

แผนกู้คืน
ระบบเทคโนโลยีสารสนเทศ
IT-DRP

ฉบับทบทวน ๒๕๖๙
สำนักงานเทคโนโลยีสารสนเทศ

สารบัญ

บทนำ ๑

วัตถุประสงค์ ๑

ขอบเขต ๒

กรอบแนวทางการจัดทำแผนกู้คืนระบบสารสนเทศองค์การสะพานปลา ๓

โครงสร้างทีมปฏิบัติการกู้คืนระบบและกระบวนการแจ้งเหตุฉุกเฉิน (DR Team Roles & Responsibilities and Call Tree Process) ๖

เกณฑ์การประเมินระดับความรุนแรงของเหตุการณ์ (Incident Severity Assessment Criteria) ๘

แนวทางการตอบสนองและปฏิบัติการตามระดับเหตุการณ์ (Incident Response Guidelines) ๙

การกลับสู่สภาวะปกติ (Return to Normal Operations / Failback) ๑๓

การทดสอบ การบำรุงรักษา และการทบทวนแผน (Plan Testing, Maintenance & Review) ๑๔

ภาคผนวก ๑๖

บทนำ

แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan: IT-DRP) ฉบับนี้ จัดทำขึ้นเพื่อให้องค์การสะพานปลา (อสป.) มีแนวทางปฏิบัติที่ชัดเจนในการรับมือและกู้คืนระบบงานในสภาวะวิกฤตหรือเหตุฉุกเฉิน อาทิ ภัยธรรมชาติ (อัคคีภัย อุทกภัย) ภัยคุกคามทางกายภาพ (การจลาจล) รวมถึงภัยคุกคามทางไซเบอร์ (Cyber Threats) เช่น มัลแวร์เรียกค่าไถ่ (Ransomware) หรือการโจมตีระบบเครือข่าย ที่อาจส่งผลให้ระบบสารสนเทศหลักไม่สามารถให้บริการได้

แผนฉบับนี้ถูกพัฒนาขึ้นบนพื้นฐานของการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) และการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยมุ่งเน้นการกู้คืนระบบโครงสร้างพื้นฐานและระบบงานที่สำคัญยิ่งยวด (Critical Information Systems) ได้แก่ **ระบบบริหารจัดการเครื่องแม่ข่าย, ระบบบัญชี และระบบบริหารจัดการตลาด (Myket Pro)** ซึ่งเป็นหัวใจหลักในการบริหารจัดการท่าเทียบเรือและการให้บริการแก่เกษตรกรและชาวประมง

การจัดทำแผน IT-DRP นี้ มีวัตถุประสงค์เพื่อให้องค์การสะพานปลาสามารถกู้คืนระบบงานและข้อมูลสำคัญให้กลับมาดำเนินงานได้ตามเป้าหมายระยะเวลาที่กำหนด ได้แก่ ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (MTPD) เป้าหมายระยะเวลาในการกู้คืนระบบ (RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (RPO) ตลอดจนเพื่อลดผลกระทบเชิงลบต่อภารกิจหลัก สร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้ส่วนเสีย และเพื่อให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) ในการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างเคร่งครัด

วัตถุประสงค์

๑. เพื่อเป็นกรอบแนวทางปฏิบัติที่ชัดเจนสำหรับองค์การสะพานปลา ในการเตรียมความพร้อมรับมือ และกู้คืนระบบเทคโนโลยีสารสนเทศที่สำคัญ (Critical Information Systems) เมื่อเกิดเหตุภัยพิบัติหรือสภาวะวิกฤต ให้สามารถกลับมาดำเนินการได้ตามเป้าหมายที่กำหนด ได้แก่ ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (MTPD) เป้าหมายระยะเวลาในการกู้คืนระบบ (RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (RPO)

๒. เพื่อให้ผู้บริหาร คณะทำงาน เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ และบุคลากรที่เกี่ยวข้องทราบถึงบทบาท หน้าที่ และขั้นตอนการปฏิบัติงานในสภาวะฉุกเฉินอย่างเป็นระบบ ซึ่งจะช่วยลดผลกระทบจากการหยุดชะงักของการให้บริการแก่เกษตรกร ชาวประมง และผู้มีส่วนได้ส่วนเสีย ตลอดจนรักษาชื่อเสียงขององค์กร

๓. เพื่อรักษาความมั่นคงปลอดภัยของระบบและข้อมูลสารสนเทศ ทั้งในด้านความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) โดยให้ความสำคัญสูงสุดกับการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) และสอดคล้องกับ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ขอบเขต

แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (IT-DRP) ฉบับนี้ จะถูกประกาศใช้เมื่อเกิดเหตุการณ์ภัยพิบัติ สภาวะวิกฤต หรือเหตุขัดข้องรุนแรงที่ส่งผลให้ระบบเทคโนโลยีสารสนเทศหยุดชะงัก และไม่สามารถกู้คืนได้ภายในระยะเวลาที่กำหนด โดยมีขอบเขตการบังคับใช้ ดังนี้

๑. ขอบเขตด้านสถานการณ์และภัยคุกคาม (Disaster Scenarios)

ครอบคลุมเหตุการณ์ที่ทำให้ศูนย์คอมพิวเตอร์หลัก (Primary Site) ขององค์การสะพานปลา หรือระบบโครงสร้างพื้นฐานได้รับความเสียหาย แบ่งเป็น ๓ ประเภทหลัก ได้แก่

๑) ภัยธรรมชาติและภัยทางกายภาพ (Physical & Natural Threats) เช่น อัคคีภัย อุทกภัย แผ่นดินไหว หรืออาคารสำนักงานได้รับความเสียหาย

๒) ภัยจากการกระทำของมนุษย์ (Man-made Threats) เช่น การชุมนุมประท้วง จลาจล การวินาศกรรม หรือการเข้าถึงพื้นที่ปฏิบัติงานหลักไม่ได้

๓) ภัยคุกคามทางไซเบอร์และโครงสร้างพื้นฐาน (Cyber & Infrastructure Threats) เช่น การโจมตีทางไซเบอร์ (มัลแวร์เรียกค่าไถ่ Ransomware, การเจาะระบบขโมยข้อมูล) , ระบบไฟฟ้าขัดข้องเป็นเวลานาน, หรือระบบเครือข่ายสื่อสารหลักล่ม

๒. ขอบเขตด้านระบบงานและข้อมูล (In-Scope Systems & Data)

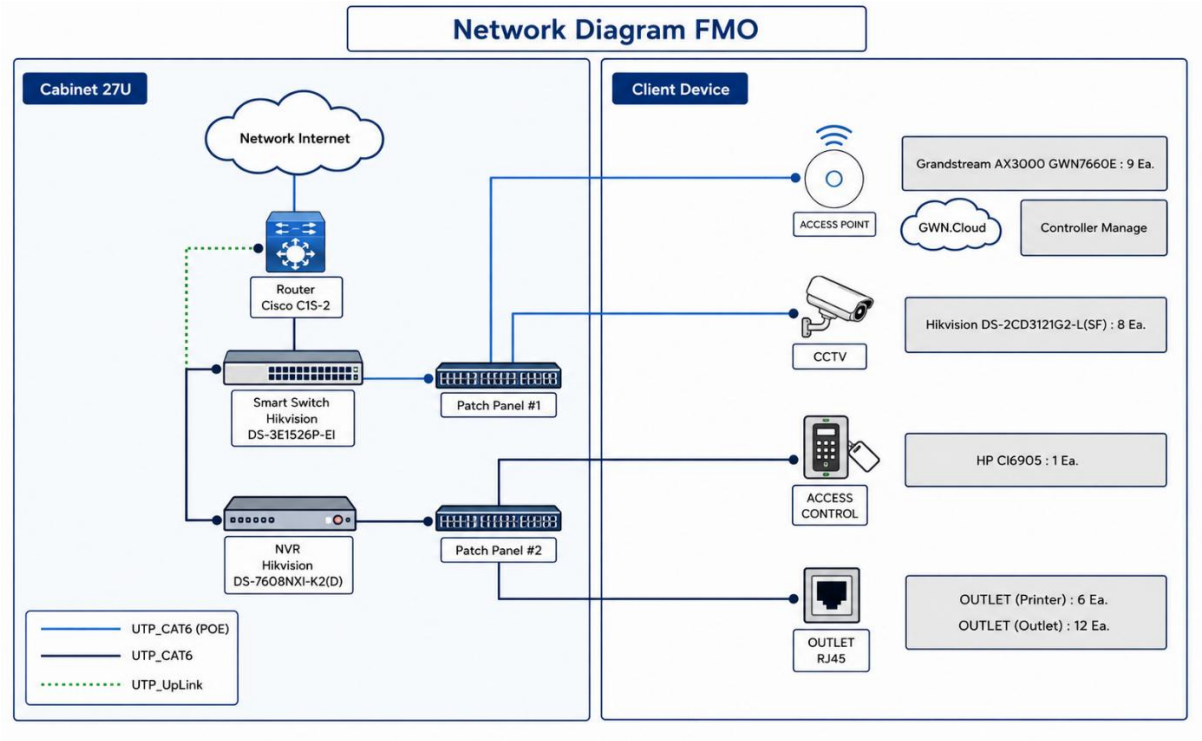
ครอบคลุมเฉพาะระบบเทคโนโลยีสารสนเทศที่ได้รับการจัดลำดับความสำคัญในระดับวิกฤต (Critical Systems) ตามรายงานการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) ได้แก่

- ระบบบริหารจัดการเครื่องแม่ข่าย (Server)
- ระบบบัญชีออนไลน์ (MyAccount Cloud)
- ระบบบริหารงานบุคคล (ATHM)
- ระบบบริหารจัดการตลาด (Horga Market App)
- ระบบสินเชื่อ (Core Loan)

๓. ขอบเขตด้านสถานที่ (Locations)

ครอบคลุมการประเมินสถานการณ์ การตัดสินใจย้ายระบบ และการปฏิบัติงานกู้คืนระบบจากศูนย์คอมพิวเตอร์หลัก (Primary Site) ไปยังศูนย์คอมพิวเตอร์สำรอง (DR Site) รวมถึงการจัดเตรียมความพร้อมในการกลับคืนสู่สภาวะปกติ (Return to Normal)

กรอบแนวทางการจัดทำแผนกู้คืนระบบสารสนเทศองค์การสะพานปลา



ผังโครงสร้างระบบเครือข่ายองค์การสะพานปลา

๑. ระบบแม่ข่ายแอปพลิเคชันและฐานข้อมูล (Application Servers & Databases) ระบบงานคอมพิวเตอร์และฐานข้อมูลที่ปฏิบัติงานอยู่บนระบบบริหารจัดการเครื่องแม่ข่าย (Server) ภายในศูนย์คอมพิวเตอร์ ประกอบด้วย

- ระบบงานสำคัญระดับวิกฤต (Critical Systems) ได้แก่ ระบบเครือข่ายอินเทอร์เน็ต ระบบเว็บไซต์ ระบบบัญชี ซึ่งเป็นระบบข้อมูลหลักขององค์กร เช่น การจัดการด้านบัญชี การจัดเก็บรายได้ และฐานข้อมูลลูกค้า (เกษตรกร ชาวประมง และคู่ค้า)
- ระบบงานสนับสนุน (Support Systems) ได้แก่ ระบบบริหารจัดการสำนักงาน (e-Office)

๒. โครงสร้างพื้นฐานระบบเครือข่ายและระบบรักษาความปลอดภัย (Network & Security Infrastructure) อ้างอิงตามผังโครงสร้างระบบเครือข่าย (Network Diagram) ขององค์การสะพานปลา ครอบคลุมอุปกรณ์และระบบดังต่อไปนี้

- ระบบเครือข่ายภายใน (LAN/WLAN) การกระจายสัญญาณภายในอาคารผ่านอุปกรณ์สวิตช์ (Smart Switch Hikvision DS-3E1526P-SI) และจุดกระจายสัญญาณเครือข่ายไร้สาย (Access Point Grand stream AX3000) ซึ่งบริหารจัดการผ่านระบบคลาวด์ (GWN Cloud)

• ระบบรักษาความปลอดภัยทางกายภาพ (Physical Security) ระบบที่เชื่อมต่อผ่านเครือข่ายเพื่อรักษาความปลอดภัยของพื้นที่ ได้แก่ อุปกรณ์บันทึกภาพ (NVR Hikvision), กล้องวงจรปิด (CCTV) และระบบควบคุมการเข้า-ออก (Access Control HIP Ci690S)

๓. ส่วนงานที่เกี่ยวข้องและผู้ใช้งานระบบสารสนเทศหลัก (Key Stakeholders & System Users) ส่วนงานที่มีบทบาทสำคัญในการใช้งานระบบ และทำหน้าที่เป็น "เจ้าของข้อมูล (Data Owner)" ซึ่งต้องร่วมประเมินผลกระทบและยืนยันความถูกต้องของข้อมูลเมื่อเข้าสู่กระบวนการกู้คืนระบบ ประกอบด้วย

• ส่วนงานบริหารทรัพยากรบุคคล: รับผิดชอบข้อมูลบุคลากร

• ส่วนงานบัญชีการเงิน: รับผิดชอบข้อมูลบัญชี การจัดเก็บรายได้ และระบบบัญชีหลัก

• ส่วนงานสินเชื่อ: รับผิดชอบข้อมูลสินเชื่อและลูกหนี้

• ส่วนงานสะพานปลาและท่าเทียบเรือประมง: รับผิดชอบฐานข้อมูลลูกค้า และระบบบริหารจัดการตลาด

• ส่วนงานเทคโนโลยีสารสนเทศ (IT): เป็นหน่วยงานหลัก (Core Team) ในการบริหารจัดการโครงสร้างพื้นฐาน การสำรองข้อมูล และการดำเนินการกู้คืนระบบเครือข่ายและเครื่องแม่ข่ายทั้งหมด

การดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance)

• ฐานทางกฎหมาย (Legal Basis): การประมวลผลและการจัดเก็บข้อมูลระบบบริหารงานบุคคล และระบบบัญชี (เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า สินเชื่อ) อาศัย ฐานสัญญา (Contract) และฐานความจำเป็นในการปฏิบัติตามกฎหมาย (Legal Obligation) * หน้าที่ของเจ้าของข้อมูล (Data Owner Role): ตามข้อ ๓ ส่วนงานต่าง ๆ ในฐานะเจ้าของข้อมูล (Data Owner) ตามกรอบธรรมาภิบาลข้อมูล (Data Governance) ต้องกำหนดระดับความสำคัญชั้นความลับของข้อมูล และต้องมั่นใจว่าในระหว่างที่มีการกู้คืนระบบข้อมูลส่วนบุคคลจะไม่ถูกเปิดเผยต่อผู้ที่ไม่มีสิทธิเกี่ยวข้อง (Access Control)

• มาตรการรักษาความปลอดภัยทางกายภาพ: ระบบในข้อ ๒ (CCTV และ Access Control) ถือเป็นมาตรการเชิงกายภาพที่ป้องกันไม่ให้ผู้ไม่มีอำนาจเข้าถึงห้องปฏิบัติการหรือตู้สื่อสาร (Cabinet 27U) ซึ่งเป็นที่ตั้งของฐานข้อมูลสำคัญ

การจัดลำดับความสำคัญของระบบงานและเป้าหมายการกู้คืน (System Criticality and Recovery Objectives)

เพื่อให้การบริหารจัดการความต่อเนื่องทางธุรกิจและการกู้คืนระบบเทคโนโลยีสารสนเทศขององค์การสะพานปลา (อสป.) ดำเนินไปอย่างมีประสิทธิภาพ และสอดคล้องกับผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) จึงได้กำหนดกระบวนการหลักที่ต้องให้ความสำคัญสูงสุด (Critical Processes) พร้อมทั้งกำหนดกรอบระยะเวลาเป้าหมายในการกู้คืนระบบ ดังนี้

๑. นิยามและเป้าหมายระยะเวลาการกู้คืนในภาพรวม

• เป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) กำหนดไว้ที่ ๑ วัน (๒๔ ชั่วโมง) หมายถึง ระยะเวลาเป้าหมายสูงสุดที่องค์การสะพานปลายอมรับได้ในการกู้คืนระบบสารสนเทศให้กลับมาพร้อมใช้งาน นับตั้งแต่เกิดเหตุขัดข้องจนถึงเวลาที่ระบบสามารถให้บริการได้ตามปกติ

• เป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) กำหนดไว้ที่ ๐.๕ วัน (๑๒ ชั่วโมง) หมายถึง ปริมาณข้อมูลสูงสุดที่องค์กรยอมรับได้ว่าอาจสูญหายไปจากเหตุการณ์วิกฤต ซึ่งบ่งบอกถึงความถี่ในการสำรองข้อมูล (Backup Frequency) ว่าต้องดำเนินการอย่างน้อยทุก ๆ ๑๒ ชั่วโมง

• ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerable Period of Disruption: MTPD) กำหนดไว้ที่ ๓.๕ วัน (๘๔ ชั่วโมง) หมายถึง ระยะเวลาสูงสุดที่กระบวนการปฏิบัติงานหลักสามารถหยุดชะงักได้ ก่อนที่จะส่งผลกระทบรุนแรงจนไม่อาจยอมรับได้ต่อภารกิจ ชื่อเสียง และสถานะทางการเงินขององค์กร

๒. การจัดลำดับความสำคัญของระบบงานหลัก (System Priority List) คณะกรรมการ/คณะทำงานได้พิจารณาจัดลำดับความสำคัญของระบบสารสนเทศหลัก เพื่อให้ทีมกู้คืนระบบ (DR Team) ใช้เป็นเกณฑ์ในการจัดสรรทรัพยากรและลำดับคิวก่อน-หลังในการกู้คืนระบบ ดังตารางต่อไปนี้

ลำดับความสำคัญ	กระบวนการหลัก / ระบบงาน	รายละเอียดของระบบงานและข้อมูล	RTO (วัน)	RPO (วัน)	MTPD (วัน)
๑	ระบบบัญชี (MyAccount Cloud)	ระบบประมวลผลงานบัญชีและการเงินทั้งหมดขององค์กร รวมถึงการรับ-จ่ายเงินของ อสป.	๑	๐.๕	๓.๕
๒	ระบบบริหารงานบุคคล (HR)	ระบบจัดการข้อมูลบุคลากรทั้งหมด ข้อมูลเงินเดือน สวัสดิการ และประวัติพนักงาน อสป.	๑	๐.๕	๓.๕
๓	ระบบสินเชื่อ (Core loan	ระบบจัดการข้อมูลลูกหนี้ สัญญาประเภทต่าง ๆ	๑	๐.๕	๓.๕
๔	ระบบบริหารจัดการตลาด (Horga Market App)	ระบบจัดการพื้นที่เช่าสำหรับสะพานปลาและท่าเทียบเรือประมง สัญญาเช่า การจัดเก็บรายได้ และฐานข้อมูลลูกค้า	๑	๐.๕	๓.๕

โครงสร้างทีมปฏิบัติการกู้คืนระบบและกระบวนการแจ้งเหตุฉุกเฉิน (DR Team Roles & Responsibilities and Call Tree Process)

การกู้คืนระบบเทคโนโลยีสารสนเทศในสภาวะวิกฤต จำเป็นต้องมีการกำหนดโครงสร้างคณะทำงานที่ชัดเจน เพื่อให้การสั่งการและการปฏิบัติงานเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ โดยมีรายละเอียดดังนี้

๑. โครงสร้างและบทบาทหน้าที่ของคณะทำงานกู้คืนระบบเทคโนโลยีสารสนเทศ (IT-DR Team) กำหนดให้เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศและผู้ที่เกี่ยวข้อง ปฏิบัติหน้าที่แบ่งตามบทบาทความรับผิดชอบ ดังต่อไปนี้

๑.๑ ผู้อำนวยการกู้คืนระบบ (IT-DR Commander): โดยตำแหน่ง หัวหน้าสำนักเทคโนโลยีสารสนเทศ

- ทำหน้าที่ประเมินสถานการณ์ ตัดสินใจประกาศใช้แผนกู้คืนระบบ (Activate IT-DRP)
- อนุมัติการเคลื่อนย้ายระบบไปยังศูนย์คอมพิวเตอร์สำรอง (DR Site) หรือการใช้ระบบสำรอง
- รายงานสถานการณ์ต่อผู้บริหารระดับสูงขององค์การสะพานปลา (อสป.) อย่างต่อเนื่อง

๑.๒ ผู้ประสานงานเหตุฉุกเฉิน (Incident Coordinator) * ทำหน้าที่บริหารจัดการการแจ้งเตือน (Call Tree) ให้บุคลากรในทีมรับทราบเมื่อเกิดภัยพิบัติ

- เป็นศูนย์กลางในการสื่อสารและสั่งการไปยังส่วนงานที่เกี่ยวข้อง (User/Data Owner)
- ประสานงานกับผู้ให้บริการภายนอก (Third Party / Vendor) เช่น ผู้ให้บริการเครือข่าย อินเทอร์เน็ต (ISP) หรือผู้รับจ้างบำรุงรักษาระบบ (MA)

๑.๓ ทีมปฏิบัติการเชิงเทคนิค (Technical Recovery Team): เจ้าหน้าที่ IT Network, System, Database

- ดำเนินการจัดเตรียมอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่ายที่จำเป็นต่อการกู้คืน
- ดำเนินการตั้งค่าระบบ (Configuration) อัปโหลดข้อมูลสำรอง (Restore Backup) และเชื่อมต่อระบบเครือข่ายให้เป็นไปตามค่าเป้าหมาย RTO/RPO ที่กำหนด
- ดำเนินการทดสอบระบบ (System Testing) เบื้องต้นก่อนส่งมอบให้ส่วนงานเจ้าของข้อมูลทดสอบความถูกต้อง

๒. กระบวนการแจ้งเหตุและการสั่งการ (Call Tree & Incident Reporting) เมื่อมีการเฝ้าระวังหรือตรวจพบเหตุผิดปกติที่อาจลุกลามเป็นภัยพิบัติ ให้ดำเนินการตามขั้นตอนการสื่อสารฉุกเฉิน (Call Tree) ดังนี้:

๑) การตรวจพบและรายงาน เจ้าหน้าที่ผู้พบเหตุ (หรือระบบแจ้งเตือนอัตโนมัติ) รายงานเหตุการณ์ต่อ หัวหน้าสำนักเทคโนโลยีสารสนเทศ ทันที

๒) การประเมินและการสั่งการ หัวหน้าสำนักฯ ประเมินความรุนแรง หากประเมินแล้วระบบหลักหยุดชะงักและไม่สามารถแก้ไขได้ในเวลาปกติ ให้สั่งการเปิดใช้แผนกู้คืนระบบ

๓) การกระจายข่าวสาร (Call Tree Activation): แจ้งไปยัง ผู้ประสานงานเหตุฉุกเฉิน เพื่อดำเนินการใช้แผนผังการติดต่อฉุกเฉิน (Call Tree) โทรศัพท์หรือส่งข้อความแจ้งเตือนสมาชิกในทีมปฏิบัติการทั้งหมดให้รับทราบและเตรียมพร้อมปฏิบัติหน้าที่ตามแผนทันที

การดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance)

• มาตรการรักษาความปลอดภัยด้านการสื่อสาร: ในระหว่างการสื่อสารเหตุฉุกเฉินผ่าน Call Tree หรือกลุ่มแอปพลิเคชันสนทนา ห้ามมิให้มีการส่งต่อ หรือเปิดเผยข้อมูลส่วนบุคคลที่อาจรั่วไหลจากระบบ (เช่น ข้อมูลบัญชี ข้อมูลลูกค้า) ลงในช่องทางการสื่อสารที่ไม่มีการเข้ารหัส หรือช่องทางส่วนตัว

• สิทธิความเป็นส่วนตัวของพนักงาน: รายชื่อและหมายเลขโทรศัพท์ส่วนตัวของทีมงานในเอกสาร Call Tree ให้ถือเป็นข้อมูลที่มีชั้นความลับ (Confidential) การจัดเก็บและแจกจ่ายให้จำกัดเฉพาะผู้ที่มีหน้าที่เกี่ยวข้องในการกู้คืนระบบเท่านั้น

ศูนย์ปฏิบัติการสำรองและการจัดเตรียมทรัพยากรเพื่อการกู้คืนระบบ (Disaster Recovery Site & Resource Preparation)

เพื่อให้การกู้คืนระบบเทคโนโลยีสารสนเทศดำเนินไปได้อย่างรวดเร็วและเป็นไปตามเป้าหมาย (RTO/RPO) ที่กำหนด องค์การสะพานปลาได้กำหนดแนวทางการจัดเตรียมสถานที่ อุปกรณ์ และระบบเครือข่ายสำรอง ดังต่อไปนี้

๑. ศูนย์ปฏิบัติการสำรอง (Disaster Recovery Site: DR-Site)

• กำหนดให้ใช้บริการโครงสร้างพื้นฐานคลาวด์ (Cloud Infrastructure) จากผู้ให้บริการภายนอก (Cloud Service Provider) เป็นศูนย์คอมพิวเตอร์สำรอง

• มีการจัดเตรียมพื้นที่และสภาพแวดล้อม (Environment) ล่วงหน้าให้มีความเหมาะสมและสอดคล้องกับระบบบริหารจัดการเครื่องแม่ข่าย (Smart Switch Hikvision DS-3E1526P-SI) ขององค์การสะพานปลา เพื่อให้พร้อมรองรับการเปิดใช้งานระบบงานหลัก (เช่น ระบบบริหารงานบุคคล และระบบบัญชี) ได้ทันทีเมื่อมีการประกาศใช้แผนกู้คืนระบบ

๒. การจัดเตรียมอุปกรณ์คอมพิวเตอร์และฮาร์ดแวร์ฉุกเฉิน (Emergency Hardware)

• ในสภาวะวิกฤต ให้ทีมปฏิบัติการกู้คืนระบบ (IT-DR Team) เบิกใช้เครื่องคอมพิวเตอร์พกพา (Notebook) สำรองที่มีอยู่ในระบบทะเบียนทรัพย์สินขององค์การสะพานปลา

• เครื่องคอมพิวเตอร์พกพาดังกล่าวต้องมีคุณสมบัติพร้อมเชื่อมต่อเครือข่ายอินเทอร์เน็ต และต้องได้รับการติดตั้งระบบปฏิบัติการที่อัปเดตแพตช์ (Patch) ล่าสุด รวมถึงซอฟต์แวร์ป้องกันไวรัส

(Antivirus/Endpoint Protection) เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ที่ไม่ได้มาตรฐานเชื่อมต่อเข้าสู่ระบบ DR-Site

๓. การเชื่อมต่อเครือข่ายอินเทอร์เน็ตสำรอง (Backup Internet Connection)

• กรณีที่ระบบเครือข่ายหรืออินเทอร์เน็ตของศูนย์คอมพิวเตอร์หลัก (Primary Site) ขัดข้อง ให้ทีมปฏิบัติการกู้คืนระบบใช้อินเทอร์เน็ตผ่านช่องทางสำรอง เช่น อุปกรณ์กระจายสัญญาณเคลื่อนที่ (Mobile Hotspot 4G/5G)

• การใช้เครื่องคอมพิวเตอร์พกพาเชื่อมต่ออินเทอร์เน็ตสำรองเพื่อเข้าสู่ระบบ Cloud DR-Site สำหรับการตั้งค่าระบบ (Configuration) หรือการอัปโหลด/กู้คืนฐานข้อมูล (Database Restore) จะต้องดำเนินการผ่านช่องทางการเชื่อมต่อที่ปลอดภัยและมีการเข้ารหัส (เช่น VPN - Virtual Private Network หรือ HTTPS) เพื่อป้องกันการดักจับข้อมูลระหว่างทาง (Data Interception)

การดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance) และความมั่นคงปลอดภัย

• สัญญากับผู้ให้บริการ (Data Processing Agreement) การใช้บริการ Cloud DR-Site ผู้ให้บริการคลาวด์มีฐานะเป็น “ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)” ดังนั้น องค์การสะพานปลา (ในฐานะผู้ควบคุมข้อมูล) ต้องมั่นใจว่าผู้ให้บริการมีมาตรการรักษาความมั่นคงปลอดภัยที่ได้มาตรฐาน (เช่น ISO/IEC 27001, ISO/IEC 27701) และมีข้อตกลงการไม่เปิดเผยข้อมูลอย่างรัดกุม

• การเข้ารหัสข้อมูล (Encryption) ฐานข้อมูลลูกค้า ข้อมูลพนักงาน และข้อมูลบัญชี ที่ต้องทำการ Upload หรือ Sync ไปยัง Cloud DR-Site จะต้องมีการเข้ารหัสข้อมูลทั้งในขณะพัก (Data at Rest) และขณะส่งผ่านเครือข่าย (Data in Transit)

• การควบคุมการเข้าถึง (Access Control) การใช้ Notebook นอกสถานที่หรือเชื่อมต่อผ่าน Hotspot ต้องมีการพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ก่อนอนุญาตให้เจ้าหน้าที่ IT เข้าสู่ระบบจัดการ Cloud DR-Site

เกณฑ์การประเมินระดับความรุนแรงของเหตุการณ์ (Incident Severity Assessment Criteria)

ระดับเหตุการณ์	ประเภทของเหตุการณ์	คำอธิบายและผลกระทบ (Description & Impact)	การตอบสนองและเกณฑ์การประกาศใช้แผน (Response & Escalation)
๐	เหตุการณ์ขัดข้องทั่วไป / แจ้งขอรับบริการ (Minor Incident / Service Request)	ผลกระทบต่ำ: ระบบงานสำคัญขององค์กรยังสามารถให้บริการได้ตามปกติ เป็นเพียงปัญหาที่เกิดกับผู้ใช้งานบางราย หรืออุปกรณ์ปลายทาง (Endpoint) เช่น เครื่องคอมพิวเตอร์เปิดไม่ติด, ปัญหาการเชื่อมต่อเครือข่ายเฉพาะจุด, ผู้ใช้งานลืมรหัสผ่าน หรือข้อผิดพลาดจากการปฏิบัติงาน (Human Error)	ดำเนินการแก้ไขตามขั้นตอนปกติของส่วนงานสนับสนุน (IT Helpdesk) ตามกรอบเวลาการให้บริการ (SLA)

ระดับเหตุการณ์	ประเภทของเหตุการณ์	คำอธิบายและผลกระทบ (Description & Impact)	การตอบสนองและเกณฑ์การประกาศใช้แผน (Response & Escalation)
๑	เหตุการณ์รุนแรง / ขัดข้องวงกว้าง (Warning / Alert)	ผลกระทบปานกลาง: เกิดเหตุการณ์ผิดปกติทางกายภาพหรือทางไซเบอร์ แต่ยังไม่ส่งผลให้ระบบหลักหยุดชะงัก เช่น ไฟไหม้/น้ำท่วมในบริเวณใกล้เคียงพื้นที่องค์กร, การชุมนุมประท้วงปิดกั้นเส้นทางรอบนอก, หรือระบบตรวจพบความพยายามเจาะระบบ (Port Scanning/Phishing) แต่ระบบรักษาความปลอดภัยยังป้องกันไว้ได้	ทีม IT แจ้งเตือนผู้เกี่ยวข้อง (Incident Coordinator) เฝ้าระวังสถานการณ์อย่างใกล้ชิด และเตรียมความพร้อมหากเหตุการณ์ยกระดับความรุนแรง
๒	เหตุการณ์เฝ้าระวัง (Major Incident)	ผลกระทบสูง: เหตุการณ์ที่ส่งผลให้ระบบงานสำคัญ (เช่น ระบบบัญชี, MIS) หยุดชะงัก ไม่สามารถให้บริการได้ หรือถูกโจมตีทางไซเบอร์ (เช่น มัลแวร์, ระบบเครือข่ายล่ม, ไฟฟ้าหลักดับเป็นเวลานาน) แต่ยังสามารถเข้าถึงศูนย์คอมพิวเตอร์หลัก (Primary Site) ได้ และมีแนวโน้มที่จะแก้ไขได้ภายในเวลา RTO	หัวหน้าสำนักงานเทคโนโลยีสารสนเทศ สั่งการระดมทีมเทคนิคเข้าแก้ไขปัญหาทันที หากประเมินว่าไม่สามารถแก้ไขได้ภายในเวลา RTO ที่กำหนด (๑ วัน) ให้ยกระดับเป็นเหตุการณ์ระดับ ๓
๓	สภาวะวิกฤต / ภัยพิบัติ (Disaster)	ผลกระทบรุนแรงสูงสุด: โครงสร้างพื้นฐานหรือศูนย์คอมพิวเตอร์หลักได้รับความเสียหายอย่างหนักจากภัยธรรมชาติ (อัคคีภัย, อุทกภัย) หรือถูกโจมตีทางไซเบอร์ขั้นรุนแรง (เช่น Ransomware เข้ารหัสฐานข้อมูลทั้งหมด) ไม่สามารถเข้าถึงพื้นที่ปฏิบัติงานหลักได้ หรือระบบล่มอย่างสมบูรณ์ และไม่สามารถกู้คืนได้ทันตามเป้าหมาย	ผู้อำนวยการฝ่ายกู้คืนระบบ ประกาศใช้แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Activate IT-DRP) และสั่งการให้ย้ายระบบไปทำงานที่ศูนย์คอมพิวเตอร์สำรอง (Cloud DR-Site) ทันที

แนวทางการตอบสนองและปฏิบัติการตามระดับเหตุการณ์ (Incident Response Guidelines)

ระดับเหตุการณ์	oผลกระทบและสถานการณ์ (Impact & Situation)	แนวทางปฏิบัติและขั้นตอนการตอบสนอง (Response Actions & Procedures)
o	เหตุการณ์ปกติ (Minor Incident) ระบบสำคัญยังสามารถใช้งานได้ปกติ เป็นเพียงการขัดข้องเฉพาะจุด หรืออุปกรณ์ของผู้ใช้งานปลายทาง	๑. รับแจ้งเหตุผ่านระบบรับแจ้งปัญหา (IT Helpdesk/Service Desk) ๒. ดำเนินการแก้ไขปัญหาตามคู่มือปฏิบัติงาน (SOP) และข้อตกลงระดับการให้บริการ (SLA) ๓. บันทึกรายละเอียดการแก้ไขปัญหาลงในระบบเพื่อเป็นฐานความรู้ (Knowledge Base)

ระดับเหตุการณ์	๐ผลกระทบและสถานการณ์ (Impact & Situation)	แนวทางปฏิบัติและขั้นตอนการตอบสนอง (Response Actions & Procedures)
๑	เหตุการณ์เฝ้าระวัง (Warning / Alert) เกิดเหตุการณ์ผิดปกติ เช่น การชุมนุมประท้วง น้ำท่วม หรือไฟไหม้บริเวณข้างเคียง แต่ระบบสารสนเทศสำคัญยังใช้งานได้	๑. แจ้งเหตุการณ์ต่อผู้เกี่ยวข้องผ่านผังการสื่อสาร (Call Tree) ระดับเฝ้าระวัง ๒. ติดตามและประเมินสถานการณ์อย่างใกล้ชิด (Monitor) ๓. ตรวจสอบสถานะการสำรองข้อมูลล่าสุด (Backup Status) ของระบบบัญชีและระบบ MIS ให้มั่นใจว่ามีความสมบูรณ์และเป็นไปตามค่า RPO (๐.๕ วัน) ๔. เตรียมความพร้อมของทรัพยากรบุคคลและอุปกรณ์กู้คืนระบบเบื้องต้น
๒	เหตุการณ์รุนแรง / ขัดข้องวงกว้าง (Major Incident) ระบบสำคัญไม่สามารถใช้งานได้ (เช่น ไฟฟ้าขัดข้อง, ถูกโจมตีด้วยมัลแวร์/ไวรัสคอมพิวเตอร์) ประเมินว่าต้องใช้เวลานานในการแก้ไข แต่ยังเข้าออกศูนย์คอมพิวเตอร์หลักได้	๑. สั่งการแจ้งเหตุฉุกเฉินผ่าน Call Tree เต็มรูปแบบไปยัง IT-DR Team ๒. กรณีภัยไซเบอร์ (เช่น ไวรัส/Ransomware): ให้ทำการตัดการเชื่อมต่อเครือข่าย (Isolate Network) ของเครื่องที่ติดเชื้อทันที เพื่อป้องกันการแพร่กระจาย ๓. เข้าตรวจสอบพื้นที่ ประเมินความเสียหาย และพยายามแก้ไขระบบหลักให้อยู่ในกรอบเวลา RTO (๑ วัน) ๔. จัดเตรียมคอมพิวเตอร์สำรอง (Notebook) พร้อมระบบอินเทอร์เน็ตมือถือ (Mobile Hotspot) ที่ผ่านการตั้งค่าความปลอดภัย (VPN) ๕. เตรียมการตั้งค่า (Configuration) โครงสร้างพื้นฐานบน Cloud DR-Site ล่วงหน้า ๖. หากประเมินว่าไม่สามารถแก้ไขได้ทันเวลา RTO ให้เตรียมนำเสนอผู้อำนวยการฯ เพื่อยกระดับเหตุการณ์เป็นระดับ ๓
๓	สภาวะวิกฤต / ภัยพิบัติ (Disaster) เหตุการณ์รุนแรงที่สุด (เช่น อัคคีภัย อุทกภัย) โครงสร้างพื้นฐานเสียหายหนัก ระบบสำคัญหยุดให้บริการเป็นเวลานาน และไม่สามารถเข้าถึงพื้นที่ปฏิบัติงานหลักได้	๑. แจ้งเหตุผู้บริหารระดับสูงผ่าน Call Tree และ ประกาศใช้แผนกู้คืนระบบเทคโนโลยีสารสนเทศ (Activate IT-DRP) อย่างเป็นทางการ ๒. ให้ทีม IT ย้ายไปปฏิบัติงาน ณ พื้นที่ปลอดภัย หรือเชื่อมต่อผ่านอุปกรณ์สำรอง ๓. เปิดใช้งานระบบงานสำรอง (Failover) บน Cloud DR-Site ๔. กู้คืนฐานข้อมูล (Restore Database) และทดสอบความถูกต้องของระบบและข้อมูลร่วมกับส่วนงานเจ้าของข้อมูล (Data Owner) ๕. แจ้งประสานงานไปยังสำนักงานสาขา ท่าเทียบเรือประมง และหน่วยงานที่เกี่ยวข้อง ให้เปลี่ยนเส้นทาง (Reroute) มาใช้งานผ่านระบบ DR-Site ๖. สื่อสารความคืบหน้าให้ผู้บริหารและผู้ใช้บริการทราบเป็นระยะจนกว่าสถานการณ์จะคลี่คลาย

การดำเนินการด้านกฎหมายและมาตรฐานที่เกี่ยวข้อง

• พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในเหตุการณ์ระดับ ๒ หากเป็นการโจมตีทางไซเบอร์ ทีม IT ต้องรักษาหลักฐานทางดิจิทัล (Digital Forensics) และห้ามทำลาย Log file โดยเด็ดขาด เพื่อใช้สืบสวนหาต้นตอของการโจมตี

• พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)

◦ มาตรการรักษาความปลอดภัย ในขั้นตอนการเตรียม Notebook และ Mobile Hotspot (ระดับ ๒ และ ๓) อุปกรณ์ดังกล่าวต้องมีการเข้ารหัสข้อมูล (Encryption) และห้ามดาวน์โหลดข้อมูลส่วนบุคคล (เช่น ฐานข้อมูลพนักงาน/ลูกค้า) ลงบนเครื่อง Notebook ในท้องถิ่น (Local Drive) โดยตรง เพื่อป้องกันความเสี่ยง (Data Minimization & Security)

◦ การรายงานเหตุละเมิด: หากเหตุการณ์ระดับ ๒ หรือ ๓ ทำให้ข้อมูลส่วนบุคคลรั่วไหล ต้องปฏิบัติตามนโยบายการแจ้งเหตุละเมิดข้อมูลส่วนบุคคลภายใน ๗๒ ชั่วโมง

มาตรการลดความเสี่ยงที่อาจทำให้ระบบหยุดชะงัก

ระบบสารสนเทศหลัก (Critical Systems)	ปัจจัยเสี่ยงและภัยคุกคาม (Risk Factors & Threats)	มาตรการป้องกันและลดความเสี่ยง (Mitigation Measures)
ระบบบริหารงานบุคคล และ ระบบบัญชี	๑.๑ ภัยคุกคามทางไซเบอร์ มัลแวร์เรียกค่าไถ่ (Ransomware) หรือไวรัสคอมพิวเตอร์ ๑.๒ ความผิดพลาดของระบบ ข้อผิดพลาดจากการอัปเดตระบบปฏิบัติการ หรือ ซอฟต์แวร์ (Patch Update Failure)	ผู้ให้บริการ • ติดตั้งและอัปเดตระบบป้องกันมัลแวร์ระดับปลายทาง (Endpoint Detection and Response: EDR / Antivirus)ตรวจสอบการตั้งค่า Firewall • ตรวจสอบและปรับปรุงนโยบายการตั้งค่าอุปกรณ์รักษาความปลอดภัย (Firewall / WAF) อย่างสม่ำเสมอ • จัดทำกระบวนการทดสอบแพตช์ (Patch Management) ในสภาพแวดล้อมทดสอบ (Test Environment) ก่อนนำไปติดตั้งจริง • จัดทำระบบสำรองข้อมูลแบบจำลองสถานะ (Snapshot) และจัดเก็บเวอร์ชันย้อนหลัง (Versioning) เพื่อให้ย้อนกลับได้ทันที
ระบบบริหารจัดการเครื่องแม่ข่าย (Server / Smart Switch Hikvision DS-3E1526P-SI)	๒.๑ ความเสียหายทางกายภาพและสภาพแวดล้อมอัคคีภัย, ระบบไฟฟ้าขัดข้อง, อุณหภูมิสูงเกินกำหนด ๒.๒ ฮาร์ดแวร์เสื่อมสภาพ	• ดำเนินการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance: PM) ผ่านสัญญาจ้างบริการ (MA) อย่างต่อเนื่อง • ควบคุมสภาพแวดล้อมของศูนย์คอมพิวเตอร์ (Server Room) ให้ได้มาตรฐาน เช่น ติดตั้งเครื่องสำรองไฟ (UPS), ระบบปรับอากาศสำรอง, ระบบตรวจจับและดับเพลิงอัตโนมัติ

ระบบสารสนเทศหลัก (Critical Systems)	ปัจจัยเสี่ยงและภัยคุกคาม (Risk Factors & Threats)	มาตรการป้องกันและลดความเสี่ยง (Mitigation Measures)
		• มีระบบควบคุมการเข้า-ออกพื้นที่ (Physical Access Control) และบันทึกภาพด้วยกล้องวงจรปิด (CCTV)
โครงสร้างพื้นฐานระบบเครือข่าย (Network & Internet)	๓.๑ วงจรสื่อสารขัดข้อง ระบบอินเทอร์เน็ตหลักล่ม หรือสายสัญญาณภายนอกขาด ๓.๒ อุปกรณ์หรือสายสัญญาณภายในชำรุด	• ออกแบบสถาปัตยกรรมเครือข่ายแบบความพร้อมใช้งานสูง (High Availability: HA) โดยติดตั้งวงจรหลักเป็น MPLS และวงจรสำรองผ่าน Fiber Optic ต่างผู้ให้บริการ • จัดเตรียมอุปกรณ์กระจายสัญญาณอินเทอร์เน็ตผ่านเครือข่ายโทรศัพท์เคลื่อนที่ (Mobile Hotspot 4G/5G) สำหรับกรณีฉุกเฉิน • กำหนดจุดติดตั้งอุปกรณ์กระจายสัญญาณ (Access Point) สำรองในพื้นที่ปฏิบัติงานสำคัญ • สำรองไฟล์การตั้งค่า (Configuration Backup) ของ Router และ Switch อย่างสม่ำเสมอ
ฐานข้อมูล (Database)	๔.๑ การโจมตีฐานข้อมูล การเจาะระบบเพื่อขโมยหรือทำลายข้อมูล ๔.๒ ความผิดพลาดของบุคลากร (Human Error): ผู้ใช้งานหรือผู้ดูแลระบบลบ/แก้ไขข้อมูลสำคัญโดยอุบัติเหตุ	• กำหนดสิทธิการเข้าถึงฐานข้อมูลตามความจำเป็นของหน้างาน (Least Privilege) และบังคับใช้รหัสผ่านที่ซับซ้อน • เปิดใช้งานระบบบันทึกประวัติการใช้งานฐานข้อมูล (Database Audit Log • ตั้งเวลาสำรองฐานข้อมูลอัตโนมัติอย่างน้อยวันละ ๒ ครั้ง (ให้สอดคล้องกับค่า RPO = ๐.๕ วัน) และแยกเก็บข้อมูลสำรองแบบออฟไลน์ (Offline Backup) เพื่อป้องกัน Ransomware
ระบบสินเชื่อ (Core loan)	๕.๑ ความล้มเหลวของซอฟต์แวร์หรือฮาร์ดแวร์ ๕.๒ ข้อมูลเอกสารสัญญาอิเล็กทรอนิกส์สูญหาย	• มีสัญญาการบำรุงรักษาระบบซอฟต์แวร์ (Software MA) จากผู้พัฒนาเพื่อให้คำปรึกษาและแก้ไขข้อบกพร่อง (Bug) ทันที • สำรองไฟล์เอกสารสัญญาและฐานข้อมูลของระบบไปยังพื้นที่จัดเก็บแยกต่างหากอย่างสม่ำเสมอ

การดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance)

มาตรการลดความเสี่ยงที่ระบุในตาราง ถือเป็น “มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (Appropriate Security Measures)” ตามที่กฎหมาย PDPA กำหนด โดยเน้นย้ำในประเด็นต่อไปนี้

• การป้องกันข้อมูลรั่วไหล: การติดตั้ง Firewall, EDR และการกำหนดสิทธิเข้าถึงฐานข้อมูล (Access Control) เป็นการรักษาความลับ (Confidentiality) ของข้อมูลเกษตรกร ชาวประมง และพนักงาน

• ความพร้อมใช้และความถูกต้อง: การทำ Snapshot, การทำ MA เครื่องแม่ข่าย และการสำรองข้อมูล (Backup) ช่วยรับประกันความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคล

• การเข้าถึงระบบเพื่อทำ MA โดยผู้ให้บริการภายนอก (Third-Party/Vendor) จะต้องมีการลงนามใน ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) และ ข้อตกลงการรักษาความลับ (NDA) ทุกครั้ง

การกลับสู่สภาวะปกติ (Return to Normal Operations / Failback)

เมื่อสถานการณ์ภัยพิบัติหรือสภาวะวิกฤตได้คลี่คลายลง และศูนย์คอมพิวเตอร์หลัก (Primary Site) ได้รับการซ่อมแซมจนมีความพร้อม คณะทำงานกู้คืนระบบต้องดำเนินการย้ายระบบงานและข้อมูลจากศูนย์คอมพิวเตอร์สำรอง (DR-Site) กลับสู่ศูนย์หลัก โดยมีขั้นตอนดังต่อไปนี้

ข้อ ๑. การประเมินความพร้อมและกำหนดช่วงเวลา (Readiness Assessment & Scheduling)

• ผู้อำนวยการกู้คืนระบบ (IT-DR Commander) ร่วมกับทีมปฏิบัติการเชิงเทคนิค ตรวจสอบความสมบูรณ์ของโครงสร้างพื้นฐาน ระบบไฟฟ้า ระบบเครือข่าย และสภาพแวดล้อมของศูนย์คอมพิวเตอร์หลัก

• กำหนดช่วงเวลา (Maintenance Window) ในการดำเนินการย้ายระบบกลับ (Failback) โดยให้เป็นช่วงเวลาที่มีการใช้งานระบบน้อยที่สุด (Off-peak Hours) เพื่อหลีกเลี่ยงผลกระทบต่อผู้ใช้งาน

ข้อ ๒. การซิงโครไนซ์ข้อมูลและการย้ายระบบกลับ (Data Synchronization & Failback Execution)

• ทีมปฏิบัติการเชิงเทคนิคดำเนินการซิงโครไนซ์ (Synchronize) ฐานข้อมูลที่มีการเปลี่ยนแปลงระหว่างที่ปฏิบัติงานอยู่บน Cloud DR-Site (เช่น ข้อมูลระบบบัญชี, การบันทึกเวลาพนักงานในระบบ MIS) กลับมายังเครื่องแม่ข่าย (Server) ณ ศูนย์คอมพิวเตอร์หลัก

• ดำเนินการปรับเปลี่ยนเส้นทางเครือข่าย (Network Rerouting) และ DNS กลับมาใช้หมายเลข IP ของศูนย์คอมพิวเตอร์หลัก

ข้อ ๓. การทดสอบและยืนยันความถูกต้อง (Validation & Sign-off)

• ประสานงานกับส่วนงานที่เป็นเจ้าของข้อมูล (Data Owner) ได้แก่ ส่วนงานบัญชีการเงิน ส่วนงานทรัพยากรบุคคล ฯลฯ เพื่อทดสอบการใช้งานและตรวจสอบความถูกต้องครบถ้วนของข้อมูล (Data Integrity)

• เมื่อได้รับการยืนยันความถูกต้อง ให้ผู้อำนวยการกู้คืนระบบประกาศ “ยุติการใช้แผน IT-DRP” และแจ้งให้ผู้บริหารและผู้ใช้งานทราบว่าระบบกลับสู่สภาวะปกติแล้ว

การทดสอบ การบำรุงรักษา และการทบทวนแผน (Plan Testing, Maintenance & Review)

เพื่อให้แผนกู้คืนระบบเทคโนโลยีสารสนเทศมีความทันสมัยและสามารถนำไปปฏิบัติได้จริงในยามฉุกเฉิน องค์การสะพานปลาต้องดำเนินการดังต่อไปนี้:

ข้อ ๔. การทดสอบแผนกู้คืนระบบ (IT-DRP Testing)

• กำหนดให้มีการทดสอบแผนกู้คืนระบบ **อย่างน้อยปีละ ๑ ครั้ง**

รูปแบบการทดสอบ: ให้พิจารณาเลือกรูปแบบที่เหมาะสม ได้แก่

○ การซ้อมแผนบนโต๊ะ (Tabletop Exercise): การจำลองสถานการณ์สมมติเพื่อทบทวนขั้นตอนการประสานงานและหน้าที่ความรับผิดชอบ

○ การทดสอบเสมือนจริง (Simulation / Parallel Test): การกู้คืนระบบไปยัง DR-Site จริง ควบคู่ไปกับระบบหลัก เพื่อประเมินว่าสามารถทำได้ตามระยะเวลาเป้าหมาย (RTO / RPO) หรือไม่ โดยไม่กระทบต่อผู้ใช้งาน

• ต้องมีการจัดทำรายงานสรุปผลการทดสอบ (DR Test Report) ระบุปัญหา อุปสรรค และข้อเสนอแนะ นำเสนอต่อคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ (BCM Committee)

ข้อ ๕. การทบทวนและการปรับปรุงแผน (Plan Review & Maintenance)

• ต้องทบทวนและปรับปรุงเนื้อหาของแผน IT-DRP ทันทีเมื่อเกิดการเปลี่ยนแปลงอย่างมีนัยสำคัญ ได้แก่:

○ มีการติดตั้ง เปลี่ยนแปลง หรือยกเลิกระบบงานที่สำคัญ

○ มีการเปลี่ยนแปลงโครงสร้างบุคลากรที่อยู่ในผังการสื่อสาร (Call Tree)

○ ภายหลังจากการเกิดเหตุการณ์จริง (Post-Incident) หรือภายหลังการทดสอบแผนประจำปี เพื่อนำข้อบกพร่อง (Lessons Learned) มาปรับปรุง

• ให้มีกระบวนการตรวจสอบและอัปเดตข้อมูลการติดต่อของผู้ให้บริการภายนอก (Third-Party / Vendor) และรายละเอียดฮาร์ดแวร์ให้เป็นปัจจุบันเสมอ

การดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance)

• การทำลายข้อมูลบนศูนย์สำรอง (Data Disposal): หลังจากขั้นตอนการย้ายระบบกลับ (Failback) เสร็จสิ้นสมบูรณ์ และข้อมูลได้รับการยืนยันว่าครบถ้วน ข้อมูลส่วนบุคคลที่ถูกทำสำเนาหรือ

ประมวลผลอยู่บนระบบ Cloud DR-Site ต้องถูกตั้งค่า ระยะเวลาจัดเก็บ (Retention Period) ชั่วคราว และต้องถูกลบหรือทำลายอย่างปลอดภัย (Secure Wipe) เพื่อไม่ให้มีข้อมูลตกค้าง ตามหลัก Data Minimization

• การใช้ข้อมูลเพื่อการทดสอบแผน (Data for Testing): ในการซักซ้อมแผนประจำปี (DR Testing) ให้หลีกเลี่ยงการใช้ข้อมูลส่วนบุคคลจริง (Real Data) โดยให้ใช้ข้อมูลจำลอง (Dummy Data) หรือข้อมูลที่ผ่านการทำพรางข้อมูล (Data Anonymization/Pseudonymization) เพื่อป้องกันข้อมูลรั่วไหลระหว่างการซ้อม

• การประเมิน DPIA หากองค์การสะพานปลามีการเปลี่ยนผู้ให้บริการ Cloud DR-Site รายใหม่ จะต้องดำเนินการทำ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) ใหม่ทุกครั้ง ก่อนทำการเชื่อมต่อและส่งข้อมูล

ภาคผนวก

การดำเนินการด้านการคุ้มครองข้อมูลส่วนบุคคล (PDPA Compliance)

- มาตรการรักษาความลับ เอกสารภาคผนวก ก. (รายชื่อและเบอร์โทรศัพท์ส่วนตัว) ถือเป็นข้อมูลส่วนบุคคลที่มีชั้นความลับ ห้ามทำสำเนาแจกจ่ายแก่ผู้ไม่มีส่วนเกี่ยวข้องโดยเด็ดขาด
- ระยะเวลาจัดเก็บ (Retention Period) แบบฟอร์มตามภาคผนวก ค. และ ง. ที่มีการบันทึกการทำงานแล้ว ให้จัดเก็บไว้เป็นเวลา ๓ ปี เพื่อใช้เป็นหลักฐานประกอบการตรวจสอบทางกฎหมายและการประเมิน SE-AM จากนั้นให้ทำลายทิ้งด้วยวิธีที่ปลอดภัย (Secure Destruction)

ภาคผนวก ก
แผนผังและรายชื่อผู้ติดต่อในสภาวะฉุกเฉิน (Emergency Call Tree & Contact List)

ก.๑ โครงสร้างการแจ้งเหตุ (Call Tree Workflow)

๑) ผู้พบเหตุการณ์ ➔ แจ้ง ➔ **ผู้ประสานงานเหตุฉุกเฉิน (IT Helpdesk/Coordinator)**

๒) ผู้ประสานงานเหตุฉุกเฉิน ➔ แจ้ง ➔ **ผู้อำนวยการกู้คืนระบบ (หัวหน้าสำนักเทคโนโลยีสารสนเทศ)**

๓) ผู้อำนวยการกู้คืนระบบ ➔ สั่งการ ➔ **ทีมปฏิบัติการเชิงเทคนิค (IT-DR Team)** และแจ้ง **ผู้บริหารระดับสูง**

ก.๒ ทะเบียนรายชื่อคณะทำงาน (IT-DR Team Contact List)

บทบาทหน้าที่	ชื่อ-นามสกุล	ตำแหน่ง	เบอร์โทรศัพท์มือถือ/อีเมล
ผู้อำนวยการกู้คืนระบบ	นางสาวรณิดา โชติธนาอุดม (รักษาการหัวหน้า)	หัวหน้าสำนักเทคโนโลยีสารสนเทศ	๐๖-๕๙๔๐-๘๓๑๙ ranida.c@fishmarket.co.th
ผู้ประสานงานเหตุฉุกเฉิน	นางสาวณัฐอนงค์ แสงจันทร์งาม	เจ้าหน้าที่บริหารงานทั่วไป	๐๙-๖๘๕๔-๔๒๔๑ natanong.s@fishmarket.co.th
ทีมเทคนิค (Network/Server)	นางสาวรณิดา โชติธนาอุดม	หัวหน้าสำนักเทคโนโลยีสารสนเทศ	๐๖-๕๙๔๐-๘๓๑๙ ranida.c@fishmarket.co.th
ทีมเทคนิค (Database/App)	นางสาวณัฐอนงค์ แสงจันทร์งาม	เจ้าหน้าที่บริหารงานทั่วไป	๐๙-๖๘๕๔-๔๒๔๑ natanong.s@fishmarket.co.th

ภาคผนวก ข

ข้อมูลติดต่อผู้ให้บริการภายนอก (Third-Party / Vendor Contact List)

ประเภทบริการ	ชื่อบริษัท / ผู้ให้บริการ	ข้อมูลผู้ติดต่อ (ชื่อ/เบอร์โทร/อีเมล)	เลขที่สัญญา / SLA	บริการที่รับผิดชอบ
ผู้ให้บริการ Cloud DR-Site	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) : GDCC	๐๒-๐๒๔-๑๙๙๙ กด ๐ หรือ helpdesk@gdcc.onde.go.th	R ๐๑๐๑๙๐๐๐๓๓-๒๔๐๑๐๐๐๒๘ (Call Center ๒๔ ชม.)	ดูแลระบบ Cloud Server
ผู้ให้บริการอินเทอร์เน็ต (ISP)	บริษัท ซิมโฟนี คอมมูนิเคชั่น จำกัด	คุณ นนทนันทน์ ไชยมงคล ๐๙-๒๒๕๔-๓๓๓๘ Nonthanan.c@symphony.net.th	ใบสั่งจ้างที่ ๑๕/๒๕๖๙ (Call Center ๒๔ ชม.)	Link หลัก (MPLS) และสำรอง (Fiber)
ระบบบัญชีออนไลน์ (MyAccount Cloud)	บริษัท โปรซอฟต์ ซีอาร์เอ็ม จำกัด	คุณ ปาณิศา ตาทูน ๐๒-๔๐๒-๘๐๘๖ info@myaccount-cloud.com	๘ x ๕ เวลา ๙.๐๐ - ๑๘.๐๐ น. (โปรแกรมเป็นกรรมสิทธิ์ของ อสป.)	แก้ไขปัญหาระบบงานบัญชี
ระบบบริหารจัดการตลาด (Horga Market App)	บริษัท ฮอร์แกไนซ์ จำกัด	คุณ น้ำหนึ่ง ๐๙-๔๗๙๔-๑๑๔๑ sirinya.lp@horganice.in.th	ใบสั่งจ้างที่ ๕๐/๒๕๖๙ ๙.๐๐ - ๑๘.๐๐ น.	แก้ไขปัญหาระบบบริหารจัดการพื้นที่เช่า
ผู้ดูแลระบบ Server/Network	บริษัท เน็กเทคซ์ เอเชีย จำกัด	คุณ กัญญ์วรรณ ตุงคณาคร ๐๙-๕๘๒๐-๕๘๕๖ kanyawan@nextech-asia.com	ใบสั่งจ้างที่ ๔๑/๒๕๖๙ (๗ x ๗)	MA อุปกรณ์ Router, Switch, NVR

ภาคผนวก ค

แบบฟอร์มรายงานเหตุการณ์และประกาศใช้แผน (Incident Report & IT-DRP Declaration Form)

(ใช้เพื่อเป็นหลักฐานการประเมินสถานการณ์และการตัดสินใจยกระดับเหตุการณ์ ตามเกณฑ์ DT-6.3 และ DT-6.4)

ส่วนที่ 1: การรับแจ้งและประเมินสถานการณ์ (กรอกโดยผู้ประสานงาน/ผู้พบเหตุ)

- **วัน/เวลาที่เกิดเหตุ:** .....
- **ระบบที่ได้รับผลกระทบ:** [ ] ระบบบัญชี [ ] ระบบ MIS [ ] ระบบ e-Contract [ ] เครือข่าย [ ] อื่นๆ..
- **รายละเอียดเหตุการณ์เบื้องต้น:** .....
- **การประเมินความรุนแรง (เบื้องต้น):** [ ] ระดับ 0 [ ] ระดับ 1 [ ] ระดับ 2 [ ] ระดับ 3

ส่วนที่ 2: การตัดสินใจของผู้อำนวยการกู้คืนระบบ (กรอกโดยหัวหน้าสำนัก IT)

- **การตัดสินใจ:** [ ] สามารถแก้ไขได้ภายในเวลา RTO (ไม่ต้องประกาศใช้แผน) [ ] **อนุมัติประกาศใช้แผน IT-DRP** และให้ย้ายระบบไปที่ Cloud DR-Site
- **เหตุผลที่ประกาศใช้แผน:** .....
- **ลงชื่อผู้อนุมัติ:** ..... **เวลาที่ประกาศใช้แผน:** .....

ภาคผนวก ง

แบบฟอร์มลงนามรับรองความถูกต้องของระบบและข้อมูล

(System/Data Validation & Failback Sign-off)

(ใช้เมื่อทำการย้ายระบบกลับ (Failback) เพื่อยืนยันว่าข้อมูลไม่สูญหายและพร้อมเปิดใช้งานตามปกติ)

ข้อมูลการทดสอบระบบหลังการกู้คืน

- **วันที่ทดสอบระบบ:** .....
- **ชื่อระบบงานที่ทดสอบ:** .....
- **ผลการตรวจสอบข้อมูล (Data Integrity):**

  [ ] ข้อมูลครบถ้วนสมบูรณ์ตาม RPO (สูญหายไม่เกิน 0.5 วัน)

  [ ] ไม่พบความผิดปกติของระบบงาน

  [ ] พบข้อบกพร่อง (ระบุ): .....

การรับรองจากส่วนงานเจ้าของข้อมูล (Data Owner): ข้าพเจ้าในฐานะตัวแทนส่วนงานเจ้าของข้อมูล ได้ทำการทดสอบระบบงานและตรวจสอบความถูกต้องของข้อมูลแล้ว ขอยืนยันว่าระบบมีความพร้อมสำหรับการเปิดให้บริการตามปกติ

- **ลงชื่อ (ตัวแทนส่วนงานผู้ใช้บริการ):** ..... ตำแหน่ง: .....
- **ลงชื่อ (ผู้อำนวยการกู้คืนระบบ / IT):**..... ตำแหน่ง: .....