



**ประกาศองค์การสะพานปลา**  
**เรื่อง นโยบายและกรอบทิศทางการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล**  
**(Digital Governance) ขององค์การสะพานปลา**  
**พ.ศ. ๒๕๖๙**

ด้วยองค์การสะพานปลา มุ่งมั่นสู่การเป็นรัฐวิสาหกิจดิจิทัลเพื่อยกระดับการบริหารจัดการ  
ท่าเทียบเรือประมง และการบริการสาธารณะที่มีประสิทธิภาพ โดยให้ความสำคัญกับการนำเทคโนโลยีดิจิทัล  
มาเพิ่มขีดความสามารถในการให้บริการแก่ชาวประมง เกษตรกร และผู้มีส่วนได้ส่วนเสียทุกภาคส่วน ภายใต้  
มาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศที่เป็นสากล และการคุ้มครองข้อมูลส่วนบุคคลตามกฎหมาย

อาศัยอำนาจตามความในมาตรา ๒๓ แห่งพระราชบัญญัติจัดระเบียบกิจการแพปลา พ.ศ. ๒๕๔๖  
และที่แก้ไขเพิ่มเติม ประกอบกับข้อบังคับองค์การสะพานปลาว่าด้วยการบริหารงานและระเบียบที่เกี่ยวข้อง  
ผู้อำนวยการองค์การสะพานปลาจึงออกประกาศนโยบายและกรอบทิศทางการกำกับดูแลด้านการบริหาร  
จัดการเทคโนโลยีดิจิทัล (Digital Governance) เพื่อใช้เป็นกรอบการดำเนินงานสำหรับบุคลากรและหน่วยงาน  
ภายใน ดังต่อไปนี้

**หมวดที่ ๑ บททั่วไป**

ข้อ ๑ วัตถุประสงค์ ประกาศฉบับนี้จัดทำขึ้นเพื่อกำหนดกรอบทิศทาง หลักการ บทบาทหน้าที่  
และกลไกการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัลขององค์การสะพานปลา (อสป.) ให้สอดคล้อง  
กับยุทธศาสตร์องค์กร หลักธรรมาภิบาล มาตรฐานที่เกี่ยวข้อง เช่น COBIT 2019 และ ISO/IEC 38500  
หลักเกณฑ์การประเมินผลรัฐวิสาหกิจ (SE-AM) ตลอดจนกฎหมายและข้อกำหนดที่เกี่ยวข้อง

ข้อ ๒ ขอบเขตการบังคับใช้ ประกาศฉบับนี้ให้ใช้บังคับกับผู้บริหาร พนักงาน ลูกจ้าง  
ผู้ปฏิบัติงานทุกประเภท หน่วยงานภายใน ระบบงาน ข้อมูล โครงสร้างพื้นฐานดิจิทัล โครงการด้านเทคโนโลยี  
ดิจิทัล และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงหรือใช้ทรัพยากรของ อสป.

ข้อ ๓ หลักการกำกับดูแล ให้ยึดหลักการสร้างคุณค่าและความคุ้มค่า ความสอดคล้องกับ  
ยุทธศาสตร์ การบริหารความเสี่ยง การใช้ทรัพยากรอย่างเหมาะสม ความโปร่งใสตรวจสอบได้ ความมั่นคง  
ปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล และการปรับปรุงอย่างต่อเนื่อง

**หมวดที่ ๒ โครงสร้าง บทบาท และความรับผิดชอบ**

ข้อ ๔ กลไกการกำกับดูแล ให้คณะกรรมการองค์การสะพานปลา หรือคณะอนุกรรมการ หรือ  
คณะทำงานที่ได้รับมอบหมาย ทำหน้าที่ประเมิน กำหนดทิศทาง และติดตามผล (Evaluate, Direct and

Monitor: EDM) ด้านเทคโนโลยีดิจิทัล รวมทั้งพิจารณาความเสี่ยง ผลการดำเนินงาน และประเด็นที่มีนัยสำคัญต่อองค์กร

ข้อ ๕ บทบาทของผู้บริหารระดับสูง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) และผู้บริหารหน่วยงาน ต้องร่วมกันกำหนดทิศทาง จัดสรรทรัพยากร กำกับโครงการและบริการดิจิทัล บริหารความเสี่ยง และทำให้การใช้เทคโนโลยีดิจิทัลสนับสนุนภารกิจขององค์กรอย่างเป็นรูปธรรม

ข้อ ๖ บทบาทของสำนักงานเทคโนโลยีสารสนเทศ ให้รับผิดชอบจัดทำมาตรฐาน วิธีปฏิบัติ แผนงาน สถาปัตยกรรมองค์กร การบริหารบริการเทคโนโลยีสารสนเทศ การรักษาความมั่นคงปลอดภัย การติดตาม ตัวชี้วัด และการรายงานผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง

ข้อ ๗ บทบาทของเจ้าของข้อมูลและเจ้าของระบบ ให้กำหนดชั้นความลับ คุณภาพ การใช้ การเข้าถึง การเก็บรักษา และการทำลาย หรือสารสนเทศในความรับผิดชอบ ตลอดจนทบทวนสิทธิการเข้าถึง อย่างสม่ำเสมอ โดยประสานงานกับสำนักงานเทคโนโลยีสารสนเทศและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

### **หมวดที่ ๓ การคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยไซเบอร์**

ข้อ ๘ การประมวลผลข้อมูลส่วนบุคคล ต้องมีวัตถุประสงค์และฐานทางกฎหมายที่เหมาะสม เก็บรวบรวมข้อมูลเท่าที่จำเป็น แจ้งรายละเอียดการประมวลผลอย่างโปร่งใส รักษาความถูกต้องของข้อมูล กำหนดระยะเวลาเก็บรักษาตามความจำเป็นและกฎหมาย และจัดให้มีกระบวนการรองรับการใช้สิทธิของเจ้าของข้อมูล

ข้อ ๙ การคุ้มครองข้อมูลส่วนบุคคลตั้งแต่การออกแบบ ให้โครงการหรือระบบใหม่ รวมถึงการเปลี่ยนแปลงระบบที่มีนัยสำคัญ ประยุกต์ใช้หลัก Privacy by Design และ Privacy by Default และจัดทำ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) เมื่อการประมวลผลอาจก่อให้เกิดความเสี่ยงสูง

ข้อ ๑๐ การรักษาความมั่นคงปลอดภัย ต้องจัดให้มีมาตรการควบคุมที่เหมาะสมตามระดับ ความเสี่ยง ครอบคลุมการยืนยันตัวตนและควบคุมสิทธิ การบันทึกและติดตามเหตุการณ์ การจัดการช่องโหว่ การสำรองและกู้คืนข้อมูล การเข้ารหัส การป้องกันมัลแวร์ การรักษาความมั่นคงปลอดภัยของเครือข่าย อุปกรณ์ปลายทาง ระบบคลาวด์ และการพัฒนาระบบอย่างมั่นคงปลอดภัย

ข้อ ๑๑ การบริหารเหตุการณ์ผิดปกติ ให้มีช่องทางรายงานเหตุ ขั้นตอนจำแนกและยกระดับเหตุ การควบคุมความเสียหาย การเก็บรักษาพยานหลักฐาน การกู้คืนบริการ การสื่อสารกับผู้เกี่ยวข้องและการแจ้ง หน่วยงานกำกับดูแลหรือเจ้าของข้อมูลภายในระยะเวลาที่กฎหมายกำหนด พร้อมจัดทำบทเรียนหลังเหตุการณ์

### **หมวดที่ ๔ การบริหารความเสี่ยง การลงทุน และโครงการดิจิทัล**

ข้อ ๑๒ การบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ให้ระบุ วิเคราะห์ ประเมิน จัดการ ติดตาม และรายงานความเสี่ยงอย่างเป็นระบบ โดยเชื่อมโยงกับกรอบบริหารความเสี่ยงระดับองค์กร และ กำหนดเจ้าของความเสี่ยง แผนจัดการ ระยะเวลา และระดับความเสี่ยงที่ยอมรับได้อย่างชัดเจน

ข้อ ๑๓ การลงทุนและโครงการดิจิทัล ต้องมีเหตุผลความจำเป็น ผลลัพธ์ที่คาดหวัง เจ้าของโครงการ ขอบเขต งบประมาณ ระยะเวลา ตัวชี้วัด ความเสี่ยง ความพร้อมด้านบุคลากรและโครงสร้างพื้นฐาน ตลอดจนการประเมินความคุ้มค่าและประโยชน์ที่องค์กรหรือผู้รับบริการจะได้รับ ก่อนเสนออนุมัติ

ข้อ ๑๔ การบริหาร...

ข้อ ๑๔ การบริหารโครงการ ให้กำหนดจุดควบคุมและการอนุมัติที่เหมาะสมตลอดวงจรชีวิตโครงการ ตั้งแต่การริเริ่ม วางแผน จัดหา พัฒนา ทดสอบ นำขึ้นใช้งาน ส่งมอบ และปิดโครงการ รวมถึงควบคุมการเปลี่ยนแปลง การยอมรับระบบ การส่งมอบเอกสารและซอร์สโค้ด และการประเมินผลหลังใช้งาน

ข้อ ๑๕ ความต่อเนื่องของบริการ ให้ระบบงานสำคัญมีแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบที่สอดคล้องกับผลการวิเคราะห์ผลกระทบทางธุรกิจ มีการกำหนดเป้าหมายการกู้คืน ทดสอบแผนตามรอบและปรับปรุงจากผลการทดสอบหรือเหตุการณ์จริง

#### **หมวดที่ ๕ การกำกับดูแลข้อมูลและผู้ให้บริการภายนอก**

ข้อ ๑๖ การกำกับดูแลข้อมูล ให้กำหนดเจ้าของข้อมูล มาตรฐานข้อมูล คุณภาพข้อมูล คำอธิบายข้อมูล การเชื่อมโยงแลกเปลี่ยนข้อมูล ชั้นความลับ สิทธิการเข้าถึง และวงจรชีวิตข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน ปลอดภัย และนำไปใช้ประโยชน์ได้อย่างเหมาะสม

ข้อ ๑๗ การบริหารผู้ให้บริการภายนอก ต้องดำเนินการตรวจสอบความเหมาะสมก่อนว่าจ้าง กำหนดข้อกำหนดด้านระดับการให้บริการ ความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล สิทธิในการตรวจสอบ การแจ้งเหตุ การส่งคืนหรือทำลายข้อมูล การบริหารผู้รับจ้างช่วง และแผนรองรับเมื่อสิ้นสุดสัญญา พร้อมติดตามผลการปฏิบัติงานตามความเสี่ยง

#### **หมวดที่ ๖ การติดตาม ประเมินผล และการปฏิบัติตามข้อกำหนด**

ข้อ ๑๘ การติดตามผล ให้กำหนดตัวชี้วัดด้านความสอดคล้องเชิงยุทธศาสตร์ ความพร้อมใช้ และคุณภาพบริการ ความสำเร็จของโครงการ การใช้ทรัพยากร เหตุการณ์ด้านความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล และความพึงพอใจของผู้ใช้บริการ โดยรายงานต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องตามรอบที่กำหนด

ข้อ ๑๙ การประเมินและตรวจสอบ ให้มีการประเมินตนเอง การทบทวนการควบคุม การตรวจสอบภายในหรือการตรวจสอบโดยผู้เชี่ยวชาญตามความเหมาะสม รวมทั้งติดตามการแก้ไขข้อบกพร่องจนแล้วเสร็จ และเก็บรักษาหลักฐานที่จำเป็นเพื่อให้ตรวจสอบย้อนหลังได้

ข้อ ๒๐ การไม่ปฏิบัติตาม ผู้ปฏิบัติงานต้องรายงานข้อบกพร่อง เหตุขัดข้อง หรือการไม่ปฏิบัติตามนโยบายต่อผู้บังคับบัญชาและหน่วยงานที่รับผิดชอบโดยเร็ว การอนุมัติข้อบกพร่องต้องเป็นลายลักษณ์อักษรระบุเหตุผล ความเสี่ยง มาตรการชดเชย ผู้รับผิดชอบ และระยะเวลาสิ้นสุดอย่างชัดเจน

#### **หมวดที่ ๗ การสื่อสาร การทบทวน และการมีผลใช้บังคับ**

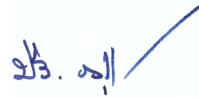
ข้อ ๒๑ การสื่อสารและพัฒนาความรู้ ให้สำนักงานเทคโนโลยีสารสนเทศร่วมกับหน่วยงานที่เกี่ยวข้องสื่อสารนโยบาย จัดทำแนวปฏิบัติ และพัฒนาความรู้ความตระหนักแก่บุคลากรและผู้เกี่ยวข้องตามบทบาทและระดับความเสี่ยง พร้อมประเมินผลการรับรู้และการนำไปปฏิบัติ

ข้อ ๒๒ การทบทวน...

ข้อ ๒๒ การทบทวน ให้ทบทวนนโยบายและกรอบทิศทางอย่างน้อยปีละ ๑ ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญด้านยุทธศาสตร์ โครงสร้างองค์กร เทคโนโลยี ภัยคุกคาม กฎหมาย หรือ ข้อกำหนดของหน่วยงานกำกับดูแล และเสนอผู้มีอำนาจพิจารณาอนุมัติ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๘ กันยายน พ.ศ.๒๕๖๙



(นายปรีดา ยังสุขสถาพร)

ผู้อำนวยการองค์การสะพานปลา

# เอกสารแนบท้ายประกาศ

แนวทางการกำหนดกรอบทิศทางการกำกับดูแล  
ด้านการบริหารจัดการเทคโนโลยีดิจิทัล  
(Digital Governance) ขององค์การสะพานปลา

พ.ศ. ๒๕๖๙

## คำนำ

ในยุคปัจจุบันที่เทคโนโลยีดิจิทัลเข้ามามีบทบาทสำคัญในการพลิกโฉมรูปแบบการดำเนินธุรกิจ และการให้บริการภาครัฐ องค์การสะพานปลา (อสป.) ในฐานะรัฐวิสาหกิจที่มีภารกิจหลักในการบริหารจัดการท่าเทียบเรือประมงและการขนถ่ายสินค้าสัตว์น้ำไทย เล็งเห็นถึงความจำเป็นอย่างยิ่งยวดในการขับเคลื่อนองค์กรสู่การเป็น “รัฐวิสาหกิจดิจิทัล” เพื่อยกระดับประสิทธิภาพการให้บริการแก่เกษตรกร ชาวประมง ผู้ประกอบการ และผู้มีส่วนได้ส่วนเสียทุกภาคส่วน ให้มีความสะดวกรวดเร็ว โปร่งใส และตรวจสอบได้

เพื่อรองรับการเปลี่ยนผ่านดังกล่าวและให้การบริหารจัดการเทคโนโลยีดิจิทัลเป็นไปอย่างมีระบบ องค์การสะพานปลาจึงได้จัดทำ “คู่มือแนวทางการกำหนดกรอบทิศทางกำกับการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance Framework Manual)” ฉบับนี้ขึ้น โดยบูรณาการหลักการตามมาตรฐานสากล ได้แก่ COBIT และ ISO/IEC ๓๘๕๐๐ ตลอดจนสอดคล้องกับหลักเกณฑ์การประเมินผลการดำเนินงานรัฐวิสาหกิจ (SE-AM) ด้านการพัฒนาเทคโนโลยีดิจิทัล (DT) ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.)

คู่มือฉบับนี้มีวัตถุประสงค์เพื่อใช้เป็นกรอบมาตรฐานในการปฏิบัติงาน (Standardized Practice) ที่ครอบคลุมตั้งแต่โครงสร้างการกำกับดูแล การส่งมอบผลประโยชน์และคุณค่าจากการลงทุนด้านดิจิทัล การบริหารจัดการทรัพยากรอย่างคุ้มค่า และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ นอกจากนี้ ยังให้ความสำคัญสูงสุดกับการปฏิบัติตามกฎหมายที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่ง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) เพื่อปกป้องข้อมูลของชาวประมงและบุคลากร และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

องค์การสะพานปลา หวังเป็นอย่างยิ่งว่า คู่มือฉบับนี้จะเป็นกลไกสำคัญที่ช่วยขับเคลื่อนให้คณะกรรมการ ผู้บริหาร และบุคลากรทุกระดับ มีความรู้ความเข้าใจและตระหนักถึงบทบาทหน้าที่ของตนเองในการกำกับดูแลเทคโนโลยีดิจิทัล อันจะนำไปสู่การพัฒนานวัตกรรมทางการประมง การสร้างความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย และการนำพาองค์การสะพานปลาให้เติบโตอย่างยั่งยืนต่อไป

องค์การสะพานปลา

## สารบัญ

|                                                                                                                                                    |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------|----|
| ส่วนที่ ๑ คำจำกัดความและความหมาย หลักการและเหตุผล วัตถุประสงค์ .....                                                                               | ๑  |
| คำจำกัดความและความหมาย .....                                                                                                                       | ๑  |
| หลักการและเหตุผล .....                                                                                                                             | ๑  |
| วัตถุประสงค์ .....                                                                                                                                 | ๒  |
| ส่วนที่ ๒ รายละเอียด .....                                                                                                                         | ๓  |
| ๑. กระบวนการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance) .....                                                                | ๓  |
| ๒. กรอบการกำกับดูแลด้านการบริหารจัดการทรัพยากรเทคโนโลยีดิจิทัลอย่างเหมาะสม (Benefits Delivery and Resource Opsonization Framework Setting) .....   | ๕  |
| ๓. กรอบการกำกับดูแลด้านการดำเนินงานให้มีประสิทธิภาพและมีความโปร่งใส (Performance Measurement and Stakeholder Transparency Framework Setting) ..... | ๑๒ |
| ๔. กรอบการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Risk Optimization Framework Setting) .....                                     | ๑๙ |
| ๕. การกำหนดหลักการการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance Guiding Principles) .....                                    | ๒๒ |
| ๖. การสื่อสารหลักการการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance Guiding Principle Communications) .....                    | ๒๖ |
| ๗. การกำหนดแนวทางในการพัฒนาความรู้ความสามารถด้านเทคโนโลยีดิจิทัลของบุคลากรในองค์กรทุกระดับ (Human Behavior & Digital Literacy) .....               | ๒๗ |

## ส่วนที่ ๑ คำจำกัดความและความหมาย หลักการและเหตุผล วัตถุประสงค์

### แนวทางการกำหนดกรอบทิศทางกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล

(Digital Governance)

#### คำจำกัดความและความหมาย

๑. องค์การสะพานปลา (อสป.) หมายความว่า รัฐวิสาหกิจในสังกัดกระทรวงเกษตรและสหกรณ์ ที่มีภารกิจหลักด้านการบริหารจัดการท่าเทียบเรือประมง และการจำหน่ายสัตว์น้ำ

๒. การกำกับดูแลด้านเทคโนโลยีดิจิทัล (Digital Governance) หมายถึง ระบบ โครงสร้าง และกระบวนการที่คณะกรรมการองค์การสะพานปลา หรือคณะทำงานที่ได้รับมอบหมาย ใช้ในการประเมิน (Evaluate) สั่งการ (Direct) และติดตามผล (Monitor) เพื่อให้มั่นใจว่าการนำเทคโนโลยีดิจิทัลมาใช้จะสนับสนุนและขับเคลื่อนยุทธศาสตร์ขององค์กรให้บรรลุเป้าหมาย

๓. เทคโนโลยีดิจิทัล (Digital Technology) หมายถึง ทรัพยากรสารสนเทศทั้งหมดขององค์กร ประกอบด้วย ระบบงาน (Application) ข้อมูล (Data) โครงสร้างพื้นฐาน (Infrastructure) และบุคลากรด้านดิจิทัล (People)

๔. ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลที่ทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ข้อมูลของเกษตรกร ชาวประมง ผู้ประกอบการ และผู้ใช้บริการ ท่าเทียบเรือประมง ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)

๕. ผู้มีส่วนได้ส่วนเสีย (Stakeholders) หมายถึง บุคคลหรือกลุ่มบุคคลที่มีส่วนเกี่ยวข้อง ได้รับผลกระทบ หรือมีส่วนได้ส่วนเสียจากการดำเนินงานด้านเทคโนโลยีดิจิทัลของ อสป. ทั้งภายใน (เช่น ผู้บริหาร พนักงาน) และภายนอก (เช่น ชาวประมง คู่ค้า หน่วยงานกำกับดูแล)

#### หลักการและเหตุผล

องค์การสะพานปลา (อสป.) อยู่ในช่วงการขับเคลื่อนการเปลี่ยนผ่านสู่รัฐวิสาหกิจดิจิทัล อย่างเต็มรูปแบบ เพื่อยกระดับประสิทธิภาพการบริหารจัดการท่าเทียบเรือประมงและการให้บริการสาธารณะ จากผลการประเมินผลการดำเนินงานรัฐวิสาหกิจตามระบบประเมินผล SE-AM ด้านที่ ๕ การพัฒนาเทคโนโลยีดิจิทัล พบว่า อสป. จำเป็นต้องยกระดับกระบวนการกำกับดูแลด้านเทคโนโลยีดิจิทัลให้มีแนวทางปฏิบัติอย่างเป็นระบบ สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice) รวมถึงต้องมีการนำเทคโนโลยีดิจิทัลมาสร้างคุณค่าเชิงสาธารณะ (Public Value) และมูลค่าทางธุรกิจ (Business Value) อย่างเป็นรูปธรรม

ดังนั้น เพื่อให้การบริหารจัดการเทคโนโลยีดิจิทัลสอดคล้องกับมาตรฐานสากล หลักธรรมาภิบาล และกฎหมายที่เกี่ยวข้อง โดยเฉพาะพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ อสป. จึงได้จัดทำกรอบทิศทางกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance) ขึ้น เพื่อใช้เป็นกลไกหลักในการบริหารจัดการความเสี่ยง สร้างความโปร่งใส และผลักดันให้การลงทุนด้านดิจิทัลเกิดความคุ้มค่าสูงสุด

## วัตถุประสงค์

๑. เพื่อกำหนดโครงสร้างและกระบวนการกำกับดูแลด้านเทคโนโลยีดิจิทัลให้เป็นระบบ มีมาตรฐานเดียวกันทั่วทั้งองค์กร (Standardized Practice) และสามารถปฏิบัติซ้ำได้ (Repeatable Practice)
๒. เพื่อให้มั่นใจว่าแผนปฏิบัติการดิจิทัลและการนำเทคโนโลยีดิจิทัลมาใช้ มีความสอดคล้องและสนับสนุนยุทธศาสตร์และภารกิจหลักของ อสป.
๓. เพื่อกำกับดูแลให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล การรักษาความมั่นคงปลอดภัยไซเบอร์ และการประมวลผลข้อมูลส่วนบุคคลของชาวประมงและผู้ให้บริการ อย่างถูกต้องตามกฎหมายและมีความปลอดภัย
๔. เพื่อกำหนดกลไกการวัดผลลัพธ์ (Outcome) การติดตาม วิเคราะห์ และประเมินประสิทธิผลของกระบวนการ เพื่อนำไปสู่การปรับปรุงและพัฒนาอย่างต่อเนื่อง (Continuous Improvement)

## ส่วนที่ ๒ รายละเอียด

### แนวทางการกำหนดกรอบทิศทางกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance)

#### ๑. กระบวนการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance)

องค์การสะพานปลาได้กำหนดกรอบทิศทางกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance Framework) โดยประยุกต์ใช้มาตรฐานสากล COBIT (Control Objectives for Information and Related Technologies) ซึ่งเป็นกรอบการปฏิบัติที่เป็นที่ยอมรับในระดับสากลสำหรับการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร (Enterprise IT Governance)

ทั้งนี้ องค์การได้ให้ความสำคัญกับ “ความต้องการของผู้มีส่วนได้ส่วนเสีย (Stakeholder Needs)” เพื่อนำมาเป็นปัจจัยขับเคลื่อน (Drivers) สำคัญในการออกแบบระบบการกำกับดูแลและบริหารจัดการเทคโนโลยีดิจิทัลที่ดี มีธรรมาภิบาล และสอดคล้องกับทิศทางยุทธศาสตร์ โดยมุ่งเน้นการตอบสนองวัตถุประสงค์หลักของผู้มีส่วนได้ส่วนเสีย ๓ ประการ ดังนี้

๑) การส่งมอบผลประโยชน์และความคุ้มค่า (Benefits Realization) เพื่อให้มั่นใจว่าการลงทุนและการนำเทคโนโลยีดิจิทัลมาปรับใช้ในการดำเนินงาน จะสามารถสร้างคุณค่า (Value Creation) สนับสนุนเป้าหมายขององค์กร และก่อให้เกิดประโยชน์สูงสุดต่อผู้มีส่วนได้ส่วนเสียอย่างเป็นรูปธรรม

๒) การบริหารจัดการความเสี่ยงให้เหมาะสม (Risk Optimization) เพื่อให้มั่นใจว่าองค์กรมีกระบวนการประเมินและบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล (รวมถึงความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล) อย่างรัดกุม และควบคุมให้อยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite)

๓) การบริหารจัดการทรัพยากรให้เกิดประโยชน์สูงสุด (Resource Optimization) เพื่อให้มั่นใจว่ามีการจัดสรรและบริหารจัดการทรัพยากรด้านเทคโนโลยีดิจิทัล ทั้งในส่วนของระบบงาน โครงสร้างพื้นฐาน ข้อมูล และบุคลากรด้านดิจิทัล อย่างเหมาะสม คุ้มค่า และมีประสิทธิภาพสูงสุด

คู่มือฉบับนี้มุ่งเน้นกระบวนการกำกับดูแลด้านเทคโนโลยีดิจิทัล (Digital Governance) โดยประยุกต์ใช้กรอบมาตรฐานสากลการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี (COBIT) ในโดเมนการประเมิน สั่งการ และติดตามผล (Evaluate, Direct, and Monitor EDM) ซึ่งประกอบด้วย ๕ กระบวนการหลัก ได้แก่

(๑) การกำหนดและรักษากรอบการกำกับดูแล (Ensure Governance Framework Setting and Maintenance) เพื่อให้มั่นใจว่าองค์กรมีโครงสร้างและกระบวนการกำกับดูแลที่เป็นมาตรฐานเดียวกัน (Standardized Practice) และสามารถปฏิบัติซ้ำได้ (Repeatable Practice)

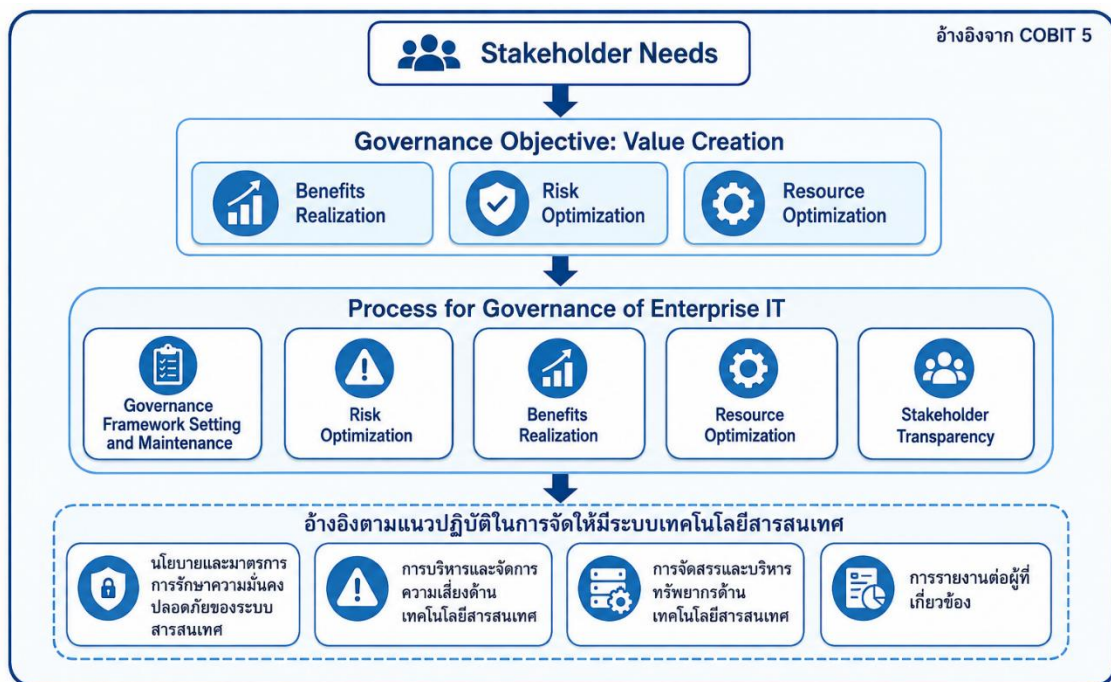
(๒) การบริหารจัดการความเสี่ยงให้เหมาะสม (Ensure Risk Optimization) เพื่อกำกับดูแลความเสี่ยงด้านดิจิทัล รวมถึงความเสี่ยงที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) และการคุ้มครองข้อมูลส่วนบุคคล (PDPA) ให้อยู่ในระดับที่องค์กรยอมรับได้

(๓) การส่งมอบผลประโยชน์และความคุ้มค่า (Ensure Benefits Delivery) เพื่อให้มั่นใจว่าการลงทุนและการนำเทคโนโลยีดิจิทัลมาปรับใช้ (Digital Transformation) สามารถสร้างคุณค่าและสนับสนุนยุทธศาสตร์ขององค์กรได้อย่างเป็นรูปธรรม

(๔) การบริหารจัดการทรัพยากรให้เกิดประโยชน์สูงสุด (Ensure Resource Optimization) เพื่อกำกับดูแลให้มีการจัดสรรและใช้งานทรัพยากรสารสนเทศ ข้อมูล และบุคลากรด้านดิจิทัลอย่างเหมาะสมและคุ้มค่า

(๕) การสร้างความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย (Ensure Stakeholder Transparency) เพื่อให้มั่นใจว่ามีการสื่อสาร การถ่ายทอดแนวทางปฏิบัติ และการรายงานผลการดำเนินงานด้านเทคโนโลยีดิจิทัลต่อผู้มีส่วนได้ส่วนเสียอย่างครบถ้วนและโปร่งใส

โดยกระบวนการทั้ง ๕ ประการข้างต้น ได้ถูกนำมาเทียบเคียงและบูรณาการเข้ากับหลักเกณฑ์ว่าด้วยการจัดให้มีระบบเทคโนโลยีสารสนเทศ ตามคู่มือการประเมินผลการดำเนินงานรัฐวิสาหกิจ (SE-AM) เพื่อเป็นแนวปฏิบัติในการขับเคลื่อนองค์การสะพานปลาสู่การเป็นรัฐวิสาหกิจดิจิทัลที่มีประสิทธิภาพ มีความมั่นคงปลอดภัย และกำกับดูแลข้อมูลได้อย่างมีธรรมาภิบาล



ภาพประกอบที่ ๑ กระบวนการการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

## ๒. กรอบการกำกับดูแลด้านการบริหารจัดการทรัพยากรเทคโนโลยีดิจิทัลอย่างเหมาะสม (Benefits Delivery and Resource Opsonization Framework Setting)

เพื่อให้องค์กรมีการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี (Enterprise Governance of IT EGIT) คณะกรรมการและผู้บริหารระดับสูงควรพิจารณากำหนดกรอบการดำเนินงานที่ครอบคลุมองค์ประกอบสำคัญ ดังนี้

๑) การส่งมอบผลประโยชน์ (Benefits Delivery) สร้างคุณค่าจากการนำเทคโนโลยีมาใช้ตอบ โจทย์กลยุทธ์องค์กร

๒) การใช้ทรัพยากรให้เกิดประโยชน์สูงสุด (Resource Optimization) บริหารจัดการ ทรัพยากร (บุคคล, เทคโนโลยี, ข้อมูล) อย่างคุ้มค่าและมีประสิทธิภาพ

๓) การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม (Risk Optimization) (รายละเอียดในหัวข้อถัดไป)

๔) ความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Transparency) (รายละเอียดในหัวข้อ ถัดไป)

โดยองค์กรอาจพิจารณาเน้นดำเนินการในส่วนการส่งมอบผลประโยชน์และการใช้ทรัพยากร ให้เกิดประโยชน์สูงสุด ดังนี้

๒.๑ การส่งมอบผลประโยชน์ (Benefits Delivery) และการใช้ทรัพยากรให้เกิดประโยชน์ สูงสุด (Resource Optimization)

เพื่อให้เกิดการใช้ทรัพยากรสารสนเทศอย่างคุ้มค่า ตอบสนองความต้องการตามภารกิจ หลักอย่างมีประสิทธิภาพและประสิทธิผล ภายใต้ระดับต้นทุนและความเสี่ยงที่ยอมรับได้ องค์กรสะพานปลา ควรยึดหลักการและดำเนินการ ดังนี้

### หลักการจัดการเทคโนโลยี (Technology Management Principles)

๑) นโยบายที่ชัดเจน กำหนดและประกาศใช้นโยบายด้านการจัดการเทคโนโลยีที่ชัดเจน สื่อสารให้ผู้บริหาร พนักงาน และผู้เกี่ยวข้องรับทราบ และนำไปปฏิบัติจริงอย่างเป็นรูปธรรม

๒) การกำหนดบทบาทหน้าที่ มอบหมายหน้าที่ความรับผิดชอบในการจัดการเทคโนโลยี แก่บุคคล หรือหน่วยงานที่มีความรู้ความสามารถอย่างแท้จริง และเหมาะสมกับลักษณะงาน

๓) การวางแผนเชิงรุก จัดทำแผนการปฏิบัติงานล่วงหน้า โดยศึกษาข้อมูลเบื้องต้น กำหนดภารกิจและเป้าหมายให้ชัดเจน รวมถึงวางแผนการดำเนินงาน การติดตาม และการประเมินผล เพื่อให้ ทราบว่าการดำเนินงานเป็นไปตามเป้าหมายหรือไม่

๔) การจัดสรรทรัพยากรอย่างเหมาะสม วิเคราะห์ลักษณะงานตามความจำเป็น เพื่อ จัดสรรทรัพยากรและงบประมาณสำหรับการปฏิบัติงานให้เพียงพอและคุ้มค่า

๕) การพัฒนาบุคลากร จัดฝึกอบรมบุคลากรให้ตรงกับลักษณะงาน เพื่อเพิ่มพูนความรู้ ทักษะทางดิจิทัล (Digital Literacy) และเพิ่มประสิทธิภาพในการปฏิบัติงานจริง

ผู้บริหารระดับสูงควรจัดทำแผนกลยุทธ์และนโยบาย ดังต่อไปนี้

### ๒.๑.๑ การจัดทำแผนปฏิบัติการดิจิทัลและงบประมาณด้านเทคโนโลยีสารสนเทศ

การจัดทำแผนปฏิบัติการดิจิทัล (Digital Roadmap / IT Strategic Plan) และงบประมาณ ควรมีความสอดคล้อง (Alignment) กับยุทธศาสตร์องค์กรในภาพรวม โดยปัจจัยที่ควรนำมาพิจารณา ประกอบด้วย

๑. ความต้องการของผู้มีส่วนได้ส่วนเสียและประเด็นเชิงยุทธศาสตร์ ประเมินระดับความสำคัญของเทคโนโลยีสารสนเทศในปัจจุบันและอนาคตที่มีต่อยุทธศาสตร์องค์กร อาทิ ระดับการพึ่งพิงระบบสารสนเทศ ความสามารถและความรู้ความเข้าใจด้านดิจิทัลของบุคลากร

๒. ความคุ้มค่าและความมั่นคงปลอดภัย พิจารณาความน่าเชื่อถือ ความมั่นคงปลอดภัยทางไซเบอร์ และความคุ้มค่าในการใช้งานทรัพยากรสารสนเทศที่มีอยู่ รวมถึงการจัดหาทรัพยากรเพิ่มเติม

๓. ความสอดคล้องทางยุทธศาสตร์ ตรวจสอบความสอดคล้องระหว่างกลยุทธ์ด้านดิจิทัลและยุทธศาสตร์องค์กรในภาพรวม โดยพิจารณาจากเป้าหมายผลตอบแทนในการลงทุน (Return on Investment ROI) หรือความคาดหวังเชิงคุณค่าสาธารณะ (Public Value)

๔. โอกาสและความท้าทาย พิจารณาประโยชน์ โอกาส และความท้าทายที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศปัจจุบันและเทคโนโลยีอุบัติใหม่ (Emerging Technologies) มาใช้

๕. โครงสร้างการตัดสินใจ กำหนดบทบาทหน้าที่ ความรับผิดชอบ และโครงสร้างการตัดสินใจ (Decision-making Structure) ที่เหมาะสม เพื่อให้การลงทุนด้านเทคโนโลยีดิจิทัลสร้างคุณค่าแก่องค์กรอย่างแท้จริง

๖. เกณฑ์การจัดลำดับความสำคัญ กำหนดเงื่อนไขหรือเกณฑ์ในการตัดสินใจเกี่ยวกับการดำเนินงานหรือการลงทุนที่สำคัญ โดยพิจารณาจากความเสี่ยง แผนการใช้งาน งบประมาณ และผลตอบแทนที่จะได้รับ

#### แนวทางปฏิบัติในการจัดทำงบประมาณและการอนุมัติ

- **การครอบคลุมต้นทุน** การจัดทำงบประมาณควรครอบคลุมทุกรายการที่เกี่ยวข้องกับการปฏิบัติงาน เช่น ทรัพย์สินสารสนเทศ การใช้ทรัพยากรส่วนกลาง บุคลากร ผู้ให้บริการภายนอก (Outsource) ค่าลิขสิทธิ์ และระบบรักษาความมั่นคงปลอดภัย

- **การอนุมัติและการสื่อสาร** แผนปฏิบัติการดิจิทัลและงบประมาณ ควรได้รับอนุมัติจากคณะกรรมการด้านเทคโนโลยีดิจิทัล หรือคณะกรรมการองค์การสะพานปลา และสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ

- **การติดตามผล** กำหนดเป้าหมายการดำเนินงาน และจัดให้มีวิธีการติดตามผลการดำเนินงานตามแผนงานและงบประมาณที่มีประสิทธิภาพ

๒.๑.๒ การจัดทำนโยบายการจัดสรร บริหารทรัพยากร และการจัดการบุคลากรด้านเทคโนโลยีดิจิทัล องค์กรควรจัดทำนโยบายการจัดสรรและบริหารทรัพยากร เพื่อให้มั่นใจว่าทรัพยากร (โดยเฉพาะบุคลากร) มีความเพียงพอ และบริหารจัดการความเสี่ยงจากการขาดแคลนทรัพยากร โดยพิจารณาแนวทาง ดังนี้

๑. กลยุทธ์การจัดหาทรัพยากร พิจารณาทางเลือกในการจัดหาและพัฒนาทรัพยากรให้เพียงพอต่อความต้องการในปัจจุบันและอนาคต รวมถึงแหล่งที่มาของทรัพยากร (Sourcing Strategy)

๒. หลักเกณฑ์การจัดสรร กำหนดหลักเกณฑ์ในการจัดสรรและบริหารทรัพยากร รวมถึงขีดความสามารถ (Capacity) เพื่อให้หน่วยงานด้านเทคโนโลยีดิจิทัลสามารถตอบสนองความต้องการขององค์กรได้ตามระดับสมรรถนะที่ต้องการ (SLA) ความเร่งด่วน และข้อจำกัดด้านงบประมาณ

๓. ความสอดคล้องกับโครงสร้างองค์กร จัดทำแผนการจัดสรรทรัพยากรและการจัดโครงสร้างภายในที่สอดคล้องกับการบริหารทรัพยากรบุคคลโดยรวมขององค์กร เพื่อความคุ้มค่าและลดความเสี่ยง

#### การอนุมัติและการติดตามผล

• นโยบายนี้ถือเป็นส่วนหนึ่งของการกำกับดูแลเทคโนโลยีดิจิทัล (EGIT) ซึ่งควรได้รับการอนุมัติจากคณะกรรมการ/คณะอนุกรรมการที่รับผิดชอบ มีการสื่อสารไปยังผู้เกี่ยวข้อง และมีการสอบทานปรับปรุงอย่างสม่ำเสมอ

• องค์กรควรกำหนดวิธีการติดตามและประเมินผลที่มีประสิทธิภาพ ประกอบด้วย

๔. การกำหนดเป้าหมายและตัวชี้วัด กำหนดเป้าหมาย ตัวชี้วัดความสำเร็จ (Key Performance Indicators KPIs) สำหรับการจัดสรรทรัพยากร

๕. การป้องกันรักษาทรัพยากร กำหนดหลักเกณฑ์ป้องกันการสูญเสียบุคลากรที่มีความเชี่ยวชาญ (Talent Management) และการป้องกันความเสียหายต่อทรัพย์สินสารสนเทศ

๖. การติดตามสมรรถนะ ติดตามผลการทำงานของทรัพยากร (บุคลากร ระบบงาน อุปกรณ์) เทียบกับเป้าหมาย หากพบข้อบกพร่องต้องตรวจสอบหาสาเหตุและวางแผนแก้ไขอย่างเหมาะสม

๒.๒ บทบาทหน้าที่ โครงสร้างองค์กร และการบริหารจัดการบุคลากรในการกำกับดูแลเทคโนโลยีดิจิทัลระดับองค์กรที่ดี

๒.๒.๑ บทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการเทคโนโลยีดิจิทัล องค์การสะพานปลา เพื่อให้การกำกับดูแลเป็นไปอย่างมีประสิทธิภาพ องค์การสะพานปลา (อสป.) ได้กำหนดบทบาทหน้าที่ไว้ ดังนี้

#### ผู้อำนวยการองค์การสะพานปลา และคณะผู้บริหาร

๑. การกำกับดูแลภาพรวม กำกับดูแลองค์กร จัดสรร และควบคุมทรัพยากรขององค์กรโดยรวม

๒. การส่งเสริมและสนับสนุน ส่งเสริมและสนับสนุนการขับเคลื่อนการบริหารจัดการเทคโนโลยีดิจิทัลขององค์กร

๓. **การมอบหมายอำนาจ** มอบหมายให้คณะกรรมการด้านเทคโนโลยีดิจิทัล ทำหน้าที่ให้คำปรึกษา แนะนำ และนำเสนอข้อมูลเชิงลึกด้านเทคโนโลยีดิจิทัลและนวัตกรรมทางการประมง พร้อมกำหนดทิศทางและกลยุทธ์ เพื่อผลักดันให้เกิดการกำกับดูแลที่ดี

๔. **การกำหนดขอบเขต** กำหนดขอบเขต วงรอบการกำกับดูแล และระบุผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง (ชาวประมง คู่ค้า พนักงาน)

๕. **การอนุมัตินโยบาย** อนุมัตินโยบายการกำกับดูแลเทคโนโลยีดิจิทัล และจัดให้มีการกำหนดขั้นตอน วิธีปฏิบัติงานให้สอดคล้องกับนโยบาย

๖. **การสื่อสารนโยบาย** สื่อสารนโยบาย ขั้นตอน และกระบวนการให้บุคลากรที่เกี่ยวข้องรับทราบ และสนับสนุนให้มีการปฏิบัติตามแบบเดียวกันทั่วทั้งองค์กร

๗. **การติดตามและสอบทาน** ติดตามเพื่อให้มั่นใจว่ากิจกรรมการกำกับดูแลดำเนินการอย่างมีประสิทธิภาพ อาทิ จัดให้มีการควบคุมภายในที่เหมาะสม มีการตรวจสอบโดยหน่วยตรวจสอบภายใน (Internal Audit) และมีการรายงานผลต่อคณะกรรมการองค์การสะพานปลาอย่างสม่ำเสมอ

๘. **การทบทวนนโยบาย** ทบทวนและปรับปรุงนโยบาย อย่างน้อยปีละ ๑ ครั้ง หรือทันทีเมื่อมีเหตุการณ์สำคัญที่อาจส่งผลกระทบต่อองค์กร

#### **คณะกรรมการด้านเทคโนโลยีดิจิทัล (หรือคณะทำงานที่ได้รับมอบหมาย)**

- หน้าที่หลัก ให้คำปรึกษา แนะนำ และนำเสนอข้อมูลเชิงลึกด้านเทคโนโลยีดิจิทัล นวัตกรรมทางการประมง และการบริหารจัดการท่าเทียบเรือประมง พร้อมทั้งกำหนดทิศทางและกลยุทธ์ เพื่อผลักดันให้เกิดการกำกับดูแลที่ดีแก่ผู้บริหาร รวมถึงติดตามผลการดำเนินงาน

#### **คุณสมบัติและการพัฒนาความรู้ของคณะกรรมการฯ**

- คณะกรรมการฯ ควรมีความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีดิจิทัล พัฒนาการของเทคโนโลยีที่เปลี่ยนแปลงไป รวมถึงความเสี่ยงที่เกี่ยวข้อง (เช่น ความเสี่ยงทางไซเบอร์ และ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) เพื่อกำหนดทิศทางให้สอดคล้องกับยุทธศาสตร์องค์กร

- คณะกรรมการฯ ควรได้รับการอบรมให้ความรู้เกี่ยวกับเทคโนโลยีดิจิทัลที่เกี่ยวข้องอย่างเพียงพอและสม่ำเสมอ

- คณะกรรมการบริหารความต่อเนื่องทางธุรกิจขององค์การสะพานปลา (Business Continuity Management Committee BCM Committee) มีหน้าที่ ดังนี้

(๑) กำหนดนโยบายการสร้างความต่อเนื่องของระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเป็นรูปธรรม ให้เป็นไปตามหลักเกณฑ์ที่สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) กำหนด

(๒) จัดสรรทรัพยากรและงบประมาณที่จำเป็นสำหรับการบริหารความต่อเนื่องทางธุรกิจขององค์การสะพานปลา เพื่อให้การดำเนินงานบรรลุเป้าหมายและเป็นไปตามวัตถุประสงค์

(๓) แต่งตั้งคณะทำงานเพื่อดำเนินการบริหารความต่อเนื่องทางธุรกิจขององค์การสะพานปลาได้ตามความเหมาะสม

(๔) ดำเนินการอื่น ๆ ตามที่ได้รับมอบหมายจากคณะกรรมการองค์การสะพานปลา

- คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล (หรือคณะทำงานด้านการพัฒนาดิจิทัล องค์การสะพานปลา) มีหน้าที่ ดังนี้

(๑) กำหนดหน้าที่ความรับผิดชอบ เพื่อเพิ่มประสิทธิภาพในการดำเนินงานด้วยการ พัฒนาระบบดิจิทัล

(๒) ติดตามดูแลวิธีการใช้ประโยชน์จากการพัฒนาดิจิทัลขององค์การสะพานปลา เพื่อให้เกิดประโยชน์สูงสุดต่อองค์กร

(๓) กำกับดูแลและติดตาม การจัดการกระบวนการป้องกันความเสียหาย การปรับปรุง รวมถึงเสนอแนะแนวทางปฏิบัติที่ดีด้านการบริหารจัดการสารสนเทศแก่ฝ่ายต่าง ๆ

(๔) กำหนดทิศทางการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Management BCM) ของระบบงานหลัก และกำกับให้มีการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis BIA)

(๕) ทบทวนการบริหารจัดการที่ดี เพื่อให้สอดคล้องกับกลยุทธ์ทางด้านเทคโนโลยี ดิจิทัลขององค์กร

(๖) ติดตามการประเมินศักยภาพของระบบสารสนเทศและการจัดการอย่างสม่ำเสมอ ทั้งมิติที่เกี่ยวกับตัวเงินและมีตัวเงิน

(๗) กำหนดกระบวนการเพื่อสร้างความมั่นใจถึงความสมดุล ระหว่างผลตอบแทนจาก การลงทุนด้านสารสนเทศ (Value Delivery) กับความเสี่ยงที่อาจเกิดขึ้น (Risk Optimization)

(๘) จัดสร้างเกณฑ์วัดคุณภาพงาน และผลสำเร็จของกลยุทธ์ นโยบาย หรือการจัดการ ด้านสารสนเทศที่กำหนดไว้

(๙) ควบคุมและผลักดันให้มีการดำเนินการตามมาตรฐานสากลด้านการรักษาความ มั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001) ในกิจกรรมตามแผนให้ครบถ้วน

(๑๐) กำหนดและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk) รวมถึงกำกับ ให้มีการบริหารจัดการความเสี่ยงตามองค์ประกอบอย่างครบถ้วน

(๑๑) จัดทำหรือทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศขององค์การสะพานปลา

(๑๒) ควบคุมการดำเนินงานด้านระบบสารสนเทศของทุกฝ่าย/สำนัก ให้สอดคล้องกับ เกณฑ์การประเมินผลการดำเนินงานรัฐวิสาหกิจ (SE-AM)

(๑๓) ปฏิบัติหน้าที่อื่น ๆ ตามที่ได้รับมอบหมาย

- คณะทำงานบริหารความต่อเนื่องทางธุรกิจขององค์การสะพานปลา (BCM Working Group) มีหน้าที่ ดังนี้

(๑) กำหนดโครงสร้างและหน้าที่ของทีมนักกู้คืนระบบเทคโนโลยีสารสนเทศ (Disaster Recovery Team)

(๒) ดำเนินการประเมินผลกระทบ กำหนดแนวทางการกู้คืนระบบเทคโนโลยีสารสนเทศที่สำคัญให้สามารถกลับมาให้บริการได้ตามระยะเวลาที่กำหนด (RTO/RPO) รวมถึงนำเสนอแนวทางการป้องกันหรือการรับมือเหตุการณ์วิกฤต

(๓) จัดทำ ทบทวน และปรับปรุงแผนการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT DRP) ขององค์กรสะพานปลา

(๔) ดำเนินการทดสอบแผนความต่อเนื่องของระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ และรายงานผลการทดสอบให้คณะกรรมการบริหารความต่อเนื่องทางธุรกิจ และคณะอนุกรรมการด้านเทคโนโลยีดิจิทัลรับทราบ

(๕) ปฏิบัติหน้าที่อื่น ๆ ตามที่ได้รับมอบหมาย

• ผู้อำนวยการองค์การสะพานปลา (หรือผู้มีอำนาจสั่งการตามโครงสร้างการบริหารขององค์กร) มีหน้าที่ ดังนี้

(๑) ติดตามการบริหารจัดการเทคโนโลยีดิจิทัล และทำให้มั่นใจว่าองค์การสะพานปลามีแผนการบูรณาการบริหารจัดการเทคโนโลยีดิจิทัลที่เหมาะสม สอดคล้องกับวิสัยทัศน์ พันธกิจ และเป้าหมายขององค์กร

(๒) ส่งเสริมนโยบายการบริหารจัดการเทคโนโลยีดิจิทัล (Tone at the Top) เพื่อให้มั่นใจว่าแนวปฏิบัติดังกล่าวได้รับการนำไปปฏิบัติอย่างเป็นรูปธรรมทั่วทั้งองค์กร

• ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer CIO) มีหน้าที่ ดังนี้

(๑) ดูแลรับผิดชอบการดำเนินงานด้านเทคโนโลยีสารสนเทศในภาพรวม โดยมีบทบาทในการกำหนดนโยบาย มาตรฐาน และการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

(๒) ติดตามการบริหารจัดการโครงการดิจิทัลที่สำคัญภายใต้สายบังคับบัญชา และทำให้มั่นใจได้ว่าองค์กรมีการบูรณาการระบบงานอย่างเหมาะสม

(๓) ส่งเสริมนโยบายการกำกับดูแล โดยผลักดันให้ผู้อำนวยการฝ่าย/สำนัก ให้ความสำคัญและตระหนักถึงความมั่นคงปลอดภัยและการบริหารจัดการเทคโนโลยีดิจิทัล

• ผู้อำนวยการฝ่าย / ผู้อำนวยการสำนัก มีหน้าที่ ดังนี้

(๑) รับนโยบาย แนวทาง และมาตรการด้านการบริหารจัดการเทคโนโลยีดิจิทัลไปดำเนินการในหน่วยงานของตน

(๒) ส่งเสริมให้บุคลากรทุกคนในหน่วยงานตระหนักถึงความสำคัญของการบริหารจัดการเทคโนโลยีดิจิทัล และการรักษาความมั่นคงปลอดภัยทางไซเบอร์

(๓) สนับสนุนให้บุคลากรมีส่วนร่วมในการปฏิบัติตามกรอบการกำกับดูแลเทคโนโลยีดิจิทัล

(๔) มอบหมายผู้รับผิดชอบในส่วนงาน เพื่อดำเนินการตามแนวปฏิบัติด้านการบริหารจัดการเทคโนโลยีดิจิทัล

- ผู้อำนวยการกอง หรือหัวหน้างาน (หรือตำแหน่งที่เทียบเท่า) มีหน้าที่ ดังนี้

(๑) ประเมินผลการดำเนินงานที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลในส่วนของการใช้งบประมาณ และการปฏิบัติงานประจำวันของหน่วยงาน

(๒) รายงานผลการดำเนินงาน ปัญหา และอุปสรรคที่เกี่ยวข้องกับระบบเทคโนโลยีดิจิทัล ต่อผู้บังคับบัญชาตามสายงาน

(๓) จัดทำรายงานติดตามผลการปฏิบัติงานด้านดิจิทัลที่อยู่ในความรับผิดชอบ

(๔) กำกับและติดตามการดำเนินการตามมาตรการด้านเทคโนโลยีดิจิทัลของบุคลากร ในสังกัด

- บุคลากรผู้ปฏิบัติงานด้านเทคโนโลยีดิจิทัล และพนักงานทั่วไป มีหน้าที่ ดังนี้

(๑) ดำเนินการและปฏิบัติงานตามแผนงาน นโยบาย และมาตรฐานด้านเทคโนโลยีดิจิทัลที่องค์กรกำหนด

(๒) รายงานผลการดำเนินงาน หรือแจ้งเหตุผิดปกติเกี่ยวกับระบบเทคโนโลยีดิจิทัลต่อผู้บังคับบัญชาตามสายงานโดยทันที

## ๒.๒.๒ โครงสร้างการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี

โครงสร้างองค์กรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี ควรมีผู้รับผิดชอบหลัก (Accountable Person) คือ คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล โดยต้องจัดให้มีโครงสร้างที่เอื้อต่อการกำกับดูแลอย่างเหมาะสม และสอดคล้องกับ หลักการแบ่งแยกหน้าที่ความรับผิดชอบ ๓ ระดับ (Three Lines of Defense) ทั้งนี้ โครงสร้างดังกล่าวต้องยึดหลักการถ่วงดุลอำนาจอย่างอิสระ (Check and Balance) และการแบ่งแยกหน้าที่อย่างเหมาะสม (Segregation of Duties) อันได้แก่

ระดับที่ ๑ หน่วยงานที่ทำหน้าที่ปฏิบัติงาน (First Line of Defense)

ระดับที่ ๒ หน่วยงานที่ทำหน้าที่กำกับดูแล (Second Line of Defense)

ระดับที่ ๓ หน่วยงานที่ทำหน้าที่ตรวจสอบ (Third Line of Defense)

**ระดับที่ ๑ หน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (First Line of Defense)**

หมายถึง บุคลากรหรือหน่วยงานที่ปฏิบัติงานทางด้านเทคโนโลยีสารสนเทศโดยตรง (เช่น ฝ่ายเทคโนโลยีสารสนเทศ) รวมถึงหน่วยงานที่เป็น "ผู้ใช้งานระบบ (Business Users)" ขององค์การสะพานปลา บุคลากรในกลุ่มนี้จัดเป็นผู้มีหน้าที่รับผิดชอบ (Responsible Person) ในการปฏิบัติงานให้บรรลุเป้าหมาย บริหารจัดการความเสี่ยงรายวัน และต้องปฏิบัติตามแนวทางการควบคุมและมาตรฐานที่องค์กรกำหนดอย่างเคร่งครัด

**ระดับที่ ๒ หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (Second Line of Defense)**

หมายถึง บุคลากรหรือหน่วยงานที่มีหน้าที่กำกับดูแลให้มีการปฏิบัติตามกฎระเบียบ นโยบาย และหลักเกณฑ์ต่าง ๆ โดยมีบทบาทในการกำหนดกรอบการบริหารความเสี่ยงด้านเทคโนโลยี

สารสนเทศ สื่อสารความเสี่ยงใหม่ ๆ ที่เกิดขึ้น ติดตามและสนับสนุนกระบวนการกำกับดูแล (IT Governance) ตลอดจนประเมินความเพียงพอของการควบคุมภายใน บุคลากรในกลุ่มนี้อาจประกอบด้วย ฝ่ายบริหารความเสี่ยง หน่วยงานกำกับการปฏิบัติตามกฎหมาย (Compliance) และคณะทำงานด้านเทคโนโลยีดิจิทัล

### ระดับที่ ๓ หน่วยงานที่ทำหน้าที่ตรวจสอบด้านเทคโนโลยีสารสนเทศ (Third Line of Defense)

หมายถึง บุคลากรหรือหน่วยงานที่มีหน้าที่ในการตรวจสอบการปฏิบัติงานของหน่วยงาน ระดับที่ ๑ และระดับที่ ๒ อย่างเป็นอิสระ เพื่อให้คณะกรรมการองค์การสะพานปลาและผู้บริหารระดับสูงมั่นใจว่า มีการปฏิบัติตามนโยบาย มาตรฐาน และกฎหมาย (เช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์) อย่างถูกต้องและมีประสิทธิภาพ บุคลากรในกลุ่มนี้ได้แก่ ฝ่ายตรวจสอบภายใน (Internal Audit) หรือผู้ตรวจสอบอิสระจากภายนอก



### ๓. กรอบการกำกับดูแลด้านการดำเนินงานให้มีประสิทธิภาพและมีความโปร่งใส (Performance Measurement and Stakeholder Transparency Framework Setting)

๓.๑ การกำกับดูแลด้านการดำเนินงานให้มีประสิทธิภาพ องค์การสะพานปลา ตระหนักถึงความสำคัญของการกำกับดูแลกิจการที่ดี (Good Corporate Governance) โดยมุ่งมั่นในการเสริมสร้างและพัฒนาแนวทางการปฏิบัติงานตามหลักธรรมาภิบาลที่สามารถปฏิบัติได้จริง เพื่อเป็นการเสริมสร้างและจัดให้มีระบบการบริหารจัดการที่ดีในรัฐวิสาหกิจ บรรลุวัตถุประสงค์ในการดำเนินงานอย่างโปร่งใส มีความรับผิดชอบ

ต่อสังคมและสิ่งแวดล้อม ตามหลักการและแนวทางการกำกับดูแลกิจการที่ดีในรัฐวิสาหกิจ ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) กระทรวงการคลัง

**๓.๒ นโยบายการกำกับดูแลกิจการที่ดี** องค์การสะพานปลา มีเจตนารมณ์ที่จะส่งเสริมให้ผู้บริหาร พนักงาน และบุคลากรผู้ปฏิบัติงาน ดำเนินงานด้วยความโปร่งใส เป็นธรรม และตรวจสอบได้ อันจะส่งผลให้องค์กรเติบโตอย่างยั่งยืนบนรากฐานที่มั่นคงและแข็งแกร่ง จึงได้กำหนดนโยบายการกำกับดูแลกิจการที่ดีและการแสดงความรับผิดชอบต่อสังคม ดังนี้

๑. ให้ผู้บริหาร พนักงาน และบุคลากรผู้ปฏิบัติงาน ดำเนินงานโดยยึดหลักการกำกับดูแลกิจการที่ดี ๗ ประการ คือ

(๑) ความรับผิดชอบต่อผลการปฏิบัติหน้าที่ (Accountability)

(๒) ความสำนึกในหน้าที่ด้วยขีดความสามารถและประสิทธิภาพที่เพียงพอ (Responsibility)

(๓) การปฏิบัติต่อผู้มีส่วนได้ส่วนเสียโดยสุจริต และคำนึงถึงความเท่าเทียมกัน (Equitable Treatment)

(๔) ความโปร่งใส (Transparency)

(๕) การสร้างมูลค่าเพิ่มแก่กิจการทั้งในระยะสั้นและระยะยาว (Value Creation)

(๖) การส่งเสริมพัฒนาการกำกับดูแล และจรรยาบรรณที่ดีในการดำเนินงาน (Ethics)

(๗) การมีส่วนร่วม โดยส่งเสริมให้เกิดการกระจายโอกาสแก่ประชาชนและผู้มีส่วนได้ส่วนเสีย (เช่น เกษตรกร ชาวประมง ชุมชนโดยรอบท่าเทียบเรือ) ให้มีส่วนร่วมในการแสดงความคิดเห็นเกี่ยวกับการดำเนินการใด ๆ ที่อาจมีผลกระทบต่อสิ่งแวดล้อม สุขภาพอนามัย คุณภาพชีวิต และความเป็นอยู่ของชุมชนหรือท้องถิ่น (Participation)

๒. ผู้บริหารระดับสูงต้องเป็นผู้นำและต้นแบบ (Tone at the Top) ที่แสดงให้เห็นถึงความมุ่งมั่นต่อการปฏิบัติตามกฎหมายและมีจริยธรรม รวมถึงสร้างบรรยากาศในองค์กร สร้างแรงจูงใจ และกำกับดูแลให้พนักงานและบุคลากรร่วมกันปฏิบัติตามกฎหมายและจรรยาบรรณอย่างเคร่งครัด

๓. ส่งเสริมให้ผู้บริหาร พนักงาน และบุคลากร ปฏิบัติงานด้วยความทุ่มเท รับผิดชอบต่อบทบาทหน้าที่ที่ได้รับมอบหมาย โดยยึดมั่นผลประโยชน์ขององค์การสะพานปลาเป็นสำคัญ และบริหารจัดการด้วยหลักคุณธรรม มีความรับผิดชอบต่อผู้มีส่วนได้ส่วนเสีย สังคม และสิ่งแวดล้อม

จากโครงสร้างการกำกับดูแลกิจการที่ดีขององค์การสะพานปลา จะเห็นว่าการกำกับดูแลกิจการที่ดีและการแสดงความรับผิดชอบต่อสังคม มีโครงสร้างที่สอดคล้องกับแนวคิดการกำกับดูแลของ OECD และ สคร. กล่าวคือ มีโครงสร้างการบริหารระดับนโยบาย (Policy Management) โดยคณะกรรมการองค์การสะพานปลา ได้มอบหมายหรือแต่งตั้งคณะกรรมการ/คณะทำงานที่เกี่ยวข้อง เพื่อรับนโยบายลงมาปฏิบัติ และมีการบริหารงานประจำวัน (Daily Management) โดยบูรณาการร่วมกับงานบริหารความเสี่ยง ซึ่งทำหน้าที่เป็นผู้ประสานงาน (Coordinator) กับฝ่าย/กอง/สำนัก ที่เกี่ยวข้อง ทั้งนี้ ข้อมูลที่สะท้อนถึงการกำกับดูแลกิจการที่ดีขององค์การสะพานปลา ประกอบด้วย

- ๑) การปฏิบัติหน้าที่ของคณะกรรมการองค์การสะพานปลา
- ๒) การบริหารความเสี่ยง (Risk Management)
- ๓) การตรวจสอบภายใน (Internal Audit)
- ๔) การควบคุมภายใน (Internal Control)
- ๕) การเปิดเผยสารสนเทศด้วยความโปร่งใส (Information Disclosure)
- ๖) การปฏิบัติตามกฎหมาย จริยธรรม และจรรยาบรรณ (Compliance)
- ๗) การแสดงความรับผิดชอบต่อสังคม (CSR/Sustainability)

ทั้งนี้ เพื่อสร้างความโปร่งใสในการดำเนินงาน เพิ่มคุณค่าให้กับองค์กรในระยะยาว คำนึงถึงผู้มีส่วนได้ส่วนเสียทุกภาคส่วน สร้างความสามารถในการแข่งขัน และเพื่อให้องค์การสะพานปลามีความเจริญเติบโตอย่างยั่งยืน

**๓.๓ ความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Transparency)** เพื่อให้มั่นใจว่า การรายงานและการสื่อสารผลการดำเนินงานด้านการบริหารจัดการเทคโนโลยีดิจิทัลกับผู้มีส่วนได้ส่วนเสีย มีประสิทธิภาพและทันเวลา การดำเนินงานโดยรวมควรมีการพัฒนาอย่างต่อเนื่อง และวัตถุประสงค์รวมทั้งกลยุทธ์ที่เกี่ยวข้องกับเทคโนโลยีดิจิทัลต้องมีความสอดคล้องกับแผนวิสาหกิจขององค์กร ซึ่งมีแนวทางปฏิบัติที่ควรพิจารณา ดังนี้

#### **(๑) การประเมินความต้องการของผู้มีส่วนได้ส่วนเสียในการรายงานผลการดำเนินงาน**

- องค์กรควรพิจารณาข้อกำหนดด้านการรายงานภาคบังคับ (Mandatory Reporting) ทั้งในปัจจุบันและอนาคตที่เกี่ยวข้องกับการใช้เทคโนโลยีดิจิทัลภายในองค์กร (เช่น การรายงานตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์) รวมทั้งกำหนดขอบเขตและกรอบระยะเวลาในการรายงานที่เหมาะสม
- นอกเหนือจากประเด็นข้างต้น การรายงานยังต้องพิจารณาถึงความต้องการข้อมูลข่าวสารสำหรับผู้มีส่วนได้ส่วนเสียอื่น ๆ ทั้งในปัจจุบันและอนาคต รวมถึงขอบเขตและเงื่อนไขในการรายงานที่แตกต่างกัน
- องค์กรควรจัดให้มีหลักเกณฑ์การรายงานต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร รวมทั้งรูปแบบและช่องทางการสื่อสารที่เหมาะสม

#### **(๒) การสื่อสารผลการดำเนินงานและบริหารจัดการเทคโนโลยีดิจิทัลที่เหมาะสม**

- องค์กรควรมีการกำหนดกลยุทธ์และแผนการสื่อสาร (Communication Plan) กับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร
- ควรมีการกำหนดวิธีการสอบทานเพื่อให้มั่นใจว่า ข้อมูลการรายงานเป็นไปตามหลักเกณฑ์สำหรับข้อกำหนดของการรายงานภาคบังคับขององค์กรทั้งหมด
- ควรมีกระบวนการในการตรวจสอบความถูกต้องและอนุมัติรายงานก่อนเผยแพร่
- มีกระบวนการและลำดับชั้นการรายงานที่ชัดเจน

### (๓) การติดตามการสื่อสารกับผู้มีส่วนได้ส่วนเสีย

- องค์กรควรมีการประเมินประสิทธิภาพของการรายงานผลอย่างสม่ำเสมอ เพื่อให้มั่นใจในความถูกต้องและความน่าเชื่อถือของรายงานที่จัดทำขึ้น
- องค์กรควรมีการประเมินประสิทธิภาพของวิธีการสื่อสารและผลลัพธ์ของการสื่อสารกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร (เช่น การสำรวจการรับรู้) และประเมินว่าการสื่อสารดังกล่าวสามารถตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียที่หลากหลายได้อย่างครบถ้วนหรือไม่

### ๓.๔ การปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล (IT Compliance)

องค์การสะพานปลา (อสป.) ให้ความสำคัญสูงสุดในการดำเนินงานภายใต้กรอบของกฎหมาย ระเบียบ และข้อบังคับของรัฐ เพื่อสร้างความตระหนักรู้ ความโปร่งใส และความน่าเชื่อถือให้แก่ผู้มีส่วนได้ส่วนเสีย ทั้งชาวประมง ผู้ประกอบการแพปลา และประชาชนทั่วไป โดยการพัฒนาและบริหารจัดการเทคโนโลยีดิจิทัลขององค์กร จะต้องสอดคล้องกับกฎหมายสำคัญ ซึ่งสามารถแบ่งออกเป็น ๓ กลุ่มหลัก ดังนี้

#### กลุ่มที่ ๑ กฎหมายด้านการบริหารงาน นโยบาย และการให้บริการภาครัฐ (Policy and Digital Government)

เป็นกลุ่มกฎหมายแม่บทที่ใช้กำหนดนโยบายและทิศทางการเปลี่ยนผ่านสู่รัฐบาลดิจิทัล เพื่อลดขั้นตอนและอำนวยความสะดวกแก่ประชาชน ได้แก่

- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ องค์การสะพานปลาต้องปรับปรุงกระบวนการทำงานและการให้บริการให้เทียบเรือให้เป็นรูปแบบดิจิทัล (Digital Service) รวมถึงต้องมีการบูรณาการเชื่อมโยงข้อมูล (Data Integration) กับหน่วยงานรัฐอื่น ๆ เช่น กระทรวงเกษตรและสหกรณ์ และกรมประมง ผ่านศูนย์กลางข้อมูลภาครัฐ
- พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ๒๕๖๐ เพื่อกำหนดทิศทางการนำเทคโนโลยีดิจิทัลมาใช้ในการบริหารจัดการเทียบเรือให้สอดคล้องกับแผนระดับชาติ

#### กลุ่มที่ ๒ กฎหมายด้านธุรกรรมทางอิเล็กทรอนิกส์และโครงสร้างพื้นฐาน (Electronic Transactions and Infrastructure)

เป็นกลุ่มกฎหมายที่สนับสนุนให้เกิดความเชื่อมั่นในการทำธุรกรรมทางออนไลน์และการใช้เอกสารอิเล็กทรอนิกส์ขององค์การสะพานปลา ได้แก่

- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ (และที่แก้ไขเพิ่มเติม) เพื่อรองรับผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ เช่น การใช้ลายมือชื่ออิเล็กทรอนิกส์ (e-Signature) ในการทำสัญญาเช่าพื้นที่ท่าเทียบเรือ การออกใบเสร็จรับเงินอิเล็กทรอนิกส์ (e-Receipt/e-Tax Invoice) รวมไปถึงการใช้ระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID) สำหรับผู้ประกอบการและชาวประมงที่เข้าใช้บริการระบบของ อสป.

### กลุ่มที่ ๓ กฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล (Cybersecurity and Data Protection)

เป็นกลุ่มกฎหมายที่มุ่งเน้นการปกป้องระบบสารสนเทศและสิทธิขั้นพื้นฐานของประชาชน ซึ่งองค์การสะพานปลาต้องปฏิบัติตามอย่างเคร่งครัด ได้แก่

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (และที่แก้ไขเพิ่มเติม) องค์การต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Files) ของระบบเครือข่ายและระบบให้บริการอย่างน้อย ๙๐ วัน เพื่อใช้เป็นหลักฐานกรณีเกิดเหตุละเมิด

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ องค์การสะพานปลาต้องประเมินและยกระดับโครงสร้างพื้นฐานสารสนเทศให้มีความมั่นคงปลอดภัย มีแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Plan) และจัดให้มีการประเมินความเสี่ยงตามมาตรฐานสากล (ISO/IEC 27001)

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ในการพัฒนาระบบดิจิทัลที่มีการประมวลผลข้อมูลส่วนบุคคลของชาวประมง ผู้ประกอบการ บุคลากร และผู้มาติดต่อ องค์การสะพานปลาต้องปฏิบัติตามดังนี้

(ก) ฐานทางกฎหมาย (Legal Basis) การเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูล ต้องดำเนินการภายใต้ฐานความจำเป็นเพื่อการปฏิบัติหน้าที่ตามกฎหมายของหน่วยงานรัฐ (Public Task/Legal Obligation) ฐานสัญญา (Contract) หรือฐานความยินยอม (Consent)

(ข) การลดจำนวนข้อมูล (Data Minimization) ห้ามจัดเก็บข้อมูลส่วนบุคคลเกินกว่าความจำเป็นต่อวัตถุประสงค์ในการให้บริการหรือการดำเนินงาน

(ค) สิทธิของเจ้าของข้อมูล ต้องจัดให้มีช่องทาง (Privacy Notice & Consent Form) ที่ชัดเจน เพื่อรองรับการใช้สิทธิของเจ้าของข้อมูล เช่น สิทธิขอเข้าถึง ขอแก้ไข หรือขอลบข้อมูล

(ง) ระยะเวลาการจัดเก็บ (Retention Period) กำหนดระยะเวลาจัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็นตามอายุความ หรือไม่เกิน ๕-๑๐ ปี (ขึ้นอยู่กับประเภทเอกสาร) และต้องมีแนวทางการลบหรือทำลายข้อมูลอย่างปลอดภัยเมื่อพ้นกำหนด

(จ) การประเมินผลกระทบ (DPIA) หากองค์การสะพานปลามีการออกแบบระบบงานใหม่ หรือนำเทคโนโลยีใหม่มาใช้ประมวลผลข้อมูลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคล ต้องจัดทำแบบประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment DPIA) ก่อนเริ่มโครงการทุกครั้ง

#### ๓.๔ การปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล (IT Compliance)

รัฐบาลได้ผลักดันการออกกฎหมายที่เกี่ยวกับการส่งเสริมและพัฒนาเศรษฐกิจและสังคมดิจิทัล เพื่อเป็นรากฐานในการขับเคลื่อนการดำเนินงานด้านรัฐบาลอิเล็กทรอนิกส์ (e-Government) โดย

องค์การสะพานปลา (อสป.) ในฐานะหน่วยงานของรัฐ มีหน้าที่ต้องทำความเข้าใจและปฏิบัติตามกฎหมายระเบียบ และข้อบังคับที่เกี่ยวข้องอย่างเคร่งครัด ดังตารางสรุปต่อไปนี้

ตารางที่ ๑ สรุปกฎหมายเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการดำเนินงานขององค์กร

| ลำดับ | กฎหมาย ระเบียบ ข้อบังคับ                                                                  | สาระสำคัญและเหตุการณ์นำไปปฏิบัติขององค์การสะพานปลา                                                                                                                                                                                                                                                                                                            |
|-------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ๑     | พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (และที่แก้ไขเพิ่มเติม)                       | <p><b>สาระสำคัญ</b> เป็นกฎหมายพื้นฐานที่รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ให้มีผลเสมอกับการทำเป็นหนังสือ และรับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ (e-Signature)</p> <p><b>การนำไปปฏิบัติ</b> เพื่อให้อสป. สามารถให้บริการทำสัญญาทางอิเล็กทรอนิกส์กับคู่ค้าและชาวประมง รวมถึงการใช้อยานหลักฐานทางอิเล็กทรอนิกส์ได้อย่างถูกต้องและมีความน่าเชื่อถือ</p> |
|       | ๑.๑ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙  | <p><b>สาระสำคัญ</b> กำหนดให้หน่วยงานรัฐที่ให้บริการทางระบบอิเล็กทรอนิกส์ (เช่น การยื่นคำขอจดทะเบียน ชำระเงิน) ต้องมีระบบที่ได้มาตรฐาน</p> <p><b>การนำไปปฏิบัติ</b> อสป. ต้องจัดให้มีระบบเอกสารอิเล็กทรอนิกส์ นโยบายความมั่นคงปลอดภัย และนโยบายคุ้มครองข้อมูลส่วนบุคคล เพื่อสร้างความเชื่อมั่นแก่ประชาชนผู้มาใช้บริการ</p>                                     |
|       | ๑.๒ พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓           | <p><b>สาระสำคัญ</b> กำหนดระดับความปลอดภัยในการทำธุรกรรม (ระดับพื้นฐาน ระดับกลาง ระดับเคร่งครัด) ตามความสำคัญของภารกิจ</p> <p><b>การนำไปปฏิบัติ</b> อสป. ต้องประเมินและจัดระดับความปลอดภัยของระบบงานสารสนเทศขององค์กรให้เหมาะสมและเตรียมความพร้อมในการรับมือสถานการณ์ฉุกเฉิน</p>                                                                               |
| ๒     | พระราชบัญญัติว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (และที่แก้ไขเพิ่มเติม) | <p><b>สาระสำคัญ</b> กำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ (เช่น การเจาะระบบ การโจมตีด้วยไวรัส)</p> <p><b>การนำไปปฏิบัติ</b> อสป. ต้องมีระบบป้องกันเครือข่ายที่รัดกุม และต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Files) เพื่อใช้เป็นหลักฐานและป้องกันผลกระทบต่อเศรษฐกิจและความมั่นคง</p>                                                     |

| ลำดับ | กฎหมาย ระเบียบ ข้อบังคับ                                                            | สาระสำคัญและเหตุผลการนำไปปฏิบัติ<br>ขององค์การสะพานปลา                                                                                                                                                                                                                                                                                                  |
|-------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ๓     | พระราชบัญญัติข้อมูลข่าวสารของ<br>ราชการ พ.ศ. ๒๕๔๐                                   | <p>สาระสำคัญ มุ่งเน้นความโปร่งใสและเปิดโอกาสให้<br/>ประชาชนตรวจสอบการดำเนินงานของรัฐ ผ่านการเปิดเผย<br/>ข้อมูลข่าวสาร</p> <p>การนำไปปฏิบัติ อสป. ต้องจัดทำและเปิดเผยข้อมูลผ่าน<br/>ช่องทางอิเล็กทรอนิกส์ โดยจัดทำเป็นชุดข้อมูล (Data Set)<br/>ที่นำไปต่อยอดได้ พร้อมทั้งมีมาตรการระมัดระวังไม่เปิดเผย<br/>ข้อมูลส่วนบุคคลหรือข้อมูลด้านความมั่นคง</p>   |
| ๔     | พระราชบัญญัติลิขสิทธิ์ พ.ศ.<br>๒๕๓๗ (และที่แก้ไขเพิ่มเติม)                          | <p>สาระสำคัญ คุ้มครองทรัพย์สินทางปัญญาและป้องกันการ<br/>ละเมิดลิขสิทธิ์ในยุคดิจิทัล เช่น การทำซ้ำ ดัดแปลง หรือ<br/>หลีกเลี่ยงมาตรการทางเทคโนโลยี</p> <p>การนำไปปฏิบัติ อสป. ต้องบริหารจัดการลิขสิทธิ์<br/>ซอฟต์แวร์ขององค์กรอย่างถูกต้อง และป้องกันมิให้<br/>บุคลากรใช้คอมพิวเตอร์ขององค์กรในการละเมิดผลงานของ<br/>ผู้อื่น</p>                          |
| ๕     | พระราชบัญญัติการอำนวยความสะดวก<br>สะดวกในการพิจารณาอนุญาตของ<br>ทางราชการ พ.ศ. ๒๕๕๘ | <p>สาระสำคัญ กำหนดให้ส่วนราชการจัดทำคู่มือสำหรับ<br/>ประชาชน และเปิดเผยผ่านช่องทางอิเล็กทรอนิกส์ เพื่อลด<br/>ขั้นตอนการติดต่อราชการ</p> <p>การนำไปปฏิบัติ อสป. ต้องจัดทำคู่มือการให้บริการ (เช่น<br/>การขอใช้พื้นที่ท่าเทียบเรือ) และจัดให้มีระบบที่สามารถยื่น<br/>คำขอและเอกสารหลักฐานผ่านช่องทางอิเล็กทรอนิกส์แทน<br/>การเดินทางมาด้วยตนเอง</p>       |
| ๖     | พระราชบัญญัติการพัฒนาดิจิทัล<br>เพื่อเศรษฐกิจและสังคม พ.ศ.<br>๒๕๖๐                  | <p>สาระสำคัญ เป็นกฎหมายแม่บทที่กำหนดนโยบายและแผน<br/>ระดับชาติ เพื่อบูรณาการการใช้เทคโนโลยีดิจิทัลของภาครัฐ<br/>ให้คุ้มค่าและเชื่อมโยงกัน</p> <p>การนำไปปฏิบัติ แผนปฏิบัติการดิจิทัลของ อสป. ต้อง<br/>สอดคล้องกับแผนระดับชาติ โดยมุ่งเน้นการแบ่งปัน<br/>ทรัพยากร (Resource Optimization) การสร้างนวัตกรรม<br/>และลดความเหลื่อมล้ำในการเข้าถึงบริการ</p> |
| ๗     | พระราชบัญญัติคุ้มครองข้อมูลส่วน<br>บุคคล พ.ศ. ๒๕๖๒ (PDPA)                           | <p>สาระสำคัญ กำหนดหลักเกณฑ์และมาตรการคุ้มครอง<br/>ข้อมูลส่วนบุคคล เพื่อป้องกันการล่วงละเมิดสิทธิความเป็น<br/>ส่วนตัวและให้มีมาตรการเยียวยา</p>                                                                                                                                                                                                          |

| ลำดับ | กฎหมาย ระเบียบ ข้อบังคับ                                | สาระสำคัญและเหตุการณ์นำไปปฏิบัติ<br>ขององค์การสะพานปลา                                                                                                                                                                                                                                                  |
|-------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |                                                         | <b>การนำไปปฏิบัติ</b> อสป. ต้องมีมาตรการจัดเก็บ ใช้ และเปิดเผยข้อมูลของชาวประมง คู่ค้า และบุคลากรอย่างรัดกุม มีการขอความยินยอมตามกฎหมาย และกำหนดระยะเวลาจัดเก็บ (Retention Period) ที่ชัดเจน                                                                                                            |
| ๘     | พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ | <b>สาระสำคัญ</b> ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อย<br><b>การนำไปปฏิบัติ</b> อสป. ต้องยกระดับความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสารสนเทศ จัดทำแผนรับมือเหตุฉุกเฉิน และประสานงานกับหน่วยงานที่เกี่ยวข้องเมื่อเกิดภัยคุกคามทางไซเบอร์ |

๔. กรอบการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล (Digital Risk Optimization Framework Setting)

องค์การสะพานปลา (อสป.) ตระหนักดีว่าการนำเทคโนโลยีดิจิทัลมาใช้ขับเคลื่อนองค์กร นั้นมาพร้อมกับความเสี่ยงในรูปแบบใหม่ ๆ โดยเฉพาะภัยคุกคามทางไซเบอร์และการรั่วไหลของข้อมูล เพื่อให้การดำเนินงานบรรลุเป้าหมายตามยุทธศาสตร์ คณะกรรมการองค์การสะพานปลา และคณะอนุกรรมการด้านเทคโนโลยีดิจิทัล จึงได้กำหนดกรอบการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล ให้สอดคล้องกับมาตรฐาน ISO/IEC 27001 และหลักการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management ERM) ดังนี้



**๔.๑ หลักการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล (IT Risk Principles)** การบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัลขององค์กร ต้องตั้งอยู่บนหลักการสำคัญ ๓ ประการ ได้แก่

(๑) ความเสี่ยงด้านเทคโนโลยีดิจิทัลต้องถูกบูรณาการเข้าเป็นส่วนหนึ่งของการบริหารความเสี่ยงระดับองค์กร (ERM)

(๒) การตัดสินใจลงทุนหรือดำเนินโครงการดิจิทัลใด ๆ ต้องพิจารณาถึงความสมดุลระหว่างผลประโยชน์ที่จะได้รับ (Value Delivery) และความเสี่ยงที่อาจเกิดขึ้น (Risk Optimization) โดยความเสี่ยงต้องอยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite)

(๓) ต้องมีการสื่อสารและสร้างความตระหนักรู้ด้านความเสี่ยงทางไซเบอร์ให้แก่บุคลากรทุกระดับอย่างต่อเนื่อง

**๔.๒ กระบวนการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล (IT Risk Management Process)** องค์กรสะพานปลากำหนดให้มีกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัลที่เป็นมาตรฐานเดียวกัน (Standardized Practice) และทำซ้ำได้ (Repeatable Practice) ประกอบด้วยขั้นตอนดังนี้

**๔.๒.๑ การระบุความเสี่ยง (Risk Identification)**

• จัดทำและทบทวน ทะเบียนทรัพย์สินสารสนเทศ (IT Asset Inventory) อย่างสม่ำเสมอ เพื่อระบุระบบงาน ข้อมูล โครงสร้างพื้นฐาน และบุคลากรที่สำคัญต่อภารกิจขององค์กร

• ระบุภัยคุกคาม (Threats) และช่องโหว่ (Vulnerabilities) ที่อาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของระบบสารสนเทศ

**๔.๒.๒ การประเมินความเสี่ยง (Risk Assessment)**

• ประเมินโอกาสที่จะเกิดเหตุการณ์ (Likelihood) และผลกระทบ (Impact) ที่มีต่อองค์กร ทั้งในด้านการเงิน การดำเนินงาน กฎหมาย และชื่อเสียง

• กำหนดระดับความเสี่ยง (Risk Level) เพื่อจัดลำดับความสำคัญในการจัดการ

**๔.๒.๓ การจัดการและตอบสนองต่อความเสี่ยง (Risk Treatment)** กำหนดกลยุทธ์ในการตอบสนองต่อความเสี่ยง ๔ แนวทาง ได้แก่

• การยอมรับความเสี่ยง (Accept) กรณีที่ความเสี่ยงอยู่ในระดับที่ยอมรับได้ (Risk Appetite) หรือต้นทุนในการจัดการสูงกว่าผลกระทบ

• การลดความเสี่ยง (Mitigate) การนำมาตรการควบคุม (Controls) ตามมาตรฐาน ISO/IEC 27001 มาบังคับใช้ เช่น การติดตั้งระบบ Firewall, การจัดการสิทธิการเข้าถึง (Access Control)

• การถ่ายโอนความเสี่ยง (Transfer) เช่น การทำประกันภัยความเสี่ยงทางไซเบอร์ (Cyber Insurance) หรือการใช้บริการ Outsource ที่มีมาตรฐานความปลอดภัยรองรับ

- การหลีกเลี่ยงความเสี่ยง (Avoid) การยุติหรือยกเลิกกิจกรรมที่ก่อให้เกิดความเสี่ยงสูงเกินกว่าที่องค์กรจะรับได้

#### ๔.๒.๔ การติดตามและรายงานผล (Risk Monitoring and Reporting)

- หน่วยงานที่รับผิดชอบต้องติดตามสถานะความเสี่ยงอย่างต่อเนื่อง และประเมินประสิทธิผลของมาตรการควบคุม (Control Effectiveness)
- จัดทำรายงานสรุปความเสี่ยงด้านเทคโนโลยีดิจิทัล (IT Risk Register Report) นำเสนอต่อคณะกรรมการด้านเทคโนโลยีดิจิทัล และคณะกรรมการบริหารความเสี่ยงระดับองค์กร อย่างน้อยไตรมาสละ ๑ ครั้ง

๔.๓ การบูรณาการการคุ้มครองข้อมูลส่วนบุคคลในกระบวนการบริหารความเสี่ยง (PDPA Risk Integration) เนื่องจากองค์การสะพานปลามีการประมวลผลข้อมูลของชาวประมง คู่ค้า และบุคลากร องค์กรจึงกำหนดมาตรการบริหารความเสี่ยงที่สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังนี้

(๑) การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment DPIA) กำหนดให้ทุกโครงการดิจิทัลที่มีการนำเทคโนโลยีใหม่มาใช้ หรือมีการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูง ต้องดำเนินการประเมิน DPIA ก่อนเริ่มโครงการเสมอ เพื่อค้นหาและลดความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูล

(๒) การเก็บรวบรวมข้อมูลเท่าที่จำเป็น (Data Minimization) มาตรการลดความเสี่ยง ตั้งแต่ต้นทาง โดยห้ามจัดเก็บข้อมูลส่วนบุคคลเกินกว่าความจำเป็นต่อวัตถุประสงค์ในการปฏิบัติงานหรือการให้บริการ

(๓) ฐานทางกฎหมายและการใช้สิทธิ (Legal Basis & Data Subject Rights) การประมวลผลข้อมูลต้องมีฐานทางกฎหมายรองรับ (เช่น ฐานการปฏิบัติหน้าที่ของรัฐ ฐานสัญญา หรือฐานความยินยอม) และระบบสารสนเทศต้องได้รับการออกแบบให้รองรับการใช้สิทธิของเจ้าของข้อมูล (เช่น สิทธิขอเข้าถึง แก้ไข หรือลบข้อมูล)

(๔) ระยะเวลาการจัดเก็บและการทำลาย (Retention & Disposal) ข้อมูลส่วนบุคคลจะถูกจัดเก็บตามระยะเวลาที่กฎหมายกำหนด หรือไม่เกิน ๕-๑๐ ปี (ตามประเภทเอกสาร) โดยเมื่อพ้นกำหนดระยะเวลา องค์กรต้องมีกระบวนการหรือมาตรการทางเทคนิคในการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้อย่างปลอดภัย เพื่อป้องกันความเสี่ยงข้อมูลหลุดรอด

๔.๔ การเตรียมความพร้อมรับมือเหตุการณ์คุกคามทางไซเบอร์ (Cybersecurity Incident Response) เพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ องค์กรต้องจัดทำ “แผนรับมือเหตุการณ์คุกคามทางไซเบอร์ (Incident Response Plan)” โดยกำหนดขั้นตอนการตรวจจับ การยับยั้ง การแก้ไขฟื้นฟู และการรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยต่อคณะกรรมการฯ และหน่วยงานกำกับดูแลภาครัฐ (สกมช. หรือ สคส.) ภายในระยะเวลาที่กฎหมายกำหนด (เช่น ภายใน ๗๒ ชั่วโมง กรณีข้อมูลส่วนบุคคลรั่วไหล)

## ๕. การกำหนดหลักการการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance Guiding Principles)

### ๕.๑ การกำหนดและรักษากรอบการกำกับดูแลและบริหารจัดการ (Governance Framework Setting and Maintenance)

เพื่อให้การกำกับดูแลและบริหารจัดการเทคโนโลยีดิจิทัลขององค์การสะพานปลา มีความสอดคล้องกับวัตถุประสงค์เชิงยุทธศาสตร์ขององค์กร มีประสิทธิภาพ มีความโปร่งใส และเป็นไปตามกฎหมาย ระเบียบ และข้อบังคับต่าง ๆ อย่างเคร่งครัด คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล (หรือคณะกรรมการที่ได้รับมอบหมาย) ต้องพิจารณากำหนดและจัดทำ "นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีดิจิทัลระดับองค์กรที่ดี (Enterprise Governance of IT Policy)" เพื่อใช้เป็นกรอบมาตรฐานในการควบคุมระบบและกระบวนการทางด้านสารสนเทศ โดยนโยบายดังกล่าวต้องครอบคลุมองค์ประกอบหลักอย่างน้อย ๓ ประการ ดังนี้

(๑) การบริหารจัดการความเสี่ยงด้านเทคโนโลยีดิจิทัล (IT Risk Management) ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการกำหนดมาตรการควบคุมความเสี่ยง (รวมถึงความเสี่ยงทางไซเบอร์และความเสี่ยงด้านการละเมิดข้อมูลส่วนบุคคล) ให้อยู่ในระดับที่องค์กรยอมรับได้ (Risk Appetite)

(๒) การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีดิจิทัล (IT Resource Management) ครอบคลุมถึงการจัดสรรทรัพยากร (งบประมาณ บุคลากร และระบบงาน) ให้เพียงพอต่อการขับเคลื่อนภารกิจขององค์กร รวมถึงการกำหนดแผนรองรับ (Contingency Plan) ในกรณีที่ไม่สามารถจัดสรรทรัพยากรได้เพียงพอตามที่กำหนดไว้

(๓) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy) การกำหนดมาตรฐานความปลอดภัยในการเข้าถึงและใช้งานระบบสารสนเทศ เพื่อป้องกันการเข้าถึงข้อมูลโดยมิชอบ สอดคล้องกับมาตรฐานสากลและกฎหมายที่เกี่ยวข้อง

ทั้งนี้ ขั้นตอนในการจัดทำและพัฒนากรอบนโยบายการกำกับดูแลด้านเทคโนโลยีดิจิทัลระดับองค์กรที่ดี องค์การสะพานปลาจะดำเนินการตามแนวทาง ดังต่อไปนี้

- การวิเคราะห์สภาพแวดล้อม (Context Analysis) วิเคราะห์และระบุปัจจัยสภาพแวดล้อมทั้งภายในและภายนอกองค์กร ประกอบด้วย กฎหมาย (เช่น พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์, พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล) ระเบียบข้อบังคับ ภาระผูกพันตามสัญญา รวมทั้งแนวโน้มการเปลี่ยนแปลงทางธุรกิจและอุตสาหกรรมประมง ที่อาจมีผลต่อการออกแบบกรอบการกำกับดูแล

- การประเมินความสำคัญของเทคโนโลยี (IT Criticality Assessment) พิจารณาระดับความสำคัญของระบบเทคโนโลยีดิจิทัล รวมทั้งบทบาทของเทคโนโลยีที่มีต่อการดำเนินงานหลักและการให้บริการขององค์การสะพานปลา (เช่น ระบบบริหารจัดการท่าเทียบเรือ ระบบการเงินและบัญชี)

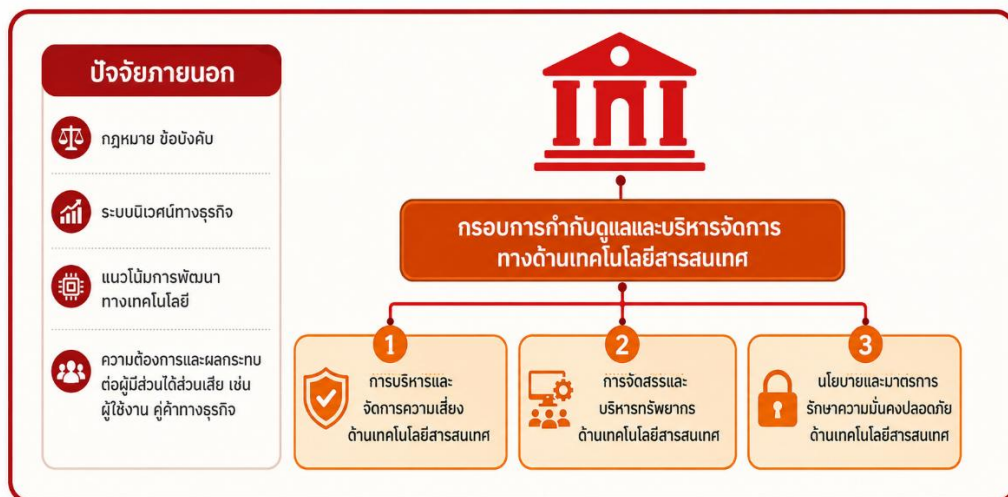
- การประเมินผลกระทบต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Impact Assessment) พิจารณาผลกระทบจากการนำเทคโนโลยีดิจิทัลมาใช้ ที่มีต่อผู้มีส่วนได้ส่วนเสียทั้งภายใน (บุคลากร) และ

ภายนอก (ชาวประมง ผู้ประกอบการ คู่ค้า) เพื่อให้มั่นใจว่าเทคโนโลยีนั้นสร้างความคุ้มค่าและสอดคล้องกับเป้าหมายองค์กร

- การประเมินสภาพแวดล้อมการควบคุม (Control Environment) พิจารณานัยสำคัญของสภาพแวดล้อมการควบคุมภายในโดยทั่วไปขององค์กร (Internal Control) ที่มีผลต่อกระบวนการทางด้านเทคโนโลยีดิจิทัล

- การกำหนดรูปแบบการตัดสินใจที่เหมาะสม (Optimal Decision-Making Model) กำหนดหลักการสำคัญที่จะใช้เป็นแนวทางสำหรับการออกแบบการกำกับดูแลและการตัดสินใจ โดยทำความเข้าใจวัฒนธรรมองค์กร และพิจารณาปัจจัยต่าง ๆ อย่างรอบด้าน เช่น ปัจจัยด้านความคุ้มค่า (ROI) ปัจจัยด้านผลกระทบต่อบุคลากร และปัจจัยด้านการปฏิบัติตามข้อกำหนดทางกฎหมาย

- การกำหนดระดับการมอบหมายอำนาจอนุมัติ (Delegation of Authority DOA) กำหนดระดับอำนาจอนุมัติ บทบาท ความรับผิดชอบ รวมทั้งข้อกำหนดที่เกี่ยวข้องสำหรับการตัดสินใจในโครงการหรือการจัดหาทางด้านเทคโนโลยีดิจิทัลให้มีความชัดเจนและเหมาะสมตามโครงสร้างการบริหารงานขององค์กรสะพานปลา



ภาพประกอบที่ ๕ กรอบการกำกับดูแลและบริหารจัดการทางด้านเทคโนโลยีสารสนเทศ

โดยเนื้อหาที่เกี่ยวข้องของนโยบายแต่ละด้าน อาจประกอบด้วย

(๑) การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(๒) การจัดสรรและบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศ

(๓) นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ทั้งนี้ เพื่อให้นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีดิจิทัลระดับองค์กรที่ดี มีผลบังคับใช้ทั่วทั้งองค์กรอย่างเป็นรูปธรรม องค์กรสะพานปลาควรพิจารณากำหนดบทบาทของบุคลากรที่เกี่ยวข้อง และจัดให้มีแนวทางการสื่อสารที่เหมาะสม ดังนี้

(๑) กำหนดช่องทางที่เหมาะสมในการสื่อสารนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีดิจิทัล ไปยังบุคลากรทุกระดับ รวมทั้งมีกระบวนการสื่อสารเพื่อให้ผู้ปฏิบัติงานรับทราบข้อมูลเพียงพอต่อการนำนโยบายไปปฏิบัติจริง

(๒) ขยายขอบเขตการสื่อสารนโยบายฯ ให้ครอบคลุมถึงพนักงาน บุคลากรผู้ช่วยปฏิบัติงาน ตลอดจน **ผู้ให้บริการภายนอก (Outsource / Third-party)** ที่ได้รับสิทธิในการเข้าถึงระบบสารสนเทศหรือข้อมูลขององค์กร เพื่อให้ตระหนักถึงมาตรฐานความมั่นคงปลอดภัย

(๓) นอกเหนือจากการสื่อสาร องค์กรต้องมีการบังคับใช้และสนับสนุนให้เกิดการปฏิบัติตามนโยบายฯ อย่างเคร่งครัด ตัวอย่างเช่น

- การกำหนดบทลงโทษ มีการกำหนดมาตรการทางวินัยหรือบทลงโทษที่ชัดเจน ในกรณีที่มีการกระทำขัดต่อจริยธรรม หรือฝ่าฝืนนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร

- การให้ผลประโยชน์ตอบแทน (Incentives) มีการพิจารณาให้รางวัล เช่น การประกาศเกียรติคุณ การนำไปประกอบการประเมินผลงานประจำปี หรือรางวัลพิเศษอื่นๆ เมื่อบุคลากรหรือหน่วยงานปฏิบัติงานได้ตามมาตรฐานและเป็นแบบอย่างที่ดี (Best Practice)

เพื่อเป็นการวัดผลการปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีดิจิทัล คณะอนุกรรมการด้านเทคโนโลยีดิจิทัล (หรือคณะกรรมการที่ได้รับมอบหมาย) ควรกำหนดกระบวนการประเมินผล ซึ่งประกอบด้วยแนวทาง ดังนี้

๑) กำหนดกรอบระยะเวลาที่ชัดเจนในการประเมินผล และรายงานต่อคณะกรรมการองค์การสะพานปลา หรือผู้มีส่วนได้ส่วนเสีย อย่างน้อยปีละ ๑ ครั้ง โดยการประเมินผลการปฏิบัติตามนโยบายฯ ประกอบด้วยข้อมูลจาก ๒ แหล่งหลัก ได้แก่

- รายงานจากฝ่ายเทคโนโลยีสารสนเทศ เน้นหาควรครอบคลุมถึงผลการปฏิบัติงานด้านการบริหารความเสี่ยง การจัดการทรัพยากร ความคืบหน้าของโครงการดิจิทัลที่สำคัญ การปฏิบัติตามกฎระเบียบข้อบังคับ ประสิทธิภาพและประสิทธิผลในการนำเทคโนโลยีมาใช้ รวมถึงปัญหาและอุปสรรคที่เกิดขึ้น

- รายงานจากสำนักตรวจสอบภายใน (Internal Audit) เน้นหาควรครอบคลุมถึงแผนการตรวจสอบระบบสารสนเทศตามฐานความเสี่ยง (Risk-based IT Audit Plan) ทั้งระยะสั้นและระยะยาว ผลการตรวจสอบตามแผน และความคืบหน้าในการติดตามการแก้ไขข้อบกพร่อง (Defect Tracking) ที่พบจากการตรวจสอบ

๒) ในกรณีที่พบข้อบกพร่องในการออกแบบกระบวนการ หรือการปฏิบัติตามนโยบายฯ ซึ่งอาจส่งผลกระทบต่อองค์กรอย่างมีนัยสำคัญ หน่วยงานที่รับผิดชอบต้องรายงานต่อคณะกรรมการโดยไม่มีข้อกั๊ก พร้อมทั้งกำหนดผู้รับผิดชอบและวิธีการแก้ไขข้อบกพร่องนั้นๆ ให้แล้วเสร็จตามกำหนดเวลา

## ๕.๒ แนวปฏิบัติเพื่อสนับสนุนให้การดำเนินงานด้านเทคโนโลยีดิจิทัลบรรลุวัตถุประสงค์

เพื่อให้การดำเนินงานด้านเทคโนโลยีดิจิทัล สามารถบรรลุวัตถุประสงค์เชิงยุทธศาสตร์ขององค์การสะพานปลา องค์การได้ประยุกต์ใช้กรอบแนวปฏิบัติมาตรฐานสากล (COBIT) โดยแบ่งกระบวนการกำกับดูแลและบริหารจัดการออกเป็น ๕ กลุ่มหลัก ดังนี้

### ๑) กลุ่ม EDM - Evaluate, Direct and Monitor (ประเมิน สั่งการ และติดตามผล)

- ระบบเทคโนโลยีดิจิทัลที่มีอยู่นั้น สามารถสนับสนุนพันธกิจและยุทธศาสตร์ขององค์กรได้หรือไม่
- มีการวัดประสิทธิภาพของระบบเทคโนโลยีสารสนเทศ เพื่อพยากรณ์และจัดการปัญหา ก่อนที่ปัญหานั้นจะเกิดขึ้นจริงหรือไม่
- มีการติดตามและรายงานผลเกี่ยวกับความเสี่ยง การควบคุม การปฏิบัติตามกฎเกณฑ์ และประสิทธิภาพ ไปยังผู้บริหารระดับสูงขององค์กรอย่างสม่ำเสมอหรือไม่

### ๒) กลุ่ม APO - Align, Plan and Organism (จัดวางแนวทาง จัดทำแผน และจัดระบบ)

- ทำให้ผู้บริหารขององค์กรได้รับทราบว่า แผนปฏิบัติการดิจิทัลและยุทธศาสตร์ทางธุรกิจดำเนินไปในทิศทางเดียวกัน (IT-Business Alignment) หรือไม่
- เพื่อให้มั่นใจว่าผู้ปฏิบัติงานมีความรู้ ความเข้าใจเกี่ยวกับความเสี่ยงทางเทคโนโลยีสารสนเทศ และมีวิธีการบริหารจัดการความเสี่ยงดังกล่าวอย่างเหมาะสมหรือไม่

### ๓) กลุ่ม BAI - Build, Acquire and Implement (จัดสร้าง จัดทำ และนำไปใช้งาน)

- โครงการด้านเทคโนโลยีดิจิทัลที่กำลังพัฒนาหรือดำเนินการจัดทำนั้น สามารถนำมาใช้แก้ไขปัญหา หรือสนับสนุนการปฏิบัติงานขององค์การสะพานปลาได้จริงหรือไม่
- โครงการดังกล่าวสามารถส่งมอบและนำมาใช้งานได้ตรงตามขอบเขต ทันตามระยะเวลา และอยู่ภายใต้งบประมาณที่กำหนดไว้หรือไม่

### ๔) กลุ่ม DSS - Deliver, Service and Support (ส่งมอบ ให้บริการ และสนับสนุน)

- ระบบสารสนเทศใหม่ที่นำมาใช้งาน สามารถให้บริการได้อย่างมีประสิทธิภาพและตรงตามความต้องการ (SLA) ขององค์กรหรือไม่
- การเปลี่ยนแปลงระบบงาน (Change Management) ส่งผลกระทบเชิงลบต่อการปฏิบัติงานหรือการให้บริการในปัจจุบันหรือไม่

### ๕) กลุ่ม MEA - Monitor, Evaluate and Assess (ติดตาม วัดผล และประเมินผล)

- การให้บริการด้านเทคโนโลยีดิจิทัล สามารถสนับสนุนการปฏิบัติงานได้อย่างสอดคล้องกับเป้าหมายและพันธกิจขององค์กรหรือไม่
- บุคลากรขององค์กรสามารถใช้งานระบบสารสนเทศได้อย่างมีประสิทธิภาพและมีความมั่นคงปลอดภัยหรือไม่

- ระบบเทคโนโลยีสารสนเทศที่ใช้งานอยู่ในปัจจุบัน มีการรักษาความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) เพียงพอและเป็นไปตามมาตรฐานหรือไม่

## ๖. การสื่อสารหลักการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance Guiding Principle Communications)

องค์การสะพานปลา (อสป.) ให้ความสำคัญกับการสื่อสารนโยบายและหลักการกำกับดูแลด้านเทคโนโลยีดิจิทัล เพื่อให้เกิดการนำไปปฏิบัติอย่างเป็นมาตรฐานเดียวกันทั่วทั้งองค์กร (Standardized Practice) โดยมีแนวทางและกระบวนการสื่อสาร ดังนี้

### ๖.๑ รูปแบบการสื่อสารในองค์กร (Organizational Communication Methods)

การสื่อสารภายในองค์การสะพานปลา ประกอบด้วย ๒ รูปแบบหลัก ได้แก่

(๑) การสื่อสารที่เป็นทางการ (Formal Communication) เป็นการติดต่อสื่อสารที่มีระเบียบแบบแผน มีขั้นตอนชัดเจน ผ่านโครงสร้างการบริหารงานขององค์กร โดยอาจเป็นการสื่อสารจากผู้บริหารระดับสูงลงสู่ผู้ปฏิบัติงาน (Top-down) จากผู้ปฏิบัติงานขึ้นสู่ผู้บริหาร (Bottom-up) หรือการสื่อสารในระดับเดียวกัน (Horizontal) เช่น การออกประกาศคำสั่ง ระเบียบปฏิบัติ หรือบันทึกข้อความ

(๒) การสื่อสารที่ไม่เป็นทางการ (Informal Communication) เป็นการติดต่อสื่อสารระหว่างบุคคลในองค์กรผ่านเครือข่ายสังคม หรือความสัมพันธ์ส่วนบุคคล โดยไม่ยึดติดกับโครงสร้างการบริหารงาน เช่น การพบปะพูดคุย การให้คำปรึกษา การแลกเปลี่ยนเรียนรู้ (Knowledge Sharing) หรือการบอกกล่าวแบบปากต่อปาก ซึ่งประสิทธิภาพของการสื่อสารรูปแบบนี้จะช่วยเสริมสร้างวัฒนธรรมองค์กรและสร้างความตระหนักรู้ (Awareness) ได้อย่างรวดเร็ว

### ๖.๒ วัตถุประสงค์ของการสื่อสารหลักการกำกับดูแลด้านเทคโนโลยีดิจิทัล

(๑) เพื่อถ่ายทอดนโยบายและทิศทาง เพื่อให้การกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัลที่จัดทำขึ้น สามารถกระจายลงสู่บุคลากรและผู้ปฏิบัติงานในทุกระดับได้อย่างมีประสิทธิภาพ

(๒) เพื่อสร้างมาตรฐานการปฏิบัติงาน (Standardized Practice) เพื่อให้ผู้ปฏิบัติงานมีความรู้ ความเข้าใจ ในกรอบนโยบาย กระบวนการกำกับดูแลด้านเทคโนโลยีดิจิทัล (รวมถึงกฎหมายที่เกี่ยวข้อง เช่น PDPA และ Cybersecurity) และสามารถนำไปปฏิบัติให้บรรลุวัตถุประสงค์ขององค์กรในทิศทางเดียวกัน

(๓) เพื่อสร้างความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย เพื่อให้ผู้มีส่วนได้ส่วนเสีย ทั้งบุคลากรภายในและผู้ให้บริการภายนอก (เช่น ชาวประมง ผู้ประกอบการ) รับทราบถึงความมุ่งมั่นขององค์กรในการบริหารจัดการเทคโนโลยีดิจิทัลอย่างมีธรรมาภิบาล

### ๖.๓ ช่องทางการสื่อสารการกำกับดูแลด้านเทคโนโลยีดิจิทัล (Communication Channels)

องค์การสะพานปลากำหนดช่องทางในการประชาสัมพันธ์และถ่ายทอดหลักการกำกับดูแล ให้ครอบคลุมกลุ่มเป้าหมาย ดังนี้

(๑) ไปรษณีย์อิเล็กทรอนิกส์ (E-mail) การส่งสารบรรณอิเล็กทรอนิกส์หรืออีเมลเวียนผ่านระบบขององค์กร (เช่น Outlook) เพื่อแจ้งประกาศหรือนโยบายใหม่ให้บุคลากรทราบโดยตรง

(๒) บอร์ดประชาสัมพันธ์ (Notice Boards) การปิดประกาศตามบอร์ดประชาสัมพันธ์ ณ สำนักงานใหญ่ และสำนักงานท่าเทียบเรือประมงต่าง ๆ เพื่อให้บุคลากรและผู้มาติดต่อรับทราบ

(๓) ระบบอินทราเน็ต (Intranet) และเว็บไซต์ การประชาสัมพันธ์ผ่านทางเว็บไซต์หลักขององค์การสะพานปลา และการอัปโหลดไฟล์คู่มือ นโยบาย หรือระเบียบปฏิบัติ ไว้บนระบบ Intranet เพื่อเป็นศูนย์กลางการเรียนรู้ให้บุคลากรสามารถสืบค้นและดาวน์โหลดไฟล์ได้ตลอดเวลา

(๔) การจัดอบรมหรือการประชุมชี้แจง (Training & Townhall) การสอดแทรกเนื้อหาด้านการกำกับดูแลเทคโนโลยีดิจิทัล การรักษาความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล เข้าไปในหลักสูตรปฐมนิเทศพนักงานใหม่ หรือการจัดประชุมชี้แจงประจำปี

#### ๖.๔ การประเมินผลการรับรู้และประสิทธิผลของการสื่อสาร (Awareness Evaluation)

เพื่อให้เป็นไปตามเกณฑ์การประเมินผลรัฐวิสาหกิจ (SE-AM) องค์การสะพานปลาต้องจัดให้มีการประเมินผลภายหลังการสื่อสาร ดังนี้

(๑) การประเมินความตระหนักรู้ (Awareness Survey) จัดทำแบบสำรวจความเข้าใจของบุคลากรที่มีต่อนโยบายการกำกับดูแลด้านเทคโนโลยีดิจิทัล อย่างน้อยปีละ ๑ ครั้ง

(๒) การนำผลประเมินไปปรับปรุง นำผลลัพธ์ที่ได้จากการสำรวจมาวิเคราะห์ช่องว่าง (Gap Analysis) เพื่อปรับปรุงแผนการสื่อสาร (Communication Plan) หรือจัดทำหลักสูตรฝึกอบรมเพิ่มเติมให้เหมาะสมกับกลุ่มเป้าหมายที่มีระดับความเข้าใจแตกต่างกัน

### ๗. การกำหนดแนวทางในการพัฒนาความรู้ความสามารถด้านเทคโนโลยีดิจิทัลของบุคลากรในองค์กรทุกระดับ (Human Behavior & Digital Literacy)

ระบบเทคโนโลยีดิจิทัลและสารสนเทศ มีความสำคัญอย่างยิ่งต่อการขับเคลื่อนการดำเนินงานในทุกระดับขององค์กร ในระดับผู้ปฏิบัติงาน เทคโนโลยีจะช่วยเพิ่มประสิทธิภาพ ลดขั้นตอน และประหยัดเวลาในการปฏิบัติงานประจำวัน ในขณะที่ระดับผู้บริหาร จะใช้เทคโนโลยีและระบบฐานข้อมูลขนาดใหญ่ (Big Data) เพื่อสนับสนุนการตัดสินใจ วางแผนเชิงยุทธศาสตร์ และแก้ปัญหาต่าง ๆ ที่เกิดขึ้น องค์กรจึงต้องมีการบริหารจัดการข้อมูล (Data Management) ที่ดี เพื่อให้ได้มาซึ่งสารสนเทศที่เป็นระบบ ถูกต้อง รวดเร็ว และนำไปสู่การเป็นองค์กรที่ขับเคลื่อนด้วยข้อมูล (Data-Driven Organization) เพื่อเพิ่มขีดความสามารถในการให้บริการแก่ชาวประมงและผู้มีส่วนได้ส่วนเสียในยุคดิจิทัลที่ไร้พรมแดน

องค์การสะพานปลา (อสป.) ได้ให้ความสำคัญกับการพัฒนา "คน" ควบคู่ไปกับ "เทคโนโลยี" จึงได้กำหนดแนวทางในการพัฒนาบุคลากรในองค์กร ให้สอดคล้องกับแผนวิสาหกิจ พ.ศ. ๒๕๖๖ - ๒๕๗๐ และแผนปฏิบัติการดิจิทัล ดังนี้

**ยุทธศาสตร์ (Strategy)** พัฒนาทักษะและสมรรถนะของบุคลากรภายในองค์การสะพานปลา ให้มีความรู้ความเข้าใจด้านเทคโนโลยีดิจิทัล การรักษาความมั่นคงปลอดภัยไซเบอร์ การบริหารจัดการข้อมูล และการวิเคราะห์ข้อมูล

**เป้าหมาย (Goals)** บุคลากรขององค์การสะพานปลาทุกระดับ มีทักษะดิจิทัลที่เหมาะสมกับตำแหน่งงาน สามารถบริหารจัดการข้อมูลในความรับผิดชอบ และสามารถนำข้อมูลมาวิเคราะห์เพื่อพัฒนางาน ตลอดจนสนับสนุนการตัดสินใจเชิงยุทธศาสตร์ได้อย่างมีประสิทธิภาพ

**มาตรการในการพัฒนา (Measure)** ดำเนินการยกระดับทักษะ (Upskill) และปรับเปลี่ยนทักษะ (Reskill) ของบุคลากรองค์การสะพานปลา ให้มีความรู้พื้นฐานและทักษะประยุกต์ใช้ในด้านเทคโนโลยีดิจิทัล การกำกับดูแลข้อมูล และการรักษาความปลอดภัยของข้อมูล

#### ๗.๑ มาตรการหลักในการพัฒนาความรู้ความสามารถด้านเทคโนโลยีดิจิทัลของบุคลากรในองค์กรทุกระดับ (Human Behavior)

องค์การสะพานปลา ได้กำหนดมาตรการหลักเพื่อส่งเสริมพฤติกรรมและการเรียนรู้ด้านดิจิทัล ดังนี้

(๑) การส่งเสริมทักษะการใช้เครื่องมือดิจิทัล (Digital Tools & Workspace) ส่งเสริมและพัฒนาทักษะในการนำเครื่องมือ อุปกรณ์ และเทคโนโลยีดิจิทัลที่มีอยู่ในปัจจุบัน (เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์เคลื่อนที่ โปรแกรมสำนักงาน และสื่อออนไลน์) มาประยุกต์ใช้ให้เกิดประโยชน์สูงสุดในการสื่อสาร การปฏิบัติงาน และการทำงานร่วมกัน (Collaboration) เพื่อยกระดับกระบวนการทำงานหรือระบบงานในองค์กร ให้มีความทันสมัยและคล่องตัว

(๒) การส่งเสริมทักษะด้านความมั่นคงปลอดภัยและคุ้มครองข้อมูล (Cybersecurity & Data Protection) ส่งเสริมและพัฒนาทักษะของบุคลากรด้านการจัดเก็บและปรับปรุงข้อมูลอย่างปลอดภัย รวมถึงการปกป้องข้อมูลจากการถูกทำลาย การลักลอบใช้งาน การโจมตีทางไซเบอร์ หรือการแก้ไขโดยไม่ชอบ ตลอดจนการสร้างความรู้ในการปกป้องข้อมูลส่วนบุคคล (PDPA) จากอุบัติเหตุที่อาจเกิดจากความบกพร่องภายในระบบหรือจากความรู้เท่าไม่ถึงการณ์

(๓) การส่งเสริมทักษะด้านการวิเคราะห์ข้อมูลเพื่อการตัดสินใจ (Data Analytics & Decision Support) ส่งเสริมและพัฒนาทักษะของบุคลากรในการรวบรวม จัดเก็บ เข้าถึง และวิเคราะห์ข้อมูล เพื่อใช้งานร่วมกับระบบสนับสนุนการตัดสินใจ (Decision Support System DSS) การสืบค้นข้อมูล (Query) และการสร้างรายงานเชิงวิเคราะห์ (Dashboard/Reporting) สำหรับการบริหารจัดการท่าเทียบเรือและตลาดสินค้าสัตว์น้ำ

(๔) การส่งเสริมทักษะด้านเทคโนโลยีอุบัติใหม่ (Emerging Technologies) ส่งเสริมและพัฒนาให้บุคลากรได้เรียนรู้การใช้เครื่องมือวิเคราะห์ขั้นสูง เช่น ปัญญาประดิษฐ์ (AI) หรือ Machine Learning ในการจัดการข้อมูล เพื่อให้สามารถเข้าใจความสัมพันธ์ของข้อมูล (เช่น แนวโน้มปริมาณสัตว์น้ำ หรือความผันผวนของราคาสินค้า) ซึ่งจะช่วยในการทำนายหรือพยากรณ์ข้อมูลในอนาคตได้อย่างแม่นยำ

(๕) การส่งเสริมงานวิจัยและนวัตกรรม (Research & Innovation) ส่งเสริมการทำวิจัยและพัฒนา นวัตกรรมด้านการบริหารจัดการทำเทียบเรือประมง เพื่อให้ได้องค์ความรู้ใหม่ทั้งในเชิงทฤษฎีและปฏิบัติ อันจะช่วยแก้ปัญหาได้อย่างตรงจุด ช่วยผู้บริหารในการวินิจฉัยตัดสินใจได้อย่างเหมาะสม และนำไปสู่การปรับปรุงกระบวนการให้บริการขององค์การสะพานปลาให้มีประสิทธิภาพยิ่งขึ้น

(๖) การส่งเสริมทักษะด้านการกำกับดูแลข้อมูล (Data Governance) ส่งเสริมและพัฒนาความรู้ความเข้าใจของบุคลากรเกี่ยวกับกรอบธรรมาภิบาลข้อมูล เพื่อให้บุคลากรตระหนักถึงหน้าที่ความเป็นเจ้าของข้อมูล (Data Owner) และสามารถนำข้อมูลไปใช้บูรณาการร่วมกับหน่วยงานอื่น (เช่น กรมประมง) ได้อย่างมีประสิทธิภาพ ถูกต้อง และมีมาตรฐานเดียวกัน

## ภาคผนวก

## ภาคผนวก ก อภิธานศัพท์และคำจำกัดความ (Glossary of Terms)

เพื่อให้บุคลากรขององค์กรสะพานปลามีความเข้าใจที่ตรงกันในการนำคู่มือฉบับนี้ไปปฏิบัติ จึงกำหนดคำนิยามศัพท์ที่สำคัญ ดังนี้

- การกำกับดูแลเทคโนโลยีสารสนเทศระดับองค์กร (Enterprise Governance of IT EGIT) ระบบที่คณะกรรมการและผู้บริหารระดับสูงใช้ในการประเมิน สั่งการ และติดตามผล เพื่อให้มั่นใจว่าการใช้เทคโนโลยีดิจิทัลจะสร้างคุณค่าและสนับสนุนยุทธศาสตร์ขององค์กร

- ผู้มีส่วนได้ส่วนเสีย (Stakeholders) บุคคลหรือกลุ่มบุคคลที่ได้รับผลกระทบ หรือมีส่วนได้ส่วนเสียจากการดำเนินงานขององค์กร ทั้งภายใน (เช่น ผู้บริหาร พนักงาน) และภายนอก (เช่น ขาวประมง ผู้ประกอบการแพปลา คู่ค้า ประชาชน)

- ความตระหนักรู้ด้านความมั่นคงปลอดภัย (Security Awareness) ความรู้ความเข้าใจของบุคลากรเกี่ยวกับภัยคุกคามทางไซเบอร์ และวิธีปฏิบัติตนเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลและระบบสารสนเทศขององค์กร

- การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment DPIA) กระบวนการประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ก่อนริเริ่มโครงการหรือระบบงานใหม่

- ค่าเป้าหมายเวลาในการกู้คืนระบบ (Recovery Time Objective RTO) ระยะเวลาที่องค์กรยอมรับได้ในการกู้คืนระบบสารสนเทศให้กลับมาใช้งานได้ตามปกติ หลังจากเกิดเหตุขัดข้องหรือภัยพิบัติ (ใช้ในงาน BCM)

- จุดเหมาะสมของข้อมูลที่กู้คืน (Recovery Point Objective RPO) ปริมาณข้อมูลที่องค์กรยอมรับได้ว่าอาจสูญหายไปในช่วงเวลาที่เกิดเหตุขัดข้อง (ใช้ในงาน BCM)

ภาคผนวก ข ตารางกำหนดบทบาทและความรับผิดชอบ (RACI Chart)

เพื่อให้กระบวนการกำกับดูแลด้านเทคโนโลยีดิจิทัล (ตามกรอบ COBIT) มีความชัดเจน องค์กร  
สะพานปลาจึงกำหนดตารางความรับผิดชอบ (RACI) ดังนี้

ความหมายของสัญลักษณ์ (RACI)

R (Responsible) ผู้รับผิดชอบหลัก ผู้ที่ลงมือปฏิบัติงานเพื่อให้กระบวนการสำเร็จ

A (Accountable) ผู้อนุมัติ/ผู้รับผิดชอบสูงสุด ผู้ที่มีอำนาจตัดสินใจอนุมัติ (มีได้เพียง ๑ คน/  
คณะ ในแต่ละงาน)

C (Consulted) ผู้ให้คำปรึกษา ผู้ที่ให้ข้อมูล ความเห็น หรือข้อเสนอแนะก่อนการตัดสินใจ

I (Informed) ผู้รับทราบ ผู้ที่รับทราบผลการดำเนินงานหรือผลการตัดสินใจ

ตารางกำหนดบทบาทและความรับผิดชอบ (RACI Chart)

| กระบวนการกำกับดูแล<br>(EDM Domain)                                                 | คณะกรรมการ<br>อสป. | คณะ<br>อนุกรม<br>การด้าน<br>ดิจิทัล | ผอ. | CIO / สนง.<br>เทคโนโลยี<br>สารสนเทศ | ฝ่าย<br>ตรวจสอบ<br>ภายใน | ผู้ใช้งาน /<br>ฝ่ายอื่น ๆ |
|------------------------------------------------------------------------------------|--------------------|-------------------------------------|-----|-------------------------------------|--------------------------|---------------------------|
| ๑. การกำหนดกรอบการ<br>กำกับดูแล (Governance<br>Framework Setting)                  | A                  | R                                   | C   | C                                   | I                        | I                         |
| ๒. การส่งมอบผลประโยชน์<br>และความคุ้มค่า (Benefits<br>Delivery)                    | I                  | A                                   | R   | R                                   | I                        | C                         |
| ๓. การบริหารจัดการความ<br>เสี่ยง (Risk Optimization)                               | I                  | A                                   | R   | R                                   | C                        | I                         |
| ๔. การบริหารจัดการ<br>ทรัพยากร (Resource<br>Optimization)                          | A                  | C                                   | R   | R                                   | I                        | I                         |
| ๕. การสร้างความโปร่งใสต่อผู้<br>มีส่วนได้ส่วนเสีย<br>(Stakeholder<br>Transparency) | I                  | A                                   | R   | R                                   | C                        | I                         |
| ๖. การประเมินและ<br>ตรวจสอบความสอดคล้อง (IT<br>Audit & Compliance)                 | I                  | I                                   | I   | R                                   | A                        | I                         |

## ภาคผนวก ค รายการอ้างอิงและกฎหมายที่เกี่ยวข้อง (References & Legal Compliance)

คู่มือฉบับนี้ถูกจัดทำขึ้นโดยอ้างอิงกรอบมาตรฐานและกฎหมาย ดังต่อไปนี้

๑. พระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม
๓. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)
๔. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๕. แผนวิสาหกิจ องค์การสะพานปลา พ.ศ. ๒๕๖๖ - ๒๕๗๐
๖. คู่มือการประเมินผลการดำเนินงานรัฐวิสาหกิจ (State Enterprise Assessment Model SE-AM) ด้านการพัฒนาเทคโนโลยีดิจิทัล (DT) ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ฉบับปรับปรุง ปี ๒๕๖๗
๗. มาตรฐานสากลด้านการกำกับดูแลเทคโนโลยีสารสนเทศระดับองค์กร (COBIT 2019 และ ISO/IEC 38500)
๘. มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001)

## ภาคผนวก ง รายการแบบฟอร์มตรวจสอบเบื้องต้นสำหรับโครงการดิจิทัล (Digital Project Checklist)

(ใช้แนบประกอบการเสนอขออนุมัติโครงการด้านเทคโนโลยีสารสนเทศของ อสป.)

ผู้เสนอโครงการต้องตรวจสอบและทำเครื่องหมาย (✓) เพื่อยืนยันว่าโครงการได้ผ่านการประเมินตามหลักการกำกับดูแลเทคโนโลยีดิจิทัลแล้ว

[ ] โครงการมีความสอดคล้องกับยุทธศาสตร์และแผนวิสาหกิจของ อสป.

[ ] มีการประเมินความคุ้มค่าของการลงทุน (ROI / Public Value) เรียบร้อยแล้ว

[ ] มีการระบุความต้องการทรัพยากร (งบประมาณ, บุคลากร, โครงสร้างพื้นฐาน) อย่างครบถ้วน

[ ] ประเด็นด้านความปลอดภัยไซเบอร์ โครงการได้ประเมินช่องโหว่และมีมาตรการรักษาความปลอดภัยตามมาตรฐานองค์กรแล้ว

[ ] ประเด็นด้านข้อมูลส่วนบุคคล (PDPA):

[ ] โครงการมีการเก็บ รวบรวม ใช้ ข้อมูลส่วนบุคคล (หากมี ต้องระบุฐานทางกฎหมาย)

[ ] โครงการได้ดำเนินการทำแบบประเมินผลกระทบ (DPIA) เรียบร้อยแล้ว (เฉพาะโครงการที่มีความเสี่ยงสูง)

[ ] ระบบงานรองรับการจัดเก็บข้อมูลตามระยะเวลา (Retention Period) และมีระบบลบทำลายข้อมูล