





2022 - 2025
OREGON MEDICAL BOARD
**INFORMATION TECHNOLOGY
STRATEGIC PLAN**

TABLE OF CONTENTS

Mission	2
Values	2
Introduction	2
Goals and Strategies	2
 Appropriately Secure Agency Information Assets	4
 Replace CORE Business Suite Software	6
 Support Users in All Work Environments	8
 Maintain a Reliable Infrastructure that Utilizes Current Technology	10
 Respond to Evolving Legislative and Enterprise Requirements	12
Change Log	14

MISSION

The mission of the Oregon Medical Board is to protect the health, safety, and wellbeing of Oregon citizens by regulating the practice of medicine in a manner that promotes access to quality care.

VALUES

The Oregon Medical Board's values further the mission and shape the culture of the agency. In 2022, the Management Team restated that five core values guide the agency. These values are incorporated into the agency and Information Technology Strategic Plans:

1. **INTEGRITY** – a commitment to acting honestly, ethically, and fairly.
2. **ACCOUNTABILITY** – a willingness to accept responsibility for actions in a transparent manner.
3. **EXCELLENCE** – an expectation of the highest quality work and innovation.
4. **CUSTOMER SERVICE** – a dedication to provide equitable, caring service to all Oregonians with professionalism and respect.
5. **EQUITY** – a devotion to creating and fostering an environment where everyone has access and opportunity to thrive.

INTRODUCTION

In May 2022, the Oregon Medical Board (in this document also called the “Board” or the “OMB”) embarked on a formal planning process to outline its information technology path for the next three years. The agency began this Information Technology Strategic Plan to proactively set direction and sees the plan as a living work in progress rather than a static document. With this plan we recognize that technology and the business requirements of technology change much more rapidly than agency-level strategic plans. The agency information technology team must remain flexible; this plan will be reviewed and updated on a quarterly basis to reflect changes in Enterprise, legislative, agency, and technology direction as well as resource availability.

As with the [Agency Strategic Plan](#), this Information Technology Strategic Plan directs the Oregon Medical Board in fulfilling its mission by establishing goals. Each goal is followed by a purpose statement, explaining why the goal is needed and how the goal relates to the agency's guiding values. The Information Technology Strategic Plan then identifies strategies and action items to move the agency towards fulfilling the goal.

GOALS, STRATEGIES, AND ACTION ITEMS

The Oregon Medical Board's Strategic Plan goals are the highest-priority purposes of the agency. Along with the Mission Statement, the OMB's goals describe the agency's desired strategic position. This Information Technology Strategic Plan supports and facilitates the agency goals.

The following provides OMB's information technology chief goals, along with a purpose statement and the strategies designed to achieve them. These strategies are expressed as directions, approaches, or policies. The action items help ensure the Oregon Medical Board is moving toward its goals. Each action item relates to one or more strategies to support the goal. The OMB Information Technology Team reviews action items regularly to ensure the actions are completed, current, and relevant. The action items noted are projects which are estimated to require a week or more of effort to accomplish. This strategic plan does not capture the hundreds of other one-off tasks requiring minutes to days of effort that will be accomplished simultaneously. A “week of effort” should be considered an estimated 40 hours of dedicated time for a member of the Information Technology Team, though the time investment generally will not occur all at once; the project may take weeks or months to complete. Weeks of effort noted does not account for the required effort of OMB staff outside of the Information Technology Team.

Finally, this plan as adopted does not include unknown work that will be required as an outcome of an FBI Audit, audits by the state, legislative changes, changing state policies, planned external penetration testing, mitigation of vulnerabilities discovered in systems and hardware, and ongoing self-assessments. Additional action items are expected to be added during progress reviews. A change log is included to help identify changes in planned activities over time.



APPROPRIATELY SECURE AGENCY INFORMATION ASSETS

As the custodian of significant amounts of highly confidential information about people, including criminal history, the Board is **accountable** for safeguarding our information assets and ensuring employees handle the information with **integrity**. At the same time, the Board provides **customer service** to the public through **equitable** access to agency data in compliance with public records requirements. The Board demonstrates **excellence** through compliance with recognized standards and best practices.

PRIMARY STAFF RESOURCE(S): ISS7 POSITIONS, SUPPORTED BY ISS3 AND LIMITED DURATION SYSTEMS ADMINISTRATOR

STRATEGIES

- 1.1 Protect sensitive agency information by obtaining and documenting compliance with relevant information security standards, including but not limited to:
 - a. Center for Internet Security (CIS) controls
 - b. National Institute of Standards and Technology (NIST) controls
 - c. Criminal Justice Information Services (CJIS) Security Standards
 - d. State of Oregon Information and Cyber Security Standards

Agency Strategic Plan Strategy 1.13

- 1.2 Keep current with changes in security threats and security tools. *Agency Strategic Plan Strategy 1.13*

- 1.3 Keep staff informed of changing security threats and provide tactics and tools to protect them from compromise. *Agency Strategic Plan Strategy 1.14*

- 1.4 Provide a reliable and tested plan for business continuity of technology and information in the event of a disaster. *Agency Strategic Plan Strategy 1.10*

ACTIONS

Due	Action	Tickets	Weeks of Effort	Strategy
2022				
22.1.a	Participate in and implement fixes to findings from FBI Audit of compliance with Criminal Justice Information (CJI) Security policy, required for storing CJI.	HD-5721 DONE	2 (All)	1.1
22.1.b	Participate in and remedy findings from state Cyber Security Services (CSS) assessment on the Center for Internet Security (CIS) controls, the most commonly used IT security standards.	HD-5059 DONE	1 (All)	1.1
22.1.c	Review and document compliance with relevant Center for Internet Security (CIS) controls.	HD-688 HD-1610 HD-4408 HD-4409 HD-4410	3 (All)	1.1
22.1.d	Review and implement fixes to findings from penetration testing.	HD-5109 DONE	(All)	1.2

Due	Action	Tickets	Weeks of Effort	Strategy
22.1.e	Evaluate, procure, and implement Security Information Event Management software (SIEM) to centralize the storage of system logs, improve compliance with all standards, and increase detection of suspicious behavior.	HD-3125 HD-4815 DENIED by EIS	4 (All)	1.2
22.1.f	Review and update agency Information Technology Disaster Recovery Plan and other elements of the agency Continuity of Operations Plan (COOP).	HD-5630 HD-5733	0.5 (ISS7)	1.2
2023				
23.1.a	Store Workstation images on Box to issue workstations more easily if the office or its systems become unavailable.	HD-432 NOT PURSUING	(SA)	1.4
23.1.b	Add Continuity of Operations Plan (COOP) webpage in SharePoint to improve agency COOP response.	HD-150	(ISS3)	1.4
23.1.c	Annually, deliver agency-wide information security training to refresh staff information security knowledge and increase awareness of new security developments.	DONE	1 (ISS3)	1.3
2024				
24.1.a	Annually, deliver agency-wide information security training to refresh staff information security knowledge and increase awareness of new security developments.		1 (ISS3)	1.3
24.1.b	Review and document compliance with relevant National Institute of Standards and Technology (NIST) controls, the most commonly used government IT security standards.		5 (All)	1.1
24.1.c	Review and document compliance with Statewide Information Security Standards.	HD-337 HD-442 HD-443 HD-446 HD-477 HD-478	4 (All)	1.1
24.1.d	Update CJIS compliance with new standards	HD-6079	5 (ISS6)	1.1
2025				
25.1.a	Annually, deliver agency-wide information security training to refresh staff information security knowledge and increase awareness of new security developments.		1 (ISS3)	1.3
25.1.b	Create or procure a governance, risk, and compliance (GRC) system to streamline assessment and reporting of compliance with various security standards.		3 (All)	1.2



REPLACE CORE BUSINESS SUITE SOFTWARE

To continue providing **excellence** in **customer service**, the Board must replace its aging Core Business Suite Software. The Board demonstrates its commitment to **integrity** and **equity** through the fair and open procurement of replacement software with project governance maintaining **accountability** to our customers and partners.

PRIMARY STAFF RESOURCE(S): ISS7 POSITIONS

STRATEGIES

- 2.1 Select a Systems Implementor who can partner with the agency to meet OMB needs for a successful implementation and long-term support. [Agency Strategic Plan Strategy 1.7](#)
- 2.2 Collaborate with the Systems Implementor and agency staff to design, configure and deploy the new system. [Agency Strategic Plan Strategy 1.7](#)
- 2.3 Ensure no current system capabilities are lost or degraded at any point in the transition to the new system. [Agency Strategic Plan Strategy 1.7](#)
- 2.4 Work with Systems Implementor to discover, design and implement opportunities for new and improved processes. [Agency Strategic Plan Strategy 1.7](#)
- 2.5 Ensure new system is configured using best practices. [Agency Strategic Plan Strategy 1.7](#)
- 2.6 Minimize project impact on day-to-day business operations. [Agency Strategic Plan Strategy 1.7](#)

ACTIONS

	Action	Tickets	Weeks of Effort	Strategy
2022				
22.2.a	Work with DAS Procurement Services, DOJ, and agency internal team to review and score Systems Implementor RFP Proposals.	HD-4072 HD-4462 HD-4488 HD-4513 DONE	5	2.1

	Action	Tickets	Weeks of Effort	Strategy
22.2.b	Utilize a Limited Duration Systems Administrator position to maintain existing agency technical infrastructure and provide user support throughout system implementation, freeing current OMB technology staff to devote their expertise in agency business processes and custom systems to the project. Collaborate with the agency Human Resources Manager to develop position description, appropriately classify, recruit, and fill the position. Target completion dates: <ul style="list-style-type: none"> Position description developed- June 20, 2022 Position description reviewed and classified- July 15, 2022 Recruitment opened- August 1, 2022 Target hire date – October 1, 2022 	HD-4937 DONE	2	2.6
22.2.c	Work with DAS Procurement Services, DOJ, and agency internal team to negotiate contract statement of work, licensing, delivery schedule, and terms with selected Systems Implementor.	HD-4847 DONE	1	2.1
22.2.d	Engage in discovery and assessment sessions with Systems Implementor and agency staff to ideate and plan system configuration elements, test strategy, data migration strategy, cutover strategy, and schedule of project activities.		2	2.3 2.5
2023				
23.2.a	Work with Systems Implementor and agency staff to design, develop, test, and release functional system through iterative sprints.		5	2.3 2.5
23.2.b	Collaborate with Systems Implementor and agency staff to clean and migrate agency data to the new system.	HD-5598	2	2.3
23.2.c	Engage with Systems Implementor to document system functionality in a manner that works for long-term use by all agency staff.		2	2.5
23.2.e	Seek an online mechanism for accepting and loading customer complaints into the CORE system while minimizing the opportunities for abuse by external users.		3	2.4
23.2.f	Seek modifications in access to Board meeting materials with a goal of direct, online information from the CORE system to eliminate the use of large PDF files.		2	2.4
2024				
24.2.a	Transition agency staff to utilizing the new system (Go Live/Cutover).		2	2.2
24.2.b	Devise a system for storing and viewing medical images so they can be reviewed by internal and external users.			2.4
24.2.	Transition techMed to end of service, maintaining only as needed to meet retention requirements.		2	2.2
24.2.e	Enter long-term maintenance and operations with the new system that includes a balance of support between the agency and the external Systems Implementor.			2.2
24.2.f	Build out automated tests	HD-6632	8	2.5

	Action	Tickets	Weeks of Effort	Strategy
2025				
25.2.a	Improve the process of managing medical records so they involve less processing for staff and are easier for internal and external users to review.		2	2.4



SUPPORT USERS IN ALL WORK ENVIRONMENTS

The agency has proven to be capable of providing **excellence** whether working in the office or working remotely. The Board must provide its staff and Board members with **customer service** in this new work model. All staff and Board members must have **equitable** opportunity to be productive regardless of work location. At the same time, the Board must ensure the **integrity** and **accountability** of work is not compromised by the increased flexibility in work locations.

PRIMARY STAFF RESOURCE(S): ISS3 POSITION, SUPPORTED BY ISS7s AND LIMITED DURATION SYSTEMS ADMINISTRATOR

STRATEGIES

- 3.1 Enact preventative changes and solutions to improve the security, efficiency and reliability of systems while keeping the frequency and impact to users at a minimum. *Agency Strategic Plan Strategy 1.6*
- 3.2 Ease changes in the use of technology through communication, training, and documentation. *Agency Strategic Plan Strategy 1.14*
- 3.3 Ensure all users have the capability of working in and out of the office on their own schedule with minimal technology disruptions. *Agency Strategic Plan Strategy 1.6*
- 3.4 Implement quality solutions to issues reported by staff and Board members. *Agency Strategic Plan Strategy 1.6*

ACTIONS

Year	Action	Tickets	Weeks of Effort	Strategy
2022				
22.3.a	Recruit, hire, and onboard an ISS3 User Support Specialist.	DONE	4 (ISS7)	3.3
22.3.b	Replace staff desktops with laptops to give all staff the capability of working remotely and flexibly within the office.	HD-3531 DONE	2 (ISS3)	3.3
22.3.c	Develop help documentation and upgrade staff to Office for M365 so they will be on the latest version of Office before the current version's mainstream support ends.	HD-5217	1 (ISS3)	3.1 3.2
22.3.d	Consider implementing a password manager for agency use to improve the ease and security of managing passwords.	HD-963	1 (ISS3/ISS6)	3.4
2023				
23.3.a	Migrate staff to SSL VPN to make setting up and connecting to VPN easier.	HD-5072 NOT PURSUING	1 (ISS6)	3.3
2024				
24.3.a	Migrate and update OMB Help	HD-5489	5 (ISS3)	
2025				



MAINTAIN A RELIABLE INFRASTRUCTURE THAT UTILIZES CURRENT TECHNOLOGY

To provide **customer service** to all internal and external users, the Board’s technology infrastructure must maintain a level of **excellence** in its availability and reliability. All users must have **equitable** access appropriate to their role and have **accountability** in accessing and modifying systems and data. All systems must enforce the **integrity** of the system and any data residing within it.

PRIMARY STAFF RESOURCE: LIMITED DURATION SYSTEMS ADMINISTRATOR

STRATEGIES

- 4.1 Update and improve the technology infrastructure to improve efficiency, reliability, availability and limit the risk of issues with compatibility, failure, and lack of support. *Agency Strategic Plan Strategy 1.6*
- 4.2 Favor simplicity in design and operation to improve maintainability and reliability without compromising on the agency’s complex needs. *Agency Strategic Plan Strategy 1.6*
- 4.3 Remedy known vulnerabilities and harden infrastructure as necessary to keep it secure. *Agency Strategic Plan Strategy 1.13*
- 4.4 Provide a robust and reliable document management system that meets agency needs, maintains security compliance, and supports legal requests. *Agency Strategic Plan Strategy 1.6*

ACTIONS

Year	Action	Tickets	Weeks of Effort	Strategy
2022				
22.4.a	Upgrade the server that centrally stores logs for sensitive systems to ensure continued vendor support.	HD-3891 DONE	1	4.1
22.4.b	Replace the agency’s chat software with Teams to reduce the number of services and systems requiring maintenance.	HD-5150 HD-5434 DONE	1	4.2
22.4.c	Migrate systems to Windows Update to reduce the time required to deploy updates and support the current deployment system.	HD-3729	1	4.2
22.4.d	Implement the patch for the high-risk Spectre/Meltdown vulnerability on the techMed database server to keep our licensee data secure.	HD-777 DONE	1	4.3
22.4.e	Implement fixes from the June 2020 penetration testing to reduce system vulnerability.	HD-1818 HD-1819 DONE	1	4.3

Year	Action	Tickets	Weeks of Effort	Strategy
22.4.f	Enable additional security policies on the firewall. Denial of service protection will make it less vulnerable to being overwhelmed by attackers. Data Leakage protection will alert when sensitive information is sent outside the agency.	HD-1386 DONE	1	4.3
22.4.g	Disable sharing of the top-level folders in Box to eliminate the risk of inadvertent sharing of files and folders outside of the agency.	HD-3577 NOT PURSUING	1	4.3
22.4.h	Set up the Board and Conference rooms to allow for Board meetings, committee meetings, and interviews to be held with a mixture of participants inside and outside the office.	HD-4393 HD-5407 HD-5535 HD-5138 DONE	2	4.1
2023				
23.4.a	Migrate Jira to the cloud prior to February 15, 2024 version end of life and product support.	HD-4144 DONE	2	4.1
23.4.b	Explore using a cloud service to sign into services, such as Box, reducing IT effort to maintain current servers.	NOT PURSUING	1	4.2
23.4.c	Investigate the potential migration of files from Box to another cloud provider to make file management more reliable and easier for staff.	NOT PURSUING	2	4.4
23.4.d	Upgrade server storage infrastructure for backups, servers, and other system needs.	HD-5011 HD-5482 HD-5727 DONE	3	4.1
2024				
24.4.a	Decommission SCCM	HD-5175	5	4.2
2025				
25.4.a	Replace servers providing essential business services that were purchased in 2015 to reduce risk of system failure.	HD-6033	4	4.1
25.4.b	Migrate on-premises SharePoint prior to July 14, 2026 version end of life and product support.	HD-4731 HD-473	2	4.1
25.4.c	Upgrade all servers to the latest version of Windows to reinstate mainstream support and updates that improve security and performance.	HD-6032	4	4.1
25.4.d	Streamline firewall management by replacing network devices with the same brand as our firewall and restructuring configuration.		2	4.2



RESPOND TO EVOLVING LEGISLATIVE AND ENTERPRISE REQUIREMENTS

The Board demonstrates its **excellence** and **accountability** to the public and licensees through compliance with state regulations. We work to remain compliant while keeping **customer service** paramount, acting with **integrity** and **equity** in all that we do.

PRIMARY STAFF RESOURCE(S): ISS7 POSITIONS, SUPPORTED BY LIMITED DURATION SYSTEMS ADMINISTRATOR

STRATEGIES

- 5.1 Ensure agency resources comply with Oregon Revised Statutes, Oregon Administrative Rules, the Oregon Accounting Manual, state and agency policies, and labor contracts. *Agency Strategic Plan Strategy 1.8*
- 5.2 Engage with Enterprise-level partners at Enterprise Information Services (EIS) and DAS to keep abreast of Enterprise initiatives and advocate for agency business needs. *Agency Strategic Plan Strategy 1.8*
- 5.3 Establish agency technology professionalism and reliability by remaining attuned to technology industry direction and adopting recognized technology best practices. *Agency Strategic Plan Strategy 1.8*

ACTIONS

Year	Action	Tickets	Weeks of Effort	Strategy
2022				
22.5.a	Participate in regular meetings and engage with partners and colleagues to keep apprised of Statewide events, gain perspective from other agencies, build interagency relationships, and share information. Examples include: <ul style="list-style-type: none"> • Assigned EIS Senior IT Portfolio Manager (SIPM) and Assistant State Chief Information Officer • Chief Information Officer Council • Information Security Council • Chief Information Officers and other staff within other state agencies 	DONE	2 (ISS7)	5.2 5.3
22.5.b	Transition agency email and email archive to Enterprise M365 Tenant.	HD-3109 DONE	2 (ISS7)	5.1
22.5.c	Build out an IT Strategic plan as requested by EIS.	HD-4551 DONE	1 (ISS7)	5.1 5.2
22.5.d	Complete secondary phase of physician assistant modernization requirements of 2021 HB 3036.	HD-3420 DONE	3 (ISS7)	5.1
22.5.e	In response to the Enterprise Data Governance Policy, create an agency Data Governance Plan, establishing metrics for reporting the efficacy and efficiency of the agency's data governance program and training of staff on data quality requirements.	HD-4677 DONE	2 (ISS7)	5.1 5.2 5.3
22.5.f	Transition agency systems and staff to utilize two-factor authentication to utilize M365 and Workday.	HD-4729 DONE	2 (ISS7)	5.1

Year	Action	Tickets	Weeks of Effort	Strategy
22.5.g	Add correspondence in Techmed to capture Board member votes on recommendations.	HD-4944 DONE	1	5.1
22.5.h	Configure Techmed to support the practice of Volunteer Practitioners according to HB 4096.	HD-4880 DONE	3	5.1
22.5.i	Rename Complaint and Notice orders to Notice of Proposed Disciplinary Action	HD-5053 DONE	2	5.1
22.5.j	Replace vulnerability scanners with State controlled devices.	HD-4992 DONE	2	5.2
2023				
23.5.a	Participate in regular meetings and engage with partners and colleagues to keep apprised of Statewide events, gain perspective from other agencies, build interagency relationships, and share information. Examples include: <ul style="list-style-type: none"> Assigned EIS Senior IT Portfolio Manager (SIPM) and Assistant State Chief Information Officer Chief Information Officer Council Information Security Council Chief Information Officers and other staff within other state agencies 	DONE	2 (ISS7)	5.2 5.3
23.5.b	Initiate final phase of physician assistant modernization requirements of 2021 HB 3036.	HD-3421 DONE	1 (ISS7)	5.1
23.5.c	Integrate all agency systems into the state's Endpoint Detection and Response (EDR) solution which would provide immediate response when detecting suspicious program behavior.	HD-5015 NOT PURSUING	1 (SA)	5.1 5.2 5.3
23.5.d	In response to the Enterprise Open Data initiative, assess privacy protections, cleaning data, and testing publishing of agency-held licensee public data. Consider potential new data sets available from the new CORE system.	DONE	1 (ISS7)	5.1 5.2 5.3
2024				
24.5.a	Participate in regular meetings and engage with partners and colleagues to keep apprised of Statewide events, gain perspective from other agencies, build interagency relationships, and share information. Examples include: <ul style="list-style-type: none"> Assigned EIS Senior IT Portfolio Manager (SIPM) and Assistant State Chief Information Officer Chief Information Officer Council Information Security Council Chief Information Officers and other staff within other state agencies 		2 (ISS7)	5.2 5.3
24.5.b	Complete final phase of physician assistant modernization requirements of 2021 HB 3036.	HD-3421	2	5.1

Year	Action	Tickets	Weeks of Effort	Strategy
24.5.c	In response to the Enterprise Open Data initiative, assess privacy protections, cleaning data, and testing publishing of agency-held licensee public data. Consider potential new data sets available from the new CORE system.		2 (ISS7)	5.1 5.2 5.3
24.5.d	Integrate agency cell phones into the state's Mobile Device Management (MDM) solution as required by the state to standardize management, security, and lower cost for these devices.	HD-6610	2 (ISS3/ ISS6)	5.1 5.2 5.3
24.5.e	HB 4010 Rename Physician Assistant to Physician Associate		5	5.1
2025				
25.5.a	Participate in regular meetings and engage with partners and colleagues to keep apprised of Statewide events, gain perspective from other agencies, build interagency relationships, and share information. Examples include: <ul style="list-style-type: none"> Assigned EIS Senior IT Portfolio Manager (SIPM) and Assistant State Chief Information Officer Chief Information Officer Council Information Security Council Chief Information Officers and other staff within other state agencies 		2 (ISS7)	5.2 5.3
25.5.b	In response to the Enterprise Open Data initiative, assess privacy protections, cleaning data, and publishing agency-held licensee public data. Consider potential new data sets for publication.		1 (ISS7)	5.1 5.2 5.3

CHANGE LOG

Action item numbering strategy: Year.Goal Number.Action Item Identifier

Date	Action Item	Change	Made by
07/20/2022		Document Adopted	
10/20/2022		Quarterly review and update	Carol Brandt, Randall Wagenmann, Mark Levy, Jen Lannigan

Date	Action Item	Change	Made by
2/9/2023		Quarterly review and update	Carol Brandt, Randall Wagenmann, Mark Levy, Jen Lannigan, Harley Tomlinson
5/3/2023		Quarterly review and update	Carol Brandt, Randall Wagenmann, Mark Levy, Jen Lannigan, Harley Tomlinson
8/1/2023		Quarterly review and update	Carol Brandt, Randall Wagenmann, Jen Lannigan, Harley Tomlinson, Elie Enderle
3/21/2024		Quarterly review and update	Carol Brandt, Randall Wagenmann, Jen Lannigan, Harley Tomlinson, Elie Enderle