นโยบายและแนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

เพื่อให้การท่าเรือแห่งประเทศไทย (กทท.) มีนโยบายและแนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพในการเตรียมรองรับเหตุการณ์ผิดปกติที่ระบบเทคโนโลยีสารสนเทศเกิดการหยุดชะงักหรือเกิดความเสียหาย และลดผลกระทบต่าง ๆ ที่อาจเกิดขึ้น รวมถึงการฟื้นฟูระบบเทคโนโลยีสารสนเทศของ กทท. ให้กลับคืนสู่สภาพปกติได้ภายในระยะเวลาที่เหมาะสมและยอมรับได้ โดยที่ กทท. สามารถดำเนินธุรกิจได้อย่างต่อเนื่องหรือได้รับผลกระทบน้อยที่สุดจากเหตุการณ์หยุดชะงัก อันเป็นการสร้างความเชื่อมั่นให้กับลูกค้าและผู้มีส่วนได้ส่วนเสียของ กทท. จึงกำหนดให้ต้องมีการดำเนินการดังต่อไปนี้

๑. มีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร และเป็นส่วนหนึ่งของแผนบริหารความต่อเนื่องทางธุรกิจด้านการให้บริการเทคโนโลยีสารสนเทศ (Business Continuity Plan for Information Technology Services) ของ กทท. ที่ได้รับการอนุมัติจากคณะกรรมการบริหารความต่อเนื่องทางธุรกิจของ กทท.

๒. การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ควรคำนึงถึงลักษณะการดำเนินธุรกิจ ปริมาณธุรกรรม ความซับซ้อนของเทคโนโลยีสารสนเทศ เหตุการณ์ความเสียหายต่าง ๆ และความเสี่ยงที่เกี่ยวข้องในการดำเนินธุรกิจที่สอดคล้องกับนโยบายการบริหารความต่อเนื่องทางธุรกิจและนโยบายการบริหารความเสี่ยงของ กทท.

๓. จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยมีผู้บริหารและพนักงานของฝ่ายงานต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย

๔. จัดให้มีการสื่อสารและการอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ แก่พนักงานและผู้มีส่วนเกี่ยวข้องอย่างครบถ้วน รวมทั้งมีการทดสอบการดำเนินงานตามแผนฯ อย่างน้อยปีละ ๑ ครั้ง

๕. จัดให้มีการทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงของกลยุทธ์ การดำเนินธุรกิจ หรือการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ

๖. สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง เพื่อสร้างการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๕ กันยายน พ.ศ. ๒๕๖๕

(นายวรพจน์ เอี่ยมรักษา)
ประธานกรรมการบริหารความเสี่ยงและควบคุมภายในของ กทท.

แนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

แนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศฉบับนี้ เป็นเอกสารแนบท้ายนโยบายและแนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยมีวัตถุประสงค์ เพื่อให้ กทท. มีแนวทางรองรับเหตุการณ์ผิดปกติที่ระบบเทคโนโลยีสารสนเทศของ กทท. เกิดหยุดชะงักหรือเกิดความเสียหาย โดยการดำเนินงานและการให้บริการของ กทท. ยังสามารถดำเนินไปได้อย่างต่อเนื่อง และสามารถกู้คืนระบบให้กลับสู่สภาพปกติในระยะเวลาที่ยอมรับได้

๑. <u>หน้าที่และความรับผิดชอบในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ</u>

๑.๑ คณะกรรมการบริหารความต่อเนื่องทางธุรกิจของ กทท.

๑.๑.๑ กำกับดูแลการจัดทำและการทบทวนปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจด้านการให้บริการเทคโนโลยีสารสนเทศ และแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ให้ความสอดคล้องกับนโยบายการบริหารความต่อเนื่องทางธุรกิจและการบริหารความเสี่ยงของ กทท.

๑.๑.๒ พิจารณาและอนุมัติแผนบริหารความต่อเนื่องทางธุรกิจด้านการให้บริการเทคโนโลยีสารสนเทศและแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เพื่อสื่อสารให้ผู้มีส่วนได้ส่วนเสียของ กทท. รับทราบ

๑.๒ คณะอนุกรรมการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ กทท.

๑.๒.๑ กำหนดนโยบายและแนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศที่เป็นลายลักษณ์อักษร

๑.๒.๒ กำหนดให้มีคณะทำงานที่รับผิดชอบในการดำเนินการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามนโยบายและแนวปฏิบัติที่ได้กำหนดไว้ เพื่อเสนอให้คณะกรรมการบริหารความต่อเนื่องทางธุรกิจของ กทท. พิจารณาอนุมัติใช้เป็นแผนในการดำเนินการ

๑.๓ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐระดับกรม (Department Chief Information Officer : DCIO) ของ กทท.

๑.๓.๑ กำกับดูแลให้พนักงานและผู้ที่เกี่ยวข้องดำเนินการจัดทำและปฏิบัติงานตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

๑.๓.๒ กำหนดแนวทางการประเมินประสิทธิภาพของนโยบายและแนวปฏิบัติในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๑.๔ ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

๑.๔.๑ สนับสนุน ผลักดันการดำเนินงานเพื่อให้บรรลุเป้าหมายตามนโยบาย โดยจัดให้มีกลยุทธ์แนวทางในการบริหารงาน ตัวชี้วัด และแผนงาน รวมถึงโครงสร้างผู้รับผิดชอบของฝ่ายเทคโนโลยีสารสนเทศในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๑.๔.๒ สื่อสาร ถ่ายทอดและเผยแพร่นโยบายอย่างทั่วถึง เพื่อสร้างการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสียในการนำไปปฏิบัติและปรับปรุงการปฏิบัติงานอย่างต่อเนื่อง

๑.๔.๓ ส่งเสริม สนับสนุนความรู้ ความเข้าใจแก่ผู้ปฏิบัติงาน

๑.๔.๔ ติดตามและทบทวนผลการดำเนินงาน รวมถึงพิจารณาการรายงานผลการดำเนินงานตามนโยบาย พร้อมนำเสนอต่อคณะอนุกรรมการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและคณะกรรมการบริหารความต่อเนื่องทางธุรกิจ ของ กทท.

๑.๕ คณะทำงานบริหารจัดการการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๕.๑ จัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยต้องมีการประเมินและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการดำเนินธุรกิจ เพื่อจัดลำดับความสำคัญของระบบเทคโนโลยีสารสนเทศ และกำหนดเป้าหมายการกู้ระบบและภารกิจหลักให้กลับคืนมาได้ภายในระยะเวลาที่ยอมรับได้

/๑.๕.๒ จัดทำ...

๑.๕.๒ จัดทำแผนการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ โดยต้องมีการทดสอบแผนฯ อย่างน้อยปีละ ๑ ครั้ง

๑.๕.๓ วิเคราะห์และจัดทำแผนบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามลำดับความสำคัญของระบบเทคโนโลยีสารสนเทศและภารกิจหลัก พร้อมรายงานผลการดำเนินงานต่อคณะอนุกรรมการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กทท. อย่างน้อยปีละ ๑ ครั้ง

๑.๕.๔ กำหนดให้มีการสื่อสาร อบรมการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศแก่ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องอย่างครบถ้วน

๑.๕.๕ รายงานผลการทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศต่อคณะอนุกรรมการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กทท. พร้อมรายงานสรุปข้อคิดเห็น ปัญหาและอุปสรรคที่พบในการทดสอบแผนฯ

๑.๕.๖ ติดตามและวิเคราะห์ประสิทธิภาพในการดำเนินงานเทียบกับเป้าหมาย สอบทานความถูกต้องของการปฏิบัติตามแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ เพื่อใช้ทบทวนและปรับปรุงประสิทธิภาพของแผนฯ อย่างน้อยปีละ ๑ ครั้ง หรือทบทวนแผนฯ เมื่อตรวจพบการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๑.๖ พนักงาน กทท.

๑.๖.๑ ศึกษาและทำความเข้าใจเกี่ยวกับนโยบาย และเป้าหมายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๑.๖.๒ รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติ เพื่อให้ กทท. บรรลุตามเป้าหมายที่กำหนดและนโยบายในการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๒. <u>กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ</u>

กระบวนการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ต้องประกอบด้วยแนวทางการดำเนินงานตามที่กำหนดในกระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องกับนโยบายและแผนบริหารความต่อเนื่องทางธุรกิจ และนโยบายการบริหารความเสี่ยงของ กทท. ประกอบด้วย

๒.๑ การประเมินความเสี่ยง (Risk Analysis) เพื่อให้ กทท. สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบเทคโนโลยีสารสนเทศ โดยมีแนวทางการดำเนินการอย่างเหมาะสมเพียงพอ ดังนี้

๒.๑.๑ ระบุเหตุการณ์ความเสี่ยง (Risk scenarios) ที่อาจทำให้กระบวนงานและระบบเทคโนโลยีสารสนเทศหยุดชะงักทั้งจากปัจจัยภายในและปัจจัยภายนอก

๒.๑.๒ ประเมินความเสี่ยงโดยพิจารณาการควบคุมที่มีอยู่ รวมถึงผลกระทบและโอกาสที่จะเกิดขึ้น พร้อมทั้งกำหนดกระบวนการและทรัพยากรที่จะใช้ในการควบคุมความเสี่ยง

๒.๑.๓ จัดทำแผนบริหารจัดการความเสี่ยง เพื่อปรับปรุงกระบวนงาน และจัดเตรียมทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๒.๒ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) ที่ครอบคลุมระบบงานที่สำคัญเพื่อทราบถึงความสำคัญของระบบเทคโนโลยีสารสนเทศที่มีผลต่อการดำเนินธุรกิจของ กทท. รวมถึงผลกระทบจากการหยุดชะงักและการเชื่อมโยงของการดำเนินธุรกิจกับระบบเทคโนโลยีสารสนเทศ ดังนี้

๒.๒.๑ ระบุระบบเทคโนโลยีสารสนเทศทั้งหมดของ กทท. และทรัพยากรที่มีการเชื่อมโยงพึ่งพาระหว่างกัน

๒.๒.๒ วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของเทคโนโลยีสารสนเทศ โดยคำนึงถึงเป้าหมายระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerance Period of Disruption : MTPD)

/๒.๒.๓ กำหนด...

๒.๒.๓ กำหนดเป้าหมายระยะเวลาในการกู้คืนระบบ (Recovery Time Objective : RTO) และเป้าหมายระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO)

๒.๓ การจัดลำดับความสำคัญของระบบงาน เพื่อพิจารณาระดับความรุนแรงหรือระดับความสำคัญในการให้บริการที่เกิดจากผลกระทบของการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ ในด้าน

๒.๓.๑ ทรัพยากรและระยะเวลาที่ใช้ในการกู้คืนระบบ

๒.๓.๒ เป้าหมายของระบบงานและข้อมูลที่ควรกู้ได้ภายหลังเกิดการหยุดชะงัก

๒.๓.๓ ทรัพยากรทางเทคโนโลยีสารสนเทศขั้นต่ำที่จำเป็นต้องใช้ในการกู้คืนระบบ

๒.๔ การระบุกลยุทธ์ของแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและจัดเตรียมทรัพยากรระบบเทคโนโลยีที่เหมาะสมตามการจัดลำดับความสำคัญของระบบงาน โดยพิจารณาครอบคลุม

๒.๔.๑ เป้าหมายระยะเวลาที่ได้จากการวิเคราะห์ผลกระทบทางธุรกิจ

๒.๔.๒ เทคโนโลยีในการสำรองและกู้คืนข้อมูล

๒.๔.๓ ความพร้อมใช้ของสถานที่ปฏิบัติงานสำรอง

๒.๔.๔ ทรัพยากรและงบประมาณ ที่จำเป็นต้องใช้เพื่อจัดเตรียมระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกิจกรรมที่ต้องดำเนินการทั้งหมด

๒.๕ การระบุขั้นตอนการสนับสนุนการปฏิบัติงาน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ รวมทั้งมีความยืดหยุ่นในการสนองต่อเหตุการณ์ต่าง ๆ ที่อาจเกิดขึ้น โดยครอบคลุม

๒.๕.๑ ชื่อแผน วัตถุประสงค์ ขอบเขต และความสัมพันธ์กับแผนอื่น ๆ ที่เกี่ยวข้อง

๒.๕.๒ ผังโครงสร้างของการบังคับบัญชาในการดำเนินงานตามแผน ผู้ปฏิบัติหน้าที่ และความรับผิดชอบ รวมถึงผู้ปฏิบัติที่หน้าที่แทนในกรณีที่ผู้ปฏิบัติหน้าที่ไม่สามารถปฏิบัติงานได้ รวมถึงการบันทึกการเปลี่ยนแปลงของแผนฯ

๒.๕.๓ รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรม แผนภาพระบบ เครือข่ายสื่อสาร เป็นต้น

๒.๕.๔ ขั้นตอนในการประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ การตอบสนองต่อเหตุการณ์ฉุกเฉินและแผนการสื่อสารให้หน่วยงานทั้งภายในและภายนอก กทท. ที่เกี่ยวข้องรับทราบ

๒.๕.๕ ขั้นตอนในการดำเนินการกู้คืนระบบ ต้องระบุรายละเอียดที่ชัดเจนและเพียงพอสำหรับใช้เป็น checklist ควบคุมไม่ให้มีการข้ามหรือละเลยขั้นตอนที่กำหนดไว้ รวมทั้งจัดทำคู่มือการกู้คืนสำหรับแต่ละระบบ ที่มีการทบทวนให้เป็นปัจจุบันอย่างสม่ำเสมอ

๒.๕.๖ ขั้นตอนในการกลับคืนสู่ภาวะปกติ (Return to Normal) และการประกาศยกเลิกแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๒.๖ แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ พร้อมเอกสารประกอบการทำงานภายใต้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ ต้องถูกจัดเก็บไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้ในสถานที่ปฏิบัติงานหลักและสำรอง

๒.๗ การสื่อสารและการฝึกอบรมแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศแก่พนักงานและผู้มีส่วนเกี่ยวข้องโดยเฉพาะอย่างยิ่งเมื่อมีการทบทวนแผนฉุกเฉินดังกล่าว โดย

๒.๗.๑ ในการสื่อสารแผนฯ ต้องมีการระบุแนวทางการสื่อสารที่ชัดเจนให้ผู้บริหารและพนักงานทุกคนที่มีส่วนเกี่ยวข้องได้รับทราบรายละเอียดในการจัดทำแผน ขั้นตอนการดำเนินงานตามแผน

๒.๗.๒ จัดให้มีการฝึกอบรมแก่ผู้ที่ส่วนเกี่ยวข้องในการดำเนินการตามแผนอย่างน้อยปีละ ๑ ครั้ง โดยครอบคลุม วัตถุประสงค์ของแผน ขั้นตอนการปฏิบัติงานตามแผน การประสานงานและการสื่อสารกันระหว่างกลุ่ม ขั้นตอนการรายงาน และความรับผิดชอบของแต่ละบุคคล ฯลฯ

/๒.๘ การทดสอบ...

๒.๘ การทดสอบ การปรับปรุงและการสอบทานแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๒.๘.๑ จัดทำแผนงานเพื่อทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศประจำปี โดยมีรายละเอียดอย่างน้อยครอบคลุมสถานการณ์จำลอง รูปแบบการทดสอบ วันเวลาและสถานที่ในการทดสอบ และบทบาทหน้าที่ของผู้เกี่ยวข้อง

๒.๘.๒ ทดสอบแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศในระดับฝ่ายและระดับองค์กร อย่างน้อยปีละ ๑ ครั้ง โดยเฉพาะระบบงานหรือข้อมูลที่มีผลกระทบต่อการให้บริการของ กทท.

๒.๘.๓ รายงานผลการทดสอบต่อคณะกรรมการบริหารความต่อเนื่องทางธุรกิจของ กทท. คณะอนุกรรมการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของ กทท. โดยมีรายละเอียดอย่างน้อยครอบคลุม วัตถุประสงค์ ขอบเขตการทดสอบ สถานการณ์จำลอง ระยะเวลาที่ใช้ในการกู้คืนระบบเทียบกับเป้าหมายที่กำหนด ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข

๒.๘.๔ ทบทวนและปรับปรุงแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น มีการเปลี่ยนแปลงกลยุทธ์ นโยบายการบริหารความเสี่ยงของ กทท. สภาพแวดล้อมในการดำเนินธุรกิจ หรือการปฏิบัติงาน/ทรัพยากร/โครงสร้างระบบเทคโนโลยีสารสนเทศ เป็นต้น