กองวิศวกรรมการแพทย์
Medical Engineering Division

แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) ของกองวิศวกรรมการแพทย์

กองวิศวกรรมการแพทย์
กรมสนับสนุนบริการสุขภาพ
กระทรวงสาธารณสุข

คำนำ

ระบบเทคโนโลยีสารสนเทศของกองวิศวกรรมการแพทย์ กรมสนับสนุนบริการสุขภาพ มีความสำคัญยิ่งต่อการปฏิบัติราชการในด้านวิศวกรรมการแพทย์ ซึ่งกองวิศวกรรมการแพทย์ ได้ตระหนักถึงการดูแลรักษาระบบสารสนเทศให้มีความมั่นคงปลอดภัยและลดความเสี่ยงต่างๆ ที่จะเกิดขึ้นกับระบบสารสนเทศ และเพื่อให้ระบบสารสนเทศของกองวิศวกรรมการแพทย์ สามารถใช้งานได้อย่างมีประสิทธิภาพ และเกิดประสิทธิผล จึงได้จัดทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) โดยรองรับและสอดคล้องกับแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) ของกรมสนับสนุนบริการสุขภาพ เพื่อเป็นกรอบแนวทางในการบำรุงรักษาป้องกันและแก้ไขปัญหาที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกองวิศวกรรมการแพทย์

กองวิศวกรรมการแพทย์
กรมสนับสนุนบริการสุขภาพ

สารบัญ

แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน
(IT Contingency Plan)

๑. <u>หลักการและเหตุผล</u>

กองวิศวกรรมการแพทย์ ได้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงาน เพื่อเป็นการเพิ่มประสิทธิภาพในการปฏิบัติงานด้านวิศวกรรมการแพทย์ แต่ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตีได้จากภยันตรายหลายสาเหตุ เช่น ภัยจากไวรัสคอมพิวเตอร์ ภัยจากการโจรกรรมข้อมูล การก่อเหตุจลาจล ระบบไฟฟ้าขัดข้อง ภัยธรรมชาติ ตลอดจนปัจจัยทั้งภายในและภายนอกต่างๆ อันอาจก่อให้เกิดความเสียหายและสร้างผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกองวิศวกรรมการแพทย์ ดังนั้น เพื่อป้องกันและแก้ไขปัญหาดังกล่าว กองวิศวกรรมการแพทย์ จึงได้จัดทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศและระบบอุปกรณ์ต่างๆ ให้สามารถแก้ไขปัญหาที่จะส่งผลกระทบต่อสารสนเทศของหน่วยงาน

๒. <u>วัตถุประสงค์</u>

๒.๑ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของกองวิศวกรรมการแพทย์

๒.๒ เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๔ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๕ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของกองวิศวกรรมการแพทย์

๓. <u>ภัยพิบัติ</u>

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบฐานข้อมูลและสารสนเทศของกองวิศวกรรมการแพทย์สามารถจำแนกได้เป็น ๒ กลุ่มหลักๆ ได้แก่

/๓.๑ ภัยพิบัติจาก...

๓.๑ ภัยพิบัติจากปัจจัยภายนอก

๑) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องคอมพิวเตอร์ ได้แก่ ภัยพิบัติอัคคีภัย อุทกภัย แผ่นดินไหว ความชื้นและอุณหภูมิที่ไม่เหมาะสม ภัยจากแมลงและสัตว์กัดแทะ เป็นต้น

๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓) ระบบการสื่อสารของเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายภายนอกกองวิศวกรรมการแพทย์ เกิดความขัดข้อง

๔) ระบบกระแสไฟฟ้าขัดข้อง หรือไฟฟ้าดับ

๕) การบุกรุกโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบฐานข้อมูลและสารสนเทศรวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๖) ไวรัสคอมพิวเตอร์

๗) ระบบเสียหายจากภัยสงคราม เหตุจลาจล และปัญหาการเกิดสถานการณ์ความไม่สงบ

๓.๒ ภัยพิบัติจากปัจจัยภายใน

๑) ระบบฐานข้อมูลหลักเสียหายหรือถูกทำลาย

๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในหน่วยงาน

๓) บุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๔. <u>แนวทางการป้องกันความเสียหายจากภัยพิบัติ</u>

๔.๑ ภัยพิบัติจากภายนอก

๔.๑.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องคอมพิวเตอร์ ได้แก่ อัคคีภัย อุทกภัย และการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงและสัตว์กัดแทะ เป็นต้น

๔.๑.๑.๑ การป้องกันและการดำเนินการอัคคีภัย

(๑) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่างๆ

(๒) อบรมแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิง การหนีไฟขั้นต้นให้แก่บุคลากรทุกราย

(๓) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์

(๔) จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

๔.๑.๑.๒ การป้องกันอุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม

(๑) ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝน

(๒) เครื่องคอมพิวเตอร์ต้องไม่อยู่ในบริเวณที่น้ำท่วมถึง

(๓) ตรวจสอบระบบไฟฟ้า หลังเลิกงาน ให้ปิดการใช้งานในส่วนที่ไม่จำเป็น

/๔.๑.๒ การโจรกรรม...

๔.๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๔.๑.๒.๑ ควบคุมการใช้คอมพิวเตอร์และการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องใช้คอมพิวเตอร์ หากจำเป็นให้มีเจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์เป็นผู้รับผิดชอบนำเข้าไป

๔.๑.๒.๒ จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์

๔.๑.๓ ระบบการสื่อสารของเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง

๔.๑.๓.๑ การตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ตลอดเวลา

๔.๑.๓.๒ ต้องจัดให้มีเครื่องสำรองข้อมูล กรณี เครื่องหลักไม่สามารถใช้งานได้

๔.๑.๔ ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

๔.๑.๔.๑ ควรติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์และมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๑๐ นาที

๔.๑.๔.๒ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔.๑.๔.๓ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้บันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่างๆ

๔.๑.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๔.๑.๕.๑ ติดตั้ง Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

๔.๑.๕.๒ จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ต เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๔.๑.๕.๓ ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่มีการใช้งาน

๔.๑.๕.๔ กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาตโดยปฏิบัติดังนี้

(๑) ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(๒) ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น

(๓) จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภั

/(๔) เปลี่ยนรหัสผ่าน...

(๔) เปลี่ยนรหัสผ่านโดยทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๕) ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย ๘ อักขระ

(๖) ตั้งรหัสผ่านโดยใช้เทคนิคส่วนตัวที่ง่ายต่อการจำรหัสผ่านที่ได้กำหนดไว้

(๗) ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

(๘) ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓, abcd เป็นต้น หรือเป็นกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑๑๑, aaa, bbb เป็นต้น

(๙) เปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ ๖ เดือน

(๑๐) เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(๑๑) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

(๑๒) ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เช่น บันทึกไว้ในหน้าจอล็อกอิน (ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง จะได้ไม่ต้องใส่รหัสผ่านอีกครั้ง)

(๑๓) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

๔.๑.๖ ไวรัสคอมพิวเตอร์

๔.๑.๖.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๔.๑.๖.๒ ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

(๑) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

(๒) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

(๓) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๔๑.๖.๓ ใช้ความระมัดระวังในการเปิด E-mail

(๑) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

(๒) ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๔.๑.๖.๔ ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต

(๑) ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ

(๒) ไม่ควรเปิด website ที่แนะนำมาทาง E-mail

(๓) ไม่ดาวน์โหลดไฟล์จาก website ที่ไม่น่าเชื่อถือ

(๔) ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ

(๕) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

/๔.๑.๗ ระบบเสียหาย...

๔.๑.๗ ระบบเสียหายจากภัยสงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

เนื่องจากเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ ในการป้องกันหากไม่สามารถย้ายสถานที่หรือป้องกันสถานที่ได้ ควรมีการ Back Up ข้อมูลไว้มากกว่า ๑ Back Up และแยกสถานที่จัดเก็บ และถ้าเกิดความเสียหายเกิดขึ้นกับข้อมูล ก็สามารถนำข้อมูลที่มีการ Back Up ไว้ และอุปกรณ์คอมพิวเตอร์สำรองมาใช้แทน

๔.๒ ภัยพิบัติจากภายใน

๔.๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๔.๒.๑.๑ การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน

๔.๒.๑.๒ การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนดทุกสัปดาห์

๔.๒.๑.๓ จัดเจ้าหน้าที่ในการบำรุงรักษาสื่อบันทึกข้อมูลของเครื่องคอมพิวเตอร์ เพื่อลดความเสียหายของข้อมูล

๔.๒.๒ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๔.๒.๒.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ

๔.๒.๒.๒ หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๔.๒.๓ บุคลากรขาดความรู้ในการใช้เครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๔.๒.๓.๑ ให้ความรู้แก่บุคลากรและหน่วยงานผ่านช่องทางต่างๆ เช่น website, หนังสือเวียน เป็นต้น

๔.๒.๓.๒ ใส่กุญแจตู้อุปกรณ์เครือข่าย เพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่ หรือบุคลากรที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

๕. <u>ขั้นตอนปฏิบัติในมาตรการที่สำคัญ</u>

๕.๑ การสำรองข้อมูล (Back Up)

๕.๑.๑ การสำรองข้อมูลอัตโนมัติโดยระบบเครื่องประมวลผลหลัก โดยสำรองข้อมูลไว้ในสื่อบันทึก แยกไว้ ๑ ชุดเสมอ

๕.๑.๒ การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนดเป็นประจำทุกสัปดาห์ โดยสำรองข้อมูล และบันทึกข้อมูลลงในสื่อบันทึก

/๖. ข้อปฏิบัติ...

๖. <u>ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ</u>

๖.๑ กรณีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย

๖.๑.๑ ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบเทคโนโลยีสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือดูแลทราบ หรือ กรณีมีเหตุอันทำให้เจ้าหน้าที่ผู้เกี่ยวข้องไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

๖.๑.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ดึงสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องโดยเร็ว

๖.๑.๓ ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง ให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๖.๑.๔ ให้เจ้าหน้าที่ที่เกี่ยวข้อง แจ้งเหตุขัดข้องนั้นให้หัวหน้า หรือผู้บังคับบัญชาทราบโดยเร็ว

๖.๑.๕ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๖.๑.๖ ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์อุปกรณ์เครือข่าย โดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๖.๑.๗ ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๖.๑.๘ รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๖.๑.๙ ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ Server และระบบเครือข่ายโดยเร็วที่สุด

๖.๑.๑๐ ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบ นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๖.๑.๑๑ ผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

๖.๒ กรณีเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

๖.๒.๑ เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆ ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

๖.๒.๒ สแกนและกำจัดไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัส

๖.๒.๓ แจ้งเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อตรวจสอบ

๖.๓ หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัยเพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติ ดังนี้

๖.๓.๑ ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

๖.๓.๒ ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

/๖.๓.๓ ควรหาทาง...

๖.๓.๓ ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉิน มิให้ปิดตาย หรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉิน เพื่อให้ไปถึงทางได้ แม้ว่าไฟดับหรือปกคลุมไปด้วยควัน

๖.๓.๔ เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้ จากนั้นออกจากอาคารแล้วแจ้งหน่วยดับเพลิงทันที

๖.๓.๕ เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

๖.๓.๖ หากเพลิงไหม้ในห้องทำงาน ให้ออกจากห้อง ปิดประตู แล้วแจ้งฝ่ายอาคารและ สถานที่เพื่อแจ้งหน่วยดับเพลิงทันที

๖.๓.๗ หากเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนออกจากอาคารให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อยๆ เปิดประตู แล้วไปยังทางหนีไฟฉุกเฉินที่ใกล้ที่สุด

๖.๓.๘ หากเพลิงไหม้อยู่บริเวณใกล้ประตู จะมีความร้อน ห้ามเปิดประตูโดยเด็ดขาด ให้รีบแจ้งหน่วยดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเพลิงไหม้ หาผ้าเปียก ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

๖.๓.๙ เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

๖.๓.๑๐ ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

๖.๔ ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับส่งมาก ดังนั้น สิ่งที่มักจะเกิดขึ้นและยากต่อการหลีกเลี่ยงคือ ผลกระทบต่างๆ ที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลสำคัญ รวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ประกอบด้วย

๖.๔.๑ เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาเปิดใช้งาน ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

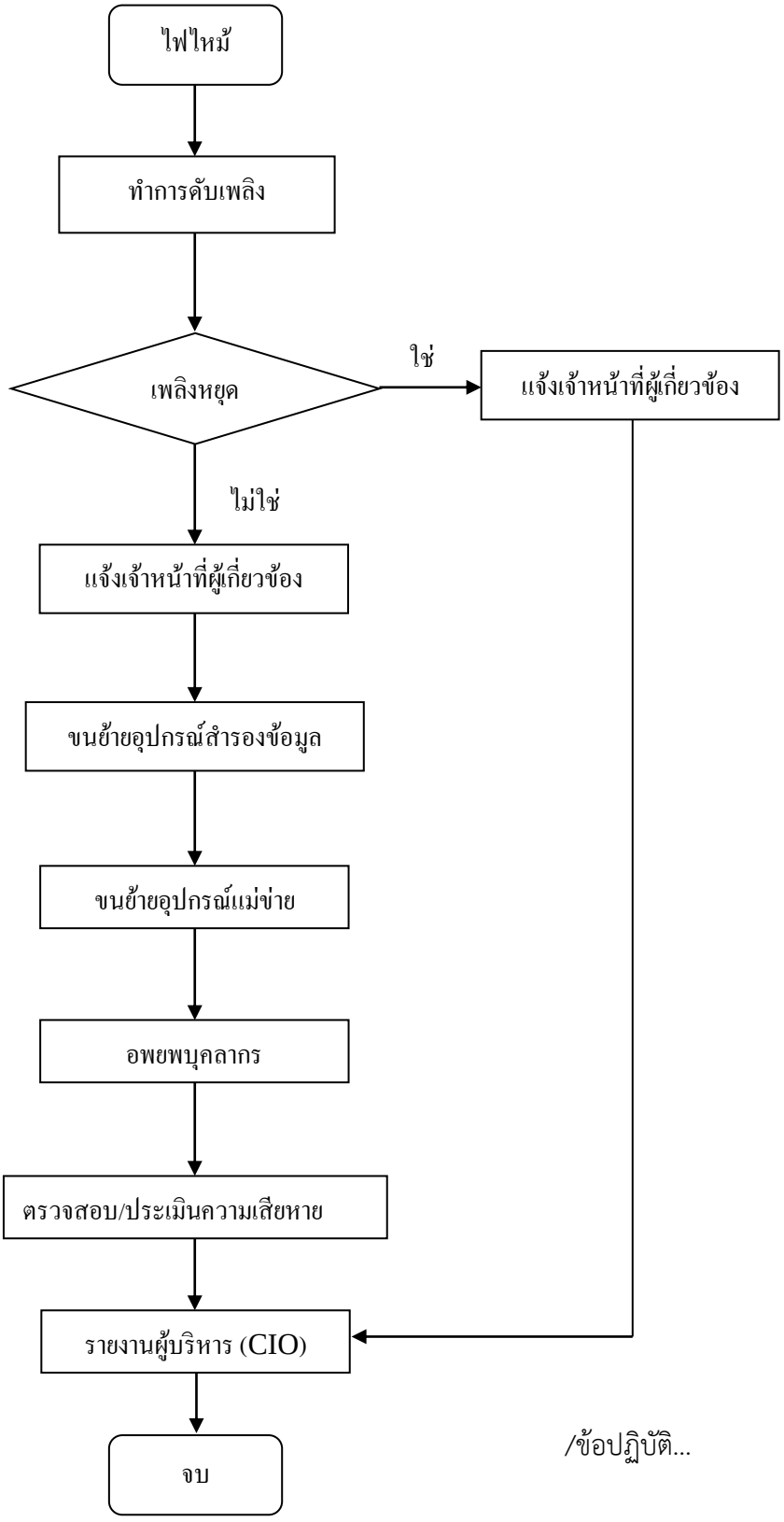
๖.๔.๒ เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

๗. <u>การบริหารจัดการแผนงานการแก้ไขปัญหาจากภัยพิบัติ (Contingency plan)</u>

ผัง Flowchart เพื่อรองรับการปฏิบัติการกรณีเกิดเหตุได้อย่างถูกต้องตามขั้นตอนที่จำเป็น และต้องปฏิบัติอย่างเคร่งครัด ดังนี้

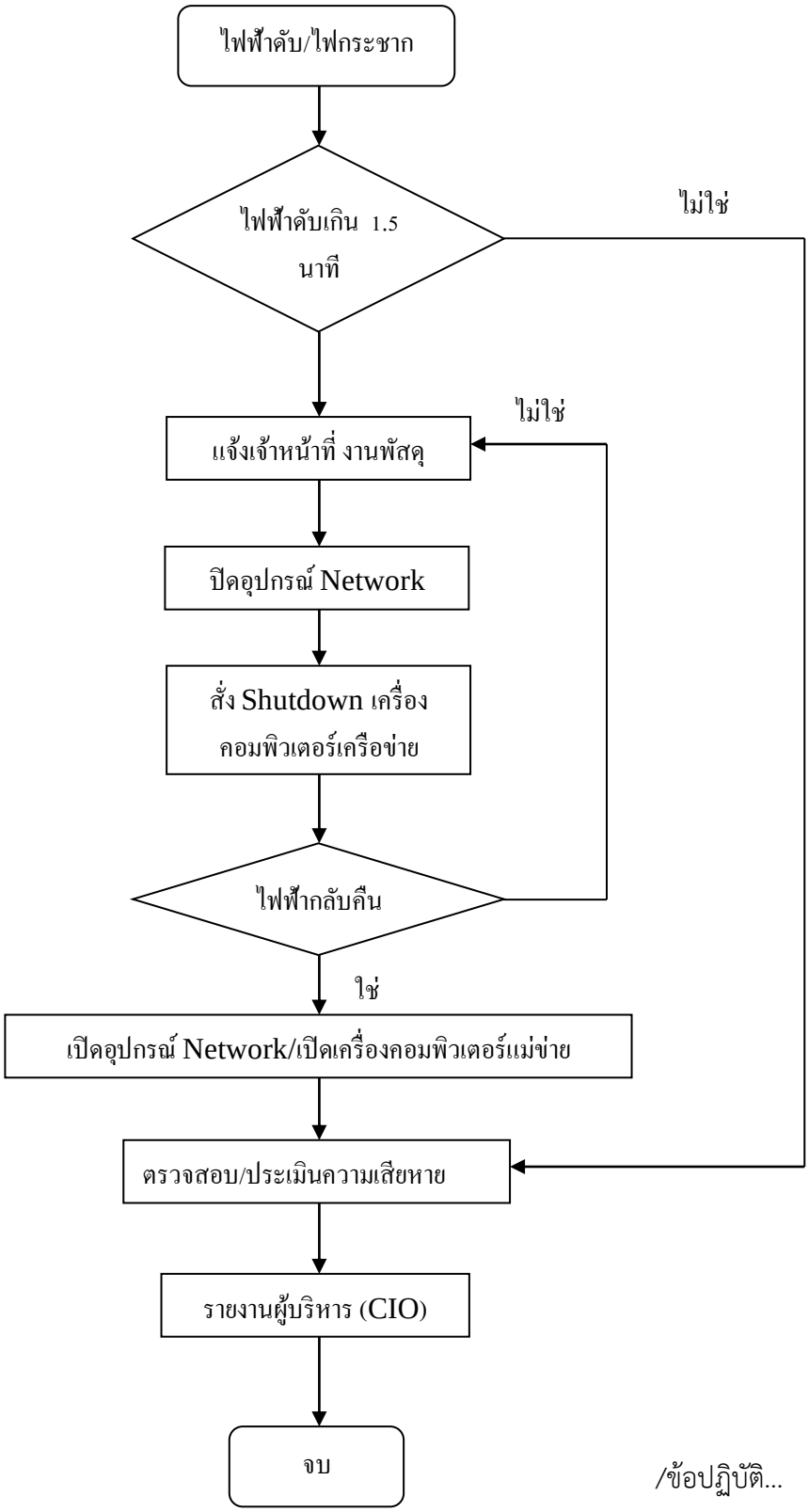
/ข้อปฏิบัติ...

ข้อปฏิบัติกรณีเกิดสถานการณ์หรือภาวะฉุกเฉิน กรณีไฟไหม้



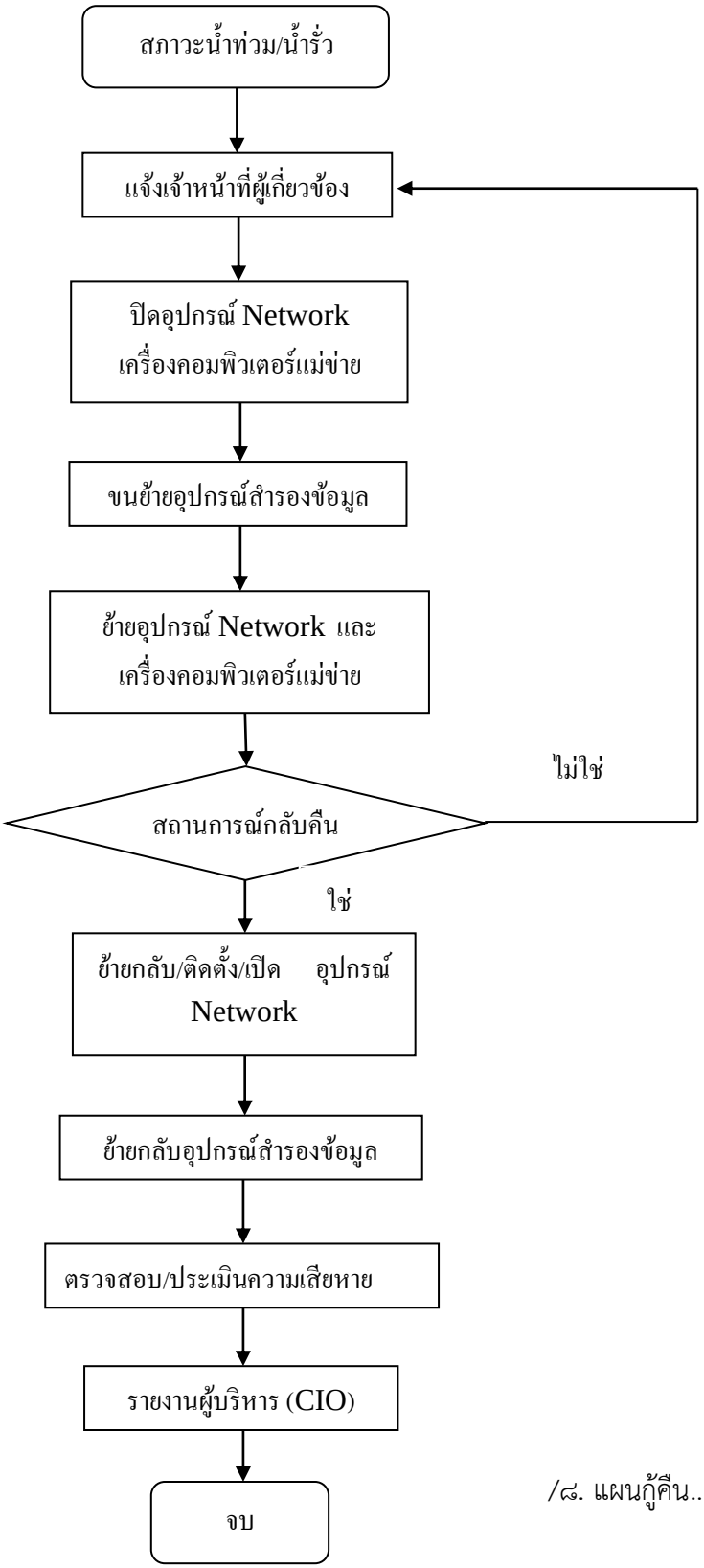
/ข้อปฏิบัติ...

ข้อปฏิบัติกรณีเกิดสถานการณ์หรือภาวะฉุกเฉิน กรณีไฟฟ้าดับ/ไฟกระชาก



/ข้อปฏิบัติ...

ข้อปฏิบัติกรณีเกิดสถานการณ์หรือภาวะฉุกเฉิน กรณีน้ำท่วม/น้ำรั่ว



/๘. แผนกู้คืน...

๘. <u>แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติ</u>

การคืนระบบเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑) จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน
๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง
๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้เป็นการชั่วคราว
๕) นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็วภายใน ๔๘ ชั่วโมง
๖) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่นๆ ที่เกี่ยวข้อง

๙. <u>ผู้รับผิดชอบ</u>

เจ้าหน้าที่ผู้ประสานการปฏิบัติ

๑.นายวินัย ฉายากุล	วิศวกรไฟฟ้าสื่อสารชำนาญการพิเศษ
๒.นายอาทิตย์ ชุมทอง	นายช่างไฟฟ้าชำนาญงาน
๓.นายธันวา โทนวิรัตน์	นายช่างเทคนิคชำนาญงาน
๔.นางสาวรัตนา สังข์เพชร	นักวิชาการคอมพิวเตอร์

๑๐. <u>การติดตามและรายงานผล</u>

กำหนดให้เจ้าหน้าที่ผู้ประสานการปฏิบัติรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้