แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ

(IT Contingency Plan)

ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ - ๒๕๗๐

ศูนย์สารสนเทศ

สำนักงานคณะกรรมการพิเศษเพื่อประสานงาน

โครงการอันเนื่องมาจากพระราชดำริ (สำนักงาน กปร.)

บทนำ

ข้อมูล ระบบฐานข้อมูล และเทคโนโลยีสารสนเทศ ล้วนมีบทบาทที่สำคัญอย่างยิ่งต่อการดำเนินงานขององค์กร เนื่องจากเป็นเครื่องมือหลักในการจัดเก็บ ประมวลผล และวิเคราะห์ข้อมูล รวมทั้งเป็นแหล่งข้อมูลประกอบการวางแผนและการตัดสินใจเชิงนโยบายของผู้บริหาร หากระบบเหล่านี้เกิดเหตุขัดข้องหรือไม่สามารถใช้งานได้จะส่งผลกระทบโดยตรงต่อความต่อเนื่องของภารกิจ ตลอดจนภาพลักษณ์ขององค์กรในภาพรวม ทั้งนี้ ความเสี่ยงที่อาจเกิดขึ้นมีความหลากหลาย ไม่ว่าจะเป็นภัยธรรมชาติ เช่น อุทกภัย ไฟไหม้ และแผ่นดินไหว ปัญหาทางเทคนิค เช่น ฮาร์ดแวร์หรือซอฟต์แวร์ขัดข้อง รวมถึงภัยคุกคามทางไซเบอร์ หรือการเข้าถึงระบบโดยไม่ได้รับอนุญาต ปัจจัยเหล่านี้ล้วนสามารถก่อให้เกิดการสูญหายหรือเสียหายของข้อมูล ระบบฐานข้อมูล และสารสนเทศ

สำนักงาน กปร. ได้ตระหนักถึงความสำคัญของข้อมูล ระบบฐานข้อมูล และสารสนเทศ ที่อาจได้รับผลกระทบจากปัจจัยข้างต้นดังกล่าว ดังนั้น ศูนย์สารสนเทศจึงได้จัดทำ “แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)” เพื่อกำหนดแนวทางการป้องกัน การตอบสนอง และการกู้คืนระบบสารสนเทศอย่างเป็นระบบ แผนดังกล่าวมุ่งเน้นการลดผลกระทบจากเหตุการณ์ที่ไม่คาดคิด และสร้างความมั่นคงปลอดภัยเพื่อให้ข้อมูล ระบบฐานข้อมูล และสารสนเทศสามารถกลับเข้าสู่ภาวะปกติได้ภายในเวลาที่เหมาะสม นอกจากนี้ แผนฉบับนี้ยังมีเป้าหมายเพื่อพัฒนาศักยภาพของบุคลากรในการรับมือกับเหตุการณ์ฉุกเฉิน ส่งเสริมการทำงานอย่างบูรณาการระหว่างหน่วยงานที่เกี่ยวข้อง และสนับสนุนการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานให้สอดคล้องกับกฎหมายที่เกี่ยวข้องและเป็นไปตามมาตรฐานสากล อันจะช่วยให้การดำเนินภารกิจของสำนักงาน กปร. เป็นไปอย่างต่อเนื่อง มั่นคง ปลอดภัย และมีประสิทธิภาพสูงสุด

ศูนย์สารสนเทศ สำนักงาน กปร.
ตุลาคม ๒๕๖๘

สารบัญ

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ
ที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ
(IT Contingency Plan)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ – ๒๕๗๐

๑. หลักการและเหตุผล

ข้อมูล ระบบฐานข้อมูล และเทคโนโลยีสารสนเทศ ของสำนักงานคณะกรรมการพิเศษเพื่อประสานงานโครงการอันเนื่องมาจากพระราชดำริ (สำนักงาน กปร.) ถือเป็นทรัพย์สินที่มีความสำคัญต่อทางราชการ หากได้รับความเสียหายจากปัจจัยภายในและภายนอกอันได้แก่ ไวรัสคอมพิวเตอร์ การถูกโจมตี บุคลากร ปัญหาไฟฟ้า อัคคีภัยหรือภัยอื่นๆ อาจทำให้ฐานข้อมูลและสารสนเทศเกิดความเสียหาย ซึ่งจะส่งผลกระทบต่อการดำเนินงานของสำนักงาน กปร. จึงจำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ ดังนั้น เพื่อเป็นการป้องกันและแก้ไขปัญหาดังกล่าว ศูนย์สารสนเทศ สำนักงานคณะกรรมการพิเศษเพื่อประสานงานโครงการอันเนื่องมาจากพระราชดำริ (สำนักงาน กปร.) ได้เล็งเห็นถึงความสำคัญที่จะต้องมี “แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ - ๒๕๗๐” สำหรับใช้เป็นกรอบแนวทางในการดูแลรักษาระบบและแก้ไขปัญหาที่อาจจะส่งผลกระทบดังกล่าว

๒. วัตถุประสงค์

๒.๑ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของสำนักงาน กปร.

๒.๒ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัย ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๓ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้น

๒.๔ เพื่อลดความเสียหายที่อาจเกิดขึ้น

๒.๕ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๓. การประเมินสถานการณ์ความเสี่ยง

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศของสำนักงาน กปร. พบว่าความเสี่ยงที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศ สามารถแบ่งตามปัจจัยออกเป็น ๒ กลุ่ม ดังนี้

๓.๑ <u>ปัจจัยภายนอก</u>

๑) การเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย และภัยพิบัติทางธรรมชาติ ได้แก่ วาตภัย อุทกภัย อัคคีภัย แผ่นดินไหว ฯลฯ

๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูลจากระบบฐานข้อมูลและสารสนเทศ

๓) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๔) การถูกบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศรวมทั้งสร้างความเสียหายหรือทำลายระบบฐานข้อมูลและสารสนเทศ

๕) ระบบสื่อสารของเครื่องแม่ข่ายเชื่อมต่อระบบอินเตอร์เน็ตเกิดขัดข้อง

๖) ไวรัสคอมพิวเตอร์

๗) โรคระบาด

๓.๒ ปัจจัยภายใน

๑) ระบบเครื่องแม่ข่าย ระบบฐานข้อมูลหลัก เกิดการชำรุด เสียหายหรือถูกทำลาย

๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๓) เจ้าหน้าที่หรือบุคลากรขาดความรู้ความเข้าใจในการใช้และดูแลรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ ทั้งฮาร์ดแวร์และซอฟต์แวร์อาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้/หยุดการทำงาน

๔. มาตรการสำคัญเพื่อเตรียมการเบื้องต้น

๔.๑ การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมความพร้อมรับภัยพิบัติหรือสถานการณ์ความไม่แน่นอนหรือเกิดภาวะฉุกเฉินที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ศูนย์สารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นอย่างเพียงพอ ดังนี้

๑) ไฟล์ระบบปฏิบัติการ ระบบเครือข่าย ไฟล์ระบบงานที่สำคัญ

๒) ฮาร์ดดิสก์สำหรับสำรองข้อมูลระบบงานที่สำคัญ

๓) Driver ของอุปกรณ์ต่อพ่วง โปรแกรม Antivirus

๔) อุปกรณ์สำหรับการประชุมออนไลน์ การปฏิบัติงานนอกสถานที่ อุปกรณ์ปล่อยสัญญาณอินเตอร์เน็ต

๕) อุปกรณ์สำรองต่างๆ ที่จำเป็นของระบบคอมพิวเตอร์ เช่น ฮาร์ดดิสก์, RAM, สาย LAN

๔.๒ การสำรองข้อมูล (Back Up)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล ซึ่งมีแนวทางปฏิบัติด้วยการตั้งค่าระบบให้มีการสำรองข้อมูล (Back Up) อัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่าย รวมทั้งเครื่องแม่ข่ายเว็บไซต์ (Back Up Site) ด้วย เป็นประจำทุกเดือน ซึ่งข้อมูลจะถูกเก็บไว้ในฮาร์ดดิสก์สำรองสามารถนำกลับมาใช้งานได้ตามปกติ ทั้งนี้ ศึกษาได้จากคู่มือการสำรองข้อมูล (Back Up)

๔.๓ การกู้ข้อมูล (Recovery)

ดำเนินการทดสอบ Recovery ฐานข้อมูลและระบบปฏิบัติการของเครื่องแม่ข่ายสำรอง ที่ได้ทำการสำรองไว้เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย เป็นประจำอย่างน้อยปีละ ๒ ครั้ง สามารถศึกษาขั้นตอนการ Recovery ได้จากคู่มือการกู้ข้อมูล (Recovery)

๔.๔ การป้องกันไวรัส

สำหรับผู้ดูแลระบบ : มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และตั้งค่าอัพเดทข้อมูลไวรัสอัตโนมัติในช่วงที่มีการใช้งานต่ำพร้อมกำหนดสิทธิ์ไม่ให้ผู้ใช้งานถอนการติดตั้งซอฟต์แวร์ป้องกันไวรัสออกได้

สำหรับผู้ใช้งาน : จำเป็นจะต้องระมัดระวังในการใช้งานโดยเฉพาะการเชื่อมต่อกับอินเตอร์เน็ตเพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ โดยปฏิบัติ ดังนี้

๑) อัพเดตฐานข้อมูลป้องกันไวรัสอย่างสม่ำเสมอ และใช้โปรแกรมป้องกันไวรัสเพื่อทำการตรวจหาไวรัส (Scan) อย่างน้อยสัปดาห์ละ ๑ ครั้ง

๒) ติดตามข้อมูลแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ

๓) ระวังภัยจากการเปิดไฟล์จากอุปกรณ์บันทึกข้อมูลต่างๆ ด้วยการตรวจสอบหาไวรัสทุกครั้งก่อนใช้งานหรือเปิดไฟล์ เช่น Flash Drive, Memory Card, แผ่นซีดี เป็นต้น ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จัก หากมีข้อสงสัยควรปรึกษาศูนย์สารสนเทศ

๔) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet

- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น Facebook, Line
- ไม่ควรเปิดเว็บไซต์ที่แนะนำมาทางอีเมล์ หรือไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลดไฟล์จากเว็บไซต์หรือไม่น่าเชื่อถือ

๕) ใช้ความระมัดระวังและพิจารณาอย่างรอบครอบในการเปิดอีเมล์ โดยอย่าเปิดอีเมล์ หรือไฟล์แนบ ถ้าไม่ทราบแหล่งที่มาหรือควรลบอีเมล์นั้นทิ้งทันที

๔.๕ ระบบไฟฟ้า

๑) ติดตั้งเครื่องสำรองไฟฟ้าและควบคุมแรงดันอัตโนมัติ (UPS) ให้กับระบบเครื่องแม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นในกรณีเกิดกระแสไฟฟ้าขัดข้อง ซึ่งจะทำการควบคุมการจ่ายกระแสไฟฟ้าให้แก่ระบบเครือข่ายและคอมพิวเตอร์ โดยมีกระแสไฟฟ้าใช้ได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

๒) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้เครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพที่พร้อมใช้งาน

๔.๖ มาตรการอื่น ๆ ที่เกี่ยวข้อง

๑) มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหายอันอาจเกิดจากการโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์หรืออื่น ๆ โดยห้ามบุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของศูนย์สารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป ที่ประตูเข้าออกมีระบบเครื่องสแกนลายนิ้วมือบันทึกการเข้าออก

๒) มาตรการความปลอดภัยด้วยรหัสผ่าน โดยมีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศไม่สามารถเข้าถึง เพื่อการแก้ไข เปลี่ยนแปลงข้อมูลหรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่ไม่มีหน้าที่ที่เกี่ยวข้อง

๓) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของสำนักงานได้ ซึ่งเปิดใช้งาน Firewall ตลอดเวลา

๔) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า (Configuration) ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๕) มาตรการความปลอดภัยด้านอัคคีภัย ภายในห้องคอมพิวเตอร์แม่ข่ายได้ติดตั้งอุปกรณ์ตรวจจับควันความไวสูง ติดตั้งระบบส่งสัญญาณแจ้งเหตุเตือนภัย ติดตั้งอุปกรณ์ดับเพลิงอัตโนมัติ

๖) เจ้าหน้าที่ดูแลระบบจะทำการตรวจสอบระบบเครือข่ายทุกวันทำการก่อนเวลา ๘.๓๐ น. ว่าสามารถใช้งานเป็นปกติหรือไม่ หากพบต้องรีบดำเนินการแก้ไขทันที

๗) การเก็บข้อมูลผู้ใช้งานอินเตอร์เน็ต เป็นไปตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ผู้ดูแลระบบจะตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของสำนักงานอย่างสม่ำเสมอ เพื่อสังเกตปริมาณข้อมูล ความถี่และการเรียกใช้ข้อมูลบนเครือข่าย พร้อมจัดทำสรุปรายงานทุกเดือน แจ้งให้ผู้อำนวยการศูนย์สารสนเทศ และผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐระดับกรม DCIO ทราบ เพื่อหาแนวทางแก้ไข/ป้องกันต่อไป จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ได้เป็นอย่างดี

๘) มาตรการป้องกันเจ้าหน้าที่หรือบุคลากรของสำนักงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ (Human Error) ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายหรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ

โดยการเพิ่มทักษะและเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศ จึงได้จัดฝึกอบรมให้แก่เจ้าหน้าที่เพื่อเพิ่มทักษะความรู้ความเข้าใจในด้านฮาร์ดแวร์และซอฟต์แวร์ ให้เท่าทันเทคโนโลยีที่เปลี่ยนแปลงไปและความเสี่ยงที่อาจเกิดขึ้นในด้านต่างๆ

๕. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

๕.๑ <u>ระดับนโยบาย</u>

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตามกำกับดูแล ควบคุม ตรวจสอบ สั่งการเจ้าหน้าที่ในระดับอำนวยการ ระดับประสานงานเหตุฉุกเฉิน และระดับปฏิบัติการ ผู้รับผิดชอบ ได้แก่

นางพิชญดา หัศภาค รองเลขาธิการคณะกรรมการพิเศษเพื่อประสานงานโครงการอันเนื่องมาจากพระราชดำริ
ทำหน้าที่ DCIO สำนักงาน กปร.

๕.๒ <u>ระดับอำนวยการ</u>

รับผิดชอบในการควบคุมและปฏิบัติการฉุกเฉินระบบสารสนเทศ มีอำนาจสั่งการเจ้าหน้าที่ในระดับประสานงานเหตุฉุกเฉินและระดับปฏิบัติการ ให้ปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นกับระบบสารสนเทศหรือหยุดปฏิบัติการ กำหนดจุดปลอดภัยสำหรับบุคคลและอุปกรณ์ในสถานที่ที่เหมาะสม ประชุม/หารือเพื่อประเมินสถานการณ์และสั่งการปรับเปลี่ยนแผนตามความเหมาะสม และรายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐระดับกรม (DCIO) ผู้รับผิดชอบ ได้แก่

นางสาวจินจะนะ แก้วไทรแย้ม ผู้อำนวยการศูนย์สารสนเทศ
เบอร์ประสานงาน กรณีเกิดเหตุ ๐๘-๑๖๑๖-๑๙๑๐

๕.๓ <u>ระดับประสานงานเหตุฉุกเฉิน</u>

รับผิดชอบวิเคราะห์สถานการณ์ในกรณีเกิดเหตุ แจ้งเหตุต่อผู้อำนวยการศูนย์สารสนเทศ หรือปฏิบัติหน้าที่แทน ผอ.สท. (กรณีไม่อยู่) ผู้รับผิดชอบ ได้แก่

นางสาวสุชนา โรจน์เลิศจรรยา ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีสารสนเทศ
เบอร์ประสานงาน กรณีเกิดเหตุ ๐๘-๙๔๕๖-๔๓๕๐

๕.๔ <u>ระดับปฏิบัติการ</u>

๑) รับผิดชอบ กำกับดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

นางสาวสุชนา โรจน์เลิศจรรยา ผู้อำนวยการกลุ่มพัฒนาเทคโนโลยีสารสนเทศ

๒) รับผิดชอบดูแลบำรุงรักษา ระบบเครือข่ายและความปลอดภัยของฐานข้อมูลทั้งหมดโดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่ายคอมพิวเตอร์สำนักงานและเครื่องแม่ข่ายเว็บไซต์ รวมทั้งการทำสำเนาฐานข้อมูลและกู้คืน

- นายจุฑาพล ยุคแผน นักวิชาการคอมพิวเตอร์ชำนาญการ
- ว่าที่ร้อยเอก พิศาล ศรีตัมภวา นักวิชาการคอมพิวเตอร์ชำนาญการ

๓) รับผิดชอบดูแลบำรุงรักษา คอมพิวเตอร์และอุปกรณ์ โดยมีหน้าที่ตรวจสอบ บำรุงรักษาแก้ไขข้อบกพร่องต่าง ๆ ของระบบคอมพิวเตอร์และอุปกรณ์

นายณัฐพล ลักษณะ เจ้าหน้าที่ระบบงานคอมพิวเตอร์

๔) รับผิดชอบในการรักษาความปลอดภัยของแต่ละระบบสารสนเทศและฐานข้อมูล

นายจุฑาพล ยุคแผน นักวิชาการคอมพิวเตอร์ชำนาญการ

๕) รับผิดชอบงานสนับสนุนทั่วไป

- นายสุทัศน์ โพธิศิริกุล นักวิเคราะห์นโยบายและแผนชำนาญการ
- นางสาวศิริพร ดอกทุเรียน นักวิชาการคอมพิวเตอร์ชำนาญการ
- นายกฤษฎา คงฉ้ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ
- นางสาวนวลจันทร์ จันทร์เจริญ เจ้าหน้าที่สารสนเทศ
- นางวิภารัตน์ โอฬาวนิช เจ้าหน้าที่วิเคราะห์นโยบายและแผน

๖. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๖.๑ <u>กรณีที่ ๑</u> : ความเสียหายกับเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

<u>ตัวอย่างสถานการณ์</u> : น้ำท่วม, ไฟไหม้, แผ่นดินไหว, อุปกรณ์เครือข่ายชำรุดรุนแรง ฯลฯ

<u>แนวทางปฏิบัติ</u> :

๑. ตรวจพบเหตุการณ์ / แจ้งเหตุ

๒. เจ้าหน้าที่ศูนย์สารสนเทศผู้ดูแลระบบประเมินสถานการณ์เบื้องต้น ตรวจสอบความเสียหายและรีบแจ้งให้ผู้อำนวยการศูนย์สารสนเทศ (ผอ.สท.) ทราบโดยเร็ว

๓. ตัดการเชื่อมต่อระบบเครือข่ายที่ได้รับผลกระทบ

๓.๑ กรณีไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพของเครื่องสำรองไฟ

๓.๒ กรณีเพลิงไหม้ ระบบจะส่งสัญญาณแจ้งเหตุเตือนภัย และระบบดับเพลิงจะทำงานโดยอัตโนมัติ

๔. แจ้งผู้บริหาร วิเคราะห์สถานการณ์ที่เกิดขึ้น หากพบว่าไม่ปลอดภัย ให้รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

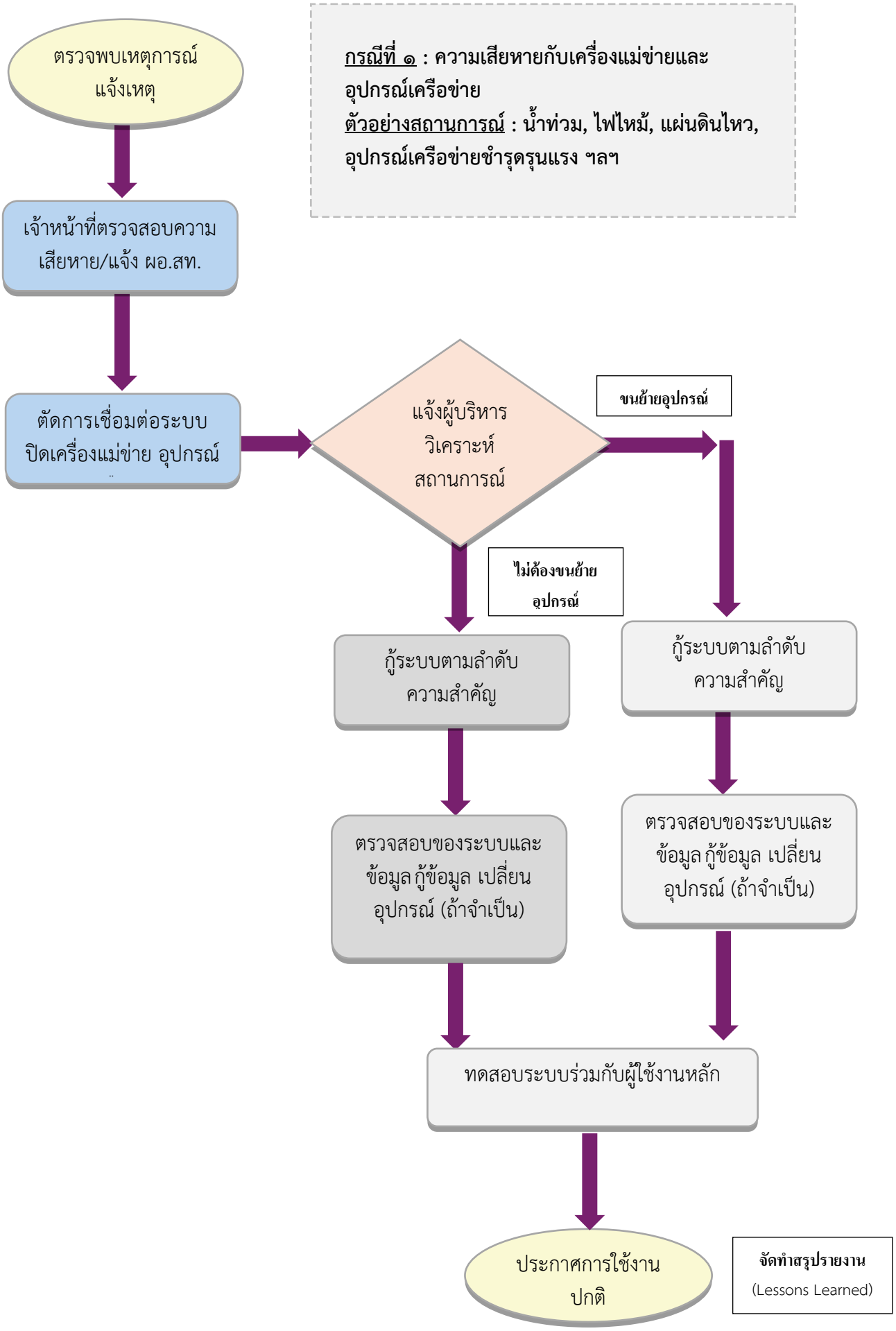
๕. กู้ระบบตามลำดับความสำคัญ

๖. ตรวจสอบความสมบูรณ์ของระบบและข้อมูล กรณีเมนบอร์ดหรือฮาร์ดดิสก์เสีย ให้รีบดำเนินการแจ้งให้ผู้อำนวยการศูนย์สารสนเทศ (ผอ.สท.) ทราบ และจัดหาชิ้นส่วนใหม่ทดแทนโดยเร็วที่สุด กรณีเมนบอร์ดเสียให้ถอดเมนบอร์ดเดิมที่ชำรุดออกแล้วติดตั้งเมนบอร์ดใหม่ทดแทน แล้วทำการบูตระบบให้ใช้งานได้ตามปกติ กรณีฮาร์ดดิสก์เสีย นำฮาร์ดดิสก์ใหม่มาเปลี่ยนแล้วติดตั้งระบบปฏิบัติการและระบบเครือข่าย นำ Back Up ที่ได้จัดทำไว้ มา Recovery เพื่อนำข้อมูลเดิมกลับมาใช้เหมือนเดิม และทำการรันเครื่องทำงานตามเดิม

๗. ทดสอบระบบร่วมกับผู้ใช้งานหลัก

๘. ประกาศให้ระบบกลับมาใช้งานปกติ

๙. สรุปรายงานเหตุการณ์ (Lessons Learned)


ตรวจพบเหตุการณ์
แจ้งเหตุ
กรณีที่ ๑ : ความเสียหายกับเครื่องแม่ข่ายและอุปกรณ์เครือข่าย
ตัวอย่างสถานการณ์ : น้ำท่วม, ไฟไหม้, แผ่นดินไหว, อุปกรณ์เครือข่ายชำรุดรุนแรง ฯลฯ
เจ้าหน้าที่ตรวจสอบความเสียหาย/แจ้ง ผอ.สท.
ตัดการเชื่อมต่อระบบ ปิดเครื่องแม่ข่าย อุปกรณ์
แจ้งผู้บริหาร วิเคราะห์ สถานการณ์
ขนย้ายอุปกรณ์
ไม่ต้องขนย้ายอุปกรณ์
กู้ระบบตามลำดับความสำคัญ
กู้ระบบตามลำดับความสำคัญ
ตรวจสอบของระบบและข้อมูล กู้ข้อมูล เปลี่ยนอุปกรณ์ (ถ้าจำเป็น)
ตรวจสอบของระบบและข้อมูล กู้ข้อมูล เปลี่ยนอุปกรณ์ (ถ้าจำเป็น)
ทดสอบระบบร่วมกับผู้ใช้งานหลัก
ประกาศการใช้งานปกติ
จัดทำสรุปรายงาน (Lessons Learned)

๖.๒ <u>กรณีที่ ๒</u> : ความเสียหายกับเครื่องลูกข่าย

<u>ตัวอย่างสถานการณ์</u> : ไวรัสคอมพิวเตอร์, ไฟฟ้าช็อต, ฮาร์ดแวร์เสียหาย ฯลฯ

<u>แนวทางปฏิบัติ</u> :

๑. ผู้ใช้งานตรวจพบปัญหา แจ้งเจ้าหน้าที่ศูนย์สารสนเทศทราบ

๒. ทีมเจ้าหน้าที่ศูนย์สารสนเทศตรวจสอบอาการเบื้องต้น

๒.๑ หากเป็นเหตุที่ไม่สามารถใช้บริการด้านเครือข่ายได้ ศูนย์สารสนเทศจะดำเนินการประกาศให้ทุกสำนัก/กอง/ศูนย์/กลุ่ม ทราบโดยเร็ว

๒.๒ หากเกิดกระแสไฟฟ้าดับให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและทำการปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้เรียบร้อย เครื่องสำรองไฟจะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลได้

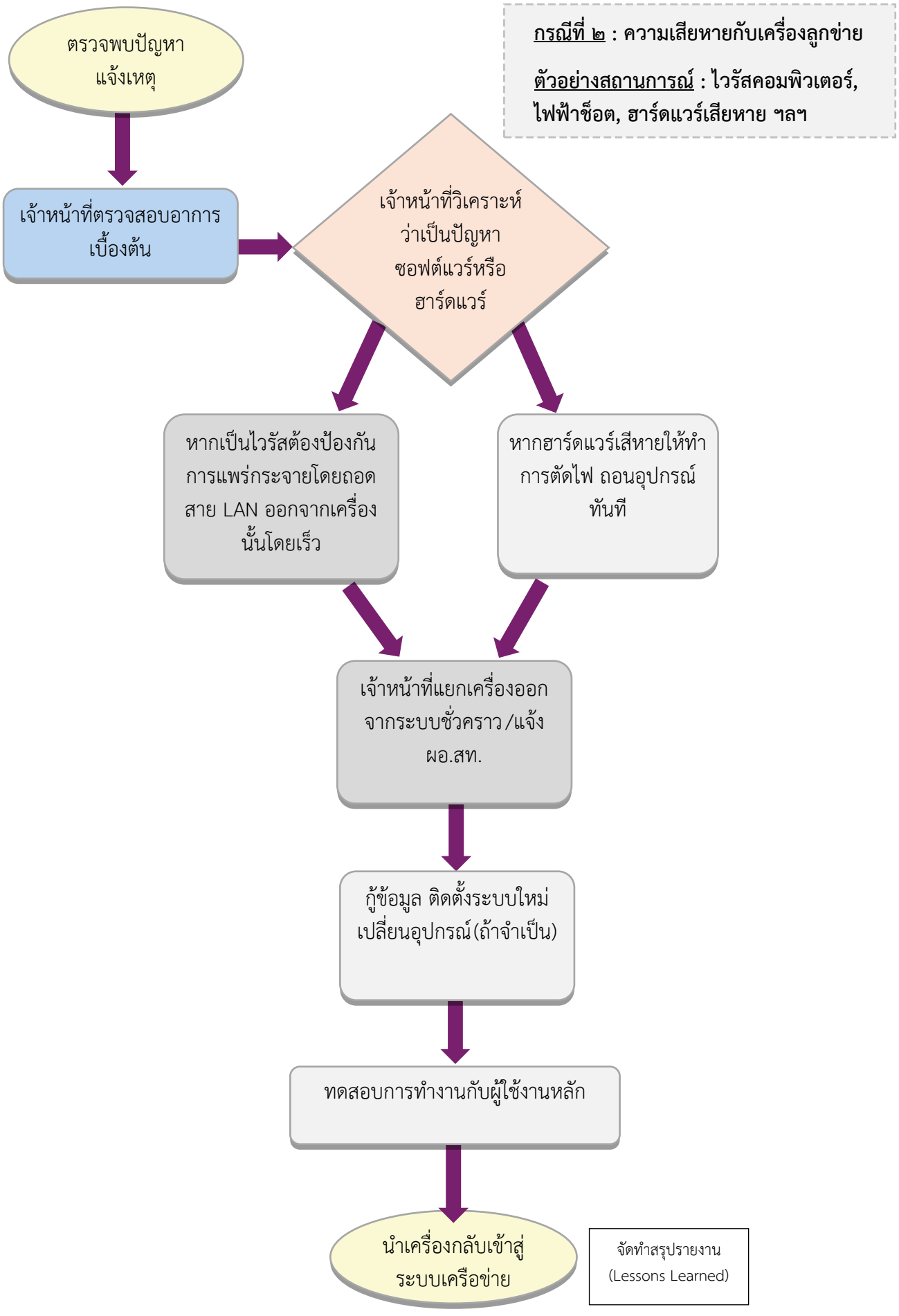
๓. เจ้าหน้าที่ศูนย์สารสนเทศวิเคราะห์ว่าเป็นปัญหาซอฟต์แวร์หรือฮาร์ดแวร์ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการถอดสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว หากความเสียหายเกิดกับฮาร์ดแวร์ให้ทำการตัดไฟ ถอนอุปกรณ์ทันที

๕. เจ้าหน้าที่ศูนย์สารสนเทศแยกเครื่องออกจากระบบชั่วคราว และแจ้งเหตุขัดข้องนั้นให้ผู้อำนวยการศูนย์สารสนเทศ (ผอ.สท.) ทราบโดยเร็ว

๖. กู้ข้อมูลจาก Backup / ติดตั้งระบบใหม่ / เปลี่ยนอุปกรณ์

๗. ทดสอบการทำงานกับผู้ใช้หลัก และนำเครื่องกลับเข้าสู่ระบบเครือข่าย

๘. สรุปรายงานเหตุการณ์ (Lessons Learned)


กรณีที่ ๒ : ความเสียหายกับเครื่องลูกข่าย
ตัวอย่างสถานการณ์ : ไวรัสคอมพิวเตอร์, ไฟฟ้าช็อต, ฮาร์ดแวร์เสียหาย ฯลฯ
ตรวจพบปัญหา แจ้งเหตุ
เจ้าหน้าที่ตรวจสอบอาการเบื้องต้น
เจ้าหน้าที่วิเคราะห์ว่าเป็นปัญหาซอฟต์แวร์หรือฮาร์ดแวร์
หากเป็นไวรัสต้องป้องกันการแพร่กระจายโดยถอดสาย LAN ออกจากเครื่องนั้นโดยเร็ว
หากฮาร์ดแวร์เสียหายให้ทำการตัดไฟ ถอนอุปกรณ์ทันที
เจ้าหน้าที่แยกเครื่องออกจากระบบชั่วคราว/แจ้ง ผอ.สท.
กู้ข้อมูล ติดตั้งระบบใหม่ เปลี่ยนอุปกรณ์(ถ้าจำเป็น)
ทดสอบการทำงานกับผู้ใช้งานหลัก
นำเครื่องกลับเข้าสู่ระบบเครือข่าย
จัดทำสรุปรายงาน (Lessons Learned)

๖.๓ <u>กรณีที่ ๓</u> : ความเสียหายจากโรคระบาดที่ส่งผลต่อบุคลากรและความต่อเนื่องของงาน

<u>ตัวอย่างสถานการณ์</u> : การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรน่า 2019

<u>แนวทางปฏิบัติ</u> :

๑. ตรวจพบสถานการณ์โรคระบาด (ประกาศจากรัฐบาล/กระทรวงสาธารณสุข)

๒. ประเมินผลกระทบต่อการปฏิบัติงานของบุคลากร (เช่น การทำงาน ณ ที่พักอาศัย Work from Home, จำกัดการเข้าสถานที่, ขาดแคลนเจ้าหน้าที่)

๓. แจ้งนโยบายและมาตรการทำงาน เช่น กำหนดบุคลากรสำคัญ (Key Persons) การอนุญาตให้ทำงาน ณ ที่พัก อาศัย Work from Home การจัดตารางเวรสลับในการเข้า-ออกสถานที่ทำงาน

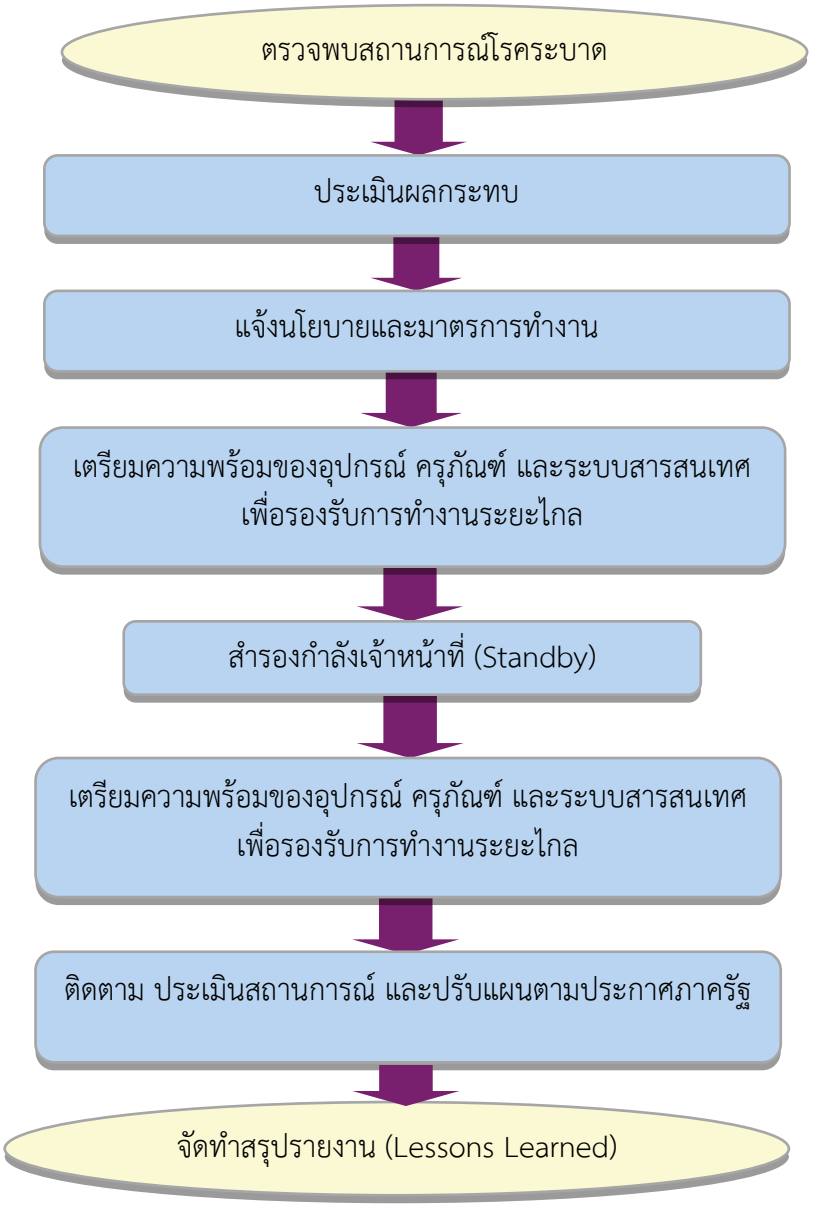
๔. เตรียมความพร้อมของอุปกรณ์ ครุภัณฑ์ และระบบสารสนเทศเพื่อรองรับการทำงานระยะไกลนอกสถานที่ เช่น คอมพิวเตอร์โน้ตบุ๊ค, แท็บเล็ตคอมพิวเตอร์, VPN, Remote Access, ระบบการประชุมออนไลน์, ระบบจัดเก็บเอกสารออนไลน์ (Cloud / File Sharing) เป็นต้น

๕. สำรองกำลังคน (Standby) กำหนดผู้แทนหากเจ้าหน้าที่หลักไม่สามารถทำงานได้

๖. ติดตามและประเมินสถานการณ์อย่างต่อเนื่อง

๗. ปรับแผนการทำงานตามประกาศภาครัฐและสถานการณ์จริง

๘. สรุปรายงานเหตุการณ์ (Lessons Learned)



<u>กรณีที่ ๓</u> : ความเสียหายจากโรคระบาดที่ส่งผลต่อบุคลากรและความต่อเนื่องของงาน
<u>ตัวอย่างสถานการณ์</u> : การแพร่ระบาดของโรคติดเชื้อไวรัสโคโรน่า 2019

๗. แผนทำระบบคอมพิวเตอร์กลับสู่สภาพปกติ

ภายหลังจากการเหตุการณ์ความไม่แน่นอน/ภัยพิบัติได้สงบลง ให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหายแล้วรายงานให้ผู้อำนวยการศูนย์สารสนเทศและผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐระดับกรม (DCIO) ทราบ กรณีพื้นที่ไม่ได้รับความเสียหายให้รีบดำเนินการกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์ จะต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑) จัดหาและเปลี่ยนอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทนชิ้นส่วนที่เสียหาย

๒) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จและสามารถใช้งานได้ภายใน ๔๘ ชั่วโมง

๓) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว ในกรณีจำเป็นเร่งด่วน

๔) นำ Back Up ฮาร์ดดิสก์ ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยทีมผู้ดูแลระบบเป็นผู้กู้ให้สามารถกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๕) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

๘. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้อำนวยการศูนย์สารสนเทศ และผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐระดับกรม (DCIO) ทราบเป็นประจำทุกเดือนและให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีที่ได้ระบุไว้

ศูนย์สารสนเทศ
สำนักงาน กปร.