OVMEB INFORMATION TECHNOLOGY STRATEGIC PLAN (2025–2030)

Introduction

The Oregon Veterinary Medical Examining Board (OVMEB) developed this Information Technology Strategic Plan in alignment with the statewide Enterprise Information Services (EIS) Strategic Framework and in accordance with direction that all agencies maintain formal IT strategic plans. The plan articulates how OVMEB will modernize systems, improve cybersecurity, comply with accessibility standards, enhance public transparency, and support agency operations over the 2025–2030 planning horizon.

This streamlined plan is intended for internal leadership, EIS partners, stakeholders, and the public to understand OVMEB's IT priorities, initiatives, and roadmap.

Executive Summary

OVMEB is a small regulatory agency with a mission centered on public and animal health. Its technology environment is limited in capacity and anchored by a legacy licensing database system. Over the next five years, OVMEB will modernize its core systems, strengthen cybersecurity, improve digital accessibility, and develop data-driven reporting tools. Foundational work began in 2025, including system assessments, cybersecurity policy updates, accessibility gap reviews, baseline metric development, and requirements gathering for modernization. These efforts position OVMEB for transformative changes aligned with statewide expectations.

Background and Purpose

In January 2023, the Governor directed agencies to create IT strategic plans aligned with the statewide EIS Strategic Framework. These plans must demonstrate how technology investments support agency missions, modernize service delivery, strengthen cybersecurity, and address statewide priorities.

This plan fulfills that requirement for OVMEB. It details the current IT environment, future state vision, strategic initiatives, metrics, and the roadmap necessary to achieve long-term modernization goals.

Agency Drivers

Agency Mission
To protect public and animal health by ensuring only qualified individuals practice veterinary medicine in Oregon and by enforcing statutory and regulatory requirements.

Drivers Influencing IT Strategy
- Need to replace the aging licensing and regulatory system.
- Cybersecurity threats and statewide security requirements.
- Mandates for digital accessibility and public transparency.
- Limited staffing capacity requiring efficient, phased modernization.
- Growth in data reporting needs for licensing and enforcement activities.
- Statewide requirement for agencies to maintain an aligned IT strategic plan.

Current IT Landscape

Summary of Current Environment
OVMEB operates a legacy licensing system with limited flexibility, dated architecture, and security constraints. System assessments highlight workflow inefficiencies, manual processes, limited integration options, and high risk for technical obsolescence.

Current Strengths
- Agency-wide completion of cybersecurity training.
- Commitment to modernization and EIS alignment.
- Cloud-based collaboration tools in use.

Challenges
- Very limited internal IT capacity.
- Legacy systems limit security, accessibility, and modernization.
- Limited web development resources for accessibility compliance.

IT Context

IT Vision
Enable secure, modern, accessible, and reliable technology that strengthens OVMEB's regulatory mission and improves service delivery for applicants, licensees, and the public.

IT Mission
Provide technology leadership and services that enhance efficiency, protect sensitive data, support regulatory operations, and ensure transparent and accessible public services.

Guiding Principles

- Modernize technology to enhance agency effectiveness.
- Maintain cybersecurity as a foundational requirement.
- Comply with accessibility standards, transparency expectations, and Oregon's plain-language requirements.
- Prioritize solutions that fit agency capacity through phased, sustainable implementation.
- Collaborate effectively with DAS EIS and vendor partners.

IT Operating Model

Given OVMEB's size, the Executive Director oversees IT governance. Staff participate in requirements gathering, training, and system adoption. Technical expertise is supported through DAS EIS and contracted vendors.

IT Strategic Initiatives

Initiative 1: Licensing System Modernization

Purpose: Replace the outdated licensing system with a secure, flexible, and accessible modern platform.

Progress to Date: System assessment completed; requirements gathering underway; Stage Gate preparation initiated.

Challenges: Limited staff capacity and strict statewide cybersecurity and accessibility standards for vendors.

Mitigation: Strong partnership with EIS; phased approach.

Initiative 2: Cybersecurity Enhancement

Purpose: Improve agency resilience and protect sensitive data.

Progress: Completed cybersecurity posture review; updated policies; 100% training compliance; MFA expansion planning underway.

Initiative 3: Website Accessibility and Transparency

Purpose: Modernize public-facing digital services.

Progress: Accessibility gaps identified; redesign planning underway; content inventory initiated.

Constraints: Limited internal development resources.

Mitigation: Use of statewide shared services or vendors.

Initiative 4: IT Foundations and Staff Support

Purpose: Ensure staff have reliable hardware, tools, and training.

Progress: Hardware inventory completed; training fully up to date; remote work needs assessed.

Initiative 5: Data Analytics and Reporting
Purpose: Develop improved data reporting capabilities.
Progress: Identified metrics for licensing, enforcement, and internal operations; documented data quality gaps.

Metrics and Targets

Baseline Metrics in Development
- System uptime baseline to be finalized in 2025.
- Licensing processing times baseline established.
- Cybersecurity incident rate remains low and monitored.
- Accessibility audit scheduled for 2026.
- User satisfaction survey under development.
- Mandatory IT training remains at 100% completion.

Future Performance Targets (2030)
- 99% uptime on new licensing system.
- 25–40% reduction in processing times.
- Zero preventable cybersecurity incidents.
- Full WCAG 2.1 AA compliance.
- User satisfaction of 80% or higher.

IT Roadmap

2025
- Complete system assessments and Stage Gate preparation.
- Continue requirements gathering and business analysis.

2026
- Submit Stage Gate 1.
- Begin procurement for modernization.
- Conduct accessibility audit.
- Begin website redesign planning.

2027
- Begin phased licensing system implementation.
- Begin website modernization.
- Develop analytics infrastructure.

2028
• Continue implementation and stabilize new system components.
• Deploy analytics and reporting functionality.

2029
• Optimize new systems; refine cybersecurity practices.
• Expand reporting and transparency capabilities.

2030
• Conduct strategic plan refresh.
• Evaluate modernization outcomes.

IT Strategy Communication

Communication Approach
• Present plan to OVMEB leadership for adoption.
• Engage DAS EIS Assistant State CIO for alignment and feedback.
• Publish final plan on OVMEB's public website.
• Submit link to Strategic Initiatives and Enterprise Accountability for inclusion on the Transparency Portal.
• Provide annual updates each June via the required IT Strategic Plan Progress Report.

IT Strategy Continuous Lifecycle

Lifecycle Management
• Annual review through governance and required progress reporting.
• Formal refresh every 3–5 years or aligned with agency strategic plan.
• Update plan to reflect new policies, technologies, or business needs.
• Maintain version posted publicly and reported to the transparency program each time it is updated.

Conclusion

OVMEB is entering a transformative period, shifting from legacy systems toward modern, secure, and accessible technology that strengthens its regulatory mission. This plan provides a comprehensive, EIS-aligned roadmap that will guide modernization, cybersecurity improvements, accessibility compliance, and better public service delivery through 2030.
