บันทึกข้อความ

ส่วนราชการ กลุ่มงานประกันสุขภาพยุทธศาสตร์ฯ โรงพยาบาลทุ่งใหญ่ โทร ๐-๗๕๔๘-๙๐๘๐

ที่ นศ ๐๐๓๓.๓๐๙(๑๑)/๒๐๒๐ **วันที่** ๒๒ สิงหาคม ๒๕๖๗

เรื่อง ขออนุมัติแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ โรงพยาบาลทุ่งใหญ่

เรียน ผู้อำนวยการโรงพยาบาลทุ่งใหญ่

ด้วยคณะกรรมการทีมสารสนเทศโรงพยาบาลทุ่งใหญ่ ได้ดำเนินการจัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT CONTINGENCY PLAN) โรงพยาบาลทุ่งใหญ่ขึ้น เพื่อเป็นแนวทางการดูแลรักษาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรให้มีเสถียรภาพ มีความพร้อมรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นได้

ในการนี้ กลุ่มงานประกันสุขภาพยุทธศาสตร์ฯ ในนามของคณะกรรมการทีมสารสนเทศ จึงขอเสนอแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT CONTINGENCY PLAN) โรงพยาบาลทุ่งใหญ่ ตามรายละเอียดเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณาอนุมัติ

(นางสาวศิริลักษณ์ สุวรรณ)
นักวิชาการคอมพิวเตอร์ชำนาญการ

ความเห็นหัวหน้ากลุ่มงานประกัน ฯ.....
.....
.....

(นางอมรรัตน์ หอมหวล)
นักวิชาการเงินและบัญชี
หัวหน้ากลุ่มงานประกันสุขภาพยุทธศาสตร์

ความเห็นผู้อำนวยการ.....
.....
.....

(นายปกป้อง เศวตชนะ)
นายแพทย์ชำนาญการ รักษาการในตำแหน่ง
ผู้อำนวยการโรงพยาบาลทุ่งใหญ่

แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT CONTINGENCY PLAN)

จัดทำโดย
ทีมสารสนเทศ (IM)
โรงพยาบาลทุ่งใหญ่

สารบัญ

๑. หลักการและเหตุผล

ระบบข้อมูลและสารสนเทศถือเป็นทรัพย์สินที่มีความสำคัญต่อโรงพยาบาล จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย และมั่นใจได้ว่าระบบฐานข้อมูลและสารสนเทศสำคัญๆของโรงพยาบาลทุ่งใหญ่จะไม่สูญหายสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

โรงพยาบาลทุ่งใหญ่ ได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศ ซึ่งอาจมีปัจจัยภายนอกและปัจจัยภายในที่ส่งผลกระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์เสียหายได้ โดยเฉพาะอย่างยิ่งฐานข้อมูลและสารสนเทศที่ใช้ในการให้บริการแก่ผู้มารับบริการ การบริหารจัดการและใช้สนับสนุนการดำเนินงานโรงพยาบาลให้บรรลุตามวิสัยทัศน์ ตลอดจนข้อมูลสารสนเทศที่เป็นความต้องการของหน่วยงานภายนอก

ดังนั้นศูนย์คอมพิวเตอร์ในนามทีมสารสนเทศ (IM) โรงพยาบาลทุ่งใหญ่ จึงจัดทำแผนแก้ไขปัญหาสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการแก้ปัญหาให้ระบบฐานข้อมูลและสารสนเทศกลับคืนสู่ความเป็นปกติ ตลอดจนการดูแลรักษาฐานข้อมูลและสารสนเทศให้มีเสถียรภาพพร้อมใช้งานได้อย่างมีประสิทธิภาพต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการปฏิบัติเพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับฐานข้อมูลและสารสนเทศ

๒.๒ เพื่อป้องกันและลดความเสียหายที่อาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อสนับสนุนให้การบริการระบบเทคโนโลยีสารสนเทศดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๓. เป้าหมาย

๓.๑ ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) ที่สำคัญได้แก่ ฐานข้อมูลโปรแกรม HOSxP, ฐานข้อมูลจัดเก็บการใช้งานอินเทอร์เน็ต (Log File)

๓.๒ อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server), เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server/ Slave Server), เครื่องคอมพิวเตอร์แม่ข่ายตรวจสอบและอัพเดต Virus (Antivirus Server), เครื่องพิมพ์ (Printer), เครื่องคอมพิวเตอร์ลูกข่าย (Client Server), อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS), อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB), อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access Point)

๔. การวิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กร สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

๑) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาหารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องคอมพิวเตอร์แม่ข่าย เช่น อัคคีภัย อุทกภัย วาตภัย ความชื้น อุณหภูมิ แผ่นดินไหว ภัยแล้ง คลื่นความร้อน ฯลฯ

๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓) ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

๔) ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

๕) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๖) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

๑) เครื่องคอมพิวเตอร์แม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๓) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๕. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

๕.๑ กรณีเครื่องคอมพิวเตอร์ลูกข่าย (Client)

๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศของหน่วยงานทราบ หรือในกรณีเกิดจากศูนย์คอมพิวเตอร์ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์คอมพิวเตอร์ต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ

๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในอาคารที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๓) ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้ แจ้งเหตุขัดข้องให้ศูนย์คอมพิวเตอร์เพื่อแก้ไขปัญหาต่อไป

๕.๒ กรณีเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ ประสิทธิภาพของเครื่องสำรองไฟฟ้าและเครื่องกำเนิดไฟฟ้า

๓) ตัดระบบจ่ายไฟฟ้า

๔) ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

๕) กรณีไฟไหม้ให้ดับเพลิงโดยใช้ถังดับเพลิงสารสะอาด ชนิดฮาโลตรอน (Halotron) BF๒๐๐๐

๖) รีบขนย้ายเครื่องคอมพิวเตอร์แม่ข่ายไว้ในที่ปลอดภัย

๗) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๘) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๙) ผู้ดูแลระบบต้องรีบแจ้งให้ผู้อำนวยการโรงพยาบาลทุ่งใหญ่ทราบโดยเร็ว

๖. แนวปฏิบัติในการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๖.๑ กรณีการป้องกันไวรัสล้มเหลว

- เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นๆ ในระบบเครือข่าย ให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายทั้งระบบ เพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

๖.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบตัด Internet Connection วิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลกระทบที่สร้างความเสียหาย โดยตรวจสอบจาก Log และตรวจสอบการตั้งค่าของ Firewal
- ผู้ดูแลระบบแจ้งหัวหน้ากลุ่มงานให้ทราบโดยด่วน
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆ ที่ทำให้ผู้บุกรุกเข้ามาได้
- Update Patch และ Virus Definitions ให้เป็นปัจจุบัน
- หากข้อมูลสูญหายทำการ Recovery และทดสอบการใช้งาน

๖.๓ กรณีไฟฟ้าขัดข้อง

ไฟฟ้าดับทั้งโรงพยาบาลให้ดำเนินการ ดังนี้

- ประสานงานกับงานซ่อมบำรุง เพื่อให้รู้สาเหตุและระยะเวลาไฟดับ
- กรณีไฟดับไม่เกิน ๑๕ นาที แจ้งหน่วยงานต่างๆ ให้แจ้งผู้ป่วยว่า ไฟฟ้าดับไม่เกิน ๑๕ นาที
- ผู้ดูแลระบบตรวจสอบเครื่องสำรองไฟฟ้า (UPS) ที่ต่อพ่วงกับอุปกรณ์เครือข่ายและ Sever ทำงานปกติหรือไม่ หากพบความผิดปกติให้ดำเนินการแก้ไขตามภาวะที่ผิดปกติ
- กรณีไฟฟ้าดับเกิน ๑๕ นาที แจ้งผู้อำนวยการหรือประธานทีมสารสนเทศเพื่อประกาศให้หน่วยงานต่างๆ ดำเนินการตามแผน BCP สำหรับศูนย์คอมพิวเตอร์ให้ดำเนินการตามแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ
- ประกาศให้หน่วยงานต่างๆ ปิดคอมพิวเตอร์
- ผู้ดูแลระบบปิดระบบเพื่อป้องกันความเสียหาย
- รอจนไฟฟ้ากลับคืนสู่สภาวะปกติ
- ผู้ดูแลระบบเปิดระบบ Start Sever และอุปกรณ์เครือข่าย
- ผู้ดูแลระบบตรวจสอบการทำงานอุปกรณ์เครือข่ายและ Server
- ทดสอบใช้งาน HOSxP
- ประกาศให้หน่วยงานต่างๆ ใช้ระบบสารสนเทศได้ตามปกติ

หากไฟฟ้าดับเฉพาะโซนห้องควบคุมระบบเครือข่าย ให้เจ้าหน้าที่ศูนย์คอมพิวเตอร์ร่วมกันดำเนินการดังนี้

- ประสานงานกับงานซ่อมบำรุง เพื่อให้รู้สาเหตุและระยะเวลาไฟดับ
- ผู้ดูแลระบบเตรียมสายไฟต่อพ่วงจากห้องควบคุมระบบเครือข่าย ไปต่อพ่วงกับหน่วยงานอื่น
- ผู้ดูแลระบบตรวจสอบอุปกรณ์เครือข่ายและ Server ทำงานปกติหรือไม่ หากพบความผิดปกติให้ดำเนินการแก้ไขตามภาวะที่ผิดปกตินั้น
- รอจนไฟฟ้ากลับคืนสู่สภาวะปกติ ต่อพ่วงเครื่องสำรองไฟฟ้าที่ห้องควบคุมระบบเครือข่ายเข้าสู่ระบบไฟฟ้าที่ห้องควบคุมระบบฯ และจัดเก็บสายไฟต่อพ่วงในตู้จัดเก็บอุปกรณ์

๖.๔ กรณีเครื่องแม่ข่ายหลัก HOSxP ล่ม ไม่สามารถใช้งานได้ให้ดำเนินการใช้เครื่องแม่ข่ายสำรอง HOSxP ทันที และดำเนินการซ่อมเครื่องแม่ข่ายหลักให้สามารถใช้งานได้ปกติโดยเร็ว

๖.๕ กรณีฐานข้อมูล HOSxP ที่เครื่องแม่ข่ายไม่สามารถใช้งานได้ให้ดำเนินการ โดยใช้เครื่องแม่ข่ายสำรอง HOSxP ทันที และดำเนินการซ่อมเครื่องแม่ข่ายหลักให้สามารถใช้งานได้ปกติโดยเร็ว

๖.๖ กรณีไฟไหม้ แบ่งเป็น ๒ สถานการณ์คือ

๑) มีเจ้าหน้าที่ปฏิบัติงานอยู่ภายในห้องควบคุมระบบเครือข่าย มีขั้นตอนปฏิบัติดังนี้

๑.๑) เมื่อเกิดเหตุไฟไหม้ให้เจ้าหน้าที่ที่อยู่ในเหตุการณ์ Shut Down ระบบคอมพิวเตอร์และปิดการใช้งานระบบเครือข่าย

๑.๒) ให้รีบดำเนินการเคลื่อนย้ายเครื่อง Server และอุปกรณ์ไปในสถานที่ที่ปลอดภัย

๑.๓) ให้เจ้าหน้าที่ที่อยู่ในเหตุการณ์ใช้อุปกรณ์ที่ศูนย์คอมพิวเตอร์ได้จัดหาไวดำเนินการดับเพลิงโดยเฉพาะ ซึ่งมีติดตั้งอยู่ภายในห้องควบคุมระบบเครือข่าย โดยการใช้ถังดับเพลิงชนิดหูหิ้วที่สามารถดับไฟประเภท C เป็นอย่างน้อย ได้แก่ อุปกรณ์ไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์ โดยไม่ทำลายหรือทำให้เกิดความเสียหายแก่อุปกรณ์ดังกล่าว ไม่ทิ้งคราบรอยสกปรก ไม่หลงเหลือน้ำยาตกค้างเมื่อฉีดใช้งาน

๑.๔) กรณีไม่สามารถแก้ไขหรือควบคุมเพลิงได้ ต้องแจ้งสถานีดับเพลิงที่ใกล้ที่สุด

๑.๕) เมื่อกลับเข้าสู่สภาวะปกติ ผู้รับผิดชอบในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบอุปกรณ์ภายในห้องควบคุมระบบเครือข่าย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้าศูนย์คอมพิวเตอร์ ประธานทีมสารสนเทศ(IM) และผู้อำนวยการโรงพยาบาลทราบ

๑.๖) เจ้าหน้าที่ศูนย์คอมพิวเตอร์ตรวจสอบความพร้อมใช้ของอุปกรณ์ หากชำรุดดำเนินการจัดซื้อทดแทน ติดตั้งและทดสอบการใช้งาน

๒) ไม่มีเจ้าหน้าที่ปฏิบัติงานอยู่ภายในห้องควบคุมระบบเครือข่าย มีขั้นตอนปฏิบัติดังนี้

๒.๑) ผู้พบเห็นเหตุการณ์ปิดประตูหรือพังประตูห้องควบคุมระบบเครือข่าย

๒.๒) นำถังดับเพลิงชนิดหูหิ้วที่สามารถดับไฟประเภท C ที่อยู่บริเวณหน้าห้องควบคุมระบบเครือข่ายเข้าสกัดเพลิงและดับเพลิง

๒.๓) กรณีไม่สามารถแก้ไขหรือควบคุมเพลิงได้ ต้องแจ้งสถานีดับเพลิงที่ใกล้ที่สุด

๒.๔) เมื่อกลับเข้าสู่สภาวะปกติ ผู้รับผิดชอบในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบอุปกรณ์ภายในห้องควบคุมระบบเครือข่าย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้าศูนย์คอมพิวเตอร์ ประธานทีมสารสนเทศ(IM) และผู้อำนวยการโรงพยาบาลทราบ

๒.๕) เจ้าหน้าที่ศูนย์คอมพิวเตอร์ตรวจสอบความพร้อมใช้ของอุปกรณ์ หากชำรุดดำเนินการจัดซื้อทดแทน ติดตั้งและทดสอบการใช้งาน

๖.๗ กรณีน้ำท่วม ห้องควบคุมระบบเครือข่าย มีขั้นตอนปฏิบัติดังนี้

๑) เมื่อมีสถานการณ์น้ำท่วม ให้แจ้งผู้อำนวยการโรงพยาบาล ประธานทีมสารสนเทศ (IM) และหัวหน้าศูนย์คอมพิวเตอร์ เพื่อทราบและสั่งการต่อไป

๒) เจ้าหน้าที่ศูนย์คอมพิวเตอร์หรือเจ้าหน้าที่ผู้อยู่ในสถานการณ์และอยู่บริเวณห้องควบคุมระบบเครือข่าย ตองนำอุปกรณ์ที่ศูนย์คอมพิวเตอร์จัดหาไว้มาดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้น โดยจะต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ จากนั้นดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญให้พ้นจากภัยน้ำท่วม (บางส่วน) ไปยังสถานที่ปลอดภัยจากภัยน้ำท่วมห้องควบคุมระบบเครือข่ายตามความเหมาะสม

๓) เมื่อกลับเข้าสู่สภาวะปกติ ผู้ดูแลระบบจะต้องดำเนินการเขาตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบฯ พรอมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้าศูนย์คอมพิวเตอร์ ประธานทีมสารสนเทศ และผู้อำนวยการโรงพยาบาลทราบ

๖.๘ กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์

เมื่อตรวจพบภัยคุกคามทางคอมพิวเตอร์ให้แจ้งหัวหน้างานศูนย์คอมพิวเตอร์เพื่อทราบและดำเนินการสั่งการแก่เจ้าหน้าที่ที่ได้รับมอบหมายให้เข้าควบคุมสถานการณ์ เพื่อให้ระบบงานและเครือข่ายได้รับความเสียหายน้อยที่สุด พร้อมทั้งทำให้ระบบรักษาความปลอดภัยกลับมาใช้งานได้เร็วที่สุด

ขั้นตอนในการกู้คืนระบบความปลอดภัย กรณีโดนเจาะระบบ และภัยคุกคามทางไซเบอร์ มีดังนี้

๑) ควบคุมสถานการณ

๑.๑) ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา

๑.๒) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย

๑.๓) เตรียมการสำหรับการกูคืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก

๒) วิเคราะห์การถูกโจมตี

๒.๑) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System File) และไฟล์อื่นๆ

๒.๒) วิเคราะห์ล็อกไฟล์ (Log File) ตรวจสอบโปรแกรมหรือข้อมูลที่ผู้บุกรุกทิ้งไว้

๒.๓) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

๒.๔) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ

๓) กู้คืนระบบคอมพิวเตอร์ (Backup & Recovery)

๓.๑) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่

๓.๒) งดใช้เซอร์วิสที่ไม่จำเป็น

๓.๓) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูลสารสนเทศ (Update Patch)

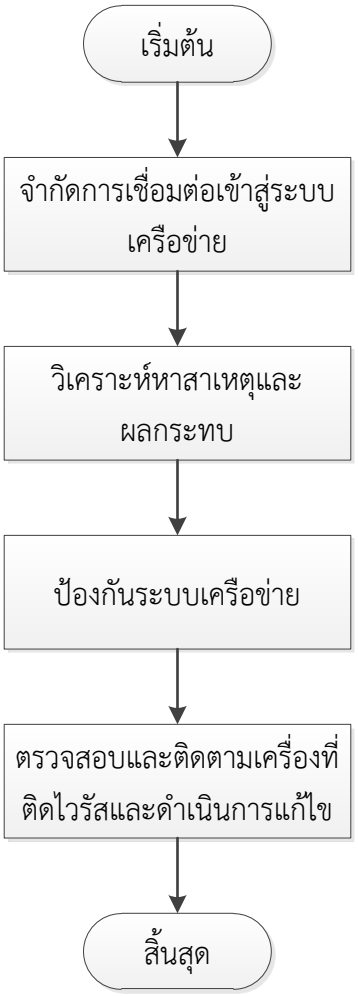
๓.๔) อุดช่องโหวในระบบเครือข่าย

๓.๕) เปลี่ยนแปลงพาสเวิร์ดใหม่ หลังจากไดแก้ไขช่องโหว่ของระบบแล้ว

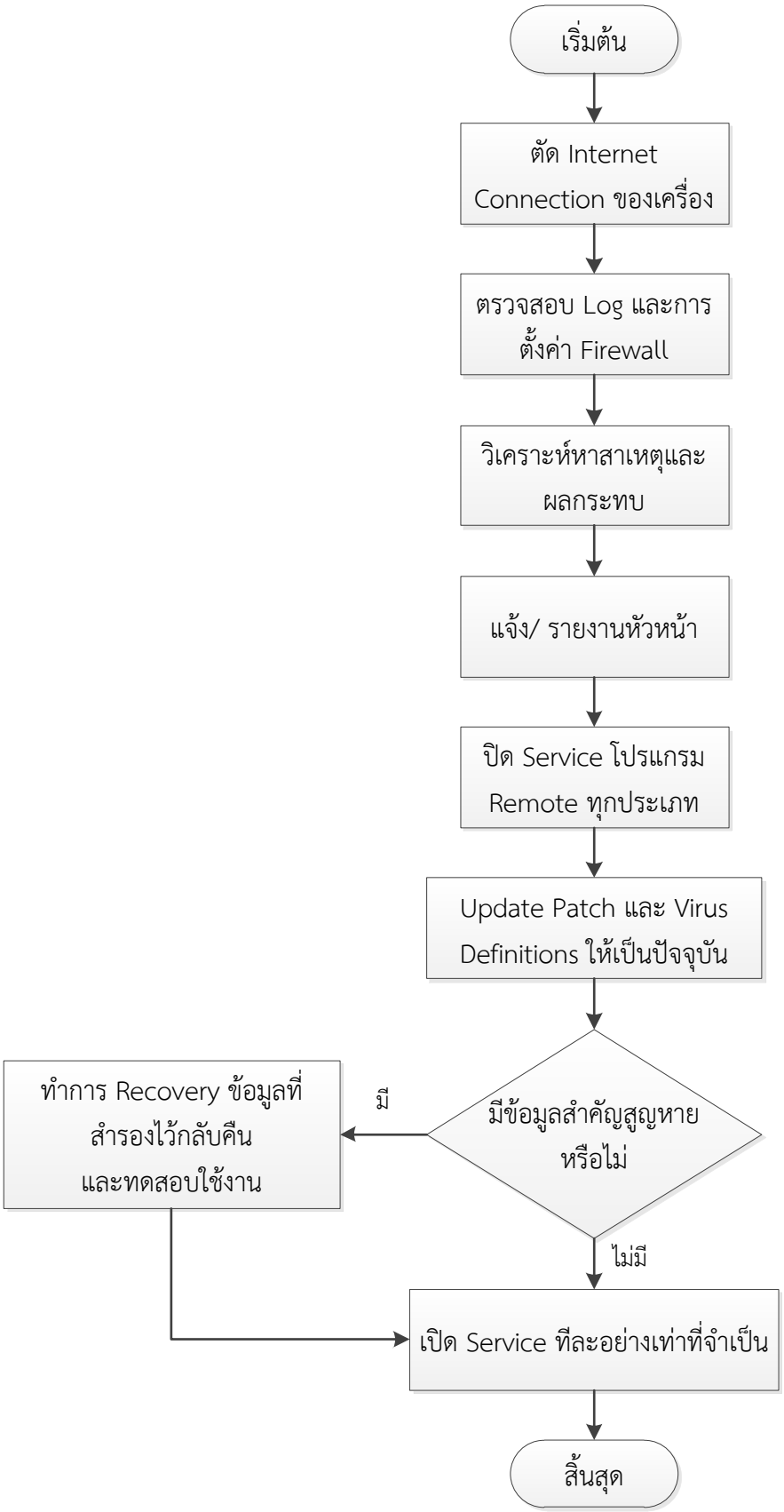
๔) เมื่อกลับเข้าสู่สภาวะปกติ ผู้ดูแลระบบจะต้องดำเนินการเขาตรวจสอบระบบงานและระบบเครือข่ายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้าศูนย์คอมพิวเตอร์ ประธานทีมสารสนเทศ (IM) และผู้อำนวยการโรงพยาบาลทุ่งใหญ่ทราบ

๗. ผังงานกระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

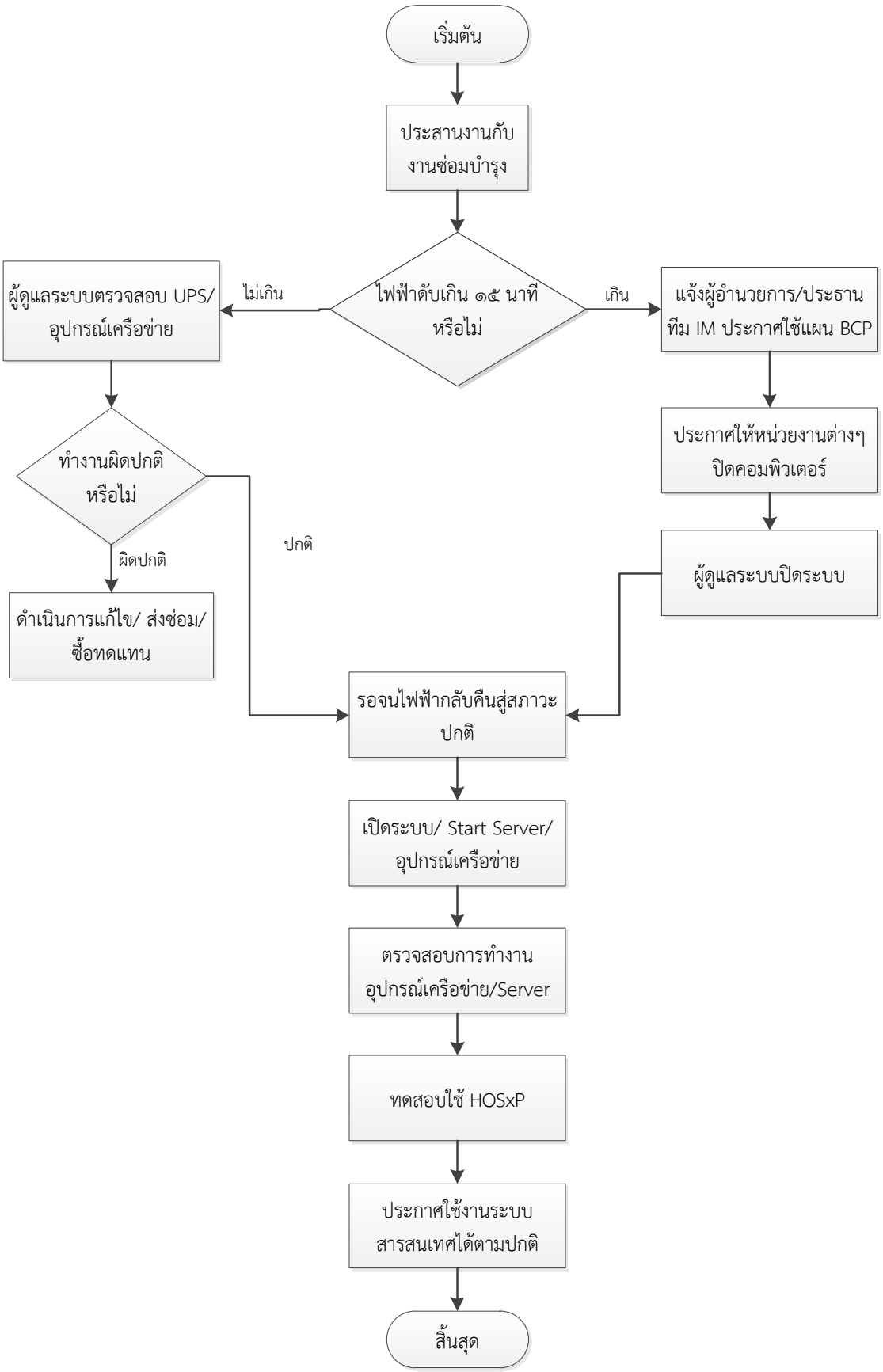
ผังงาน กรณีการป้องกันไวรัสล้มเหลว



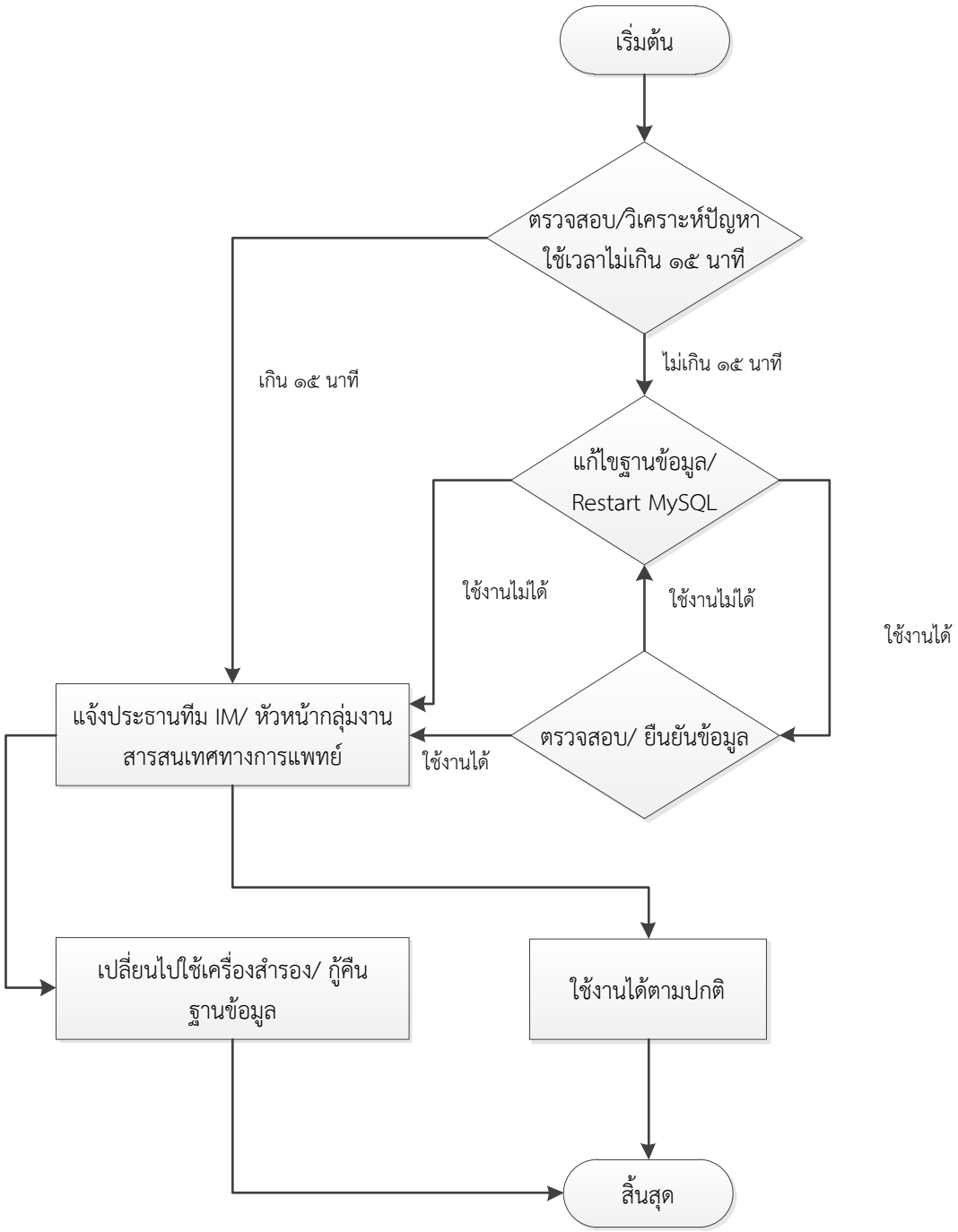
ผังงาน กรณีการป้องกันผู้บุกรุกล้มเหลว



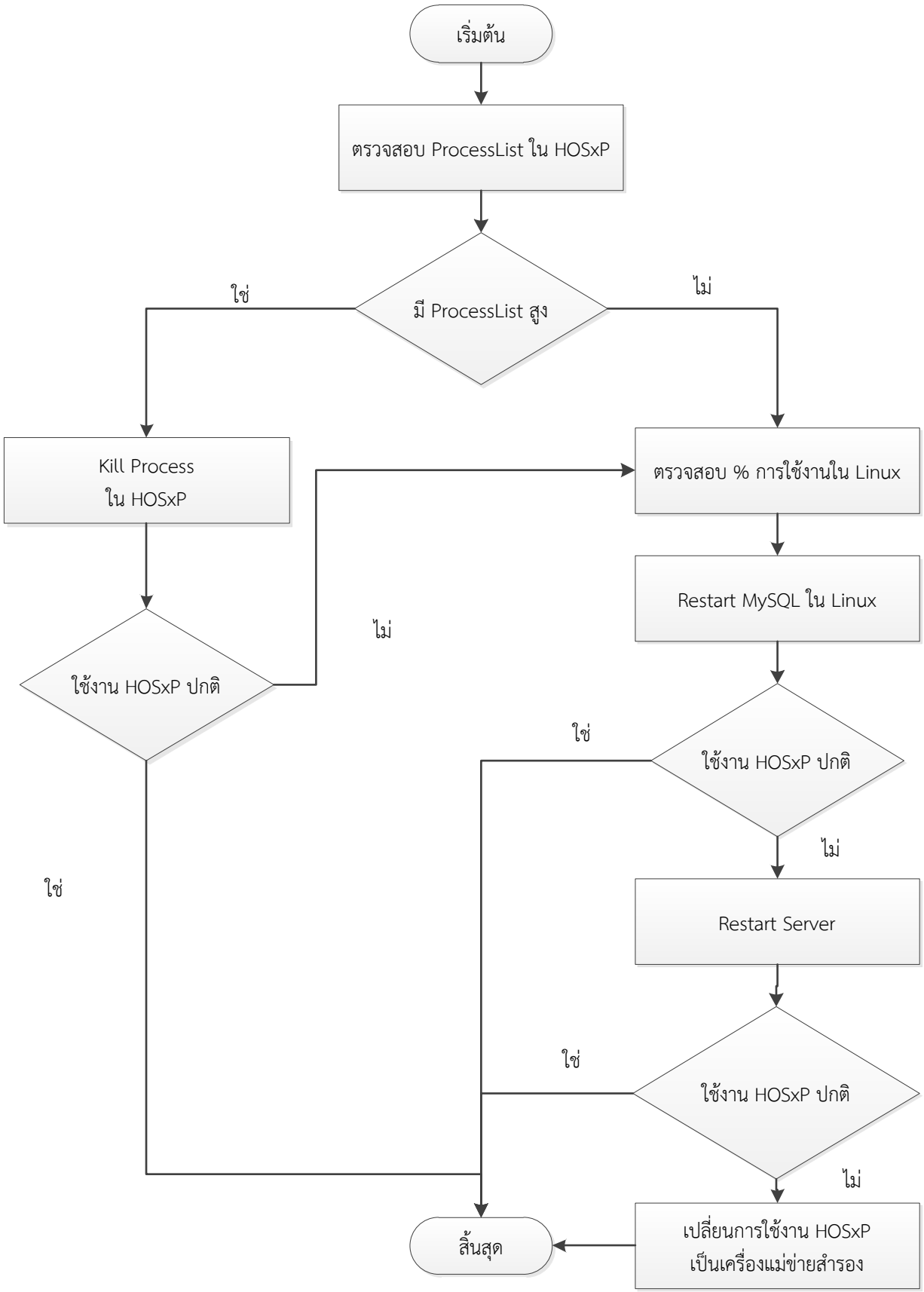
ผังงาน กรณีไฟฟ้าขัดข้อง



ผังงาน กรณีเครื่องแม่ข่ายหลัก HOSxP ล่ม

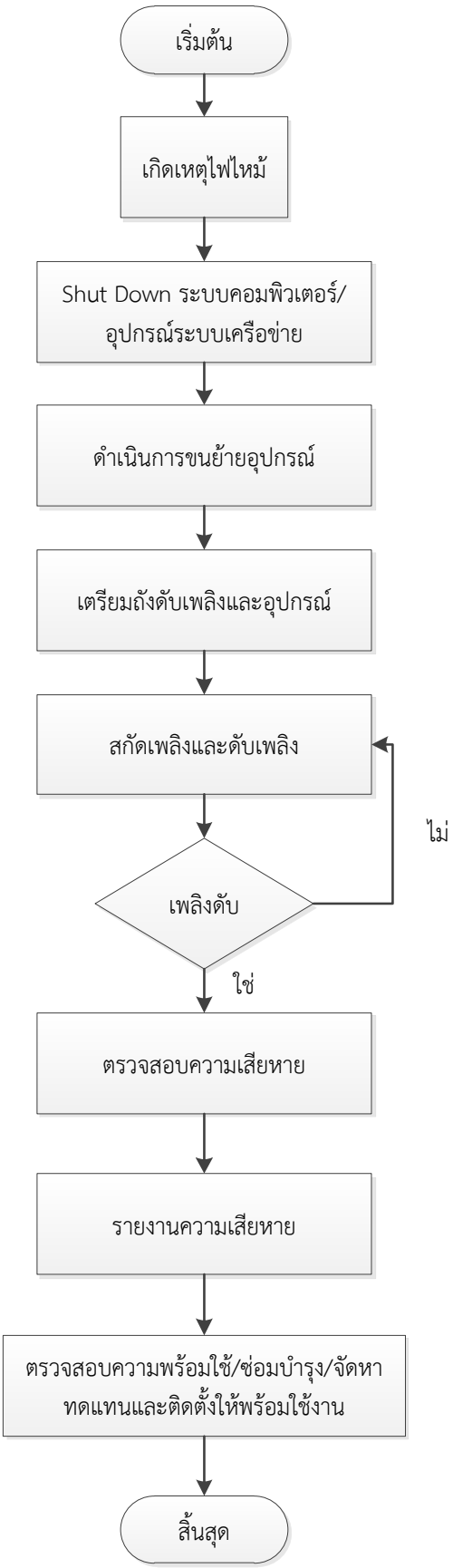


ผังงาน กรณีฐานข้อมูล HOSxP ที่เครื่องแม่ข่ายไม่สามารถใช้งานได้



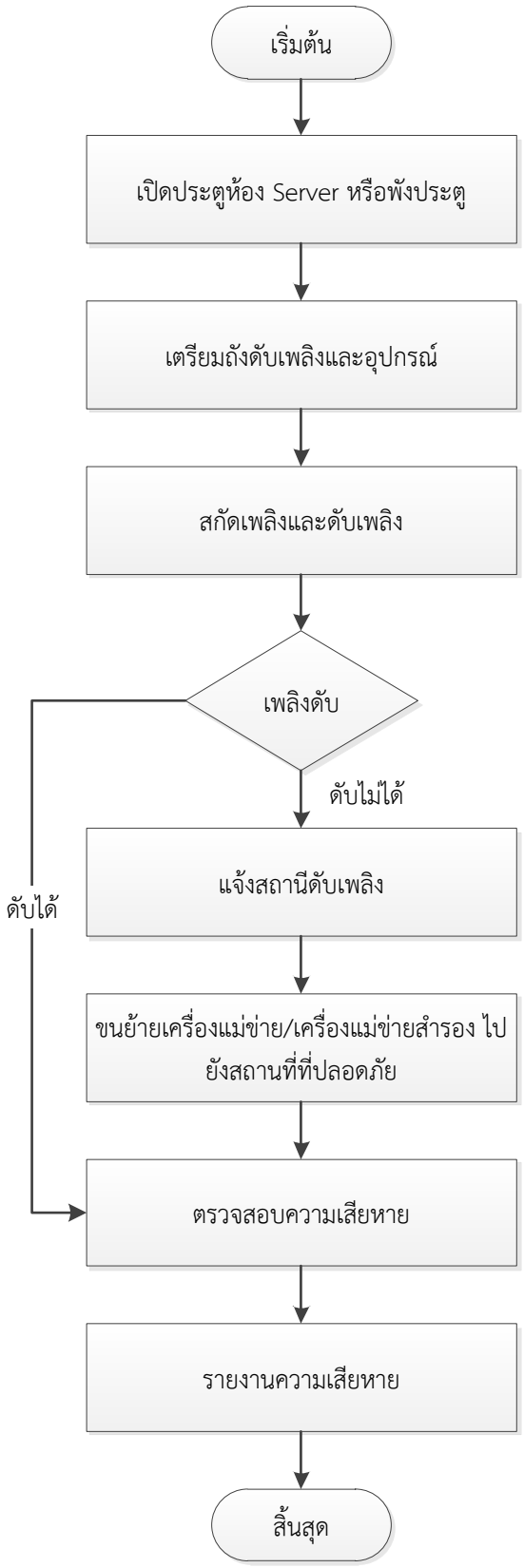
ผังงาน กรณีไฟไหม้

มีเจ้าหน้าที่ปฏิบัติงานอยู่ภายในห้องควบคุมระบบเครือข่าย

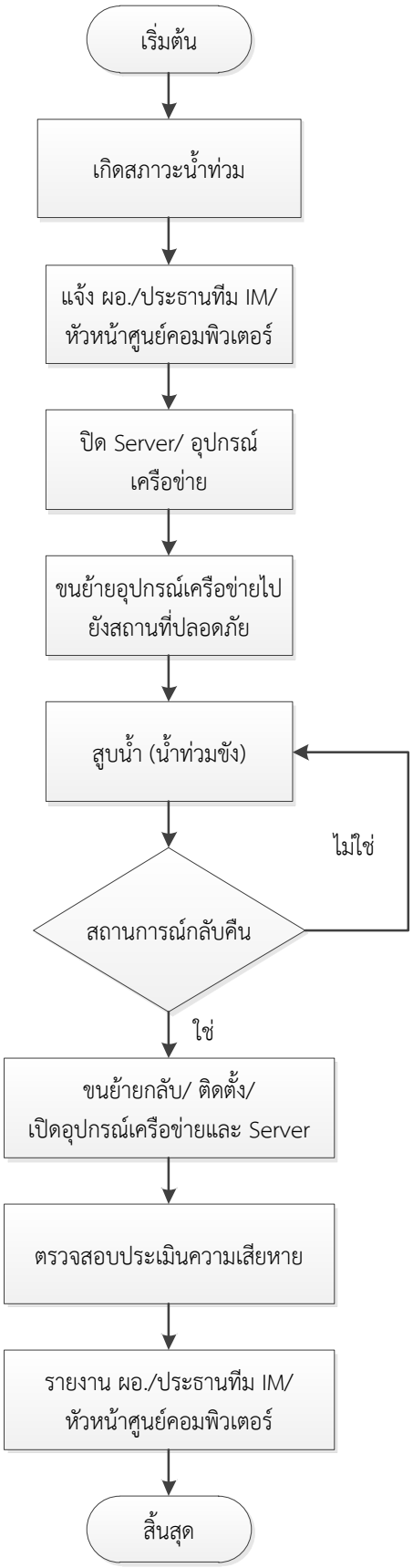


ผังงาน กรณีไฟไหม้

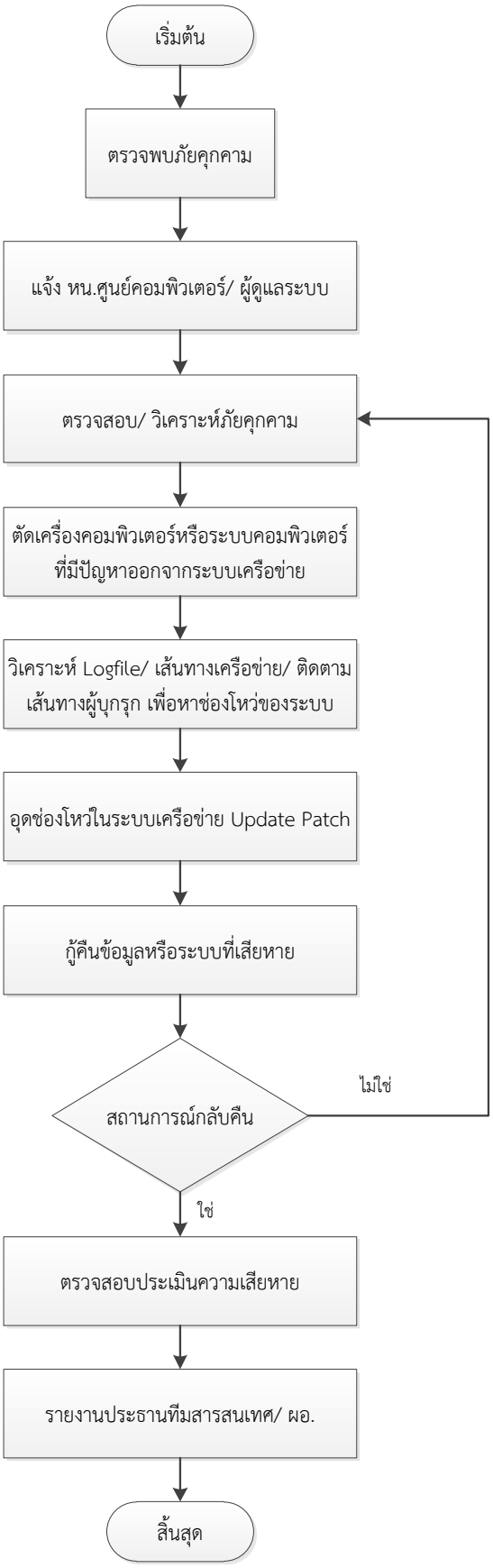
ไม่มีเจ้าหน้าที่ปฏิบัติงานอยู่ภายในห้องควบคุมระบบเครือข่าย



ผังงาน กรณีน้ำท่วม



ผังงาน กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์



๘. การกู้คืนระบบกลับสู่สภาพปกติ

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการดังนี้

๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๔) นำอุปกรณ์ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยใช้ทีมกู้ระบบตามความเหมาะสมดังนี้

๔.๑) ผู้ดูแลระบบของโรงพยาบาลทุ่งใหญ่

๔.๒) ขอสนับสนุนทีมผู้ดูแลระบบจากโรงพยาบาลใกล้เคียง

๔.๓) ทีมงานจากบริษัทที่จัดจ้างบำรุงรักษาระบบสารสนเทศ

ให้กู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๕) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆที่เกี่ยวข้องก่อนเปิดให้บริการ

๙. การทบทวน ติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้หัวหน้ากลุ่มงานสุขภาพดิจิทัลทราบ เพื่อนำเสนอรายงานสรุปให้ประธานทีมสารสนเทศและผู้อำนวยการโรงพยาบาลทุ่งใหญ่ทราบ และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบ ในทันทีที่สามารถดำเนินการได้ในทุกกรณี เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพต่อไป