



แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน
(IT Contingency Plan) ของ กก.ตชด.14
ประจำปีงบประมาณ พ.ศ. 2557-2558

ศูนย์เทคโนโลยีสารสนเทศ
กองกำกับการตำรวจตระเวนชายแดนที่ 14

คำนำ

ระบบเทคโนโลยีสารสนเทศของกองกำกับการตำรวจตระเวนชายแดนที่ 14 มีความสำคัญยิ่งต่อการบริหารระบบราชการ ซึ่งศูนย์เทคโนโลยีสารสนเทศ กองกำกับการตำรวจตระเวนชายแดนที่ 14 เป็นหน่วยงานที่รับผิดชอบในการดำเนินการตรวจสอบและควบคุมมาตรฐานการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศของกองกำกับการตำรวจตระเวนชายแดนที่ 14 ได้ตระหนักถึงการดูแลรักษาระบบสารสนเทศของกองกำกับการตำรวจตระเวนชายแดนที่ 14 ให้มีความมั่นคงปลอดภัยและลดความเสี่ยงต่าง ๆ ที่จะเกิดขึ้นกับระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของกองกำกับการตำรวจตระเวนชายแดนที่ 14 สามารถใช้งานได้อย่างมีประสิทธิภาพและประสิทธิผล จึงได้จัดทำแผนแก้ไขปัญหาาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) ของกองกำกับการตำรวจตระเวนชายแดนที่ 14 ปีงบประมาณ พ.ศ.2557-2558 เพื่อเป็นกรอบแนวทางในการบำรุงรักษา ป้องกันและแก้ไขปัญหาที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ของหน่วยงานในสังกัดกองกำกับการตำรวจตระเวนชายแดนที่ 14

ศูนย์เทคโนโลยีสารสนเทศ
กองกำกับการตำรวจตระเวนชายแดนที่ 14

สารบัญ

เนื้อหา	หน้า
1. หลักการและเหตุผล	1
2. วัตถุประสงค์.....	1
3. ภัยพิบัติ.....	1
4. แนวทางการป้องกันความเสียหายจากภัยพิบัติ.....	2
5. ขั้นตอนปฏิบัติในมาตรการที่สำคัญ.....	6
6. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ	7
7. แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม.....	8
8. ผู้รับผิดชอบ.....	9
9. การติดตามและรายงานผล.....	9

แผนแก้ไขปัญหาาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) ของกองกำกับการตำรวจตระเวนชายแดนที่ 14 ปีงบประมาณ พ.ศ.2557-2558

หลักการและเหตุผล

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากรในหน่วยงาน สำนักงานตำรวจแห่งชาติได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศรวมทั้งระบบอุปกรณ์ต่างๆ เสียหายได้

กองกำกับการตำรวจตระเวนชายแดนที่ 14 จึงได้จัดทำแผนแก้ไขปัญหาาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน(IT Contingency Plan) ของกองกำกับการตำรวจตระเวนชายแดนที่ 14 ปีงบประมาณ พ.ศ.2557-2558 เพื่อเป็นกรอบแนวทางในการดูแลรักษาาระบบ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศรวมถึงระบบอุปกรณ์ต่างๆ

วัตถุประสงค์

1. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ขององค์กร
2. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ
3. เพื่อเป็นแนวทางในการดูแลรักษาาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
4. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันที่
5. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ขององค์กร

ภัยพิบัติ

ภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของ กองกำกับการตำรวจตระเวนชายแดนที่ 14 สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

1. ภัยพิบัติจากภายนอก

- 1.1 ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น
 - 1.2 การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
 - 1.3 ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง
 - 1.4 ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ
 - 1.5 การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล
 - 1.6 ไวรัสคอมพิวเตอร์
 - 1.7 ระบบเสียหายจากภัยสงครามเหตุจลาจลและการเกิดสถานการณ์ความไม่สงบ

2. ภัยพิบัติจากภายใน

- 2.1 ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย
- 2.2 ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร
- 2.3 เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

แนวทางการป้องกันความเสียหายจากภัยพิบัติ

1. ภัยพิบัติจากภายนอก

1.1 ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

1.1.1 การป้องกันและการดำเนินการอัคคีภัย

- (1) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่างๆ
- (2) อบรมแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิง การหนีไฟขั้นต้น

ให้แก่ข้าราชการตำรวจทุกราย

- (3) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย
- (4) จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์เพื่อ

ประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

1.1.2 การป้องกันอุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม

- (1) เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น สำหรับเครื่องแม่ข่ายตลอด

24 ชั่วโมง และตรวจสอบการทำงานให้ใช้งานได้อย่างสม่ำเสมอ

(2) ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

(3) เครื่องคอมพิวเตอร์แม่ข่ายต้องไม่อยู่ในบริเวณที่น้ำท่วมถึง

1.2 การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

1.2.1 ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำเข้าไป

1.2.2 จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตน (Finger Scan) และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

1.2.3 ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

1.3 ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอก องค์กรเกิดความขัดข้อง

1.3.1 การตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ตลอดเวลา

1.3.2 ต้องจัดให้มีเครือข่ายสำรอง สำหรับใช้ในกรณีที่เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้

1.4 ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

1.4.1 แยกไฟระบบคอมพิวเตอร์แม่ข่ายออกจากสายไฟหลักที่ผ่านสะพานไฟเข้าสู่หน่วยงาน

1.4.2 ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที

1.4.3 เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ ตรวจสอบระบบสำรองไฟฟ้า (UPS) ทุกวันศุกร์

1.4.4 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้บันทึกข้อมูลที่ค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่างๆ

1.5 การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

1.5.1 สแกนหาจุดอ่อนและอัปเดต Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยใช้ซอฟต์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

1.5.2 ติดตั้ง Firewall เพื่อป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและ อินทราเน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

1.5.3 ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตขององค์กร และ กลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบ เทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

1.5.4 จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ต และ อินทราเน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ ระบบ เทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

1.5.5 ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัปเดตอย่างสม่ำเสมอ และปิด พอร์ตที่ไม่มีการใช้งาน

1.5.6 กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติดังนี้

- (1) ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น
- (2) ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น
- (3) จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย
- (4) เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้

โดยผู้อื่น

- (5) ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย 8 อักขระ
- (6) ตั้งรหัสผ่านโดยใช้เทคนิคส่วนตัวที่ง่ายต่อการจำรหัสผ่านที่ได้กำหนดไว้
- (7) ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม
- (8) ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 123, abcd เป็นต้น หรือ

เป็นกลุ่มของตัวอักขระที่เหมือนกัน เช่น 11111, aaa, bbb เป็นต้น

(9) เปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ 6 เดือน ส่วน ในกรณีของผู้ดูแลระบบ ให้เปลี่ยนรหัสผ่านใหม่ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุก ๆ 3 เดือน

(10) เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(11) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่

ระบบงาน

(12) ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เช่น บันทึกไว้ในหน้าจอล็อกอิน (ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง จะได้ไม่ต้องใส่รหัสผ่านอีก ครั้ง)

(13) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(14) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

1.5.7 ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอก โดยการนำระบบ DMZมากรอง IP ที่จะเข้ามายังระบบเครือข่าย

1.5.8 ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOSและ DDOS

1.6 ไวรัสมัลแวร์

1.6.1 ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอและต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

1.6.2 ระมัดระวังจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

- (1) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- (2) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย
- (3) ไม่ใช่สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

1.6.3 ใช้ความระมัดระวังในการเปิด E-mail

- (1) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- (2) ลบ E-mail ที่ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

1.6.4 ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต

- (1) ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ
- (2) ไม่ควรเปิด website ที่แนะนำมาทาง E-mail
- (3) ไม่ดาวน์โหลดไฟล์จาก website ที่ไม่น่าเชื่อถือ
- (4) ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ
- (5) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

1.7 ระบบเสียหายจากภัยสงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

เนื่องจากเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ ในการป้องกันหากไม่สามารถย้ายสถานที่หรือป้องกันสถานที่ได้ ควรมีการ Back Up ข้อมูลไว้มากกว่า 1 Back Up และแยกสถานที่จัดเก็บ และถ้าเกิดความเสียหายเกิดขึ้นกับข้อมูล ก็สามารถนำข้อมูลที่มีการ Back Up ไว้ และอุปกรณ์คอมพิวเตอร์ สำรองมาใช้แทน หากเกิดความเสียหายร้ายแรงควรมีศูนย์คอมพิวเตอร์สำรองเพิ่ม

๒. ภัยพิบัติจากภายใน

2.1 ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2.1.1 การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน

2.1.2 การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนดทุกสัปดาห์ โดยจะสำรองข้อมูลโครงสร้างข้อมูล Source Code และบันทึกข้อมูลลงในสื่อบันทึก

2.1.3 ทดสอบRecoveryข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้สำรองไว้ในสื่อบันทึก ทุกสัปดาห์

2.1.4 ทดสอบ Recoveryฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้สำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

2.1.5 จัดเจ้าหน้าที่ในการบำรุงรักษาสื่อบันทึกข้อมูลของเครื่องคอมพิวเตอร์แม่ข่าย เพื่อลดความเสียหายของข้อมูล

2.2 ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

2.2.1 ติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องแม่ข่ายและลูกข่ายเพื่อให้สามารถตรวจสอบได้

2.2.2 ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตข้อมูลไวรัสอยู่เสมอ

2.2.3 หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

2.3 ข้าราชการตำรวจขาดความรู้ในการใช้เครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

2.3.1 ให้ความรู้แก่ข้าราชการตำรวจและหน่วยงานผ่านช่องทางต่างๆ เช่น website, หนังสือเวียน เป็นต้น

2.3.2 ใส่กุญแจห้องอุปกรณ์เครือข่ายเพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่ หรือบุคลากรที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

ขั้นตอนปฏิบัติในมาตรการที่สำคัญ

1. การสำรองข้อมูล (Back Up)

1.1 การสำรองข้อมูลอัตโนมัติโดยระบบเครื่องประมวลผลแม่ข่าย โดยสำรองข้อมูลไว้ในสื่อบันทึก 1 ชุด

1.2 การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตาม ระยะเวลาที่กำหนดเป็นประจำทุกสัปดาห์ โดยสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในสื่อบันทึก

2. การกู้ข้อมูล (Recovery)

2.1 ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูลที่ได้สำรองไว้ในสื่อบันทึก ทุกสัปดาห์

2.2 ทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้สำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียทุกสัปดาห์

ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

1. กรณีเครื่องลูกข่าย

1.1 ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบเทคโนโลยีสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้หนึ่งแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือดูแลทราบ หรือ กรณีมีเหตุอันทำให้เจ้าหน้าที่ผู้เกี่ยวข้องไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

1.2 กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ตั้งสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องโดยเร็ว

1.3 ในกรณีที่เกรงว่าเหตุที่เกิดขึ้นจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง ให้ตั้งสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

1.4 ให้เจ้าหน้าที่ที่เกี่ยวข้อง แจ้งเหตุขัดข้องนั้นให้หัวหน้า หรือผู้บังคับบัญชาทราบโดยเร็ว

2. กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

2.1 ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

2.2 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

2.3 ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

2.4 รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

2.5 ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ Server และระบบเครือข่ายโดยเร็วที่สุด

2.6 ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบ นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

2.7 ผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

3. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ให้ดำเนินการดังนี้

3.1 เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆ ตั้งสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

3.2 สแกนและกำจัดไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัส

3.3 แจ้งเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อตรวจสอบ

4. หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัยเพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติ ดังนี้

4.1 ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

4.2 ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร

4.3 เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งเพลิงไหม้ จากนั้นออกจากอาคารแล้วแจ้งหน่วยดับเพลิงทันที

4.4 หากเพลิงไหม้ในห้องทำงานให้ออกจากห้อง ปิดประตู แล้วแจ้งฝ่ายอาคารและ สถานที่เพื่อแจ้งหน่วยดับเพลิงทันที

4.5 หากเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนออกจากอาคารให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อยๆ เปิดประตู แล้วไปยังทางออกที่ปลอดภัยที่สุด

4.6 หากเพลิงไหม้อยู่บริเวณใกล้ประตู จะมีความร้อน ห้ามเปิดประตูโดยเด็ดขาด ให้รีบแจ้งหน่วยดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเพลิงไหม้ หากผ้าเปียก ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

4.7 เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

5. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับส่งมาก ดังนั้น สิ่งที่มีมักจะเกิดขึ้นและยากต่อการหลีกเลี่ยงคือ ผลกระทบต่างๆ ที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลสำคัญ รวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ประกอบด้วย

5.1 เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาเปิดใช้งาน ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

5.2 เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม

การคืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาวะปกติเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

1. จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน
2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง
4. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ในการชั่วคราว
5. นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็วภายใน ๔๘ ชั่วโมง

6. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่นๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบ

1. ระดับนโยบาย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ของหน่วย (CIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจน ติดตาม กำกับดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

2. ระดับปฏิบัติ

เจ้าหน้าที่ผู้ดูแลระบบของหน่วย รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้

ร.ต.อ.

ผู้เสนอแผน

(วุฒิพร อ่องผู้ดี)

รอง สว.๗/หน.ศทส.กก.ตชด.14

พ.ต.ท.

ผู้เห็นชอบแผน

(พงศ์พัชร นิคมภักดี)

รอง ผกก.ตชด.14

พ.ต.อ.

ผู้อนุมัติแผน

(พิระศักดิ์ กลีบจันทร์)

ผกก.ตชด.14