บันทึกข้อความ

ส่วนราชการ ภ.จว.สุราษฎร์ธานี จว.สุราษฎร์ธานี โทรสาร ๐-๗๗๓๕-๕๙๐๑

ที่ ๐๐๒๓(สฎ).๑๒/๓๖๘๗ **วันที่** ๓๐ มิถุนายน ๒๕๕๗

เรื่อง ประชาสัมพันธ์วิธีการแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน ผกก.สภ.และ สวญ.สภ.ในสังกัด ภ.จว.สุราษฎร์ธานี

ตามหนังสือ ภ.๘ ที่ ๐๐๒๓.๑๙/๒๗๗๖ ลง ๑๔ พ.ค.๕๗ ท้ายหนังสือ สทส.ที่ ๐๐๓๓.๓๔/๘๔๓ ลง ๓ เม.ย.๕๗ เรื่อง ส่งรายละเอียดตัวชี้วัดย่อยที่ ๖.๒.๓ ระดับความสำเร็จของการพัฒนาองค์การ ด้านทุนสารสนเทศประจำปีงบประมาณ พ.ศ.๒๕๕๗ นั้น

เพื่อให้การดำเนินการบรรลุตามวัตถุประสงค์ของตัวชี้วัด ที่ ๖.๒.๓ ภ.จว.สุราษฎร์ธานี ได้จัดทำคู่มือวิธีการแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ โดยสามารถดูรายละเอียดได้ทาง E-mail:**download.surat@gmail.com** **รหัสผ่าน surat1234** พร้อมรายละเอียดการจัดทำตัวชี้วัดที่ ๖.๒.๓ เพื่อดำเนินการในส่วนที่เกี่ยวข้อง

จึงแจ้งมาเพื่อทราบ และดำเนินการ

พ.ต.อ.
(เชิดศักดิ์ บุญนัดดา)
รอง ผบก.ฯปรท.ผบก.ภ.จว.สุราษฎร์ธานี

แนวทางการป้องกันความเสียหายจากภัยพิบัติ

1. ภัยพิบัติจากภายนอก

1.1 ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

1.1.1 การป้องกันและการดำเนินการอัคคีภัย

(1) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่างๆ

(2) อบรมแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิงการหนีไฟขั้นต้น ให้แก่ข้าราชการตำรวจทุกราย

(3) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์ แม่ข่าย

(4) จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

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 ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง

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) ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า30 นาที

1.4.3 เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ ตรวจสอบระบบสำรองไฟฟ้า (UPS) ทุกวันศุกร์

1.4.4 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้บันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่างๆ

1.5 การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

1.5.1 สแกนหาจุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

1.5.2 ติดตั้งFirewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

1.5.3 ติดตั้งProxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตขององค์กร และ กลั่นกรองข้อมูลที่มาทางwebsite ซึ่งจะมีการกำหนดค่าConfiguration ให้มีความปลอดภัย ต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

1.5.4 จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

1.5.5 ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอและปิดพอร์ตที่ไม่มีการใช้งาน

1.5.6 กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติดังนี้

(1) ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(2) ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น

(3) จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

(4) เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(5) ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย8อักขระ

(6) ตั้งรหัสผ่านโดยใช้เทคนิคส่วนตัวที่ง่ายต่อการจำรหัสผ่านที่ได้กำหนดไว้

(7) ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

(8) ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น123, abcd เป็นต้น หรือเป็นกลุ่มของตัวอักขระที่เหมือนกัน เช่น11111, aaa, bbb เป็นต้น

(9) เปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ6 เดือน ส่วนในกรณีของผู้ดูแลระบบ ให้เปลี่ยนรหัสผ่านใหม่ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุก ๆ3 เดือน

(10) เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(11) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

(12) ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เช่น บันทึกไว้ในหน้าจอล็อกอิน (ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลังจะได้ไม่ต้องใส่รหัสผ่านอีกครั้ง)

(13) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(14) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

1.5.7 ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอก โดยการนำระบบ DMZ มากรอง IP ที่จะเข้ามายังระบบเครือข่าย

1.5.8 ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบDOS และ DDOS

1.6 ไวรัสคอมพิวเตอร์

1.6.1 ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

1.6.2 ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

(1) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

(2) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

(3) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

1.6.3 ใช้ความระมัดระวังในการเปิดE-mail

(1) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

(2) ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

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 ข้อมูลไว้มากกว่า1 Back Up และแยกสถานที่จัดเก็บ และถ้าเกิดความเสียหายเกิดขึ้นกับข้อมูล ก็สามารถนำข้อมูลที่มีการBack Up ไว้ และอุปกรณ์คอมพิวเตอร์สำรองมาใช้แทน หากเกิดความเสียหายร้ายแรงควรมีศูนย์คอมพิวเตอร์สำรองเพิ่ม

2. ภัยพิบัติจากภายใน

2.1 ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

2.1.1 การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน

2.1.2 การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนดทุกสัปดาห์ โดยจะสำรองข้อมูล โครงสร้างข้อมูลSource Code และบันทึกข้อมูล ลงในสื่อบันทึก

2.1.3 ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้สำรองไว้ในสื่อบันทึก ทุกสัปดาห์

2.1.4 ทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการ ของเครื่องแม่ข่ายสำรองที่ได้สำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

2.1.5 จัดเจ้าหน้าที่ในการบำรุงรักษาสื่อบันทึกข้อมูลของเครื่องคอมพิวเตอร์แม่ข่าย เพื่อลดความเสียหายของข้อมูล

2.2 ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

2.2.1 ติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องแม่ข่ายและลูกข่ายเพื่อให้สามารถตรวจสอบได้

2.2.2 ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ

2.2.3 หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

2.3 ข้าราชการตำรวจขาดความรู้ในการใช้เครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์และซอฟท์แวร์ ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

2.3.1 ให้ความรู้แก่ข้าราชการตำรวจและหน่วยงานผ่านช่องทางต่างๆ เช่นwebsite, หนังสือเวียน เป็นต้น

2.3.2 ใส่กุญแจตู้อุปกรณ์เครือข่าย เพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่ หรือบุคลากรที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

ขั้นตอนปฏิบัติในมาตรการที่สำคัญ

1. การสำรองข้อมูล (Back Up)

1.1 การสำรองข้อมูลอัตโนมัติโดยระบบเครื่องประมวลผลแม่ข่าย โดยสำรองข้อมูลไว้ในสื่อบันทึก1 ชุด

1.2 การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตาม ระยะเวลาที่กำหนดเป็นประจำทุกสัปดาห์ โดยสำรองข้อมูล โครงสร้างข้อมูล และSource Code และบันทึกข้อมูลลงในสื่อบันทึก

2. การกู้ข้อมูล (Recovery)

2.1 ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูลที่ได้สำรองไว้ในสื่อบันทึก ทุกสัปดาห์

2.2 ทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้สำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสีย ทุกสัปดาห์

ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

1. กรณีเครื่องถูกข่าย

1.1 ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบเทคโนโลยีสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือดูแลทราบ หรือ กรณีมีเหตุอันทำให้เจ้าหน้าที่ผู้เกี่ยวข้องไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

1.2 กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ดึงสายเชื่อมโยงระบบเครือข่าย(LAN) ออกจากเครื่องโดยเร็ว

1.3 ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง ให้ดึงสายLAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

1.4 ให้เจ้าหน้าที่ที่เกี่ยวข้อง แจ้งเหตุขัดข้องนั้นให้หัวหน้า หรือผู้บังคับบัญชาทราบโดยเร็ว

2. กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

2.1 ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

2.2 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

2.3 ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

2.4 รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

2.5 ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ Server และระบบเครือข่ายโดยเร็วที่สุด

2.6 ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

2.7 ผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

3. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

3.1 เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆ ดึงสาย 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 การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

4.3 ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉิน มิให้ปิดตายหรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉิน เพื่อให้ไปถึงทางได้ แม้ว่าไฟดับหรือปกคลุมไปด้วยควัน

4.4 เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้ จากนั้นออกจากอาคารแล้วแจ้งหน่วยดับเพลิงทันที

4.5 เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

4.6 หากเพลิงไหม้ในห้องทำงาน ให้ออกจากห้อง ปิดประตู แล้วแจ้งฝ่ายอาคารและ สถานที่เพื่อแจ้งหน่วยดับเพลิงทันที

4.7 หากเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนออกจากอาคารให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อยๆ เปิดประตู แล้วไปยังทางหนีไฟฉุกเฉินที่ใกล้ที่สุด

4.8 หากเพลิงไหม้อยู่บริเวณใกล้ประตู จะมีความร้อน ห้ามเปิดประตูโดยเด็ดขาด ให้รีบแจ้งหน่วยดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเพลิงไหม้ หาผ้าเปียก ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

4.9 เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

4.10 ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

5. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับส่งมาก ดังนั้น สิ่งที่มักจะเกิดขึ้นและยากต่อการหลีกเลี่ยงคือ ผลกระทบต่างๆที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลสำคัญ รวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ประกอบด้วย

5.1 เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ(UPS) ตลอดระยะเวลาเปิดใช้งานทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

5.2 เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง**แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม**

การคืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการดังนี้

1. จัดหาอุปกรณ์ชิ้นส่วน เพื่อทดแทน

2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน48 ชั่วโมง

4. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้เป็นการชั่วคราว

5. นำสื่อที่ได้สำรองข้อมูลไว้กลับมRestore โดยเร็วภายใน 48 ชั่วโมง

6. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่นๆ ที่เกี่ยวข้อง

****