คู่มือปฏิบัติงาน
การจัดการคุณภาพด้านเทคโนโลยีดิจิทัล
(Digital Quality Management System Manual)

รหัสเอกสาร	อสป.-IT-QM-01	**ฉบับแก้ไข**	Rev. 1
ชื่อเอกสาร	คู่มือปฏิบัติงานการจัดการคุณภาพด้านเทคโนโลยีดิจิทัล	**สถานะ**	ฉบับควบคุม
เจ้าของเอกสาร	สำนักงานเทคโนโลยีสารสนเทศ	**ผู้กำกับดูแล**	CIO
ผู้อนุมัติ	ผู้อำนวยการองค์การสะพานปลา	**รอบทบทวน**	อย่างน้อยปีละ ๑ ครั้ง
วันที่มีผลใช้บังคับ	กันยายน ๒๕๖๙	**วันที่ทบทวนครั้งถัดไป**	กันยายน ๒๕๗๐

คำนำ

ปัจจุบันเทคโนโลยีดิจิทัลได้เข้ามามีบทบาทสำคัญอย่างยิ่งในการขับเคลื่อนและยกระดับขีดความสามารถของการบริหารงานภาครัฐและรัฐวิสาหกิจ องค์การสะพานปลา (อสป.) ในฐานะหน่วยงานที่มีพันธกิจหลักในการส่งเสริมและพัฒนาอุตสาหกรรมประมงไทย ได้กำหนดวิสัยทัศน์ที่มุ่งมั่นจะเป็น *“องค์กรที่มีประสิทธิภาพในการให้บริการแหล่งขนถ่ายและซื้อขายสัตว์น้ำที่ถูกสุขอนามัย ตลอดจนให้บริการธุรกิจเกี่ยวเนื่องอย่างครบวงจร เพื่อส่งเสริมอุตสาหกรรมประมงไทยอย่างยั่งยืน”* ซึ่งเป้าหมายดังกล่าวจะสำเร็จผลได้ ย่อมต้องอาศัยระบบสารสนเทศและเทคโนโลยีดิจิทัลที่มีคุณภาพ เสถียรภาพ และมีความมั่นคงปลอดภัยเป็นฐานรากสำคัญ

เพื่อให้การดำเนินงานด้านเทคโนโลยีดิจิทัลขององค์การสะพานปลา ทั้งในส่วนกลางและท่าเทียบเรือประมงส่วนภูมิภาคทั้ง ๑๗ แห่ง มีความเป็นมาตรฐานเดียวกัน (Standardized Practice) สำนักงานเทคโนโลยีสารสนเทศ จึงได้จัดทำ “คู่มือปฏิบัติงานการจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Digital Quality Management System Manual)” ฉบับนี้ขึ้น โดยประยุกต์ใช้หลักการตามมาตรฐานสากล ISO 9001:2015 และแนวทางการประเมินผลการดำเนินงานรัฐวิสาหกิจ (SE-AM) ด้านการพัฒนาเทคโนโลยีดิจิทัล (DT) มาเป็นกรอบในการจัดทำ

คู่มือฉบับนี้ได้รวบรวมแนวปฏิบัติที่ครอบคลุมตั้งแต่ การวางแผน การออกแบบ การพัฒนาระบบ การควบคุมผู้ให้บริการภายนอก (Outsource) ไปจนถึงการตรวจรับและการบำรุงรักษาระบบ โดยมุ่งเน้นการสร้างกระบวนการทำงานที่สามารถทำซ้ำได้ (Repeatable Practice) ลดความผิดพลาดในการปฏิบัติงาน ตลอดจนให้ความสำคัญสูงสุดกับการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ของเกษตรกร ชาวประมง และผู้มีส่วนได้ส่วนเสียทุกภาคส่วน

สำนักงานเทคโนโลยีสารสนเทศ หวังเป็นอย่างยิ่งว่า คู่มือปฏิบัติงานฉบับนี้จะเป็นเครื่องมือสำคัญให้ผู้บริหาร เจ้าหน้าที่ และผู้ที่เกี่ยวข้อง ได้ใช้เป็นแนวทางในการปฏิบัติงาน เพื่อยกระดับคุณภาพการให้บริการด้านดิจิทัลขององค์การสะพานปลาให้เกิดความโปร่งใส ตรวจสอบได้ และได้รับการพัฒนาอย่างต่อเนื่อง นำไปสู่การเสริมสร้างศักยภาพของอุตสาหกรรมประมงไทยให้ก้าวหน้าอย่างยั่งยืนต่อไป

องค์การสะพานปลา

สารบัญ

บทนำ ๑

๑. ที่มาและความสำคัญ ๑

๒. วัตถุประสงค์ ๑

๓. ขอบเขตการบังคับใช้ ๑

๔. ฐานทางกฎหมายและมาตรฐานอ้างอิง (Legal Basis and Referenced Standards) ๒

ขอบเขตของคู่มือคุณภาพ (อ้างอิงข้อกำหนดมาตรฐาน ISO 9001:2015) ๒

คำนิยามและคำจำกัดความ ๓

โครงสร้างการกำกับดูแลและความรับผิดชอบ (Governance & Responsibilities) ๘

กระบวนการจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Quality Management Process) ๑๐

การควบคุมเอกสารและการคุ้มครองข้อมูลส่วนบุคคล (Document & Data Control) ๑๒

บทบาท ความรับผิดชอบ และอำนาจหน้าที่ในระบบบริหารคุณภาพ (Organizational Roles, Responsibilities, and Authorities) ๑๓

การควบคุมเอกสารและการคุ้มครองข้อมูลส่วนบุคคล (Document & Data Control) ๑๖

การวางแผน (Planning) ๑๘

การวางแผนการเปลี่ยนแปลง (Planning of Changes) ๒๐

การสนับสนุน (Support) ๒๐

การปฏิบัติงาน (Operation) ๒๒

การประเมินสมรรถนะและการปรับปรุง (Performance Evaluation & Improvement) ๒๔

บทนำ

๑. ที่มาและความสำคัญ

ตามวิสัยทัศน์ขององค์การสะพานปลา (อสป.) ที่มุ่งมั่นเป็น “องค์กรที่มีประสิทธิภาพในการให้บริการแหล่งขนถ่ายและซื้อขายสัตว์น้ำที่ถูกสุขอนามัย ตลอดจนให้บริการธุรกิจเกี่ยวเนื่องอย่างครบวงจร เพื่อส่งเสริมอุตสาหกรรมประมงไทยอย่างยั่งยืน” ประกอบกับพันธกิจในการยกระดับการบริหารองค์กรด้วยนวัตกรรมและเทคโนโลยีดิจิทัล อย่างไรก็ตาม จากผลการประเมิน SE-AM พบว่า อสป. ยังมีความจำเป็นต้องพัฒนากระบวนการจัดการคุณภาพด้านเทคโนโลยีดิจิทัลให้มีความสมบูรณ์และเป็นมาตรฐาน

เพื่อปิดช่องว่างดังกล่าว และยกระดับขีดความสามารถด้านเทคโนโลยีสารสนเทศให้รองรับการให้บริการแก่เกษตรกร ชาวประมง และผู้ประกอบการได้อย่างรวดเร็วและปลอดภัย สำนักงานเทคโนโลยีสารสนเทศ จึงได้จัดทำ “คู่มือปฏิบัติงานการจัดการคุณภาพด้านเทคโนโลยีดิจิทัล” ขึ้น เพื่อใช้เป็นกรอบแนวทางปฏิบัติที่เป็นมาตรฐาน (Standardized Practice) และสร้างกระบวนการทำงานที่สามารถทำซ้ำได้ (Repeatable Practice) โดยมุ่งเน้นการควบคุมคุณภาพระบบงานควบคู่ไปกับการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

๒. วัตถุประสงค์

๒.๑ เพื่อใช้เป็นคู่มือมาตรฐาน (Standard Operating Procedure SOP) สำหรับบุคลากรในสำนักงานเทคโนโลยีสารสนเทศ ในการบริหารจัดการคุณภาพโครงการและบริการดิจิทัลให้มีมาตรฐานเดียวกัน

๒.๒ เพื่อสร้างระบบการทำงานที่สามารถ “ทำซ้ำได้ (Repeatable)” ลดความผิดพลาดจากตัวบุคคล (Human Error) และเพิ่มประสิทธิภาพในการให้บริการ

๒.๓ เพื่อยกระดับผลการประเมิน SE-AM ด้านที่ ๕ (DT) หัวข้อ ๒.๓ การจัดการด้านคุณภาพ (Quality Management) ให้บรรลุเป้าหมายในระดับที่ ๓

๒.๔ เพื่อเป็นกรอบในการบริหารจัดการข้อมูลส่วนบุคคลของชาวประมงและผู้ใช้บริการให้สอดคล้องกับหลักการลดทอนข้อมูล (Data Minimization) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓. ขอบเขตการบังคับใช้

คู่มือฉบับนี้มีผลบังคับใช้กับบุคลากรของสำนักงานเทคโนโลยีสารสนเทศ และผู้ที่เกี่ยวข้องกับการดำเนินการด้านเทคโนโลยีดิจิทัลขององค์การสะพานปลา ทั้งในส่วนกลางและท่าเทียบเรือประมงส่วนภูมิภาคทั้ง ๑๗ แห่ง โดยครอบคลุมกระบวนการพัฒนาระบบ การจัดหาซอฟต์แวร์/ฮาร์ดแวร์ การบำรุงรักษาระบบเครือข่าย และการควบคุมคุณภาพข้อมูล

๔. ฐานทางกฎหมายและมาตรฐานอ้างอิง (Legal Basis and Referenced Standards)

คู่มือฉบับนี้จัดทำขึ้นโดยอาศัยอำนาจและอ้างอิงมาตรฐาน ดังนี้

๑) ฐานอำนาจการบริหารจัดการ อาศัยอำนาจของผู้อำนวยการองค์การสะพานปลา ตามมาตรา ๒๑ และ มาตรา ๒๒ แห่งพระราชบัญญัติจัดระเบียบกิจการแพปลา พ.ศ. ๒๔๙๖ (และที่แก้ไขเพิ่มเติม) ในการวางระเบียบปฏิบัติงานเพื่อควบคุมคุณภาพการดำเนินงานภายในองค์กร

๒) มาตรฐานคุณภาพดิจิทัล ประยุกต์ใช้แนวทางตามมาตรฐานสากล ISO 9001:2015 (ระบบบริหารงานคุณภาพ) และ ISO/IEC 25010 (คุณภาพของระบบและซอฟต์แวร์)

๓) การคุ้มครองข้อมูลส่วนบุคคล (PDPA) การประมวลผลข้อมูลส่วนบุคคลต้องระบุวัตถุประสงค์ ฐานการประมวลผล และผู้รับผิดชอบให้ชัดเจน เก็บรวบรวมเท่าที่จำเป็น กำหนดระยะเวลาเก็บรักษาเป็นรายประเภทข้อมูล ตามกฎหมาย ภารกิจ สัญญา และตารางระยะเวลาการเก็บรักษาข้อมูลขององค์การสะพานปลา พร้อมกำหนดวิธีลบ ทำลาย หรือทำให้เป็นข้อมูลนิรนามอย่างปลอดภัยเมื่อสิ้นความจำเป็น และจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ก่อนเริ่มโครงการหรือการเปลี่ยนแปลงที่มีความเสี่ยงสูง

ขอบเขตของคู่มือคุณภาพ (อ้างอิงข้อกำหนดมาตรฐาน **ISO 9001:2015)**

คู่มือคุณภาพฉบับนี้ จัดทำขึ้นเพื่อระบุข้อกำหนดสำหรับระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัลของ องค์การสะพานปลา เพื่อแสดงถึงขีดความสามารถในการให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสารที่สนับสนุนภารกิจหลักขององค์กร ทั้งในส่วนกลางและส่วนภูมิภาค (ท่าเทียบเรือประมงและศูนย์ขนถ่ายสัตว์น้ำ)

ขอบเขตของคู่มือนี้ครอบคลุมกระบวนการบริหารจัดการวงจรชีวิตของระบบดิจิทัล (Digital Lifecycle Management) ตั้งแต่การวางแผน การจัดหา การพัฒนา การรักษาความมั่นคงปลอดภัย ไปจนถึงการให้บริการระบบข้อมูลที่ส่งเสริมอุตสาหกรรมประมงสำหรับเกษตรกร ชาวประมง ผู้ประกอบการ และประชาชนทั่วไป โดยมุ่งเน้นกระบวนการดังต่อไปนี้

๑) การควบคุมกระบวนการ (Process Control) กำหนดแนวทางปฏิบัติที่เป็นมาตรฐาน (Standardized Practice) ในการดำเนินงานด้านดิจิทัล เพื่อให้ผลลัพธ์ของงานมีความสม่ำเสมอและเป็นไปตามความต้องการของผู้ใช้บริการ

๒) การบริหารจัดการที่ทำซ้ำได้ (Repeatable Practice) สร้างกลไกที่ทำให้ขั้นตอนการทำงานด้านคุณภาพสามารถดำเนินซ้ำได้อย่างเป็นระบบในทุกโครงการ ลดความแปรปรวนของมาตรฐานงานดิจิทัล

๓) การติดตามและวัดประสิทธิผล (Monitoring and Measurement) กำหนดตัวชี้วัดคุณภาพ (Quality Metrics) ที่ชัดเจน เพื่อประเมินประสิทธิภาพของระบบสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ให้เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง

๔) การปรับปรุงอย่างต่อเนื่อง (Continual Improvement) มุ่งเน้นการวิเคราะห์ผลการดำเนินงานและข้อผิดพลาดเพื่อนำมาพัฒนาคุณภาพการบริการดิจิทัลอย่างสม่ำเสมอ สอดคล้องกับเกณฑ์การประเมินผลรัฐวิสาหกิจ SE-AM และมาตรฐานสากล ISO 9001:2015

คำนิยามและคำจำกัดความ

๑) คุณภาพ (Quality) ระดับของลักษณะที่แสดงออกของบริการดิจิทัล ระบบสารสนเทศ และข้อมูล ที่สามารถตอบสนองต่อความต้องการหรือความคาดหวังของชาวประมง เกษตรกร และผู้มีส่วนได้ส่วนเสียขององค์การสะพานปลาได้อย่างครบถ้วน

๒) ระบบบริหารคุณภาพ (Quality Management System - QMS) ส่วนของระบบการบริหารจัดการขององค์การสะพานปลาที่มุ่งเน้นในเรื่องของคุณภาพด้านเทคโนโลยีดิจิทัล เพื่อให้บรรลุวัตถุประสงค์ตามเกณฑ์ SE-AM และมาตรฐานสากล

๓) แนวปฏิบัติที่เป็นมาตรฐาน (Standardized Practice) กระบวนการทำงานด้านดิจิทัลที่ได้รับการกำหนดขั้นตอนไว้อย่างชัดเจน เป็นลายลักษณ์อักษร และบุคลากรทุกคนใน สำนักงานเทคโนโลยีสารสนเทศ ถือปฏิบัติในแนวทางเดียวกันเพื่อความเป็นเอกภาพขององค์กร

๔) กระบวนการที่ทำซ้ำได้ (Repeatable Practice) กิจกรรมหรือขั้นตอนการทำงานด้านคุณภาพที่สามารถดำเนินการซ้ำได้ในทุกโครงการหรือทุกช่วงเวลา โดยยังคงให้ผลลัพธ์และมาตรฐานคุณภาพในระดับเดียวกัน ลดความแปรปรวนที่เกิดจากตัวบุคคล

๕) ข้อมูลส่วนบุคคล (Personal Data) ข้อมูลเกี่ยวกับชาวประมง เกษตรกร คู่ค้า หรือบุคลากร ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางตรง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)

๖) การตรวจสอบด้านดิจิทัล (Digital Audit) กระบวนการตรวจสอบและประเมินระบบสารสนเทศโดยผู้มีความรู้ความเชี่ยวชาญ เพื่อยืนยันว่าการดำเนินงานเป็นไปตามนโยบาย มาตรฐานคุณภาพและความปลอดภัยที่องค์การสะพานปลากำหนด

บริบทองค์กร (Context of the Organization)

เพื่อให้ระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Digital QMS) สามารถตอบสนองต่อภารกิจหลักขององค์การสะพานปลาได้อย่างแท้จริง สำนักงานเทคโนโลยีสารสนเทศได้ดำเนินการวิเคราะห์และระบุกลุ่มผู้มีส่วนได้ส่วนเสีย (Stakeholders) ทั้งภายในและภายนอก พร้อมทั้งกำหนดความต้องการและความคาดหวังที่ต้องนำมาแปลงเป็น “แนวปฏิบัติที่เป็นมาตรฐาน (Standardized Practice)” ดังนี้

๑. แนะนำองค์กร และบริบทขององค์กร

เพื่อให้การจัดการคุณภาพด้านเทคโนโลยีดิจิทัลสอดคล้องกับทิศทางยุทธศาสตร์ขององค์การสะพานปลา สำนักงานเทคโนโลยีสารสนเทศจึงดำเนินการวิเคราะห์บริบทที่เกี่ยวข้อง ดังนี้

๑) การเข้าใจองค์กรและบริบทขององค์กร (Understanding the Organization and its Context) สำนักงานเทคโนโลยีสารสนเทศดำเนินการวิเคราะห์ปัจจัยภายในและภายนอก (Internal and External Issues) ที่ส่งผลกระทบต่อความสามารถในการบรรลุผลลัพธ์ของระบบบริหารคุณภาพด้านดิจิทัล ดังนี้

- ปัจจัยภายนอก การเปลี่ยนแปลงทางเทคโนโลยี (Digital Transformation), กฎหมายและระเบียบข้อบังคับใหม่ (เช่น PDPA และ พ.ร.บ. ไซเบอร์), ความคาดหวังของชาวประมงและผู้ประกอบการต่อการบริการแบบออนไลน์ และนโยบายรัฐวิสาหกิจดิจิทัลของ สคร.

• ปัจจัยภายใน โครงสร้างการบริหารจัดการภายในสำนักงานฯ, ทักษะและความพร้อมด้านดิจิทัลของบุคลากร (Digital Literacy), ทรัพยากรด้านงบประมาณ และระบบสารสนเทศพื้นฐานที่มีอยู่เดิม

๒. ผู้มีส่วนได้ส่วนเสียและความคาดหวังด้านคุณภาพดิจิทัล (Interested Parties and Expectations)

๑) ผู้มีส่วนได้ส่วนเสียภายนอก (External Stakeholders)

กลุ่มผู้มีส่วนได้ส่วนเสีย	ความคาดหวังด้านคุณภาพเทคโนโลยีดิจิทัล (Quality Expectations)	การคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance)
๑. เกษตรกร ชาวประมง และผู้ประกอบการแพปลา	- ระบบบริการออนไลน์ (เช่น ข้อมูลราคาสัตว์น้ำ) ที่เข้าถึงง่าย เสถียร และใช้งานได้ตลอด ๒๔ ชั่วโมง - ความโปร่งใสและถูกต้องแม่นยำของข้อมูลธุรกรรม	- สิทธิของเจ้าของข้อมูล (Data Subject Rights) มั่นใจได้ว่าข้อมูลส่วนบุคคล (เช่น เลขบัตรประชาชน บัญชีธนาคาร) จะถูกเก็บรักษาอย่างปลอดภัย ไม่ถูกนำไปใช้นอกเหนือจาก ฐานสัญญา หรือ ฐานภารกิจของรัฐ
๒. หน่วยงานกำกับดูแล *(กระทรวงเกษตรฯ, สคร., สกมช.)*	- การดำเนินงานที่สอดคล้องกับนโยบายรัฐบาลดิจิทัล - การปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ (พ.ร.บ. ไซเบอร์ฯ) และผ่านเกณฑ์ประเมิน SE-AM	- มีกระบวนการจัดเก็บ Log File ตามที่กฎหมายกำหนด เพื่อใช้ตรวจสอบเมื่อเกิดเหตุละเมิด
๓. ประชาชนทั่วไป และคู่ค้า	- การเข้าถึงข้อมูลข่าวสารองค์กรและบริการผ่านเว็บไซต์ที่ถูกต้อง ทันสมัย และมีความน่าเชื่อถือ	- มีนโยบายความเป็นส่วนตัว (Privacy Notice) แจ้งให้ทราบอย่างชัดเจนก่อนการเก็บข้อมูล

๒) ผู้มีส่วนได้ส่วนเสียภายใน (Internal Stakeholders)

กลุ่มผู้มีส่วนได้ส่วนเสีย	ความคาดหวังด้านคุณภาพเทคโนโลยีดิจิทัล (Quality Expectations)	การตอบโจทย์เกณฑ์ SE-AM
๑. ผู้อำนวยการและผู้บริหาร อสป.	- ระบบรายงานผล (Dashboard) ที่แสดงข้อมูลเชิงลึก (Data Analytics) ที่ถูกต้องและเป็นปัจจุบัน (Real-time) เพื่อช่วยในการตัดสินใจบริหารงาน	- มั่นใจได้ว่าการลงทุนด้านเทคโนโลยีดิจิทัลมีความคุ้มค่า และมีการควบคุมคุณภาพอย่างเป็นระบบ

กลุ่มผู้มีส่วนได้ส่วนเสีย	ความคาดหวังด้านคุณภาพเทคโนโลยีดิจิทัล (Quality Expectations)	การตอบโจทย์เกณฑ์ SE-AM
๒. พนักงานท่าเทียบเรือประมง (๑๗ แห่ง)	- โครงสร้างพื้นฐานและเครือข่ายอินเทอร์เน็ตที่พร้อมใช้งาน (High Availability) และระบบที่ช่วยลดขั้นตอนการใช้กระดาษ (Paperless)	- มี กระบวนการที่ทำซ้ำได้ (Repeatable Practice) เช่น คู่มือแจ้งซ่อมหรือขอความช่วยเหลือ (Helpdesk) ที่ชัดเจนและแก้ปัญหาได้รวดเร็ว
๓. เจ้าหน้าที่สำนักงานเทคโนโลยีสารสนเทศ	- มีคู่มือปฏิบัติงาน (SOP) และแบบฟอร์ม (Checklist) ที่ชัดเจน เพื่อใช้เป็นเกราะป้องกันความผิดพลาดในการปฏิบัติงานรายวัน	- มีมาตรฐานการทำงานที่ชัดเจน (Standardized Practice) ไม่ต้องคาดเดาวิธีการทำงานด้วยตนเอง

๓ ขอบเขตของระบบบริหารคุณภาพ (Scope of the Quality Management System) (อ้างอิงข้อกำหนด ISO 9001:2015)

ระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัลนี้ จัดทำขึ้นเพื่อใช้ควบคุมมาตรฐานการปฏิบัติงานของ สำนักงานเทคโนโลยีสารสนเทศ องค์การสะพานปลา โดยคำนึงถึงปัจจัยภายในและภายนอก ตลอดจนความคาดหวังของผู้มีส่วนได้ส่วนเสีย (เช่น เกษตรกร ชาวประมง ผู้ประกอบการ และบุคลากรภายใน)

การนำข้อกำหนด ISO 9001:2015 มาประยุกต์ใช้นี้ มีเป้าหมายเพื่อสร้าง “แนวปฏิบัติที่เป็นมาตรฐาน (Standardized Practice)” และ “กระบวนการที่ทำซ้ำได้ (Repeatable Practice)” โดยจัดทำเป็นเอกสารสารสนเทศ (Documented Information) ที่มีการทบทวนและปรับปรุงอย่างต่อเนื่อง เพื่อยกระดับคุณภาพการให้บริการดิจิทัลของ อสป. ทั้งในส่วนกลางและท่าเทียบเรือประมงส่วนภูมิภาค ซึ่งครอบคลุมขอบเขตการให้บริการ ๒ ส่วนหลัก ดังนี้

๑. การบริการระบบสารสนเทศ (Digital Information Systems Services) มุ่งเน้นการควบคุมคุณภาพการพัฒนาระบบ การประมวลผลข้อมูล และความถูกต้องแม่นยำของระบบงานหลัก ได้แก่

- บริการเว็บไซต์และแพลตฟอร์มออนไลน์ การเผยแพร่ข้อมูลข่าวสารและราคาสัตว์น้ำขององค์การสะพานปลา
- บริการระบบฐานข้อมูลชาวประมงและผู้ประกอบการ ระบบสารสนเทศที่เกี่ยวข้องกับการลงทะเบียนและการทำธุรกรรม ซึ่งต้องควบคุมคุณภาพการจัดเก็บข้อมูลให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)
- บริการระบบสารบรรณอิเล็กทรอนิกส์ (E-Document) สนับสนุนการทำงานแบบไร้กระดาษภายในองค์กร
- บริการระบบบริหารจัดการทรัพยากรองค์กร (ERP) ระบบบัญชี ธุรกิจ และการจัดเก็บรายได้ขององค์กร

• บริการระบบจดหมายอิเล็กทรอนิกส์ (E-mail) การสื่อสารข้อมูลภายในและภายนอกอย่างเป็นทางการ

๒. การบริการสนับสนุนด้านเทคโนโลยีสารสนเทศ (IT Support and Infrastructure Services) มุ่งเน้นการควบคุมคุณภาพการให้บริการที่รวดเร็ว (SLA) และความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน (ISMS) ได้แก่

• บริการบริหารจัดการบัญชีผู้ใช้งาน (User Account Management) การควบคุมสิทธิ์การเข้าถึงระบบตามความจำเป็น (Principle of Least Privilege)

• บริการเครือข่ายสารสนเทศและความปลอดภัย (Network & Security) การดูแลระบบเครือข่ายอินเทอร์เน็ต ทั้งในส่วนกลางและท่าเทียบเรือประมงให้พร้อมใช้งาน (Availability)

• บริการซ่อมบำรุงและแก้ไขปัญหา (IT Helpdesk & Maintenance) การจัดการเหตุการณ์ขัดข้อง การซ่อมบำรุงคอมพิวเตอร์ และอุปกรณ์ต่อพ่วง

• บริการยืม-คืน ครุภัณฑ์คอมพิวเตอร์ การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

• บริการระบบโทรศัพท์และสื่อสารภายใน (IP Phone & Collaboration) สนับสนุนการประสานงานระหว่างสำนักงาน

๔. ระบบการจัดการคุณภาพและกระบวนการ (Quality Management System and its Processes)

สำนักงานเทคโนโลยีสารสนเทศ องค์การสะพานปลา ได้จัดทำ นำไปปฏิบัติ ธำรงรักษาและปรับปรุงระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัลอย่างต่อเนื่อง รวมถึงกำหนดกระบวนการที่จำเป็นและปฏิสัมพันธ์ของกระบวนการตามข้อกำหนดของมาตรฐาน ISO 9001:2015 และ ISO/IEC 25010 โดยประยุกต์ใช้ในทุกส่วนงานที่เกี่ยวข้อง เพื่อให้เกิด “แนวปฏิบัติที่เป็นมาตรฐาน (Standardized Practice)” และสามารถ “ทำซ้ำได้ (Repeatable Practice)” ซึ่งประกอบด้วยการพิจารณาและประเมินด้านต่าง ๆ ดังนี้

๑) ความต้องการและผลที่คาดหวังจากกระบวนการต่างๆ ระบุปัจจัยนำเข้า (Inputs) และผลลัพธ์ที่คาดหวัง (Expected Outputs) จากบริการดิจิทัล เช่น ความถูกต้องของข้อมูลชาวประมง ความปลอดภัยของระบบ และความเสถียรของเครือข่ายสารสนเทศ

๒) ลำดับขั้นและปฏิสัมพันธ์ของกระบวนการต่างๆ จัดลำดับขั้นตอนการทำงาน (Workflow) อย่างเป็นระบบ เพื่อให้กระบวนการพัฒนาและให้บริการระบบสามารถดำเนินงานซ้ำได้ด้วยมาตรฐานเดียวกันในทุกท่าเทียบเรือ

๓) ประยุกต์ใช้ เกณฑ์ วิธีการ การติดตาม การวัด และตัวชี้วัดสมรรถนะของกระบวนการกำหนดตัวชี้วัดคุณภาพ (Quality Metrics/KPIs) เช่น อัตราความพร้อมใช้งานของระบบ (System Availability) และความรวดเร็วในการแก้ไขปัญหา (Response Time SLA)

๔) ทรัพยากรที่จำเป็น และทำให้มั่นใจว่ามีอยู่พร้อมและเพียงพอ บริหารจัดการโครงสร้างพื้นฐานด้านดิจิทัล เครื่องแม่ข่าย อุปกรณ์ความปลอดภัย และบุคลากร ให้พร้อมรองรับการปฏิบัติงานอย่างมีประสิทธิภาพ

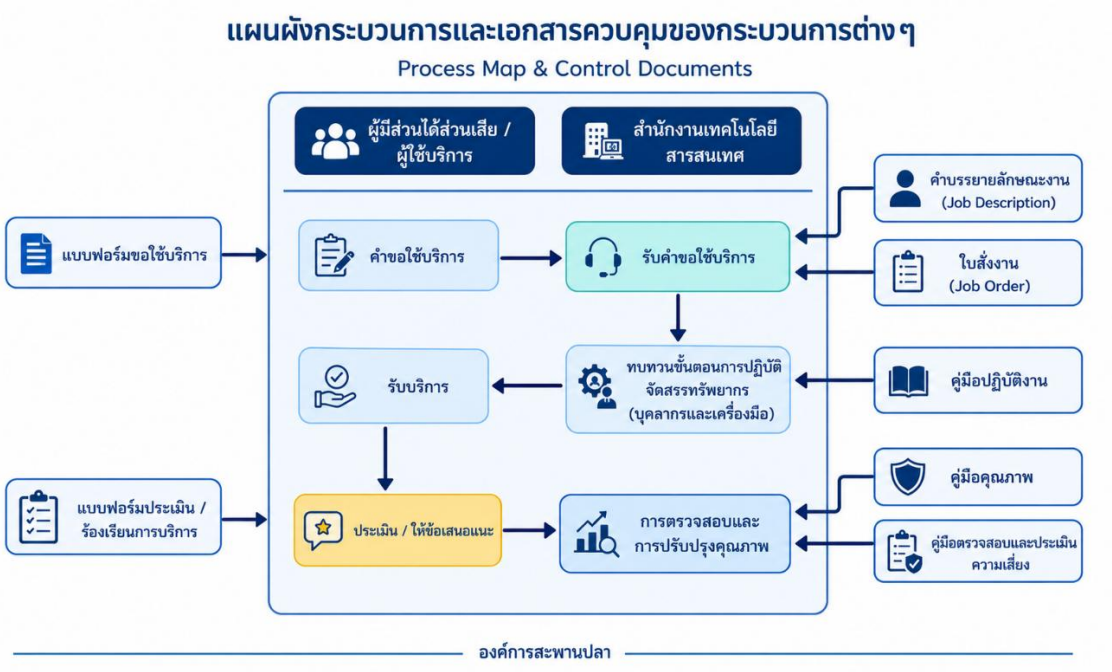
๕) การมอบหมายความรับผิดชอบและอำนาจหน้าที่ สำหรับกระบวนการต่าง ๆ กำหนดบทบาทและอำนาจการตัดสินใจ (Roles & Responsibilities) ของเจ้าหน้าที่สำนักงานเทคโนโลยีสารสนเทศในแต่ละขั้นตอนอย่างชัดเจน

๖) จัดการความเสี่ยงและโอกาสที่เกี่ยวข้อง ประเมินและจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Risks) โดยเฉพาะความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ และควบคุมการเข้าถึงข้อมูลส่วนบุคคลตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)

๗) ประเมินกระบวนการและการนำการเปลี่ยนแปลงไปปฏิบัติ ติดตามประเมินกระบวนการ และนำการบริหารการเปลี่ยนแปลง (Change Management) ไปปฏิบัติตามความจำเป็น เพื่อให้มั่นใจว่ากระบวนการปรับปรุงระบบจะไม่ส่งผลกระทบเชิงลบต่อการให้บริการ

๘) ปรับปรุงกระบวนการและระบบการบริหารคุณภาพและธำรงรักษาเอกสาร ปรับปรุงระบบอย่างต่อเนื่อง และธำรงรักษา “เอกสารสารสนเทศ (Documented Information)” เช่น คู่มือปฏิบัติงาน (SOP) บันทึกการตรวจสอบ (Log) และรายการตรวจสอบ (Checklist) เพื่อสนับสนุนการปฏิบัติการ และให้มั่นใจว่ากระบวนการได้ถูกนำไปปฏิบัติตามแผนอย่างแท้จริง

แผนผังกระบวนการและเอกสารควบคุมของกระบวนการต่าง ๆ (Process Map & Control Documents) สำนักงานเทคโนโลยีสารสนเทศ ได้จัดทำแผนผังกระบวนการหลัก (Process Flowchart) พร้อมทั้งกำหนดแบบฟอร์มมาตรฐาน (Standard Templates) และรายการตรวจสอบ (Checklists) เพื่อใช้เป็นเครื่องมือควบคุมให้ทุกกระบวนการสามารถทำซ้ำได้และสอดคล้องกับมาตรฐานที่องค์การสะพานปลากำหนด



โครงสร้างการกำกับดูแลและความรับผิดชอบ (Governance & Responsibilities)

สายการกำกับดูแลขององค์การสะพานปลาให้ถือปฏิบัติตามลำดับดังต่อไปนี้

๑. คณะกรรมการองค์การสะพานปลา กำกับทิศทางและนโยบายภาพรวม ติดตามผลการบริหารความเสี่ยงและผลสัมฤทธิ์ด้านเทคโนโลยีดิจิทัล ตลอดจนให้ข้อเสนอแนะต่อฝ่ายบริหารตามอำนาจหน้าที่

๒. ผู้อำนวยการองค์การสะพานปลา อนุมัติและประกาศใช้คู่มือ จัดสรรทรัพยากร กำกับให้หน่วยงานที่เกี่ยวข้องถือปฏิบัติ และทบทวนผลการดำเนินงานของระบบบริหารคุณภาพ

๓. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) - รองผู้อำนวยการองค์การสะพานปลาด้านบริหาร เป็นเจ้าภาพกำกับระบบบริหารคุณภาพด้านเทคโนโลยีดิจิทัล กลั่นกรองแผนและรายงาน ติดตามความเสี่ยง ตัวชี้วัด และประเด็นที่ต้องยกระดับเสนอผู้อำนวยการองค์การสะพานปลา

๔. หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ เป็นเจ้าของกระบวนการและผู้ควบคุมเอกสาร จัดทำแผนคุณภาพ ควบคุมการปฏิบัติตามมาตรฐาน รายงานผล และประสานหน่วยงานเจ้าของระบบกับผู้ให้บริการภายนอก

หลักการแบ่งแยกหน้าที่ ผู้จัดทำ ผู้ทบทวน ผู้ทดสอบ และผู้อนุมัติควรเป็นคนละบทบาทเท่าที่ทำได้ กรณีพบข้อบกพร่องระดับวิกฤต ช่องโหว่ระดับ High/Critical เหตุละเมิดข้อมูลส่วนบุคคล หรือความเสี่ยงที่ยอมรับไม่ได้ ให้ระงับการนำระบบขึ้นใช้งานจริง บันทึกเหตุผลและหลักฐาน และรายงานหัวหน้าสำนักงานเทคโนโลยีสารสนเทศกับ CIO ทันที

เพื่อให้ระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Digital Quality Management System Digital QMS) ขององค์การสะพานปลา มีการกำกับดูแลอย่างเป็นระบบ สามารถนำไปปฏิบัติเป็นมาตรฐานเดียวกัน (Standardized Practice) และขับเคลื่อนได้อย่างต่อเนื่องแม้ในสภาวะที่อยู่ระหว่างการแต่งตั้งคณะกรรมการองค์การสะพานปลา จึงกำหนดโครงสร้างการกำกับดูแลและบทบาทความรับผิดชอบไว้ดังต่อไปนี้

๑. บทบาทของผู้อำนวยการองค์การสะพานปลา (ผออ.)

ในฐานะผู้บริหารสูงสุดขององค์กรและผู้ใช้อำนาจตามมาตรา ๒๑ และ ๒๒ แห่งพระราชบัญญัติจัดระเบียบกิจการแพปลา พ.ศ. ๒๔๙๖ มีบทบาทหน้าที่ในการกำกับดูแลภาพรวม (Governance) ดังนี้

๑) การอนุมัติและบังคับใช้ พิจารณาอนุมัตินโยบาย คู่มือปฏิบัติงาน (SOP) และมาตรฐานการจัดการคุณภาพด้านเทคโนโลยีดิจิทัล เพื่อให้มีผลบังคับใช้เป็นมาตรฐานเดียวกันทั่วทั้งองค์กร

๒) การกำกับดูแลเชิงนโยบาย กำกับดูแลให้การพัฒนาระบบเทคโนโลยีดิจิทัลสอดคล้องกับแผนวิสาหกิจของ อสป. และตอบสนองต่อความต้องการของชาวประมงและผู้มีส่วนได้ส่วนเสีย

๓) การสนับสนุนทรัพยากร พิจารณาจัดสรรงบประมาณ บุคลากร และโครงสร้างพื้นฐานที่จำเป็นต่อการรักษาระบบบริหารคุณภาพและการรักษาความมั่นคงปลอดภัยสารสนเทศ

๔) การบริหารความเสี่ยงระดับองค์กร เป็นผู้ตัดสินใจสูงสุดในกรณีที่เกิดเหตุการณ์ละเมิดความมั่นคงปลอดภัยทางไซเบอร์ หรือการรั่วไหลของข้อมูลส่วนบุคคล (Data Breach) ที่ส่งผลกระทบต่อภาพลักษณ์และข้อกฎหมาย

๕) การติดตามประเมินผล รับทราบและพิจารณารายงานผลการตรวจสอบคุณภาพดิจิทัล (Digital Audit) ประจำปี จากสำนักงานเทคโนโลยีสารสนเทศ เพื่อสั่งการให้เกิดการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement)

๒. บทบาทของหัวหน้าสำนักงานเทคโนโลยีสารสนเทศ

ในฐานะเจ้าของกระบวนการ (Process Owner) และผู้บริหารจัดการระดับส่วนงาน มีหน้าที่นำนโยบายไปสู่การปฏิบัติให้เกิดเป็นกระบวนการที่ทำซ้ำได้ (Repeatable Practice) ดังนี้:

๑. การบริหารจัดการกระบวนการ ควบคุม กำกับ และผลักดันให้เจ้าหน้าที่ในสำนักงานฯ ปฏิบัติตามคู่มือ SOP และใช้แบบฟอร์มมาตรฐาน (เช่น แบบฟอร์ม QMP และ Checklist) อย่างเคร่งครัดในทุกโครงการ

๒. การพิจารณาอนุมัติระดับโครงการ เป็นผู้อนุมัติ “แผนการจัดการคุณภาพโครงการดิจิทัล (QMP)” รวมถึงพิจารณาอนุมัติให้ระบบงานขึ้นใช้งานจริง (Go-Live Approval) หลังจากผ่านการทดสอบตามเกณฑ์

๓. การกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance) ตรวจสอบให้มั่นใจว่าทุกโครงการดิจิทัลมีการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA) มีการจำกัดการเก็บข้อมูล (Data Minimization) และมีกระบวนการลบ ทำลาย หรือทำให้เป็นข้อมูลนิรนามเมื่อครบกำหนดตามตารางระยะเวลาการเก็บรักษาข้อมูลขององค์การสะพานปลา

๔. การประเมินและสอบทาน (Quality Assurance) จัดให้มีการตรวจสอบคุณภาพภายใน (Internal QA) และการทบทวนกระบวนการทำงาน (Process Review) อย่างน้อยปีละ ๑ ครั้ง

๕. การรายงานผล สรุปผลการดำเนินงานด้านคุณภาพ ตัวชี้วัด (KPIs) และผลการประเมินความเสี่ยง นำเสนอต่อผู้อำนวยการองค์การสะพานปลา หรือที่ประชุมผู้บริหาร (Executive Committee) เป็นประจำ

๓. บทบาทของเจ้าหน้าที่สำนักงานเทคโนโลยีสารสนเทศ (ผู้ปฏิบัติงาน)

ในฐานะผู้ปฏิบัติงานหลัก (Practitioners) มีหน้าที่ดำเนินการตรวจสอบ ทดสอบ และควบคุมคุณภาพในระดับปฏิบัติการ (Quality Control QC) ดังนี้

๑. การจัดทำแผนคุณภาพ รับผิดชอบในการร่าง “แผนการจัดการคุณภาพโครงการดิจิทัล (QMP)” สำหรับโครงการที่ได้รับมอบหมาย พร้อมระบุเกณฑ์การยอมรับ (Acceptance Criteria) ให้ชัดเจนก่อนเริ่มงาน

๒. การปฏิบัติตามมาตรฐาน (Standardized Execution) ดำเนินการพัฒนาระบบ ตรวจรับงาน และบำรุงรักษาระบบตามขั้นตอนที่ระบุในคู่มือ SOP โดยไม่ข้ามขั้นตอน

๓. การทดสอบและประเมินผล (QC & Testing) ใช้ “แบบฟอร์มรายการตรวจสอบคุณภาพมาตรฐาน (Quality Checklist)” ในการตรวจรับงาน การทดสอบระบบ (SIT/UAT) และการประเมินช่องโหว่ด้านความปลอดภัย ก่อนนำระบบขึ้นใช้งาน

๔. การจัดเก็บหลักฐานการทำงาน (Evidence Retention) รวบรวมและจัดเก็บเอกสาร Checklist, บันทึก Log การทำงาน, และผลการทดสอบต่างๆ เข้าสู่ระบบจัดเก็บส่วนกลาง เพื่อใช้เป็นหลักฐานแสดงการ “ทำซ้ำได้ (Repeatable)” สำหรับรองรับการตรวจประเมิน SE-AM

๕. การปกป้องข้อมูลส่วนบุคคล ปฏิบัติหน้าที่โดยยึดหลักการจำกัดสิทธิ์การเข้าถึงข้อมูล (Least Privilege) ไม่นำข้อมูลของชาวประมงหรือผู้ใช้งานไปเปิดเผย และรายงานทันทีเมื่อพบความเสี่ยงหรือข้อบกพร่อง (Defect) ของระบบ

กระบวนการจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Quality Management Process)

เพื่อให้มั่นใจว่าบริการด้านเทคโนโลยีดิจิทัลและระบบสารสนเทศขององค์การสะพานปลา (อสป.) มีคุณภาพ สอดคล้องกับความต้องการของผู้ใช้งาน มีความมั่นคงปลอดภัย และเป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล สำนักงานเทคโนโลยีสารสนเทศจึงกำหนดกระบวนการจัดการคุณภาพตลอดวงจรชีวิตของการพัฒนาระบบ (Digital Lifecycle) แบ่งเป็น ๔ ขั้นตอนหลัก ดังนี้

๑. การวางแผนคุณภาพ (Quality Planning)

เป็นขั้นตอนแรกก่อนเริ่มต้นโครงการพัฒนาระบบ จัดหาซอฟต์แวร์ หรือปรับปรุงโครงสร้างพื้นฐาน เพื่อกำหนดเป้าหมาย มาตรฐาน และวิธีการทำงานเชิงรุก (Proactive Approach)

๑.๑ การจัดทำแผนคุณภาพโครงการ (Quality Management Plan - QMP)

แนวปฏิบัติ ทุกโครงการด้านดิจิทัลต้องจัดทำแผน QMP โดยใช้ แบบฟอร์ม FMO-IT-FM-QMP-001 เพื่อระบุขอบเขตงาน (Scope) ตัวชี้วัดคุณภาพ (Quality Metrics) เช่น ความเร็วในการตอบสนอง (Response Time) อัตราความพร้อมใช้งาน (Availability) และเกณฑ์การยอมรับ (Acceptance Criteria)

การอนุมัติ แผน QMP ต้องได้รับการทบทวนโดยหัวหน้ากลุ่มงาน และอนุมัติโดยหัวหน้าสำนักงานเทคโนโลยีสารสนเทศ ก่อนเริ่มดำเนินการหรือก่อนประกาศร่าง TOR (กรณีจัดจ้างหน่วยงานภายนอก)

๑.๒ การประเมินผลกระทบด้านข้อมูลส่วนบุคคล (Data Protection Impact Assessment - DPIA):

แนวปฏิบัติ หากโครงการนั้นเกี่ยวข้องกับการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลของชาวประมง ผู้ประกอบการ หรือพนักงาน อสป. ผู้จัดการโครงการต้องทำการประเมิน DPIA เพื่อวิเคราะห์ความเสี่ยงและกำหนดมาตรการคุ้มครองความเป็นส่วนตัวตั้งแต่ขั้นตอนการออกแบบ (Privacy by Design)

ข้อกำหนด PDPA ต้องกำหนดระยะเวลาจัดเก็บข้อมูล (Retention Period) และหลักการจัดเก็บเท่าที่จำเป็น (Data Minimization) ไว้ในแผนตั้งแต่ต้น

๒. การประกันคุณภาพ (Quality Assurance - QA)

เป็นกระบวนการบริหารจัดการ “วิธีการทำงาน (Process-oriented)” ระหว่างการดำเนินโครงการ เพื่อป้องกันไม่ให้เกิดข้อผิดพลาด และสร้างความมั่นใจว่าทีมงานปฏิบัติตามมาตรฐานที่วางไว้

๒.๑ การสอบทานกระบวนการทำงาน (Peer Review)

แนวปฏิบัติ กำหนดให้มีการตรวจสอบผลงานแบบข้ามสายงาน หรือตรวจสอบโดยเพื่อนร่วมงาน/หัวหน้างานในระยะต่าง ๆ ของโครงการ (เช่น การสอบทานความต้องการของระบบ, การสอบทาน Source Code, หรือการสอบทานการตั้งค่า Firewall) ก่อนส่งมอบงานไปยังขั้นตอนถัดไป

หลักฐาน (Artifact) บันทึกการสอบทาน (Review Log) หรือลายมือชื่อผู้ทบทวนในเอกสารการออกแบบระบบ

๒.๒ การตรวจสอบด้านดิจิทัล (Digital Audit)

แนวปฏิบัติ หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย จะดำเนินการสุ่มตรวจสอบ (Audit) กระบวนการทำงานของทีมงานหรือผู้รับจ้าง (Outsource) อย่างน้อยไตรมาสละ ๑ ครั้ง ว่าได้ปฏิบัติตามคู่มือ SOP และแผน QMP ที่อนุมัติไว้หรือไม่

การจัดการ หากพบข้อบกพร่องในกระบวนการ ให้ดำเนินการออกเอกสารแจ้งให้แก้ไขปรับปรุง (Corrective Action Request) ทันที

๓. การควบคุมคุณภาพ (Quality Control - QC)

เป็นกระบวนการตรวจสอบ “ผลผลิตหรือระบบงาน (Product-oriented)” ก่อนส่งมอบให้ผู้ใช้งานจริง เพื่อค้นหาและคัดกรองข้อผิดพลาด (Defects) ที่อาจหลุดรอดมาจากกระบวนการพัฒนา

๓.๑ การทดสอบระบบโดยผู้ใช้งานจริง (User Acceptance Test - UAT)

แนวปฏิบัติ ก่อนนำระบบขึ้นใช้งานจริง (Go-Live) ต้องจัดให้มีการทดสอบ UAT โดยตัวแทนผู้ใช้งานจริง (เช่น เจ้าหน้าที่ท่าเทียบเรือประมง หรือเจ้าหน้าที่จัดเก็บรายได้) โดยอิงจากกรณีทดสอบ (Test Scenario) ที่สอดคล้องกับกระบวนการปฏิบัติงานจริง

หลักฐาน (Artifact) ใบรายงานผลการทดสอบ UAT ที่มีลายมือชื่อผู้ใช้งานรับรองว่าระบบทำงานได้ถูกต้อง

๓.๒ การจำกัดสิทธิ์การเข้าถึง (Access Control Verification)

แนวปฏิบัติ ก่อนเปิดใช้งานระบบ ต้องมีการตรวจสอบสิทธิ์ของผู้ใช้งาน (Authorization) ให้เป็นไปตามหลักการ “ให้สิทธิ์เท่าที่จำเป็นต่อการปฏิบัติงาน (Least Privilege)” เพื่อป้องกันการเข้าถึงข้อมูลสำคัญขององค์กรหรือข้อมูลส่วนบุคคลโดยมิชอบ

๓.๓ การตรวจรับงานตาม Checklist มาตรฐาน

แนวปฏิบัติ ผู้ทดสอบระบบ (QC Tester) หรือคณะกรรมการตรวจรับพัสดุ ต้องใช้แบบฟอร์มรายการตรวจสอบคุณภาพมาตรฐาน (FMO-IT-FM-QC-001) ในการตรวจสอบขั้นสุดท้าย ซึ่งครอบคลุมมิติด้านฟังก์ชันการทำงาน ความมั่นคงปลอดภัย (Security Scan) และข้อกำหนด PDPA

ผลลัพธ์ ระบบจะถูกนำขึ้นใช้งานจริง (Go-Live) ได้ ก็ต่อเมื่อผ่านเกณฑ์การตรวจสอบใน Checklist ครบถ้วน หรือได้รับการอนุมัติผ่อนผันแบบมีเงื่อนไขจากหัวหน้าสำนักงานเทคโนโลยีสารสนเทศเท่านั้น

๓.๔ การจัดการข้อบกพร่อง (Defect Management)

เมื่อพบข้อบกพร่องของระบบ ไม่ว่าจะพบในระหว่างการทดสอบ (QC) หรือพบหลังจากที่ระบบเปิดใช้งานจริงแล้ว (Production) ต้องมีกระบวนการจัดการที่เป็นมาตรฐานเพื่อแก้ไขและป้องกันการเกิดซ้ำ

๑) การบันทึกและการจัดระดับความรุนแรงของปัญหา (Defect Logging & Severity):

แนวปฏิบัติ ปัญหาทั้งหมดต้องถูกบันทึกลงในทะเบียนข้อบกพร่อง (Defect Log / Helpdesk System) และประเมินระดับความรุนแรง ได้แก่

Critical ระบบล่ม ไม่สามารถใช้งานได้ หรือข้อมูลรั่วไหล (ต้องแก้ไขทันที)

High ฟังก์ชันหลักทำงานผิดพลาด ไม่มีทางเลี่ยงอื่น (Workaround)

Medium ฟังก์ชันรองผิดพลาด แต่มีทางเลี่ยงให้ทำงานต่อได้

Low ปัญหาด้านความสวยงาม (UI) หรือข้อความพิมพ์ผิด

๒) การวิเคราะห์สาเหตุและป้องกันการเกิดซ้ำ (Root Cause Analysis & Preventive Action)

แนวปฏิบัติ เมื่อแก้ไขปัญหา (Workaround/Fix) เสร็จสิ้น ทีมงานต้องร่วมกันวิเคราะห์หาสาเหตุที่แท้จริง (Root Cause) ของปัญหาที่อยู่ในระดับ Critical และ High

การปรับปรุงอย่างต่อเนื่อง (Continuous Improvement) นำผลการวิเคราะห์ไปปรับปรุงคู่มือ SOP, แผน QMP หรือ Checklist มาตรฐานให้รัดกุมยิ่งขึ้น เพื่อป้องกันไม่ให้ความผิดพลาดลักษณะเดิมเกิดขึ้นซ้ำในโครงการหรือระบบอื่น ๆ ในอนาคต

การควบคุมเอกสารและการคุ้มครองข้อมูลส่วนบุคคล (Document & Data Control)

เพื่อให้ระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Digital QMS) มีความน่าเชื่อถือ สามารถตรวจสอบย้อนหลังได้ (Traceability) และปกป้องข้อมูลสำคัญขององค์กรและผู้มีส่วนได้ส่วนเสีย สำนักงานเทคโนโลยีสารสนเทศจึงกำหนดแนวทางการควบคุม “เอกสารสารสนเทศ (Documented Information)” และ “ข้อมูลส่วนบุคคล (Personal Data)” ดังต่อไปนี้

๑. การบริหารจัดการเอกสารคุณภาพ (Quality Document Management)

อ้างอิงตามข้อกำหนด ISO 9001:2015 ข้อ 7.5 การบริหารจัดการเอกสารคุณภาพ (เช่น คู่มือปฏิบัติงาน, แผนคุณภาพโครงการ QMP, รายการตรวจสอบ Checklist, และบันทึก Log ต่าง ๆ) ต้องดำเนินตามวงจรการควบคุมดังนี้

การควบคุมการจัดทำ (Creation & Identification)

แนวปฏิบัติ การจัดทำเอกสารคุณภาพทุกประเภท ต้องใช้ “แบบฟอร์มมาตรฐาน (Standard Templates)” ของสำนักงานเทคโนโลยีสารสนเทศเท่านั้น เพื่อให้เป็นรูปแบบเดียวกันทั้งองค์กร

การระบุตัวตน (Identification) เอกสารทุกฉบับต้องมีระบบรหัสควบคุม (Document Numbering) เช่น FMO-IT-[ประเภทเอกสาร]-[ลำดับ]-[ปี พ.ศ.] พร้อมระบุวันที่บังคับใช้ (Effective Date) และหมายเลขการแก้ไข (Revision Number) อย่างชัดเจนบนหัวกระดาษ

๒. การทบทวน (Review)

แนวปฏิบัติ ก่อนนำเอกสารไปใช้งาน ต้องผ่านการทบทวนโดยหัวหน้ากลุ่มงาน หรือผู้เชี่ยวชาญ (Subject Matter Expert) เพื่อตรวจสอบความถูกต้องทางเทคนิค ความเป็นไปได้ในการปฏิบัติจริง และต้องตรวจสอบว่าเอกสาร/แบบฟอร์มนั้นไม่มีการละเมิดข้อมูลส่วนบุคคล

๓. การอนุมัติ (Approval)

แนวปฏิบัติ เอกสารระดับนโยบายและคู่มือปฏิบัติงานหลัก (SOP) ต้องนำเสนอผู้อำนวยการองค์การสะพานปลา (ผออ.) ลงนามอนุมัติ โดยอาศัยอำนาจตามมาตรา ๒๒

เอกสารระดับปฏิบัติการ (เช่น แผน QMP โครงการ หรือ แบบฟอร์ม Checklist) หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ เป็นผู้มีอำนาจลงนามอนุมัติใช้งาน

๔. การแจกจ่ายและการจัดเก็บ (Distribution & Retention)

แนวปฏิบัติ ผู้ควบคุมเอกสาร (Document Controller) ของสำนักงานฯ ต้องนำเอกสารฉบับล่าสุด (Current Version) ขึ้นระบบ OneDrive หรือ Shared Drive กลางขององค์กร และจัดทำ “ทะเบียนควบคุมเอกสาร (Master List)”

การจำกัดสิทธิ์ (Access Control) กำหนดสิทธิ์การเข้าถึงเอกสารตามระดับความลับ (Data Classification) ห้ามมิให้ผู้ไม่เกี่ยวข้องแก้ไขหรือคัดลอกเอกสาร และเมื่อมีการปรับปรุงเวอร์ชันใหม่ ต้องเรียกคืนหรือทำเครื่องหมาย “ยกเลิก (Obsolete)” ในเอกสารฉบับเก่าทันทีเพื่อป้องกันความสับสน

บทบาท ความรับผิดชอบ และอำนาจหน้าที่ในระบบบริหารคุณภาพ (Organizational Roles, Responsibilities, and Authorities)

เพื่อให้การนำระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Digital QMS) ไปปฏิบัติใช้ประสบความสำเร็จและเกิดความยั่งยืน ผู้บริหารระดับสูงขององค์การสะพานปลา ต้องแสดงออกถึงภาวะผู้นำและความมุ่งมั่น (Leadership and Commitment) อย่างเป็นรูปธรรม ดังนี้

๑. ภาวะผู้นำและความมุ่งมั่นต่อระบบบริหารคุณภาพ (Leadership and Commitment for QMS)

ผู้อำนวยการองค์การสะพานปลา (ผออ.) และ หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ แสดงความมุ่งมั่นต่อการพัฒนาระบบบริหารคุณภาพด้านดิจิทัล ผ่านการดำเนินการดังต่อไปนี้

๑) การรับผิดชอบต่อผลลัพธ์ (Accountability) แสดงความรับผิดชอบต่อความมีประสิทธิผลของระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัล เพื่อให้มั่นใจว่าบริการดิจิทัลของ อสป. สามารถสนับสนุนภารกิจหลักได้อย่างไม่หยุดชะงัก

๒) การกำหนดทิศทาง (Strategic Alignment) สร้างความมั่นใจว่านโยบายคุณภาพและวัตถุประสงค์ด้านคุณภาพได้รับการจัดทำขึ้น และสอดคล้องกับทิศทางยุทธศาสตร์ตาม แผนวิสาหกิจ อสป. พ.ศ. ๒๕๖๖ - ๒๕๗๐

๓) การบูรณาการกระบวนการ (Process Integration) ผลักดันให้เกิดการนำข้อกำหนดด้านคุณภาพ ความมั่นคงปลอดภัย (ISMS) และการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เข้าไปเป็นส่วนหนึ่งของกระบวนการทำงานปกติของสำนักงานฯ (Standardized Practice)

๔) การสนับสนุนทรัพยากร (Resource Provision) อนุมัติและจัดสรรทรัพยากรที่จำเป็นทั้งงบประมาณ บุคลากร และเครื่องมือ เพื่อให้ระบบบริหารคุณภาพสามารถดำเนินไปได้อย่างมีประสิทธิภาพ

๕) การส่งเสริมการทำซ้ำและการปรับปรุง (Promoting Repeatability & Improvement) สื่อสารให้บุคลากรตระหนักถึงความสำคัญของการทำงานตามคู่มือมาตรฐาน (SOP) อย่างเคร่งครัด เพื่อให้เกิด “กระบวนการที่ทำซ้ำได้ (Repeatable)” และส่งเสริมให้เกิดการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement)

๒. การมุ่งเน้นที่ผู้รับบริการและผู้มีส่วนได้ส่วนเสีย (Customer and Stakeholder Focus)

ผู้บริหารระดับสูงต้องแสดงภาวะผู้นำในการมุ่งเน้นที่ผู้ใช้งาน (User-Centric) เพื่อสร้างความพึงพอใจสูงสุด โดยต้องสร้างความมั่นใจในประเด็นต่อไปนี้

๑) ความเข้าใจความต้องการ มีการกำหนดและทำความเข้าใจถึงความต้องการของเกษตรกร ชาวประมง ผู้ประกอบการ และเจ้าหน้าที่ท่าเทียบเรือทั้ง ๑๗ แห่ง อย่างชัดเจนก่อนการพัฒนาระบบงานดิจิทัลใดๆ

๒) การปฏิบัติตามกฎหมาย บริการดิจิทัลทั้งหมดต้องสอดคล้องกับข้อกำหนดทางกฎหมายที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓) การจัดการความเสี่ยง มีการระบุและจัดการกับความเสี่ยงหรือโอกาสที่อาจส่งผลกระทบต่อคุณภาพของระบบสารสนเทศ เพื่อป้องกันไม่ให้เกิดผลกระทบเชิงลบต่อการขนถ่ายและซื้อขายสัตว์น้ำ

๓. นโยบายคุณภาพด้านเทคโนโลยีดิจิทัล (Digital Quality Policy)

เพื่อให้บุคลากรทุกคนมีเป้าหมายในการทำงานร่วมกัน ผู้อำนวยการองค์การสะพานปลา (อาศัยอำนาจตามมาตรา ๒๑ และ ๒๒) จึงประกาศนโยบายคุณภาพด้านเทคโนโลยีดิจิทัล ดังนี้

ประกาศนโยบายคุณภาพด้านเทคโนโลยีดิจิทัล องค์การสะพานปลา

“สำนักงานเทคโนโลยีสารสนเทศ องค์การสะพานปลา มุ่งมั่นพัฒนาระบบเทคโนโลยีดิจิทัลที่มีประสิทธิภาพ มั่นคงปลอดภัย และใช้งานง่าย เพื่อยกระดับการให้บริการแก่ชาวประมงและผู้มีส่วนได้ส่วนเสีย เราจะดำเนินงานภายใต้มาตรฐานการปฏิบัติงานที่ชัดเจน (Standardized) สามารถตรวจสอบและทำซ้ำได้

(Repeatable) พร้อมทั้งให้ความสำคัญสูงสุดในการปกป้องข้อมูลส่วนบุคคล และมุ่งมั่นปรับปรุงคุณภาพการบริการอย่างต่อเนื่อง เพื่อสนับสนุนอุตสาหกรรมประมงไทยอย่างยั่งยืน”

๔. การสื่อสารนโยบายคุณภาพ (Communicating the Quality Policy)

สำนักงานเทคโนโลยีสารสนเทศ ต้องนำนโยบายคุณภาพดังกล่าวไปดำเนินการดังนี้

๑) จัดทำเป็นเอกสารสารสนเทศ (Documented Information) เผยแพร่ในให้ภายในองค์กร และประกาศบนบอร์ดประชาสัมพันธ์ของสำนักงานฯ หรือผ่านช่องทางสื่อโซเชียลกลางที่มีภายในองค์การสะพานปลา

๒) สื่อสาร ทำความเข้าใจ และนำไปประยุกต์ใช้กับบุคลากรทุกระดับในส่วนงานเทคโนโลยีสารสนเทศ

๓) แจ้งให้ผู้มีส่วนได้ส่วนเสียภายนอก (เช่น บริษัทผู้รับจ้าง Outsource หรือที่ปรึกษาโครงการ) รับทราบและปฏิบัติตามนโยบายนี้อย่างเคร่งครัดเมื่อต้องปฏิบัติงานร่วมกับ อสป.

๕. บทบาท ความรับผิดชอบ และอำนาจหน้าที่ในระบบบริหารคุณภาพ (Organizational Roles, Responsibilities, and Authorities)

เพื่อให้ระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัลดำเนินไปอย่างมีประสิทธิภาพและทำซ้ำได้ (Repeatable) ผู้อำนวยการองค์การสะพานปลา (ผออ.) จึงได้มอบหมายอำนาจหน้าที่และความรับผิดชอบที่เกี่ยวข้องกับระบบคุณภาพ ให้แก่ หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ ทำหน้าที่เป็น ตัวแทนฝ่ายบริหารด้านคุณภาพดิจิทัล (Digital Quality Management Representative DQMR) หรือเจ้าของกระบวนการ (Process Owner) โดยมีความรับผิดชอบและอำนาจหน้าที่ที่ต้องรายงานผ่านผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ต่อผู้อำนวยการองค์การสะพานปลา ดังต่อไปนี้

๑) ความรับผิดชอบด้านการรักษาระบบ (System Conformance)

หน้าที่ ต้องทำให้มั่นใจว่ากระบวนการด้านเทคโนโลยีดิจิทัลทั้งหมดของ อสป. สอดคล้องกับข้อกำหนดของมาตรฐาน ISO 9001:2015, เกณฑ์ประเมิน SE-AM, พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์

อำนาจที่ได้รับมอบ มีอำนาจสั่งการให้เจ้าหน้าที่ในสำนักงานฯ ทุกคนใช้แบบฟอร์ม (Templates) และคู่มือปฏิบัติงาน (SOP) ที่กำหนดไว้อย่างเคร่งครัด

๒) ความรับผิดชอบด้านการส่งมอบผลลัพธ์ (Process Deliverables)

หน้าที่ ต้องทำให้มั่นใจว่ากระบวนการพัฒนาระบบและการให้บริการเครือข่าย สามารถส่งมอบผลลัพธ์ (Outputs) ได้ตามเกณฑ์การยอมรับ (Acceptance Criteria) และระดับการให้บริการ (SLA) ที่ตกลงไว้กับผู้ใช้งานและท่าเทียบเรือประมง

อำนาจที่ได้รับมอบ (Veto Power) มีอำนาจเด็ดขาดในการ “ระงับการนำระบบขึ้นใช้งานจริง (Reject Go-Live)” หากพิจารณาจาก Checklist แล้วพบว่าระบบมีช่องโหว่ด้านความปลอดภัยระดับวิกฤต (Critical) หรือละเมิดการคุ้มครองข้อมูลส่วนบุคคล โดยไม่ต้องรอการอนุมัติจาก ผออ.

๓) ความรับผิดชอบด้านการรายงานผล (Performance Reporting)

หน้าที่ รวบรวมข้อมูล สถิติข้อบกพร่อง (Defect Log) และผลการประเมินคุณภาพ (Quality Audit) เพื่อรายงานสมรรถนะของระบบบริหารคุณภาพ และเสนอแนะโอกาสในการปรับปรุง (Opportunities for Improvement)

อำนาจที่ได้รับมอบ สามารถเรียกดูข้อมูล Log การเข้าใช้งานระบบ หรือรายงานการทดสอบ (Test Report) จากผู้รับจ้าง (Outsource) และเจ้าหน้าที่ที่เกี่ยวข้องได้ทุกเมื่อ

๔) ความรับผิดชอบด้านการมุ่งเน้นผู้ใช้งาน (Promoting Customer Focus)

หน้าที่ ส่งเสริมให้เกิดความตระหนักและยึดมั่นในการตอบสนองความต้องการของ “ชาวประมง ผู้ประกอบการ และผู้ใช้งานภายใน” ทั่วทั้งสำนักงานเทคโนโลยีสารสนเทศ

อำนาจที่ได้รับมอบ สามารถเชิญผู้แทนจากท่าเทียบเรือประมงส่วนภูมิภาค หรือส่วนงานอื่นมาร่วมเป็นคณะกรรมการทดสอบระบบ (UAT) เพื่อให้การตรวจรับงานตรงกับความต้องการใช้งานจริงมากที่สุด

๕) ความรับผิดชอบด้านการจัดการความเปลี่ยนแปลง (Change Management Integrity)

หน้าที่ ต้องทำให้มั่นใจว่าความสมบูรณ์ของระบบสารสนเทศ (Data Integrity & System Availability) จะยังคงอยู่ เมื่อมีการวางแผนหรือนำการเปลี่ยนแปลงมาใช้ (เช่น การอัปเดตเซิร์ฟเวอร์ หรือการเปลี่ยนซอฟต์แวร์ใหม่)

อำนาจที่ได้รับมอบ มีอำนาจสั่งให้ดำเนินการแผนฉุกเฉินหรือแผนกู้คืนระบบ (Rollback Plan) ทันที หากการเปลี่ยนแปลงระบบส่งผลกระทบให้การทำงานของ อสป. หยุดชะงัก

การควบคุมเอกสารและการคุ้มครองข้อมูลส่วนบุคคล (Document & Data Control)

เพื่อให้ระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Digital QMS) มีความน่าเชื่อถือ สามารถตรวจสอบย้อนหลังได้ (Traceability) และปกป้องข้อมูลสำคัญขององค์กรและผู้มีส่วนได้ส่วนเสีย สำนักงานเทคโนโลยีสารสนเทศจึงกำหนดแนวทางการควบคุม “เอกสารสารสนเทศ (Documented Information)” และ “ข้อมูลส่วนบุคคล (Personal Data)” ดังต่อไปนี้

๑. การบริหารจัดการเอกสารคุณภาพ (Quality Document Management)

อ้างอิงตามข้อกำหนด ISO 9001:2015 ข้อ 7.5 การบริหารจัดการเอกสารคุณภาพ (เช่น คู่มือปฏิบัติงาน, แผนคุณภาพโครงการ QMP, รายการตรวจสอบ Checklist, และบันทึก Log ต่าง ๆ) ต้องดำเนินตามวงจรการควบคุมดังนี้

๑) การควบคุมการจัดทำ (Creation & Identification)

แนวปฏิบัติ การจัดทำเอกสารคุณภาพทุกประเภท ต้องใช้ “แบบฟอร์มมาตรฐาน (Standard Templates)” ของสำนักงานเทคโนโลยีสารสนเทศเท่านั้น เพื่อให้เป็นรูปแบบเดียวกันทั้งองค์กร

การระบุตัวตน (Identification) เอกสารทุกฉบับต้องมีระบบรหัสควบคุม (Document Numbering) เช่น FMO-IT-[ประเภทเอกสาร]-[ลำดับ]-[ปี พ.ศ.] พร้อมระบุวันที่บังคับใช้ (Effective Date) และหมายเลขการแก้ไข (Revision Number) อย่างชัดเจนบนหัวกระดาษ

๒) การทบทวน (Review)

แนวปฏิบัติ ก่อนนำเอกสารไปใช้งาน ต้องผ่านการทบทวนโดยหัวหน้ากลุ่มงาน หรือผู้เชี่ยวชาญ (Subject Matter Expert) เพื่อตรวจสอบความถูกต้องทางเทคนิค ความเป็นไปได้ในการปฏิบัติจริง และต้องตรวจสอบว่าเอกสาร/แบบฟอร์มนั้นไม่มีการละเมิดข้อมูลส่วนบุคคล

๓) การอนุมัติ (Approval)

แนวปฏิบัติ เอกสารระดับนโยบายและคู่มือปฏิบัติงานหลัก (SOP) ต้องนำเสนอผู้อำนวยการองค์การสะพานปลา (ผออ.) ลงนามอนุมัติ โดยอาศัยอำนาจตามมาตรา ๒๒ แห่ง พ.ร.บ. จัดระเบียบกิจการแพปลา พ.ศ. ๒๔๙๖

เอกสารระดับปฏิบัติการ (เช่น แผน QMP โครงการ หรือ แบบฟอร์ม Checklist) หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ เป็นผู้มีอำนาจลงนามอนุมัติใช้งาน

๔) การแจกจ่ายและการจัดเก็บ (Distribution & Retention)

แนวปฏิบัติ ผู้ควบคุมเอกสาร (Document Controller) ของสำนักงานฯ ต้องนำเอกสารฉบับล่าสุด (Current Version) ขึ้นระบบเผยแพร่ข้อมูลสำหรับผู้ปฏิบัติงาน ขององค์การสะพานปลา หรือ Shared Drive กลางขององค์กร และจัดทำ “ทะเบียนควบคุมเอกสาร (Master List)”

การจำกัดสิทธิ์ (Access Control) กำหนดสิทธิ์การเข้าถึงเอกสารตามระดับความลับ (Data Classification) ห้ามมิให้ผู้ไม่เกี่ยวข้องแก้ไขหรือคัดลอกเอกสาร และเมื่อมีการปรับปรุงเวอร์ชันใหม่ ต้องเรียกคืนหรือทำเครื่องหมาย “ยกเลิก (Obsolete)” ในเอกสารฉบับเก่าทันทีเพื่อป้องกันการนำไปใช้ผิดพลาด

๒. แนวทางการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Guidelines PDPA)

เนื่องจากระบบเทคโนโลยีดิจิทัลของ อสป. (เช่น ระบบลงทะเบียนชาวประมง, ระบบจัดการท่าเทียบเรือ) มีการประมวลผลข้อมูลส่วนบุคคล สำนักงานเทคโนโลยีสารสนเทศจึงกำหนดมาตรฐานการจัดการข้อมูลตลอดวงจรชีวิต (Data Lifecycle) เพื่อให้สอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังนี้

๑) หลักการจัดเก็บเท่าที่จำเป็น (Data Minimization)

แนวปฏิบัติ ในขั้นตอนการออกแบบระบบงาน (System Design) หรือการจัดทำแบบฟอร์มออนไลน์ ผู้จัดการโครงการต้องกำหนดให้ระบบจัดเก็บข้อมูลส่วนบุคคล “เฉพาะเท่าที่จำเป็นต่อการให้บริการเท่านั้น” * ข้อห้าม ห้ามออกแบบระบบให้บังคับกรอกข้อมูลที่ละเอียดอ่อน (Sensitive Data) เช่น ศาสนา หมู่เลือด หรือประวัติอาชญากรรม เว้นแต่จะมีกฎหมายเฉพาะของ อสป. บังคับให้ต้องจัดเก็บ และต้องมีการแสดง “นโยบายความเป็นส่วนตัว (Privacy Notice)” ให้ผู้ใช้งานรับทราบก่อนการจัดเก็บข้อมูลเสมอ

๒) การกำหนดระยะเวลาจัดเก็บข้อมูล (Retention Period)

แนวปฏิบัติ ระบบสารสนเทศและฐานข้อมูลทุกระบบของ อสป. ต้องมีการระบุวงรอบอายุของข้อมูลอย่างชัดเจน โดยอิงจากฐานทางกฎหมาย (Legal Basis) ดังนี้

• ข้อมูลการทำธุรกรรมและประวัติการซื้อขายสัตว์น้ำ จัดเก็บไว้เป็นระยะเวลา ๑๐ ปี นับจากวันสิ้นสุดการทำธุรกรรม (เพื่อให้สอดคล้องกับ พ.ร.บ. การบัญชี และกฎหมายภาษีอากร)

• ข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ระบบเครือข่ายและแอปพลิเคชันต้องจัดเก็บ Log การเข้าใช้งานของผู้ใช้งาน ไว้ไม่น้อยกว่า ๙๐ วัน (สูงสุดไม่เกิน ๒ ปี ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์)

• ข้อมูลผู้ติดต่อ/สอบถามทั่วไป จัดเก็บไว้ไม่เกิน ๑ ปี นับจากวันที่ให้บริการเสร็จสิ้น

๓) การทำลายข้อมูลอย่างปลอดภัย (Secure Disposal)

แนวปฏิบัติ เมื่อข้อมูลส่วนบุคคลหมดความจำเป็นหรือครบกำหนดระยะเวลาจัดเก็บ (Retention Period) สำนักงานเทคโนโลยีสารสนเทศต้องดำเนินการทำลายหรือทำให้ไม่สามารถระบุตัวตนได้ (Anonymization) ด้วยวิธีการที่ปลอดภัย ดังนี้

• ข้อมูลในฐานข้อมูล (Digital Data) ใช้กระบวนการลบถาวรแบบ Secure Wipe หรือการลบกุญแจเข้ารหัส (Cryptographic Erasure) เพื่อไม่ให้สามารถกู้คืนได้

• สื่อบันทึกข้อมูล (Hard disk/Tape) หากอุปกรณ์ชำรุดหรือหมดอายุการใช้งาน ต้องดำเนินการทำลายทางกายภาพ (Physical Destruction) เช่น การเจาะทำลาย หรือ Degaussing ก่อนนำไปทิ้ง

• การทำบันทึกหลักฐาน ทุกครั้งที่มีการทำลายข้อมูลหรืออุปกรณ์ ต้องจัดทำ “บันทึกการทำลายข้อมูล (Data Disposal Log)” และลงนามร่วมกันโดยคณะกรรมการที่องค์การสะพานปลาแต่งตั้งเพื่อใช้เป็นหลักฐานแสดงความโปร่งใสต่อหน่วยงานกำกับดูแล

การวางแผน (Planning)

ทุกตัวชี้วัดต้องระบุเจ้าของตัวชี้วัด แหล่งข้อมูล สูตรคำนวณ ค่าเป้าหมาย ความถี่รายงาน และแนวทางแก้ไขเมื่อไม่บรรลุเป้าหมาย ผลการติดตามให้รายงานต่อ CIO อย่างน้อยรายไตรมาส และนำเข้าสู่การทบทวนฝ่ายบริหารอย่างน้อยปีละ ๑ ครั้ง

เพื่อให้ระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Digital QMS) สามารถบรรลุผลลัพธ์ตามที่คาดหวัง ป้องกันข้อผิดพลาด และได้รับการพัฒนาอย่างต่อเนื่อง สำนักงานเทคโนโลยีสารสนเทศองค์การสะพานปลา ได้กำหนดกระบวนการวางแผนเชิงระบบที่สามารถทำซ้ำได้ (Repeatable Practice) ดังนี้

๑. การดำเนินการกับความเสี่ยงและโอกาส (Actions to Address Risks and Opportunities)

สำนักงานเทคโนโลยีสารสนเทศ ให้ความสำคัญกับการประเมินความเสี่ยงด้านดิจิทัล (Digital Risk Assessment) ก่อนดำเนินโครงการหรือให้บริการ เพื่อป้องกันผลกระทบเชิงลบต่อองค์กรและผู้ใช้งาน โดยมีแนวปฏิบัติดังนี้

๑) **การระบุความเสี่ยง (Risk Identification)** ทุกต้นปีงบประมาณ หรือก่อนเริ่มโครงการพัฒนาระบบใหม่ ต้องมีการระบุความเสี่ยงที่อาจเกิดขึ้นใน ๓ ด้านหลัก ได้แก่

• *ความเสี่ยงด้านคุณภาพการบริการ (Service Quality Risk)* เช่น ระบบล่าช้า ระบบล่ม หรือเครือข่ายอินเทอร์เน็ตที่ท่าเทียบเรือประมงขัดข้อง

• *ความเสี่ยงด้านความมั่นคงปลอดภัย (Cybersecurity Risk)* เช่น การถูกโจมตีด้วย Ransomware หรือการถูกเจาะระบบ

• *ความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Risk)* เช่น ข้อมูลชาวประมงรั่วไหล หรือการเก็บข้อมูลเกินความจำเป็น

๒) **การประเมินและจัดการความเสี่ยง (Risk Mitigation)** นำความเสี่ยงที่ระบุได้มาประเมินระดับความรุนแรง (Impact) และโอกาสเกิด (Likelihood) หากพบความเสี่ยงระดับสูง (High) หรือวิกฤต (Critical) ต้องกำหนดมาตรการควบคุม (Control Measures) ลงใน **"แผนบริหารความเสี่ยงด้านดิจิทัล"** ทันที

๓) **การจัดการโอกาส (Opportunity Management)** นอกจากการป้องกันความเสี่ยงแล้ว ให้พิจารณานำเทคโนโลยีใหม่ๆ (เช่น Cloud Computing หรือ AI) มาเป็น "โอกาส" ในการยกระดับคุณภาพบริการของ อสป. ให้ดียิ่งขึ้น

๒ วัตถุประสงค์ด้านคุณภาพและการวางแผนเพื่อให้บรรลุผล (Quality Objectives and Planning to Achieve Them)

หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการกำหนด **"ตัวชี้วัดวัตถุประสงค์ด้านคุณภาพ (Quality KPIs)"** ประจำปี เพื่อให้เจ้าหน้าที่มีเป้าหมายการทำงานที่เป็นมาตรฐานเดียวกัน (Standardized Practice) โดยวัตถุประสงค์ต้องสอดคล้องกับนโยบายคุณภาพ และมีเกณฑ์ชี้วัดที่ชัดเจน ดังตัวอย่างต่อไปนี้

วัตถุประสงค์ด้านคุณภาพ (Quality Objectives)	ตัวชี้วัดสมรรถนะ (KPIs)	เป้าหมาย	ระยะเวลาประเมิน
๑. รักษาความพร้อมใช้งานของระบบงานหลัก (Core Systems)	อัตราความพร้อมใช้งาน (System Uptime/Availability)	≥99.5%	รายเดือน
๒. ส่งมอบระบบงาน/โครงการที่มีคุณภาพตามกำหนด	สัดส่วนโครงการที่ผ่าน UAT โดยไม่พบ Critical Defect	100%	รายโครงการ
๓. คุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย PDPA	จำนวนโครงการใหม่ที่มีการประเมินผลกระทบ (DPIA) ก่อนเริ่มงาน	๑๐๐%	รายโครงการ
๔. รักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ	จำนวนอุบัติการณ์ข้อมูลรั่วไหล (Data Breach Incident)	๐ ครั้ง	รายปี

การวางแผนเพื่อให้บรรลุเป้าหมาย สำหรับทุกวัตถุประสงค์ สำนักงานฯ ต้องกำหนดวิธีการดำเนินงาน (What to do), ทรัพยากรที่ต้องใช้ (Resources), ผู้รับผิดชอบ (Who), และวิธีการประเมินผล (How to evaluate) ไว้อย่างชัดเจนในแผนปฏิบัติการประจำปี

การวางแผนการเปลี่ยนแปลง (Planning of Changes)

เมื่อมีความจำเป็นต้องเปลี่ยนแปลงระบบสารสนเทศ (เช่น การอัปเกรดเวอร์ชันซอฟต์แวร์, การย้ายเซิร์ฟเวอร์, หรือการปรับปรุงโครงสร้างเครือข่าย) ซึ่งอาจส่งผลกระทบต่อคุณภาพการให้บริการ สำนักงานเทคโนโลยีสารสนเทศ ต้องดำเนินการผ่านกระบวนการ **การบริหารจัดการการเปลี่ยนแปลง (Change Management)** ดังนี้

๑. **การขออนุมัติการเปลี่ยนแปลง (Change Request)** ผู้ปฏิบัติงานต้องจัดทำเอกสารแจ้งรายละเอียด สิ่งที่ต้องการเปลี่ยน ผลกระทบที่อาจเกิดขึ้น และช่วงเวลาที่ดำเนินการ (Downtime)

๒. **การประเมินผลกระทบ (Impact Assessment)** หัวหน้ากลุ่มงานต้องพิจารณาผลกระทบต่อผู้ใช้งาน โดยเฉพาะที่ท่าเทียบเรือประมง และพิจารณาความสอดคล้องกับมาตรฐานความปลอดภัย

๓. **การกำหนดแผนสำรอง (Rollback Plan)** ทุกการเปลี่ยนแปลง **"ต้อง"** มีแผนกู้คืนระบบหรือแผนถอยกลับเสมอ หากการเปลี่ยนแปลงนั้นล้มเหลว เพื่อให้ระบบกลับมาใช้งานได้ตามปกติโดยเร็วที่สุด

๔. **การสื่อสาร (Communication)** ต้องแจ้งกำหนดการปรับปรุงระบบให้ผู้ใช้งาน (Users) และผู้มีส่วนได้ส่วนเสียรับทราบล่วงหน้าอย่างน้อย ๓ วันทำการ เพื่อเตรียมความพร้อม

การสนับสนุน (Support)

เพื่อให้การนำระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Digital QMS) ไปปฏิบัติใช้ บำรุงรักษา และปรับปรุงอย่างต่อเนื่องเป็นไปอย่างมีประสิทธิภาพ องค์การสะพานปลา (อสป.) โดยสำนักงานเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางการสนับสนุนทรัพยากรที่จำเป็น ดังนี้

๑. การจัดการทรัพยากร (Resources)

ผู้อำนวยการองค์การสะพานปลา และหัวหน้าสำนักงานเทคโนโลยีสารสนเทศ มีหน้าที่พิจารณาและจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินงานตามคู่มือ SOP ดังนี้

๑) ทรัพยากรบุคคล (Human Resources) จัดสรรบุคลากรที่มีจำนวนและความเชี่ยวชาญเพียงพอต่อการพัฒนาระบบ การให้บริการช่วยเหลือผู้ใช้งาน (Helpdesk) และการรักษาความมั่นคงปลอดภัย

๒) โครงสร้างพื้นฐานด้านดิจิทัล (Digital Infrastructure) จัดเตรียมเครื่องแม่ข่าย (Server) ระบบคลาวด์ (Cloud) เครือข่ายอินเทอร์เน็ต และอุปกรณ์รักษาความปลอดภัย (Firewall) ให้มีความพร้อมใช้งานสูง (High Availability) ทั้งในส่วนกลางและท่าเทียบเรือประมงส่วนภูมิภาค

๓) สภาพแวดล้อมสำหรับการดำเนินงาน (Environment for the Operation) จัดเตรียมสภาพแวดล้อมที่เหมาะสมต่อการทำงานของระบบสารสนเทศ เช่น ห้อง Data Center ที่มีระบบควบคุมอุณหภูมิและระบบสำรองไฟฟ้า รวมถึงซอฟต์แวร์เครื่องมือสำหรับการพัฒนาและทดสอบระบบ (Testing Tools) ที่มีลิขสิทธิ์ถูกต้อง

๒. ความรู้ความสามารถของบุคลากร (Competence)

เพื่อให้ผลลัพธ์ของการปฏิบัติงานเป็น "มาตรฐานเดียวกัน (Standardized Practice)" เจ้าหน้าที่สำนักงานเทคโนโลยีสารสนเทศทุกคนต้องมีความรู้ความสามารถที่เหมาะสม โดยมีแนวปฏิบัติดังนี้

๑) **การกำหนดความสามารถ (Competency Requirements)** ควบคุมให้เจ้าหน้าที่มีคุณสมบัติ ทักษะ และประสบการณ์ตรงตามใบพรรณนาหน้าที่งาน (Job Description)

๒) **การพัฒนาบุคลากร (Training & Development)** จัดทำแผนฝึกอบรมประจำปี (Annual Training Plan) เพื่อยกระดับทักษะด้านดิจิทัล (Digital Literacy/Upskill) เช่น

- หลักสูตรการเขียนโปรแกรมอย่างปลอดภัย (Secure Coding)
- หลักสูตรผู้ควบคุมข้อมูลส่วนบุคคล (DPO/PDPA Practice)
- หลักสูตรการตรวจสอบคุณภาพซอฟต์แวร์ (Software QA/QC)

๓) **การประเมินผล (Evaluation)** ประเมินประสิทธิผลของการฝึกอบรม และเก็บรวบรวมใบรับรอง (Certificates) หรือบันทึกประวัติการอบรมไว้เป็นหลักฐาน

๓. ความตระหนักรู้ (Awareness)

สำนักงานเทคโนโลยีสารสนเทศ ต้องสร้างความตระหนักรู้ให้แก่เจ้าหน้าที่ รวมถึงผู้รับจ้าง (Outsource) ที่เข้ามาปฏิบัติงานในพื้นที่หรือเชื่อมต่อกับระบบของ อสป. ให้รับทราบและเข้าใจในเรื่องต่อไปนี้

๑) นโยบายคุณภาพด้านเทคโนโลยีดิจิทัล เข้าใจเป้าหมายและวิสัยทัศน์ขององค์กร

๒) การมีส่วนร่วมในระบบคุณภาพ เข้าใจว่าตนเองมีบทบาทอย่างไรในการทำให้ระบบบรรลุตัวชี้วัด (KPIs) และความสำคัญของการปฏิบัติตามคู่มือมาตรฐาน (SOP) อย่างเคร่งครัด

๓) ผลกระทบจากการฝ่าฝืน ตระหนักถึงผลเสียหากไม่ปฏิบัติตามขั้นตอน เช่น ระบบล่ม ข้อมูลชาวประมงรั่วไหล ซึ่งอาจนำไปสู่ความผิดทางวินัยหรือความผิดตามกฎหมาย (PDPA / พ.ร.บ. คอมพิวเตอร์ฯ)

๔. การสื่อสาร (Communication)

กำหนดให้มีช่องทางและกระบวนการสื่อสารทั้งภายในและภายนอกองค์กรที่มีประสิทธิภาพ เพื่อสนับสนุนระบบบริหารคุณภาพ ดังนี้

๑) การสื่อสารภายในองค์กร (Internal Communication):

- เรื่องที่สื่อสาร การประกาศใช้คู่มือ SOP, การอัปเดตระบบสารสนเทศใหม่, การแจ้งเตือนภัยคุกคามทางไซเบอร์
- วิธีการ/ช่องทาง ระบบสารบรรณอิเล็กทรอนิกส์, อีเมลองค์กร (E-mail), หรือการประชุมชี้แจง

๒) การสื่อสารภายนอกองค์กร (External Communication):

- เรื่องที่สื่อสาร การแจ้งหยุดระบบชั่วคราว (Planned Downtime), คู่มือการใช้งานระบบลงทะเบียนชาวประมง, และการประกาศนโยบายความเป็นส่วนตัว (Privacy Notice)
- วิธีการ/ช่องทาง เว็บไซต์องค์การสะพานปลา, แอปพลิเคชัน, หรือป้ายประกาศ ณ ท่าเทียบเรือประมง

การปฏิบัติงาน (Operation)

เพื่อให้การพัฒนาระบบสารสนเทศและการให้บริการด้านเทคโนโลยีดิจิทัลขององค์การสะพานปลา (อสป.) เป็นไปตามความต้องการของผู้ใช้งาน มีความมั่นคงปลอดภัย และเป็นไปตามกฎหมาย สำนักงานเทคโนโลยีสารสนเทศจึงกำหนดกระบวนการควบคุมการปฏิบัติงานตลอดวงจรการพัฒนาระบบ (System Development Life Cycle - SDLC) ดังนี้

๑. การวางแผนและการควบคุมการปฏิบัติงาน (Operational Planning and Control)

ก่อนเริ่มโครงการดิจิทัลทุกโครงการ ไม่ว่าจะเป็นการพัฒนาด้วยบุคลากรภายใน (In-house) หรือการจ้างเหมาภายนอก (Outsource) ผู้จัดการโครงการต้องดำเนินการดังนี้

๑) จัดทำ **“แผนการจัดการคุณภาพโครงการ (QMP)”** (ใช้แบบฟอร์ม FMO-IT-FM-QMP-001) เพื่อกำหนดเกณฑ์การยอมรับ (Acceptance Criteria) และทรัพยากรที่ต้องใช้

๒) กำหนดจุดตรวจสอบคุณภาพ (Quality Checkpoints) ในแต่ละระยะของโครงการ เพื่อป้องกันข้อผิดพลาดที่อาจลุกลามไปยังขั้นตอนถัดไป

๓) ควบคุมการจัดเก็บข้อมูลส่วนบุคคลของชาวประมงและผู้ใช้งาน ให้อยู่ภายใต้หลักการจำกัดข้อมูลเท่าที่จำเป็น (Data Minimization) ตามแผน DPIA ที่ประเมินไว้

๒ การกำหนดข้อกำหนดสำหรับระบบและบริการ (Requirements for Digital Services)

การรวบรวมความต้องการ (Requirement Gathering) ถือเป็นจุดเริ่มต้นของคุณภาพ โดยต้องมีการสื่อสารกับผู้ใช้งานอย่างเป็นระบบ

๑) **การรับฟังความต้องการ** รวบรวมความต้องการจากผู้ใช้งานจริง (เช่น เจ้าหน้าที่ท่าเทียบเรือ หรือ ชาวประมง) เพื่อให้ระบบที่พัฒนาขึ้นตอบโจทย์กระบวนการทำงานจริง (Business Process)

๒) **การจัดทำขอบเขตงาน (TOR / SRS)** ต้องระบุข้อกำหนดให้ครอบคลุม ๓ ด้าน ได้แก่

- Functional Requirement ฟังก์ชันที่ระบบต้องทำได้
- Non-Functional Requirement ประสิทธิภาพ ความรวดเร็ว (SLA) และความพร้อมใช้งาน (Uptime)
- Security & Compliance มาตรฐานความปลอดภัยไซเบอร์ และข้อกำหนดตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)

๓) **การทบทวนข้อกำหนด** ก่อนลงมือพัฒนาหรือประกาศจัดจ้าง ต้องมีการลงนามรับรองความถูกต้องของข้อกำหนดโดยหน่วยงานเจ้าของระบบ (Business Owner)

๓. การออกแบบและการพัฒนาระบบ (Design and Development)

เพื่อให้ระบบมีมาตรฐานเดียวกัน (Standardized Practice) การออกแบบและพัฒนาต้องยึดหลักการดังนี้

๑) การออกแบบส่วนติดต่อผู้ใช้งาน (UI/UX Design) ออกแบบให้ใช้งานง่าย รองรับการแสดงผลบนอุปกรณ์เคลื่อนที่ (Responsive Design) เพื่ออำนวยความสะดวกแก่ชาวประมงและผู้ประกอบการ

๒) การออกแบบโดยคำนึงถึงความเป็นส่วนตัว (Privacy by Design) ระบบต้องบังคับให้มีการเข้ารหัสข้อมูลสำคัญ (Data Encryption) และมีการจัดการสิทธิ์ผู้ใช้งาน (Access Control) ตั้งแต่ขั้นตอนการเขียนโปรแกรม

๓) การพัฒนาที่ปลอดภัย (Secure Coding) นักพัฒนาต้องเขียนโปรแกรมโดยหลีกเลี่ยงช่องโหว่ตามมาตรฐานสากล (เช่น OWASP Top 10)

๔. การควบคุมผู้ให้บริการภายนอก (Control of Externally Provided Processes/Outsource)

เนื่องจาก อสป. มีการจ้างหน่วยงานภายนอก (Vendor/Outsource) พัฒนาระบบและดูแลโครงสร้างพื้นฐาน การควบคุมคุณภาพของผู้ให้บริการจึงเป็นสิ่งสำคัญยวด

๑) การคัดเลือกผู้ให้บริการ ต้องประเมินประวัติการทำงาน มาตรฐานความปลอดภัย และความเชี่ยวชาญก่อนการจัดจ้าง

๒) การทำข้อตกลงและสัญญา (Agreements) นอกเหนือจากสัญญาจ้าง (TOR) แล้ว ผู้รับจ้างต้องลงนามในเอกสารสำคัญ ๒ ฉบับ ได้แก่

- ข้อตกลงการรักษาความลับ (NDA - Non-Disclosure Agreement)
- ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (DPA - Data Processing Agreement)

ในกรณีที่ผู้รับจ้างต้องเข้าถึงฐานข้อมูลของ อสป.

๓) การติดตามประเมินผลผู้รับจ้าง (Vendor Evaluation) ประเมินผลงานของผู้รับจ้างตามรอบการส่งมอบงาน (Sprint/Milestone) หากพบว่าคุณภาพงานไม่ถึงเกณฑ์ ต้องแจ้งให้ดำเนินการแก้ไขภายในเวลาที่กำหนด

๕. การให้บริการและการสนับสนุน (Production and Service Provision)

เมื่อระบบเปิดใช้งานจริง สำนักงานเทคโนโลยีสารสนเทศ ต้องควบคุมการให้บริการประจำวัน (Daily Operations) ให้เป็นไปตามมาตรฐาน

๑) การบริหารจัดการบัญชีผู้ใช้งาน (User Access Management) ตรวจสอบสิทธิ์การเข้าถึงระบบอย่างสม่ำเสมอ หากมีพนักงานลาออกหรือย้ายแผนก ต้องระงับสิทธิ์ทันที

๒) การสนับสนุนผู้ใช้งาน (IT Helpdesk) จัดให้มีช่องทางการแจ้งปัญหา (Incident Reporting) โดยมีคู่มือการแก้ไขปัญหาเบื้องต้น (Work Instruction) เพื่อให้เจ้าหน้าที่สามารถแก้ไขปัญหาให้ท่าเทียบเรือประมงได้อย่างรวดเร็ว (Repeatable Practice)

๓) การสำรองข้อมูล (Data Backup) ดำเนินการสำรองข้อมูลตามรอบเวลาที่กำหนด และทดสอบการกู้คืนข้อมูล (Restore Test) อย่างน้อยปีละ ๑ ครั้ง เพื่อรับประกันความพร้อมใช้งานของข้อมูล (Data Availability)

๖. การส่งมอบระบบและการตรวจรับ (Release of Digital Services)

การอนุญาตให้ระบบขึ้นใช้งานจริง (Go-Live) ต้องผ่านกระบวนการคัดกรองที่เข้มงวด

๑) การทดสอบระบบ (UAT & Security Test) ระบบต้องผ่านการทดสอบจากผู้ใช้งานจริงและต้องผ่านการสแกนหาช่องโหว่ (Vulnerability Scan)

๒) การตรวจรับตามมาตรฐาน คณะกรรมการตรวจรับหรือ QA ต้องใช้ “แบบฟอร์มรายการตรวจสอบคุณภาพมาตรฐาน (FMO-IT-FM-QC-001)” เพื่อยืนยันความสมบูรณ์

๓) การอนุมัติ (Sign-off) หัวหน้าสำนักงานเทคโนโลยีสารสนเทศเป็นผู้ลงนามอนุมัติขั้นสุดท้ายก่อนเปิดใช้งานระบบ

๗. การควบคุมบริการที่ไม่เป็นไปตามข้อกำหนด (Control of Nonconforming Outputs)

หากพบว่าระบบหรือบริการทำงานผิดพลาด (Defects) หรือเกิดเหตุละเมิดความปลอดภัย

๑) การระงับและกักกัน หยุดการให้บริการระบบชั่วคราว หรือแยกเครือข่ายที่มีปัญหาออก (Isolation) เพื่อป้องกันความเสียหายลุกลาม

๒) การแจ้งเตือน (Notification) หากเหตุการณ์ส่งผลกระทบต่อข้อมูลส่วนบุคคล (Data Breach) ต้องรายงานต่อผู้บริหาร อสป. และแจ้งคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน ๗๒ ชั่วโมง ตามกฎหมาย PDPA

๓) การแก้ไข (Remediation) ดำเนินการแก้ไขข้อบกพร่อง และทำการทดสอบซ้ำ (Re-test) จนกว่าจะมั่นใจว่าระบบกลับมามีคุณภาพตามมาตรฐาน ก่อนเปิดใช้งานอีกครั้ง

การประเมินสมรรถนะและการปรับปรุง (Performance Evaluation & Improvement)

เพื่อให้ระบบบริหารจัดการคุณภาพด้านเทคโนโลยีดิจิทัล (Digital QMS) ขององค์การสะพานปลา (อสป.) มีความยั่งยืน สามารถแก้ไขข้อบกพร่องได้อย่างเป็นระบบ (Systematic) และเกิดการพัฒนาอย่างต่อเนื่อง สำนักงานเทคโนโลยีสารสนเทศจึงกำหนดกระบวนการประเมินและปรับปรุง ดังต่อไปนี้

๑. การติดตาม การวัด การวิเคราะห์ และการประเมินผล (Monitoring, Measurement, Analysis and Evaluation)

สำนักงานเทคโนโลยีสารสนเทศ ต้องเฝ้าระวังและประเมินผลการทำงานของระบบสารสนเทศและกระบวนการทำงานอย่างสม่ำเสมอ โดยมีแนวปฏิบัติดังนี้

๑) การวัดผลระบบ (System Performance Monitoring) ติดตามสถานะของเครื่องแม่ข่าย (Server) เครือข่ายอินเทอร์เน็ต และระบบฐานข้อมูลแบบเรียลไทม์ (Real-time Monitoring) เพื่อให้บรรลุเป้าหมาย Service Level Agreement (SLA) และ System Uptime ไม่น้อยกว่า ๙๙.๕%

๒) การประเมินความพึงพอใจของผู้ใช้งาน (User Satisfaction) จัดทำแบบประเมินความพึงพอใจประจำปี สำหรับผู้ใช้งานทั้งส่วนกลาง ท่าเทียบเรือประมง และชาวประมง/ผู้ประกอบการที่ใช้บริการระบบออนไลน์ เพื่อนำข้อเสนอแนะมาวิเคราะห์และจัดลำดับความสำคัญในการปรับปรุง

๓) การวิเคราะห์ข้อมูล (Data Analysis) นำข้อมูลที่ได้จากรายงานปัญหา (Helpdesk Log) ข้อบกพร่องที่พบ (Defect Log) และสถิติภัยคุกคามทางไซเบอร์ มาวิเคราะห์เพื่อหาแนวโน้ม (Trend Analysis) และวางแผนป้องกันในอนาคต

๒. การตรวจประเมินภายในด้านดิจิทัล (Digital Internal Audit)

เพื่อให้เกิดความมั่นใจว่าการปฏิบัติงานจริงสอดคล้องกับ “คู่มือมาตรฐาน (SOP)” สำนักงานเทคโนโลยีสารสนเทศ ต้องจัดให้มีการตรวจประเมินภายใน อย่างน้อยปีละ ๑ ครั้ง โดยมีแนวปฏิบัติดังนี้

๑) การวางแผนการตรวจประเมิน หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ แต่งตั้งคณะผู้ตรวจประเมิน (Internal Auditors) ซึ่งต้องเป็นผู้ที่ไม่มีส่วนได้ส่วนเสียโดยตรงกับโครงการที่ถูกตรวจสอบ (Cross-functional Audit)

๒) ขอบเขตการตรวจสอบ ตรวจสอบการใช้แบบฟอร์มแผนคุณภาพ (QMP), รายการตรวจสอบคุณภาพ (Checklist), การจัดการสิทธิ์เข้าถึงระบบ, และการปฏิบัติตามนโยบายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

๓) การรายงานผลการตรวจสอบ ผู้ตรวจประเมินต้องทำรายงานสรุปข้อบกพร่อง (Nonconformity) และโอกาสในการปรับปรุง (OFI) เสนอต่อผู้อำนวยการสำนักงานฯ เพื่อสั่งการแก้ไข

๓. การทบทวนฝ่ายบริหาร (Management Review)

ในสภาวะที่โครงสร้างการกำกับดูแลอาศัยอำนาจการบริหารของผู้อำนวยการองค์การสะพานปลา (ผออ.) สำนักงานเทคโนโลยีสารสนเทศต้องนำเสนอ “รายงานผลการดำเนินงานด้านคุณภาพดิจิทัล” เข้าสู่ ที่ประชุมบริหาร (Executive Committee) หรือรายงานตรงต่อ ผออ. อย่างน้อยปีละ ๑ ครั้ง โดยต้องมีวาระการทบทวนดังนี้

๑) สถานะของการดำเนินการแก้ไขปัญหาจากรอบการประเมินครั้งก่อน

๒) การเปลี่ยนแปลงของปัจจัยภายนอกและภายใน (เช่น เทคโนโลยีใหม่, กฎหมาย PDPA ฉบับปรับปรุง)

๓) ผลสัมฤทธิ์ของตัวชี้วัด (Quality KPIs) และความพึงพอใจของผู้ใช้งาน

๔) ผลการตรวจประเมินภายใน (Internal Audit) และผลประเมิน SE-AM จาก สคร.

๕) ข้อเสนอแนะเพื่อการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement) และการขออนุมัติทรัพยากรเพิ่มเติม

๔. การปรับปรุงอย่างต่อเนื่องและการจัดการความไม่สอดคล้อง (Improvement and Nonconformity)

เมื่อเกิดข้อผิดพลาดของระบบ (System Crash) ข้อมูลรั่วไหล (Data Breach) หรือพบการทำงานที่ไม่เป็นไปตามมาตรฐาน (Nonconformity) ต้องมีกระบวนการแก้ไขที่ “ทำซ้ำได้ (Repeatable)” ดังนี้

๑) การแก้ไขปัญหาเฉพาะหน้า (Correction) ดำเนินการระงับเหตุและแก้ไขให้ระบบกลับมาใช้งานได้โดยเร็วที่สุดเพื่อลดผลกระทบต่อธุรกิจ (Business Continuity)

๒) การวิเคราะห์สาเหตุรากเหง้า (Root Cause Analysis - RCA) จัดประชุมทีมงานเพื่อค้นหาสาเหตุที่แท้จริงของปัญหา โดยอาจใช้เครื่องมือทางคุณภาพ เช่น แผนผังก้างปลา (Fishbone Diagram) หรือ เทคนิค 5 Whys

๓) การปฏิบัติการแก้ไข (Corrective Action) กำหนดมาตรการป้องกันไม่ให้ปัญหานั้นเกิดซ้ำ เช่น การปรับปรุง Source Code การเพิ่มมาตรการ Firewall หรือการปรับปรุงเอกสาร Checklist มาตรฐาน

๔) การปรับปรุงอย่างต่อเนื่อง (Continual Improvement) นำบทเรียนที่ได้รับ (Lessons Learned) ไปปรับปรุงคู่มือปฏิบัติงานการจัดการคุณภาพ (SOP) ให้มีความรัดกุมและทันสมัยอยู่เสมอ

ภาคผนวก

ภาคผนวก ก

เอกสารควบคุม แบบฟอร์มมาตรฐานสำนักงานเทคโนโลยีสารสนเทศ

รหัสเอกสาร FMO-IT-FM-QMP-001 | **วันที่บังคับใช้** [ระบุวันที่] | **แก้ไขครั้งที่** 00

แผนการจัดการคุณภาพโครงการดิจิทัล (Quality Management Plan QMP)

องค์การสะพานปลา (FMO)

ส่วนที่ ๑ ข้อมูลทั่วไปของโครงการ (Project Information)

- **ชื่อโครงการ / ระบบงาน** .....
- **รหัสโครงการ (ถ้ามี)** .....
- **ผู้รับผิดชอบโครงการ (Project Manager)** .....
- **ระยะเวลาดำเนินโครงการ** วันเริ่ม ..... วันสิ้นสุด .....
- **ความสำคัญของโครงการต่อ อสป.** [ ] สูงมาก (Core Business) [ ] ปานกลาง [ ] ทั่วไป

ส่วนที่ ๒ มาตรฐานและตัวชี้วัดคุณภาพ (Quality Metrics & Acceptance Criteria)

(ให้ระบุเกณฑ์ที่ระบบหรือผลงานต้องผ่านการทดสอบ อ้างอิง ISO/IEC 25010)

มิติด้านคุณภาพ (Quality Factor)	ตัวชี้วัด (Metrics / KPIs)	เกณฑ์การยอมรับ (Acceptance Criteria)
๑. ฟังก์ชันการทำงาน (Functional Suitability)	ความครบถ้วนของระบบงานตาม TOR	ต้องผ่าน UAT 100% ไม่มี Critical Defect
๒. ประสิทธิภาพการทำงาน (Performance)	ความเร็วในการตอบสนอง (Response Time)	โหลดหน้าจอเสร็จสิ้นภายใน 3 วินาที
๓. ความพร้อมใช้งาน (Availability)	อัตราการทำงานต่อเนื่องของระบบ (Uptime)	ไม่น้อยกว่า 99.5% ต่อเดือน
๔. ความมั่นคงปลอดภัย (Security)	ระดับความปลอดภัยตามการประเมินความเสี่ยง	ต้องไม่มีช่องโหว่ระดับ High/Critical

ส่วนที่ ๓ บทบาทและความรับผิดชอบด้านคุณภาพ (Roles & Responsibilities)

บทบาทหน้าที่	ชื่อ-นามสกุล / ตำแหน่ง	ความรับผิดชอบด้านคุณภาพ
ผู้จัดการโครงการ (PM)	.....	ควบคุมให้โครงการเป็นไปตามแผน QMP นี้
ผู้สอบทานคุณภาพ (QA)	.....	ตรวจสอบกระบวนการทำงานให้เป็นไปตาม SOP
ผู้ทดสอบระบบ (QC/Tester)	.....	ทดสอบระบบตาม Checklist และรายงานข้อบกพร่อง

ส่วนที่ ๔ กิจกรรมการควบคุมและประกันคุณภาพ (QA & QC Activities)

(ทำเครื่องหมาย ✓ในกิจกรรมที่จะดำเนินการในโครงการนี้ เพื่อให้ทำซ้ำได้เป็นมาตรฐาน)

- [ ] **Peer Review** การตรวจสอบเอกสาร/โค้ด (Source Code) โดยเพื่อนร่วมงานก่อนส่งมอบ
- [ ] **System Testing (SIT)** การทดสอบการทำงานของระบบในสภาพแวดล้อมจำลอง
- [ ] **User Acceptance Test (UAT)** การทดสอบและลงนามรับรองโดยผู้ใช้งานจริง (เช่น เจ้าหน้าที่ท่าเทียบเรือ)
- [ ] **Vulnerability Scan** การสแกนหาช่องโหว่ด้านความปลอดภัยของระบบก่อนนำขึ้นใช้งานจริง (Go-Live)

ส่วนที่ ๕ การปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance)

(หากโครงการนี้ไม่มีการประมวลผลข้อมูลส่วนบุคคล ให้ข้ามส่วนนี้ไป)

๕.๑ ประเภทข้อมูลที่จัดเก็บ [ ] ข้อมูลชาวประมง/ผู้ประกอบการ [ ] ข้อมูลพนักงาน [ ] ข้อมูลทั่วไป

๕.๒ ฐานทางกฎหมาย (Legal Basis) [ ] ฐานสัญญา (Contract) [ ] ฐานภารกิจภาครัฐ (Public Task) [ ] ความยินยอม (Consent)

๕.๓ การประเมินผลกระทบ (DPIA) โครงการนี้ได้ทำประเมิน DPIA แล้วหรือไม่? [ ] ทำแล้ว [ ] ยังไม่ได้ทำ (ต้องทำก่อน Go-Live)

๕.๔ ระยะเวลาจัดเก็บ (Retention Period) กำหนดระยะเวลาจัดเก็บข้อมูลไว้ที่ ..... ปี นับจาก .....

๕.๕ มาตรการทำลายข้อมูล เมื่อครบกำหนด จะดำเนินการ [ ] ลบออกจากฐานข้อมูลถาวร [ ] ทำข้อมูลให้เป็นนิรนาม (Anonymization)

ส่วนที่ ๖ การจัดการข้อบกพร่อง (Defect Management)

หากพบข้อผิดพลาดหรือปัญหาคุณภาพระหว่างการพัฒนา/บริการ จะดำเนินการบันทึกลงใน **“แบบฟอร์มรายงานปัญหาและขอแก้ไข (Defect/Change Request Form)”** และให้ระบุสาเหตุ (Root Cause Analysis) ทุกครั้งเพื่อป้องกันการเกิดซ้ำ

ส่วนที่ ๗ การทบทวนและอนุมัติ (Review & Approval)

ผู้จัดทำแผนคุณภาพ (Prepared By):

ลงชื่อ .....

(.....)

ตำแหน่ง .....

วันที่ ...../...../.....

ผู้ทบทวน (Reviewed By):

ลงชื่อ .....

(.....)

ตำแหน่ง หัวหน้ากลุ่มงาน/ผู้ควบคุมเอกสาร

วันที่ ...../...../.....

ผู้อนุมัติ (Approved By):

ลงชื่อ .....

(.....)

ตำแหน่ง หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ

วันที่ ...../...../.....

ภาคผนวก ข

แบบฟอร์มรายการตรวจสอบคุณภาพมาตรฐาน (Standard Quality Checklist)

สำหรับการตรวจรับและการปล่อยระบบขึ้นใช้งานจริง (Go-Live / UAT Checklist)

ส่วนที่ ๑ ข้อมูลการตรวจสอบ (Inspection Information)

- **ชื่อระบบงาน / โครงการ** .....
- **หน่วยงานเจ้าของระบบ (Business Owner)** .....
- **ผู้พัฒนา / บริษัทผู้รับจ้าง** .....
- **วันที่ทำการตรวจสอบ** ...../...../..... **เวอร์ชันของระบบ** .....

ส่วนที่ ๒ รายการตรวจสอบคุณภาพ (Quality Checklist)

(ผู้ตรวจสอบต้องทำเครื่องหมาย ✓ในช่องผลการตรวจสอบ หากข้อใดไม่เกี่ยวข้องให้ทำเครื่องหมายที่ N/A)

ลำดับ	รายการตรวจสอบมาตรฐาน (Standard Checkpoints)	ผ่าน (Pass)	ไม่ผ่าน (Fail)	N/A	หมายเหตุ / อ้างอิง
หมวดที่ ๑ การทำงานและประสิทธิภาพ (Functional & Performance - อ้างอิง ISO 25010)					
๑.๑	ระบบทำงานได้ครบถ้วนตามความต้องการ (TOR / Requirement)	[ ]	[ ]	[ ]	
๑.๒	ผู้ใช้งานจริง (User) ได้ทำการทดสอบ (UAT) และลงนามรับรองแล้ว	[ ]	[ ]	[ ]	แนบใบ UAT
๑.๓	ระบบสามารถประมวลผลและตอบสนองได้ตามเกณฑ์ SLA ที่กำหนด	[ ]	[ ]	[ ]	
๑.๔	การแสดงผลบนหน้าจอ (UI/UX) ถูกต้องทั้งบนคอมพิวเตอร์และมือถือ	[ ]	[ ]	[ ]	
หมวดที่ ๒ ความมั่นคงปลอดภัยสารสนเทศ (Information Security - อ้างอิง ISO 27001 / DT-5)					
๒.๑	มีการเข้ารหัสผ่าน (Password Encryption) และบังคับตั้งรหัสผ่านที่รัดกุม	[ ]	[ ]	[ ]	

ลำดับ	รายการตรวจสอบมาตรฐาน (Standard Checkpoints)	ผ่าน (Pass)	ไม่ผ่าน (Fail)	N/A	หมายเหตุ / อ้างอิง
๒.๒	มีการกำหนดสิทธิ์ผู้ใช้งาน (Access Control) ตามหลัก Least Privilege	[ ]	[ ]	[ ]	
๒.๓	มีการจัดเก็บ Log การเข้าใช้งานระบบย้อนหลังได้ไม่น้อยกว่า ๙๐ วัน	[ ]	[ ]	[ ]	พ.ร.บ. คอมฯ
๒.๔	ผ่านการทดสอบเจาะระบบ (Vulnerability Scan / Penetration Test)	[ ]	[ ]	[ ]	
หมวดที่ ๓ การคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance - เชื่อมโยง DT-4 / DT-5)					
๓.๑	มีการแสดง นโยบายความเป็นส่วนตัว (Privacy Notice) ก่อนเก็บข้อมูล	[ ]	[ ]	[ ]	
๓.๒	จัดเก็บข้อมูลส่วนบุคคล เท่าที่จำเป็นเท่านั้น (Data Minimization)	[ ]	[ ]	[ ]	
๓.๓	มีการระบุ ฐานทางกฎหมาย (Legal Basis) ชัดเจน (สัญญา / ภารกิจรัฐ)	[ ]	[ ]	[ ]	
๓.๔	มีการตั้งค่า ระยะเวลาจัดเก็บ (Retention Period) และมีระบบหรือคู่มือสำหรับลบ ทำลาย หรือทำให้เป็นข้อมูลนิรนามเมื่อครบกำหนดตามตารางระยะเวลาการเก็บรักษาข้อมูล	[ ]	[ ]	[ ]	
๓.๕	(สำหรับระบบใหม่) ได้ทำการประเมินผลกระทบ (DPIA) เรียบร้อยแล้ว	[ ]	[ ]	[ ]	แนบใบ DPIA
หมวดที่ ๔ โครงสร้างพื้นฐานและการสำรองข้อมูล (Infrastructure & Backup - เชื่อมโยง DT-6)					
๔.๑	มีการตั้งค่าการสำรองข้อมูล (Backup Configuration) ตามมาตรฐาน อสป.	[ ]	[ ]	[ ]	
๔.๒	มีคู่มือการติดตั้ง (Installation Guide) และคู่มือผู้ใช้งาน (User Manual)	[ ]	[ ]	[ ]	

ส่วนที่ ๓ สรุปผลการตรวจสอบ (Inspection Conclusion)

- [ ] **ผ่านการตรวจสอบ (Approved)** อนุญาตให้นำระบบขึ้นใช้งานจริง (Go-Live) ได้
- [ ] **ผ่านแบบมีเงื่อนไข (Conditional Approval)** อนุมัติให้ใช้งานได้ แต่ต้องแก้ไข Defect เล็กน้อย ภายในวันที่ ...../...../.....
- [ ] **ไม่ผ่านการตรวจสอบ (Rejected)** ไม่อนุญาตให้ใช้งาน ต้องแก้ไข Defect ระดับ High/Critical และนำมาตรวจสอบใหม่

รายละเอียดข้อบกพร่องที่ต้องแก้ไข (Defect Summary):

.....

.....

ส่วนที่ ๔ การลงนามรับรอง (Signatures)

ผู้ทำการตรวจสอบคุณภาพ (QA / QC Tester)

ลงชื่อ .....

(.....)

ตำแหน่ง เจ้าหน้าที่สำนักงานเทคโนโลยีสารสนเทศ

วันที่ ...../...../.....

ผู้จัดการโครงการ / หัวหน้ากลุ่มงาน (Project Manager / Supervisor)

ลงชื่อ .....

(.....)

ตำแหน่ง .....

วันที่ ...../...../.....