สำนักงานคณะกรรมการป้องกันและปราบปราม
การทุจริตในภาครัฐ (สำนักงาน ป.ป.ท.)

แผนการรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ประจำปี พ.ศ. ๒๕๖๘

กลุ่มงานคอมพิวเตอร์และการสื่อสาร

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท.

มีนาคม ๒๕๖๘

สารบัญ

หน้า

๑. บทนำ ๓
๒. วัตถุประสงค์ ๓
๓. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ ๔
๔. แนวทางการป้องกันและเตรียมการเบื้องต้น ๕
๕. การเตรียมความพร้อมรับสถานการณ์จากระบบคอมพิวเตอร์
และข้อมูลเกิดความเสียหาย ๘
๖. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ ๑๑
๗. ขั้นตอนและผังกระบวนการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยี
สารสนเทศ ๑๒
๘. การกู้คืนระบบกลับสู่สภาพเดิม ๒๔
๙. การติดตามและรายงานผล ๒๕
๑๐.การจัดองค์กรและการกำหนดผู้รับผิดชอบ ๒๕

แผนการรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)
ประจำปี พ.ศ. ๒๕๖๘

๑. บทนำ

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ (สำนักงาน ป.ป.ท.) ได้พัฒนา และนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศ เพื่อความสะดวกในการสร้างข้อมูลสารสนเทศอันมีประโยชน์ต่อการวางแผน พัฒนา และบริหารจัดการองค์กร รวมถึงการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์กรจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท. ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และการให้บริการเจ้าหน้าที่รวมไปถึงประชาชนให้สะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี โดยไวรัสคอมพิวเตอร์ บุคลากร รวมถึงผู้มาติดต่อ นอกจากนี้ปัญหาระบบไฟฟ้า อัคคีภัย หรือปัจจัยทั้งภายในและภายนอกต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ส่งผลกระทบต่อการดำเนินงาน เพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ เพื่อเป็นกรอบแนวทางในการแก้ไขปัญหาให้ระบบฐานข้อมูลและสารสนเทศกลับสู่ความเป็นปกติ ตลอดจนการดูแลรักษาระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้พร้อมใช้งาน ได้อย่างมีประสิทธิภาพต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๕ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศ

๓. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์

๓.๑ การวิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน ป.ป.ท. สามารถจำแนกได้เป็น ๒ กลุ่มหลัก ดังนี้

๓.๑.๑ ภัยพิบัติจากภายนอก

๑) ภัยธรรมชาติ และการเกิดเหตุการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องคอมพิวเตอร์แม่ข่าย เช่นอัคคีภัย อุทกภัย วาตภัย ความชื้น อุณหภูมิ แผ่นดินไหว ภัยแล้ง คลื่นความร้อน ฯลฯ

๒) การชุมนุมประท้วงทางการเมือง เพื่อปิดกั้นการเข้าถึงสำนักงาน ป.ป.ท. และศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยมีจุดประสงค์ไม่ให้เจ้าหน้าที่สามารถปฏิบัติงานได้

๓) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๔) ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

๕) ระบบการแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๖) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งสร้างความเสียหายและทำลายระบบข้อมูล

๗) ไวรัสคอมพิวเตอร์ และโปรแกรมเรียกค่าไถ่ (Ransomware)

๘) โรคระบาดที่มีความร้ายแรงส่งผลกระทบในวงกว้าง

๓.๑.๒ ภัยพิบัติจากภายใน

๑) เครื่องคอมพิวเตอร์แม่ข่ายหลัก ระบบฐานข้อมูลหลัก หรือข้อมูลหลัก เสียหายหรือถูกทำลาย

๒) เครื่องมืออุปกรณ์ด้านการสื่อสารโทรคมนาคม เสียหายหรือถูกทำลาย

๓) เจ้าหน้าที่หรือบุคลากรขององค์ขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ที่ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๓.๒ การประเมินสถานการณ์ และกำหนดระดับความรุนแรง (Situation Assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติและจะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่าง ๆ (Security Log Management System) โดยเจ้าหน้าที่ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อนำมาจัดทำกระบวนการและผังงานการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ รวมทั้งแผนกู้คืนระบบกลับสู่สภาพเดิมต่อไป

ตารางที่ ๑.๑ การประเมินระดับความรุนแรงจากสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

สถานการณ์ หรือ สภาวะฉุกเฉิน	ระดับความรุนแรง (๑ รุนแรงต่ำที่สุด / ๕ รุนแรงสูงที่สุด)				คะแนนรวม	จัดลำดับ
	ต่อระบบงาน	ต่อพันธกิจตามกฎหมาย	ต่อเจ้าหน้าที่ภายในกรม	ต่อประชาชน		
ไฟไหม้	๕	๕	๕	๕	๒๐	๑
โดนเจาะระบบ / ภัยคุกคามทางไซเบอร์	๕	๓	๕	๕	๑๘	๒
ไฟฟ้าดับ/ หม้อไฟระเบิด	๕	๑	๕	๕	๑๖	๓
แผ่นดินไหว	๔	๑	๕	๔	๑๔	๔
โรคระบาดที่มีความร้ายแรงส่งผลกระทบในวงกว้าง	๓	๑	๕	๔	๑๓	๕
ชุมนุมประท้วงและก่อจลาจล	๓	๑	๔	๔	๑๒	๖

๔. แนวทางการป้องกันและเตรียมการเบื้องต้น

๔.๑ การประกาศแผน (Activation)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีการประกาศใช้แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ อย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด เมื่อเกิดเหตุการณ์ฉุกเฉิน

๔.๒ กระบวนการดำเนินงาน (Procedure)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในสำนักงาน ป.ป.ท. โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์การระบุที่มาของผู้ที่บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา และถูกต้อง ระบบงานต่าง ๆ ต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

๔.๓ การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านการรักษาความมั่นคงปลอดภัย กรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น

๔.๔ การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ ดังนี้

๑) เครื่องคอมพิวเตอร์ตั้งโต๊ะ/ เครื่องคอมพิวเตอร์พกพา

๒) อุปกรณ์สำรองข้อมูลระบบงานที่สำคัญ เช่น External Hard Disk/ SAN Storage/ NAS Storage/ Cloud

๓) โปรแกรม Antivirus / Spyware

๔) ไดร์ฟเวอร์อุปกรณ์ต่าง ๆ

๕) ระบบสำรองไฟฉุกเฉิน /ระบบสำรองไฟอัตโนมัติ

๖) อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๔.๕ การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลสูญหาย ถูกทำลายจากไวรัสคอมพิวเตอร์หรือถูกผู้บุกรุกเข้ามาทำลายข้อมูลหรือ ทำการเปลี่ยนแปลงข้อมูล ให้มีข้อมูลสำรองที่สามารถนำกลับมาใช้งานใหม่ได้ ซึ่งสำนักงาน ป.ป.ท. มีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์ ดังนี้

๑) การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลไว้โดยสำรองในเวลาตามที่ระบบกำหนดไว้ รวมถึงการสำรองไปยัง Backup Site ตามแนวทางที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนด แต่ละประเภท ตามแผนการสำรองข้อมูล

๒) การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดเจ้าหน้าที่ทำการสำรองข้อมูลตามระยะเวลาที่กำหนดเป็นประจำ โดยจะทำการสำรองข้อมูล Source Code และบันทึกข้อมูลในหน่วยจัดเก็บข้อมูลสำรอง (Secondary Storage)

๔.๖ การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟท์แวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะการเชื่อมต่ออินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ที่ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้ โดยสำนักงาน ป.ป.ท. มีนโยบายป้องกันไวรัส และซอฟต์แวร์ที่เป็นอันตราย

๔.๗ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

การป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ โดยมีระบบสำรองไฟฟ้า และปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องแม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าได้ประมาณ ๑๕-๓๐ นาที รวมถึงมีการเปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔.๘ การป้องกันการบุกรุก และภัยคุกคามทางไซเบอร์

เพื่อเป็นการป้องกัน และเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับระบบสารสนเทศและระบบเครือข่าย โดยมีแนวทาง ดังนี้

๑) มีประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงาน ป.ป.ท.

๒) มีมาตรการควบคุมการเข้าอกห้องควบคุมระบบเครือข่าย และการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็น ให้มีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นผู้รับผิดชอบนำพาเข้าไป รวมถึงมีการติดตั้งกล้องวงจรปิดปิดภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเป็นการรักษาความปลอดภัย

๓) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้โดยเปิดใช้งาน Firewall ตลอดเวลา

๔) มีการติดตั้งระบบ SSL ควบคุมการเข้าถึงและใช้บริการเครือข่ายจากภายนอก

๕) มีการติดตั้งอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)

๖) มีการติดตั้ง SSL ใบรับรองความปลอดภัยบนเครื่องคอมพิวเตอร์แม่ข่าย

๗) มีการติดตั้งระบบ Anti-Spam Mail ป้องกันอีเมล์ขยะ

๘) มีการติดตั้งระบบป้องกันมัลแวร์

๙) มีการสำรองข้อมูลอย่างสม่ำเสมอ

๑๐) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติเพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๑๑) มีการตรวจสอบด้านความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย

๑๒) มีระบบการรักษาความมั่นคงปลอดภัยของเว็บไซต์ ตามมาตรฐานการรักษาความมั่นคงปลอดภัย สำหรับเว็บไซต์ (Website Security Standard: WSS)

๑๓) มีการพัฒนาเว็บไซต์ตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บไซต์ (Web Application Security Standard: WAS)

๑๔) การดำเนินการตามประราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามทางไซเบอร์ได้เป็นอย่างดี

๑๕) มีการกำหนดแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ของ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท.

๑๖) มีการเข้าร่วมโครงการกับศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) เพื่อติดตามตรวจสอบเครือข่ายป้องกันการบุกรุก ช่วยวิเคราะห์รูปแบบการโจมตีทางไซเบอร์ที่เกิดขึ้นกับระบบเครือข่าย สำนักงาน ป.ป.ท. (Government Threat Monitoring System: GTM) และเพื่อตรวจสอบช่องโหว่เว็บไซต์ (Vulnerability Assessment) และป้องกันการโจมตีเว็บไซต์ของสำนักงาน ป.ป.ท. (Government Website Protection System: GWP)

๔.๙ การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็นกรณีแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นดินไหวโดยเตรียมอุปกรณ์ ดังนี้

๑) การเตรียมไฟฉายอุปกรณ์ยังชีพ และแจ้งให้ทุกคนทราบถึงที่เก็บ

๒) ฝึกซ้อมการปฐมพยาบาลเบื้องต้นเพื่อปฏิบัติในยามฉุกเฉิน

๓) ควรทราบตำแหน่งของวาล์วถังก๊าซ น้ำประปา และตู้ควบคุมระบบไฟฟ้าในอาคาร

๔) ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง

๕) ผูก หรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

๖) การศึกษาแผนและฝึกซ้อมการอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจนและเป็นสัดส่วนของแต่ละชั้น หรือหน่วยงาน

๕. การเตรียมความพร้อมรับสถานการณ์จากระบบคอมพิวเตอร์ และข้อมูลเกิดความเสียหาย

๕.๑ การเตรียมความพร้อมจากเหตุไฟฟ้าดับ ไฟฟ้ากระชาก หรือหม้อแปลงระเบิด

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้น เพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) การจัดทำขั้นตอนแผนผังการรับมือสถานการณ์ฉุกเฉิน กรณีไฟดับ หม้อแปลงระเบิด

๒) ติดตั้งเครื่องสำรองไฟฟ้า และปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องแม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้า โดยประมาณ ๑๕-๓๐ นาที

๓) ตรวจสอบอุปกรณ์ไฟฟ้า และอุปกรณ์ไฟฟ้าให้พร้อมใช้งานอยู่เสมอ

๔) จัดทำ Check List ระยะเวลาในการปิด/เปิดระบบสารสนเทศที่มีเครื่องแม่ข่ายติดตั้งอยู่ในห้องควบคุมระบบเครือข่าย

๕) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๖) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ค้างอยู่ทันที และทำการปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

๗) ให้มีการสำรองข้อมูลทุก ๆ ๑ เดือน เป็นอย่างน้อย

๕.๒ การเตรียมความพร้อมรับสถานการณ์จากเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) การจัดทำขั้นตอนแผนผังการรับมือสถานการณ์ฉุกเฉิน จากไฟไหม้

๒) ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคารเพื่อการควบคุมเพลิงในเบื้องต้นสำหรับห้องปฏิบัติการคอมพิวเตอร์ ควรติดตั้งถังดับเพลิงชนิดหูหิ้วที่สามารถดับไฟประเภท C ได้เป็นอย่างน้อย (อุปกรณ์ไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์)

๓) ให้มีการสำรองข้อมูลทุก ๆ ๑ เดือน เป็นอย่างน้อย

๕.๓ การเตรียมความพร้อมรับสถานการณ์จากไวรัสคอมพิวเตอร์

เป็นการป้องกันและแก้ไขปัญหาจากไวรัสคอมพิวเตอร์ เพื่อกำหนดแนวทางการดำเนินการเบื้องต้น เพื่อลดความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก

๒) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

๓) มีการอัพเดทโปรแกรมกำจัดไวรัส (Update Patch) ทุก ๆ ๑ เดือน เป็นอย่างน้อย

๕.๔ การเตรียมความพร้อมรับสถานการณ์จากภัยคุกคามทางไซเบอร์

เพื่อเป็นการป้องกันและเสริมสร้างความปลอดภัยทางไซเบอร์ให้กับระบบสารสนเทศ และระบบเครือข่าย มีแนวทาง ดังนี้

๑) การจัดทำขั้นตอนแผนผังการรับมือสถานการณ์ฉุกเฉินจากภัยคุกคามทางไซเบอร์

๒) กำหนดมาตรการควบคุมการเข้าออก ห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

๓) หากบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบเครือข่าย จะต้องให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้ดูแลระบบเครือข่าย เป็นผู้นำพาเข้าไปที่ประตูทางออก และคอยกำกับดูแลตลอดการปฏิบัติงาน

สำหรับประตูเข้าออก มีการติดตั้ง Access Control โดยใช้ Key Card และรหัสผ่าน พร้อมทั้งติดตั้งกล้องวงจรปิด เพื่อป้องกันการโจรกรรม

๔) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณของข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือมีความถี่ในการเรียกใช้ระบบสารสนเทศผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕) มีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้งานอินเตอร์เน็ตและระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๕.๕ การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ รวมถึงบุคลากรภายในองค์กรขาดทักษะ ความรู้ความเข้าใจเกี่ยวกับอุปกรณ์คอมพิวเตอร์

เป็นการสร้างความตระหนักรู้ โดยการจัดอบรมให้บุคลากรของสำนักงาน ป.ป.ท.มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ และซอฟต์แวร์เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

๑) สร้างเครือข่ายด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กรเพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

๒) การวางกฎระเบียบ ให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์ จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

๕.๖ การเตรียมความพร้อมรับสถานการณ์จากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ ให้เริ่มตั้งแต่ปัจจุบัน เพื่อติดตามสถานการณ์รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น ดังนี้

๑) ติดตามข่าวสารการเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้อง รวมถึงข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่าง ๆ ทั้งภายในและภายนอกประเทศ

๒) การสังเกตพฤติกรรมของสัตว์ เช่น แมลงสาบจำนวนมากวิ่งเพ่นพ่าน เป็นต้น

๓) การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์ที่จำเป็น

๔) การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

๕) การปฏิบัติขั้นเตรียมการ

- การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม
- การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญ และกำหนดมาตรการในการเผชิญเหตุ
- อบรมให้ความรู้การปฏิบัติตน เมื่อเกิดแผ่นดินไหว และอาคารถล่มแก่เจ้าหน้าที่ในองค์กร

๕.๗ การเตรียมความพร้อมรับสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์ จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้สามารถเชิญเหตุได้

๑) การจัดทำขั้นตอนแผนผังการรับมือสถานการณ์ฉุกเฉินจากการชุมนุมประท้วงและก่อจลาจล

๒) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุอุปกรณ์ เครื่องมือเครื่องใช้ระบบการสื่อสาร ยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

๓) ตรวจสอบระบบไฟฟ้า ระบบสำรองไฟฟ้า และระบบรักษาความปลอดภัยสำหรับห้องควบคุมระบบเครือข่าย ให้อยู่ในสภาพที่พร้อมใช้งาน

๔) ดำเนินการสำรองข้อมูล

๕) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๖) จัดเตรียมช่องทางการเข้าใช้งานระบบจากระยะไกล (Remote) กรณีที่มีเหตุขัดข้องเจ้าหน้าที่สามารถ Remote เข้ามาแก้ไขปัญหาได้ทันที โดยไม่ต้องเดินทางมาปฏิบัติงาน ณ สำนักงาน ป.ป.ท.

๗) จัดทำบัญชีรายชื่อและข้อมูลการติดต่อกับหน่วยงานภายนอก กรณีมีเหตุฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น

๕.๘ การเตรียมความพร้อมรับสถานการณ์จากโรคระบาดที่มีความร้ายแรง ส่งผลกระทบในวงกว้าง

๑) การจัดทำแนวทางการใช้เทคโนโลยีสนับสนุนการปฏิบัติงานนอกสถานที่ตั้งราชการ

๒) เพื่อเป็นการเฝ้าระวัง และตรวจสอบให้ระบบสารสนเทศพร้อมใช้งานอย่างต่อเนื่อง จึงต้องมีการจัดเวรรักษาการณ์เฝ้าระวัง ดูแลความปลอดภัยระบบเทคโนโลยีสารสนเทศ และตรวจสอบความพร้อมใช้งานของห้องควบคุมเครือข่ายคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ

๓) จัดเตรียมช่องทาง SSL VPN เพื่อให้ผู้แลระบบ สามารถเข้าถึงระบบ หรือเครื่องคอมพิวเตอร์แม่ข่ายได้อย่างปลอดภัย

๔) จัดเตรียมระบบอินเตอร์เน็ตความเร็วสูง (Fiber Optic) หรือเทคโนโลยี MPLS (Multiprotocol Label Switching) หรือ Leased Line

๕) จัดเตรียมอุปกรณ์คอมพิวเตอร์ แท็บเล็ต โน้ตบุ๊ก โทรศัพท์เคลื่อนที่ กล้องวิดีโอ หูฟัง หรืออุปกรณ์อื่น ๆ ที่สามารถเชื่อมต่อเข้ากับเครือข่ายภายในสำนักงานได้

๖) จัดเตรียมแอปพลิเคชัน และเทคโนโลยีสนับสนุนการทำงาน

๗) จัดเตรียมระบบการประชุมผ่านระบบ Conference สำรับการประชุมออนไลน์นอกสถานที่

๘) จัดเตรียมบัญชีรายชื่อติดต่อ หน่วยงาน บุคลากร สำหรับการติดต่อประสานงาน

๙) จัดเตรียมระบบเครือข่ายส่วนตัวเสมือน (VPN) ที่มีการป้องกันและความเป็นส่วนตัวสูงเมื่อใช้งานผ่านอินเตอร์เน็ต สำหรับการเข้าใช้งานแอปพลิเคชันระบบงานภายใน

๑๐) ผู้ปฏิบัติงาน จัดเตรียมอินเตอร์เน็ตความเร็วสูง หรือ อินเตอร์เน็ตไร้สาย (Mobile Broadband) หรือ ๔G/๕G mobile

๑๑) ผู้ปฏิบัติงาน จัดเตรียมอุปกรณ์คอมพิวเตอร์ แท็บเล็ต โน้ตบุ๊ก โทรศัพท์เคลื่อนที่ กล้องวิดีโอ หูฟัง หรืออุปกรณ์อื่น ๆ ที่สามารถเชื่อมต่อเข้ากับอินเตอร์เน็ต เพื่อใช้ในการปฏิบัติงานได้

๑๒) จัดเตรียมระบบสารสนเทศภายใน ให้สามารถเข้าใช้งานจากภายนอกได้

๑๓) ผู้ปฏิบัติงาน จัดเตรียมโปรแกรมประยุกต์ และเทคโนโลยีสนับสนุนการทำงานต่าง ๆ

๖. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติ ดังนี้

๖.๑ กรณีเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้งานระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุให้ผู้ดูแลระบบเครือข่าย หรือฐานข้อมูลสารสนเทศของหน่วยงานทราบ หรือในกรณีเกิดจาก ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ

๒) กรณีเกิดจากการขัดข้อง เนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้น ออกให้หมด

๓) ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้แจ้งเหตุขัดข้อง ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อแก้ไขปัญหาต่อไป

๖.๒ กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์แม่ข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ ประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓) ตัดระบบจ่ายไฟ

๔) ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

๕) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย หรือผู้เชี่ยวชาญ

๖) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรองหรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗) ผู้ดูแลระบบต้องรีบแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบโดยเร็ว

๗. ขั้นตอนและผังกระบวนการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๗.๑ ขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากไฟไหม้

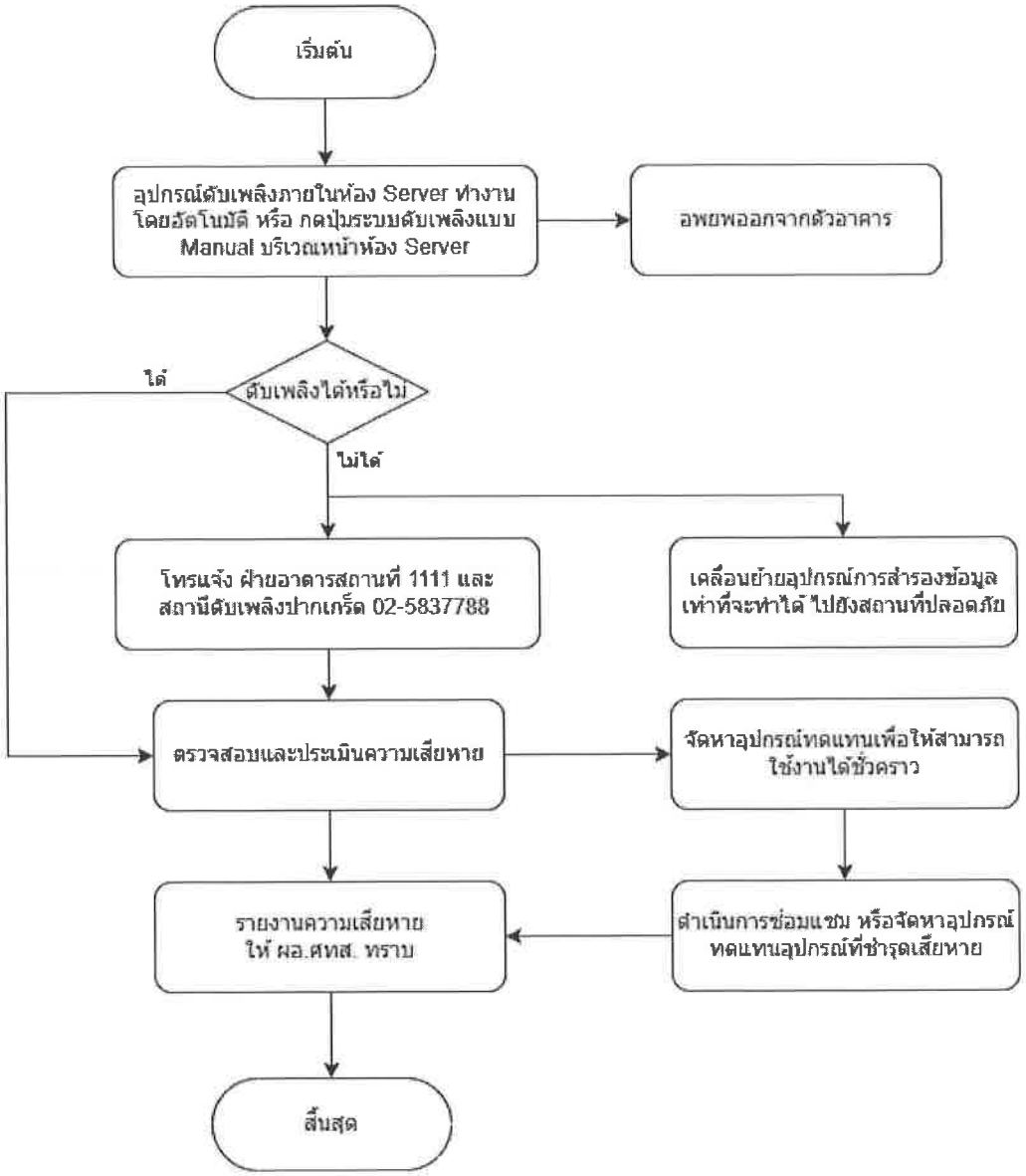
๑) หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่เพื่อดับไฟ

๒) หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ติดต่อประสานงานโทรแจ้งงานอาคารและสถานที่ หมายเลขโทรศัพท์ ๑๑๑๑ และโทรแจ้งสถานีดับเพลิงปากเกร็ด หมายเลขโทรศัพท์ ๐๒-๕๘๓-๗๗๘๘

๓) หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้

๔) อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมออย่างน้อยปีละ ๑ - ๒ ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินที่เกิดจากไฟไหม้



๗.๒ ขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากระบบไฟฟ้าขัดข้อง/ ไฟดับ

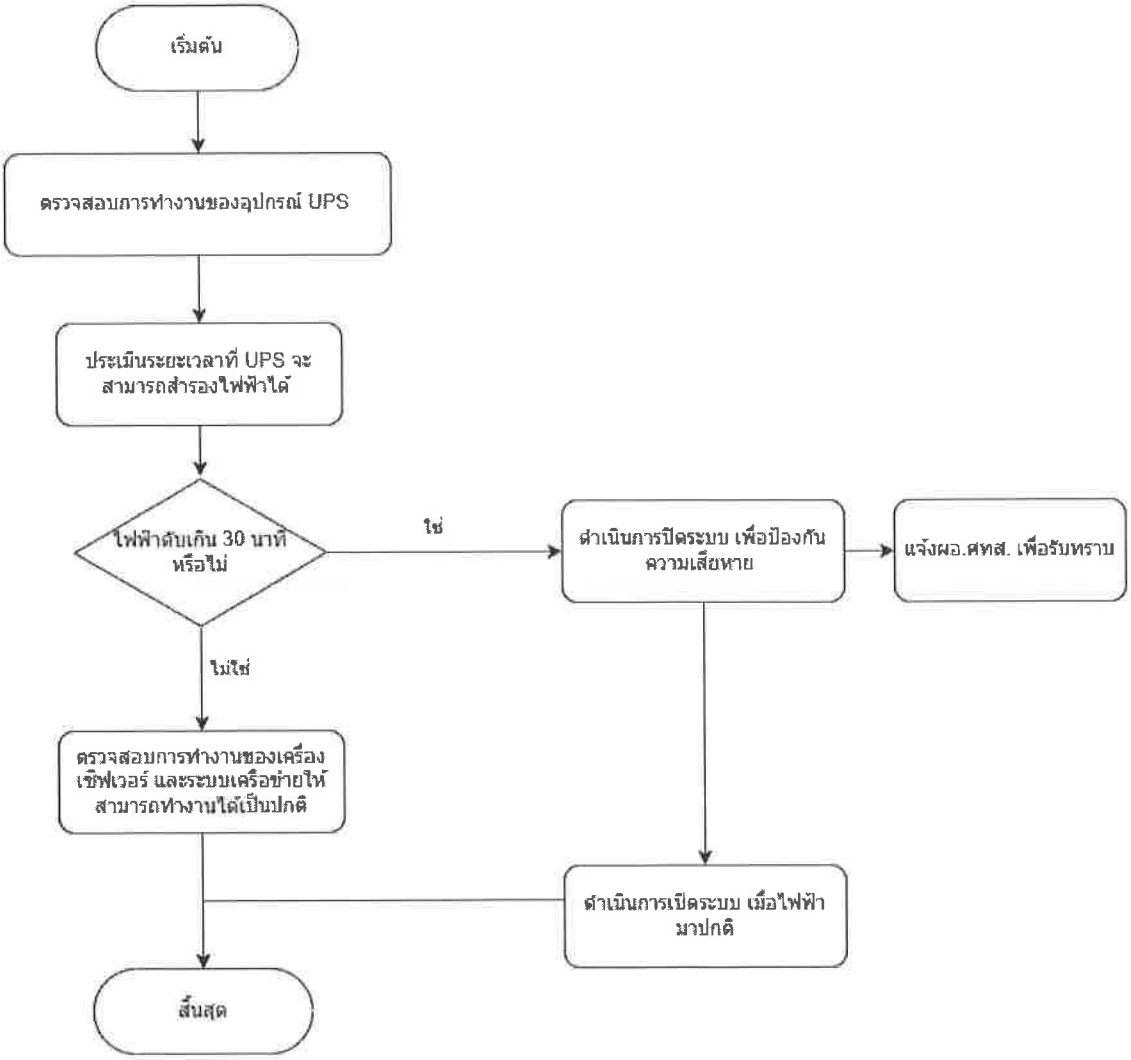
๑) เครื่องคอมพิวเตอร์แม่ข่าย มีระบบสำรองไฟฟ้า UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ประมาณ ๑ ชั่วโมง

๒) หากใกล้ครบ ๑ ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังหัวหน้างานเทคโนโลยีสารสนเทศ

๓) ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย

๔) หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้นหรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากระบบไฟฟ้าขัดข้อง/ ไฟฟ้าดับ



๗.๓ ขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากการโดนเจาะระบบ และภัยคุกคามทางไซเบอร์

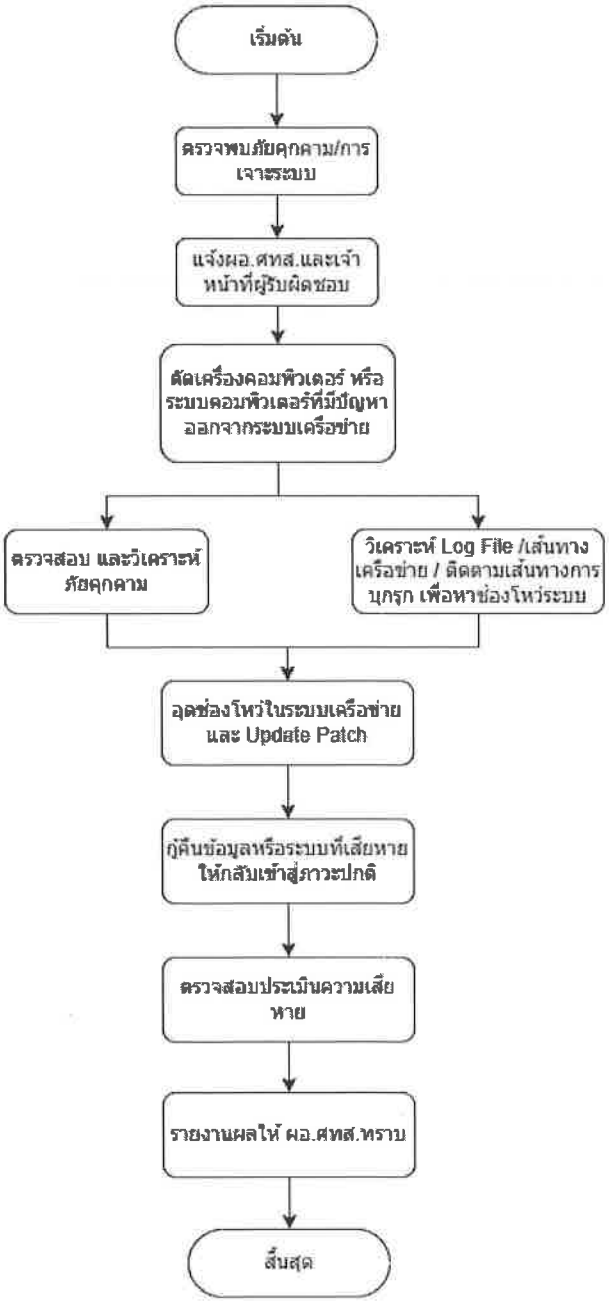
๑) ตรวจสอบภัยคุกคามเพื่อแก้ไขปัญหา
๒) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย
๓) เตรียมการสำหรับการกู้คืนระบบ โดยพิจารณาถึงผลกระทบต่อองค์กรเป็นหลัก
๔) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ และไฟล์อื่น ๆ
๕) วิเคราะห์ Log File ๙ตรวจสอบโปแกรมและข้อมูลที่ผู้บุกรุกทิ้งไว้
๖) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System
๗) ตรวจสอบติดตามเส้นทางผู้บุกรุก เพื่อหาช่องโหว่ของระบบ
๘) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่
๙) งดใช้เซอร์วิสที่ไม่จำเป็น
๑๐) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

๑๑) อุดช่องโหว่ในระบบเครือข่าย

๑๒) เปลี่ยนแปลงรหัสผ่านใหม่ หลังจากที่ได้แก้ไขช่องโหว่ของระบบแล้ว

เมื่อกลับสู่ภาวะปกติผู้รับผิดชอบจะต้องเข้าตรวจสอบระบบงาน และระบบเครือข่าย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการกลุ่มงานเครือข่ายและการสื่อสาร และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ

แผนผังแสดงขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากการโดนเจาะระบบ และภัยคุกคามทางไซเบอร์



๗.๔ ขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากแผ่นดินไหว

๑) การปฏิบัติตัวขณะเกิดแผ่นดินไหว

- ควบคุมสติ อย่าตื่นตกใจ อยู่อย่างสงบและรอฟังประกาศฉุกเฉิน
- ถ้าอยู่ในอาคาร ให้อยู่ห่างจาก หน้าต่าง ประตู กำแพงด้านนอก ชั้นวางของ ที่อาจล้มหรือหล่นใส่ได้
- อย่ารีบออกจากอาคาร เนื่องจากอาจได้รับบาดเจ็บจากฝูงชนที่ตื่นตกใจ
- ห้ามใช้เทียนไขหรือไม้ขีดไฟ หรือสิ่งที่ทำให้เกิดเปลวไฟ เนื่องจากอาจเกิดอันตรายจากก๊าซรั่วได้
- ห้ามใช้ลิฟต์โดยเด็ดขาด หากต้องอพยพให้ใช้บันได้หนีไฟที่ปลอดภัยตามแผนอพยพ
- ถ้าอยู่นอกอาคาร ให้อยู่ห่างจากอาคาร เสาไฟฟ้า สิ่งห้อยแขวน ป้ายโฆษณา โดยให้อยู่ในที่โล่งจนกว่า การสั่นไหวจะหยุด
- ถ้ากำลังขับรถยนต์ ให้จอดรถยนต์ในที่ที่ปลอดภัยโดยเร็วเท่าที่จะทำได้ และอยู่ในรถ หลีกเลี่ยงการจอดรถยนต์ใกล้ต้นไม้ อาคาร สะพาน ทางต่างระดับ เสาไฟฟ้า
- ให้อยู่ห่างจากประตูหน้าต่าง โดยเฉพาะที่เป็นกระจก และอยู่ห่างจากบริเวณที่อาจมีวัสดุหล่นใส่
- ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็ว ตามแผนอพยพหนีไฟของแต่ละอาคาร
- ถ้าไม่อยู่ใกล้ทางออกให้ “หมอบ” “ป้อง” “เกาะ” จนกว่าจะมีผู้เข้าไปช่วยเหลือ

๒) เมื่อแผ่นดินไหวสงบ

- ตรวจดูอาการบาดเจ็บของตนเอง และคนใกล้เคียง หากได้รับบาดเจ็บให้ทำการปฐมพยาบาลเบื้องต้นและนำส่งโรงพยาบาล
- รีบออกจากอาคารที่เสียหาย เพราะอาจเกิดถล่มซ้ำ
- ตรวจสอบโครงสร้างอาคาร ท่อน้ำ ก๊าซ กระแสไฟฟ้า และหากพบความเสียหายให้ปิดระบบการทำงานทั้งหมดทันที
- หากพบก๊าซรั่ว ให้เปิดหน้าต่าง และประตูทุกบานโดยรีบออกจากอาคารแล้วแจ้งเจ้าหน้าที่ทันที

๓) ข้อปฏิบัติหากติดอยู่ภายใต้ซากปรักหักพัง

- อยู่กับที่ ป้องกันศีรษะและหน้า จากกระจกที่แตก หรือวัสดุที่หล่นโดยใช้เสื้อ ผ้าห่ม หนังสือพิมพ์ กล่องกระดาษ ฯลฯ คลุมศีรษะ
- พิงตัวเองกับผนังห้องที่ไม่มีหน้าต่างกระจก / ชั้นวางของ หรือคลานไปหลบใต้โต๊ะเพื่อป้องกัน วัสดุหล่นใส่
- หากติดอยู่ในที่ปลอดภัยให้อยู่กับที่อย่าเคลื่อนย้าย เพราะอาจได้รับอันตรายจากสิ่งของแตกหักพังทลาย
- ห้ามก่อให้เกิดเปลวไฟใด ๆ ทั้งสิ้น
- ส่งสัญญาณขอความช่วยเหลือ และรอการช่วยเหลือจากหน่วยกู้ภัย

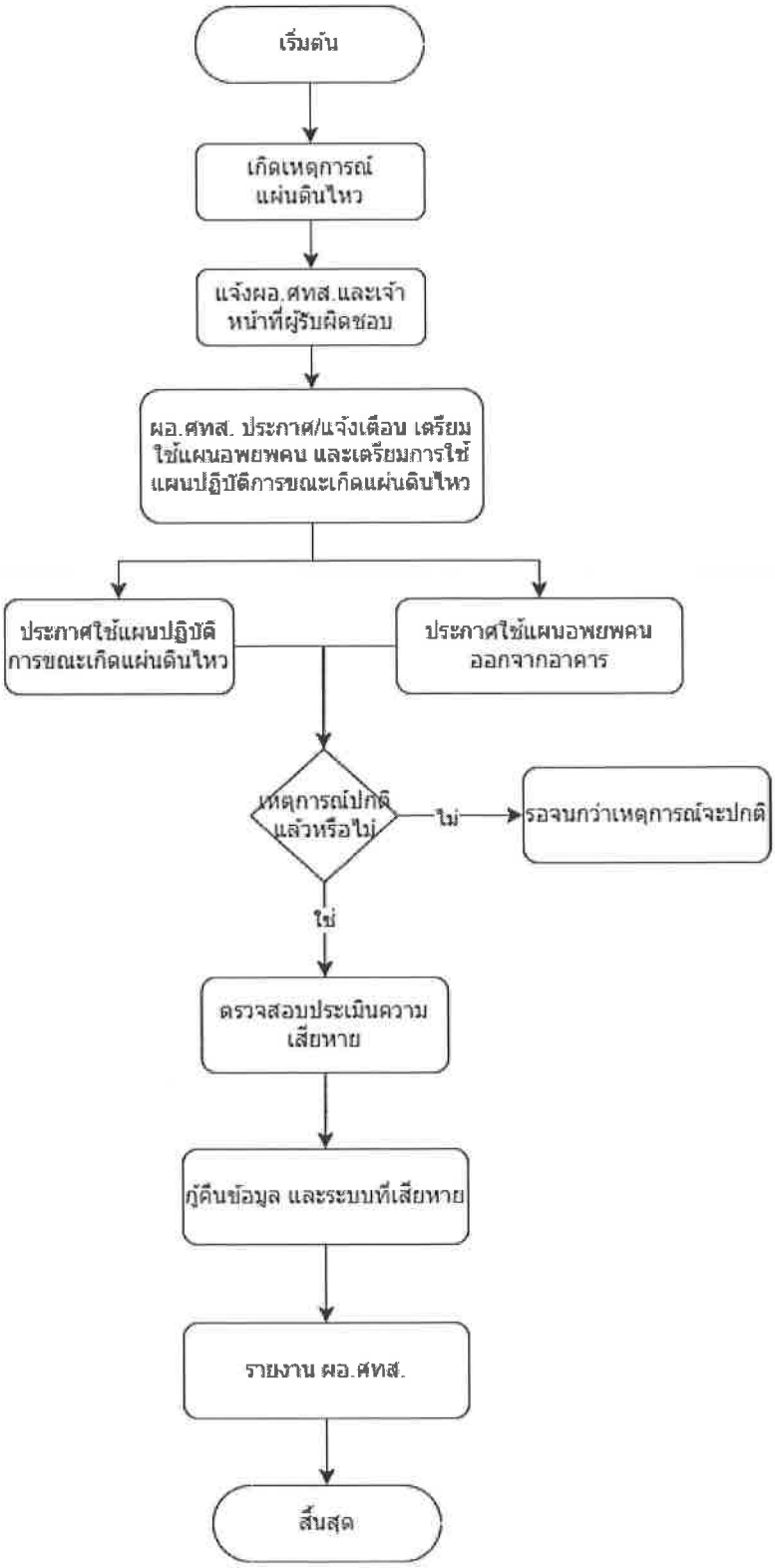
๔) การปฏิบัติตนในการอพยพหนีภัยจากแผ่นดินไหว

- ควบคุมสติอารมณ์ตามแผนอพยพ
- เชื่อฟังคำแนะนำของผู้ที่เกี่ยวข้อง
- เก็บทรัพย์สิน เอกสารสำคัญไว้ในลิ้นชักโต๊ะ และล็อคกุญแจ
- เมื่อออกมาภายนอกแล้ว ห้ามกลับเข้าไปอีกเด็ดขาด
- ห้ามขนสัมภาระใด ๆ ติดตัวขณะอพยพ
- ใช้วิธีเดินเร็ว ห้ามวิ่งหรือเดินช้า
- ใช้ช่องทางหนีไฟ เรียงแถว ขั้นบันไดละ ๒ คน
- ห้ามพูดคุย สายตามองที่บันได มือจับราวบันได ห้ามส่งเสียงเอะอะ หรือเร่งผู้อื่น ห้ามดันหรือแซง
- ห้ามใช้ลิฟต์โดยเด็ดขาด
- เมื่ออพยพถึงชั้นล่างสุด ให้ออกจากอาคารทันที
- ไปรวมพล ณ จุดนัดพบที่กำหนดไว้
- ตรวจสอบจำนวนผู้อพยพ

๕) เจ้าหน้าที่รับผิดชอบดำเนินการตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้บังคับบัญชา และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อทราบและสั่งการต่อไป

๖) เมื่อกลับเข้าสู่ภาวะปกติ ผู้รับผิดชอบดำเนินการเข้าตรวจสอบระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศ เพื่อประเมินความเสียหาย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบและสั่งการให้กู้คืนระบบ ทั้งด้านอาคารสถานที่ ระบบเครือข่าย ฮาร์ดแวร์ และซอฟต์แวร์ ให้กลับคืนสู่สภาพเดิมต่อไป

แผนผังแสดงขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากแผ่นดินไหว



๗.๕ ขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากเหตุการณ์ความไม่สงบของบ้านเมือง/การชุมนุมประท้วง/การก่อจลาจล

๑) เมื่อได้รับแจ้งเหตุให้แจ้งเจ้าหน้าที่รับผิดชอบ หรือแจ้งผู้บังคับบัญชาตามลำดับชั้น

๒) ผู้บังคับบัญชา ประกาศแนะนำแจ้งเตือนเจ้าหน้าที่ในองค์กร และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย

๓) หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนเตรียมความพร้อรับสถานการณ์ฉุกเฉินที่เตรียมไว้ล่วงหน้าตามควรแก่กรณี ดังนี้

๑) ก่อนเกิดเหตุ

- ตรวจเช็คความพร้อมของระบบไฟฟ้า เครื่องสำรองไฟฟ้า และระบบรักษาความปลอดภัย สำหรับห้องควบคุมระบบเครือข่าย
- ตรวจสอบระบบดับเพลิงอัตโนมัติ
- ตรวจสอบระบบสำรองไฟฟ้าอัตโนมัติ
- ตรวจสอบระบบแจ้งเตือนภัย
- ตรวจสอบระบบปรับอากาศ Precision Air Conditioner
- ตรวจสอบระบบควบคุมอุณหภูมิและความชื้น
- ตรวจสอบระบบกล้องวงจรปิด
- สำรองข้อมูลระบบสารสนเทศของเครื่องคอมพิวเตอร์แม่ข่ายในห้องควบคุมระบบเครือข่าย ลงบนอุปกรณ์จัดเก็บข้อมูล SAN Storage /สำรองลงสื่อบันทึกภายนอก จัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล
- ประชาสัมพันธ์แจ้งเวียนให้สำรองข้อมูลที่สำคัญจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกและจัดเก็บไว้ในที่ที่เหมาะสม
- จัดเตรียมประกาศแจ้งเตือนเหตุการณ์ผิดปกติหน้าเว็บไซต์ของสำนักงาน ป.ป.ท. พร้อมขึ้นประกาศทันทีหากมีเหตุฉุกเฉิน
- จัดเตรียมช่องทางการเข้าใช้งานระบบจากระยะไกล (Remote) กรณีที่มีเหตุขัดข้อง เจ้าหน้าที่ผู้รับผิดชอบ สามารถ Remote เข้ามาแก้ไขปัญหาได้ทันที โดยไม่ต้องเดินทางมาปฏิบัติงาน ณ สำนักงาน ป.ป.ท.
- จัดเตรียมการเฝ้าระวังระบบอินเตอร์เน็ตของผู้ให้บริการ ให้สามารถดำเนินการให้บริการเจ้าหน้าที่ และประชาชนได้อย่างต่อเนื่อง
- จัดเตรียมระบบสารสนเทศภายในให้สามารถเรียกใช้จากภายนอกได้
- ประสานงานเรื่องของความมั่นคงปลอดภัยด้านสารสนเทศกับศูนย์ประสานงานการรักษาความมั่นคงปลอดภัย
- จัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอกเพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น
- กำหนดเจ้าหน้าที่ดูแลรับผิดชอบ/จัดเวรยามรักษาการณ์ดูแลความปลอดภัยระบบเทคโนโลยีสารสนเทศ วันเสาร์-อาทิตย์ และวันหยุดนักขัตฤกษ์

๒) ขณะเกิดเหตุ

- เจ้าหน้าที่พบเหตุ แจ้งผู้บังคับบัญชาทราบถึงเหตุผิดปกติ หรือเหตุฉุกเฉิน
- ประกาสแจ้งเตือนกรณีที่มีเหตุการณ์ผิดปกติ/ฉุกเฉิน หน้าเว็บไซต์ หรือ Facebook หรือประกาศเสียงตามสาย
- เฝ้าระวังระบบอินเตอร์เน็ตของผู้ให้บริการที่สำนักงาน ป.ป.ท. เช่าใช้บริการ กรณีเกิดเหตุขัดข้องต่อผู้ให้บริการรายใดรายหนึ่ง ผู้ดูแลระบบหรือเจ้าหน้าที่ผู้รับผิดชอบจะต้องดำเนินการกำหนด DNS และปรับโหลดอินเตอร์เน็ตให้ไปใช้อินเตอร์เน็ตจากผู้ให้บริการรายที่เหลือได้อย่างต่อเนื่อง
- ปฏิบัติหน้าที่อยู่เวรยามรักษาการณ์ดูแลความปลอดภัยระบบเทคโนโลยีสารสนเทศนอกวันเวลาทำการ ในวันเสาร์ - อาทิตย์ และวันหยุดนักขัตฤกษ์
- กรณีตรวจพบวัตถุต้องสงสัย หรือเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมได้ หรือมีการทำลายทรัพย์สินของสำนักงาน ป.ป.ท. ให้แจ้งไปยังสถานีตำรวจที่ใกล้เคียง หรือหน่วยงานรับแจ้งเหตุฉุกเฉินต่าง ๆ และรายงานให้ผู้บังคับบัญชาทราบ

๓) หลังเกิดเหตุ

- ตรวจสอบระบบเครือข่าย ระบบเทคโนโลยีสารสนเทศ และความเสียหายด้านอื่น ๆ โดยละเอียด พร้อมทั้งประเมินความเสียหาย
- กรณีตรวจพบว่าระบบสารสนเทศหรือข้อมูลมีความเสียหาย ให้กู้คืนระบบกลับสู่สภาพปกติโดยใช้ข้อมูลที่สำรองไว้ ให้ข้อมูลกลับมาใช้ได้เป็นปกติโดยเร็ว

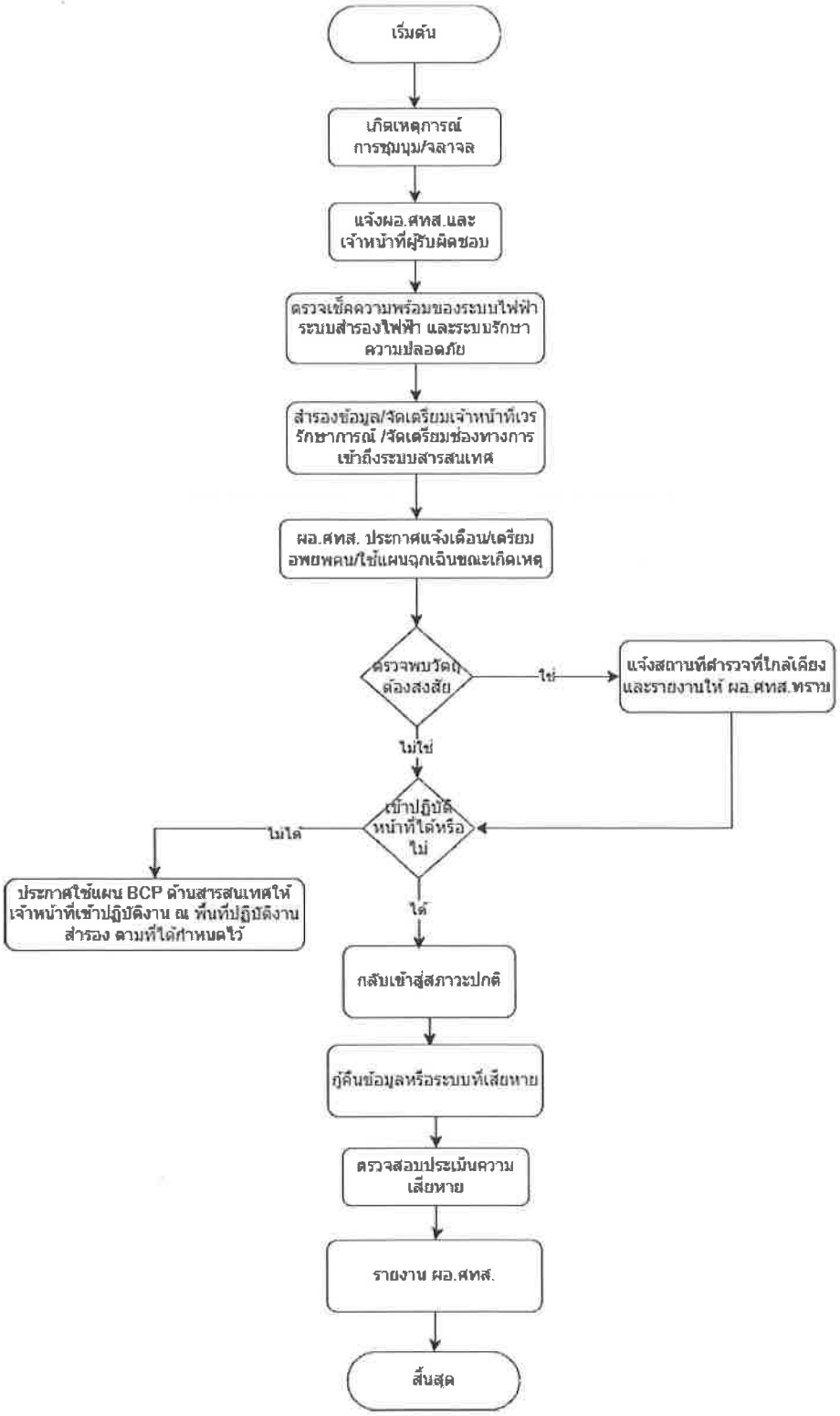
๓.๓ กรณีตรวจพบระบบคอมพิวเตอร์เสียหาย ให้ดำเนินการซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย จัดหาอุปกรณ์ชิ่นส่วนใหม่ เพื่อทดแทน ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๓.๔ รายงานผลความเสียหาย และสรุปผลการดำเนินการให้ผู้บังคับบัญชาทราบ

๔) กรณีไม่สามารถเข้ามาปฏิบัติงานในพื้นที่ของสำนักงาน ป.ป.ท. ได้ ให้ผู้บังคับบัญชาสั่งการใช้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ท. เพื่อจัดเตรียมทรัพยากรที่จำเป็น และให้เจ้าหน้าที่ สำนักงาน ป.ป.ท. เข้าปฏิบัติงาน ณ พื้นที่ปฏิบัติงานสำรองตามที่สำนักงาน ป.ป.ท. กำหนดไว้

๕) เมื่อกลับเข้าสู่สภาพวะปกติ การชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง ผู้รับผิดชอบต้องดำเนินการเข้าตรวจสอบระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศ และสำรวจความเสียหายทุกด้านอย่างละเอียดทำการประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบและสั่งการต่อไป

แผนผังแสดงขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากเหตุการณ์ความไม่สงบของบ้านเมือง/การชุมนุมประท้วง/การก่อจลาจล



๗.๖ ขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากโรคระบาดร้ายแรงที่ส่งผลกระทบในวงกว้าง

เมื่อเกิดโรคระบาดให้ดำเนินการเตรียมพร้อม ตรวจสอบ และเฝ้าระวังการใช้งานระบบสารสนเทศ โดยดำเนินการตามแผนการเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่เตรียมไว้ล่วงหน้าดังนี้

๑) ก่อนเกิดเหตุ

- จัดทำแนวทางการใช้ระบบเทคโนโลยีสารสนเทศสนับสนุนการปฏิบัติงานนอกสถานที่ตั้ง

- เพื่อเป็นการเฝ้าระวัง และตรวจสอบให้ระบบสารสนเทศของสำนักงาน ป.ป.ท. พร้อมใช้งานได้อย่างต่อเนื่อง จึงต้องมีการจัดเวรยามรักษาการณ์เฝ้าระวัง ดูแลความปลอดภัยระบบเทคโนโลยีสารสนเทศ และตรวจสอบความพร้อมใช้งานของห้องควบคุมเครือข่ายคอมพิวเตอร์ ได้แก่ ห้องควบคุมเครือข่าคอมพิวเตอร์ เครื่องสำรองไฟฟ้าอัตโนมัติ (UPS) และระบบเครื่องปรับอากาศแบบควบคุมอุณหภูมิและความชื้น (Precision Air Conditioning System)

- การจัดเตรียมช่องทาง SSL VPN เพื่อให้ดูแลระบบสามารถเข้าถึงระบบ หรือเครื่องคอมพิวเตอร์แม่ข่ายได้อย่างปลอดภัย

- จัดเตรียมระบบอินเตอร์เน็ตความเร็วสูง (Fiber Optic) หรือเทคโนโลยี MPLS (Multiprotocol Label Switching) หรือ Leased Line

- จัดเตรียมอุปกรณ์คอมพิวเตอร์ แท็บเล็ต โน้ตบุ๊ก โทรศัพท์เคลื่อนที่ พร้อมกล้องวิดีโอ หูฟังและลำโพง หรืออุปกรณ์อื่น ๆ ที่สามารถเชื่อมต่อเข้ากับเครือข่ายภายในสำนักงานได้ สำหรับการปฏิบัติงานร่วมกับผู้ที่ปฏิบัติราชการนอกสถานที่

- จัดเตรียมแอปพลิเคชัน และเทคโนโลยีสนับสนุนการทำงานต่าง ๆ สำหรับการปฏิบัติงานร่วมกันระหว่างผู้ที่ปฏิบัติงาน ณ สำนักงาน กับผู้ที่ปฏิบัติงานนอกสถานที่

- จัดเตรียมระบบสนับสนุนการทำงานร่วมกันจากทางไกล จัดเก็บเอกสารไฟล์ เข้าถึงไฟล์งานได้จากภายนอก รองรับการจัดเก็บข้อมูลต่าง ๆ แบบรวมศูนย์

- จัดเตรียมห้องประชุม สนับสนุนการประชุมทางไกลออนไลน์นอกสถานที่

- จัดเตรียมบัญชีรายชื่อติดต่อของหน่วยงาน บุคลากร สำหรับการติดต่อประสานงานระหว่างผู้ปฏิบัติงาน ณ สำนักงาน กับผู้ที่ปฏิบัติงานนอกสถานที่

- จัดเตรียมเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN) ที่มีการป้องกันและความเป็นส่วนตัวสูง เมื่อใช้งานผ่านอินเตอร์เน็ต สำหรับการเข้าใช้งานแอปพลิเคชันระบบงานภายในหน่วยงานของผู้ปฏิบัติงานนอกสถานที่

- ผู้ปฏิบัติงานจัดเตรียมอินเตอร์เน็ตความเร็วสูง (Fiber Obtic) หรืออินเตอร์เน็ตไร้สาย (Mobile broadband) หรือ ๔G/๕G Mobile

- จัดเตรียมอุปกรณ์คอมพิวเตอร์ แท็บเล็ต โน้ตบุ๊ก โทรศัพท์เคลื่อนที่ พร้อมกล้องวิดีโอ หูฟังและลำโพง หรืออุปกรณ์อื่น ๆ ที่สามารถเชื่อมต่อเข้ากับเครือข่ายความเร็วสูงได้ สำหรับการปฏิบัติงานร่วมกับผู้ที่ปฏิบัติงาน ณ สำนักงาน

- จัดเตรียมระบบสารสนเทศภายในให้สามารถเรียกใช้จากภายนอกได้

- ผู้ปฏิบัติงานจัดเตรียมโปรแกรมประยุกต์ และเทคโนโลยีที่สนับสนุนการทำงาน

๒) ขณะเกิดเหตุ

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานในพื้นที่สำนักงาน ป.ป.ท. ได้ ให้ผู้บังคับบัญชาสั่งการใช้แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ท. เพื่อจัดเตรียมทรัพยากรที่

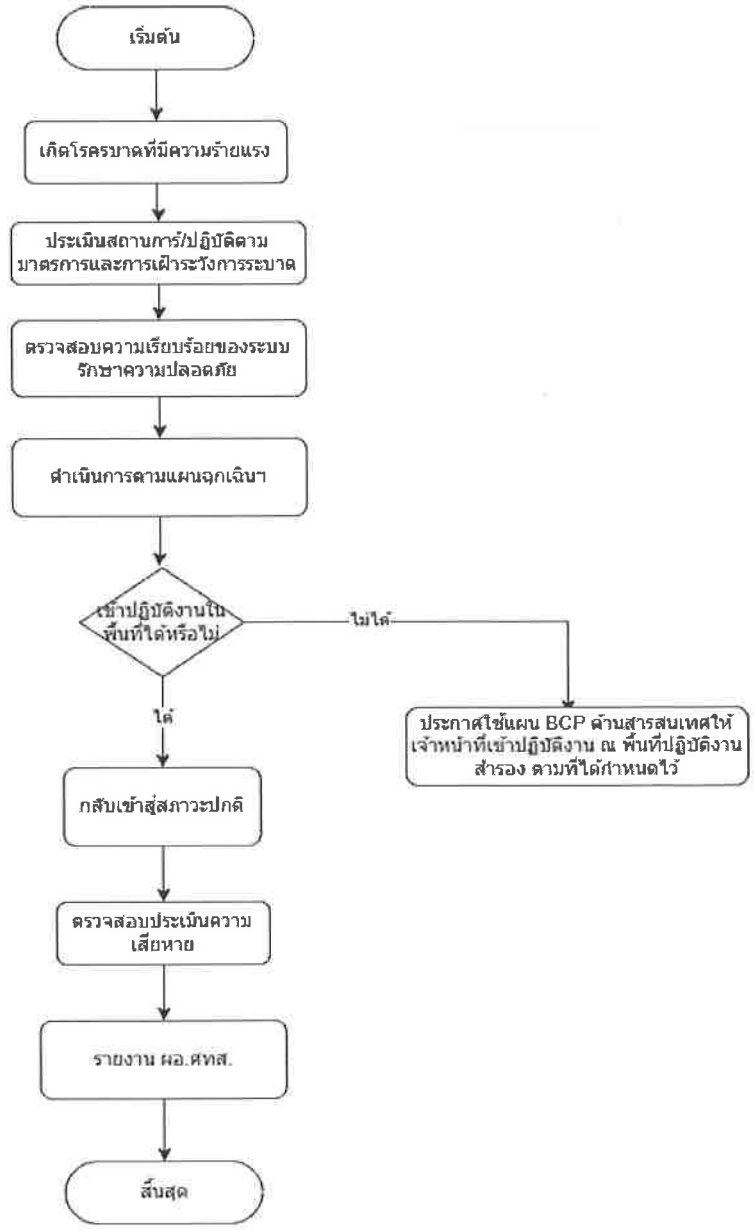
จำเป็น และให้เจ้าหน้าที่ สำนักงาน ป.ป.ท. เข้ามาปฏิบัติงาน ณ พื้นที่ปฏิบัติงานสำรองตามที่ สำนักงาน ป.ป.ท. ได้กำหนดไว้

- ดำเนินการป้องกันภัยตามแผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติเทคโนโลยีสารสนเทศ สำนักงาน ป.ป.ท.

๓) หลังเกิดเหตุ

เมื่อกลับเข้าสู่สภาวะปกติ การเกิดโรคระบาดสิ้นสุดลง ผู้รับผิดชอบและคณะประเมินความเสียหาย ต้องดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ และสำรวจความเสียหายทุกด้านอย่างละเอียด ทำการประเมินความเสียหาย พร้อมทั้งจักทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบและสั่งการต่อไป

แผนผังแสดงขั้นตอนการรองรับสถานการณ์ฉุกเฉินที่เกิดจากโรคระบาดร้ายแรง ที่ส่งผลกระทบในวงกว้าง



๘. การกู้คืนระบบกลับสู่สภาพเดิม

การกู้ระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติ ระบบเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอด ๒๕ ชั่วโมง หากไม่สามารถให้บริการได้ จำเป็นต้องกู้คืนระบบโดยเร็วที่สุด หรือเท่าที่จะดำเนินการได้ ซึ่งแผนการนี้ เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการดังนี้

๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๕) นำอุปกรณ์การสำรองข้อมูล /ซีดีรอม/ ฮาร์ดดิสก์ ที่ได้สำรองข้อมูลไว้นำกลับมา Restore ให้ระบบกลับมาใช้ได้โดยเร็ว ภายใน ๔๘ ชั่วโมง

๖) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

จากภัยพิบัติดังกล่าวไม่เพียงแต่เฉพาะทางด้าน Hardware เช่น ไฟไหม้ แผ่นดินไหว การก่อวินาศกรรม แต่ยังรวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ซึ่งอาจจะมีผลกระทบต่อรบบเทคโนโลยีสารสนเทศ หน่วยงานจึงมีแผนจัดทำการสำรองแหล่งข้อมูลที่สถานที่สำรอง เพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศให้มีความต่อเนื่องอยู่เสมอ โดยแบ่งได้ ๓ ไซต์ คือ

- Hot Site เป็นไซต์ที่มีอุปกรณ์และซอฟต์แวร์เหมือนไซต์หลักมีความพร้อมใช้งานทำให้เวลาในการกู้คืนระบบน้อย แต่จะมีต้นทุนการจัดทำที่สูง
- Warm Site เป็นไซต์ที่คล้ายกับ Hot Site แต่อาจจะมีอุปกรณ์ไม่ครบ ทำให้ความพร้อมใช้งาน ต่ำกว่า Hot Site ใช้ระยะเวลาในการกู้คืนมากกว่า แต่ต้นทุนราคา
- Cold Site เป็นไซต์ที่มีแต่สถานที่ ไม่มีอุปกรณ์ทั้งฮาร์ดแวร์ และซอฟต์แวร์ ในการกู้คืนมีต้นทุน การจัดทำต่ำแต่ระยะเวลาในการกู้คืนนาน

ขั้นตอนการดำเนินงานการกู้คืนระบบ

๑) สำรวจความต้องการของระบบสำรอง

๒) สำรวจไซต์สำรองที่เหมาะสม

๓) การประเมินความเสี่ยงจากสิ่งต่าง ๆ รวมถึงการจัดหามาตรการในการลดความเสี่ยง

๔) การจัดลำดับผลกระทบขององค์กร

๕) การจัดทำไซต์สำรอง

๖) การจัดทำแผนกู้คืน

๗) การวางแผนการแต่งตั้งคณะทำงานลำดับการทำงานหลังระบบได้รับความเสียหาย

๘) การฝึกอบรมให้แก่บุคลากร เพื่อรับทราบหน้าที่รวมถึงการฝึกอบรมทางด้านเทคนิค

๙) การทดสอบแผนกู้คืน อาจทดสอบกับระบบจำลองก่อนการทดสอบกับระบบจริง

๙. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการ หรือการตรวจสอบให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ เพื่อนำเสนอรายงานสรุปให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม หรือ DCIO และให้รายงานการเกิดปัญหา และผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณี เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) รักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันท่วงที ทั้งนี้ เพื่อเตรียมความพร้อมและสร้างความรู้ความเข้าใจตลอดจน เป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศต่อไป

๑๐. การจัดองค์กรและการกำหนดผู้รับผิดชอบ

๑๐.๑ ผู้บริหาร รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหาและสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)

๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๑๐.๒ กลุ่มงานคอมพิวเตอร์และการสื่อสาร รับผิดชอบการปฏิบัติงานระบบเครือข่ายและห้องแม่ข่าย ได้แก่

๑) ผู้อำนวยการกลุ่มงานคอมพิวเตอร์และการสื่อสาร

๒) นายจิตรพล อินกุณา นักวิชาการคอมพิวเตอร์ชำนาญการ

๓) นายเลอสันต์ หมู่หมื่นศรี นักวิชาการคอมพิวเตอร์ชำนาญการ

๔) นางสาวตรียภรณ์ กองอ้น นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๑๐.๓ กลุ่มงานบริหารเทคโนโลยีและระบบ รับผิดชอบการปฏิบัติงานระบบสารสนเทศและฐานข้อมูล ได้แก่

๑) ผู้อำนวยการกลุ่มงานบริหารเทคโนโลยีและระบบ

๒) นางสาวณัฐกฤตา วงษ์สายตา นักวิชาการคอมพิวเตอร์ชำนาญการ

๓) นางสาวอรวรรณ ผดุงเกียรติ นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๔) นายประดับ วาหะมงคล นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๑๐.๔ ทีมบริการเทคนิค รับผิดชอบการปฏิบัติงานทางเทคนิค ได้แก่

๑) นายจิตรพล อินกุณา นักวิชาการคอมพิวเตอร์ชำนาญการ

๒) นายประดับ วาหะมงคล นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๑๐.๕ ฝ่ายบริหารทั่วไปและทีมงานประสานงาน รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๑) นางอรทัย เพชรสันทัด นักวิชาการคอมพิวเตอร์ชำนาญการ

๒) นางสาวพรทิพย์ อยู่สุข นักจัดการงานทั่วไปชำนาญการ

๓) นางสาวตรียภรณ์ กองอ้น นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นางสาวตรียภรณ์ กองอ้น
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
ผู้จัดทำ