacy policies and standards.
i. Bring new IT development projects with potential cross-administration or external-agency implications to the Enterprise Technology Steering Committee for review and consideration.
j. Provide administration technical subject matter expert resources to engage in Customer Review Board/Program Review Board activities, including discussion regarding possible new technology within DSHS as directed by the Enterprise Technology Steering Committee.
k. Leverage participation in Customer Review Board/Program Review Board activities to facilitate access to technical subject matter experts across the Department.
l. Submit all new technical developments and applications for internal and external security design reviews as required, and ensure IT investments/projects and any resulting IT solutions comply with all applicable rules and regulations, and DSHS IT policies and standards, including information security and privacy policies and standards.
m. Collaborate with the administration's CIO/IT director on behalf of DSHS clients, and through the administration's CIO/IT director, escalate disagreements between any individual ETSC member(s), the DSHS Chief Information Officer, and/or the DSHS Enterprise Technology Division to the DSHS Cabinet and the DSHS Secretary for resolution.

9. **DSHS Enterprise Technology Division**
   a. Provides the following services within DSHS:
      i. DSHS IT financial management.
      ii. DSHS IT strategic planning (in collaboration with the Enterprise Technology Steering Committee).
      iii. DSHS IT portfolio management.
      iv. Enterprise architecture.
      v. IT investment planning and authorization.
      vi. Technology infrastructure provisioning.
      vii. Promotion of organizational efficiency, interoperability and communication.
      viii. Staffing (including Chair) for the Enterprise Technology Steering Committee and staffing (including Co-Chairs) for the IT and Security Customer Review Board and the Portfolio and Project Management Program Review Board meetings, setting direction and establishing meeting agendas in collaboration with the Enterprise Technology Steering Committee, Customer Review Board members and Program Review Board members.
      ix. External IT reporting as delegated by the DSHS CIO.

x. Centralized infrastructure services, IT operations support and maintenance of a portfolio of applications in support of centralized DSHS services.
xi. DSHS Information Security program management