แผนเผชิญเหตุกรณีระบบสารสนเทศของ สตม. ขัดข้อง ของกองบังคับการตรวจคนเข้าเมือง 1

กองกำกับการ 3
กองบังคับการตรวจคนเข้าเมือง 1

ข้อมูล ณ วันที่ 31 กรกฎาคม 2569

https://sub3div1immigration.com sub3imm1@gmail.com 02 553 8111 @sub3divi1

แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) กองกำกับการ 3 กองบังคับการตรวจคนเข้าเมือง 1

หลักการและเหตุผล

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัยสามารถนำไปใช้ประโยชน์ต่อการวางแผนพัฒนาองค์กรการบริหารจัดการองค์กรและการปฏิบัติงานของบุคลากรในหน่วยงาน กองกำกับการ 3 กองบังคับการตรวจคนเข้าเมือง 1 ได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์ต่างๆ เสียหายได้ จึงได้จัดทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ รวมถึงระบบอุปกรณ์ต่างๆ

วัตถุประสงค์

1.เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร

2. เพื่อลดความเสี่ยงและความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ

3.เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ให้มีเสถียรภาพและมีความพร้อมสาหรับการใช้งาน

4.เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

5.เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์กร ภัยพิบัติ ภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของกองกำกับการ 3 กองบังคับการตรวจคนเข้าเมือง 1 สามารถจำแนกได้เป็นภัยพิบัติจากภายนอก และภัยพิบัติจากภายใน

1. ภัยพิบัติจากภายนอก

1.1 ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน ได้แก่ อัคคีภัย อุทกภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

1.2 การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงานที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

1.3 ระบบการสื่อสารของเครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงานที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง

1.4 ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

1.5 การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงเครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

1.6 ไวรัสคอมพิวเตอร์

1.7 อุปกรณ์คอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงานเสียหายจากภัยสงครามเหตุจลาจลและการเกิดสถานการณ์ความไม่สงบ

2. ภัยพิบัติจากภายใน

2.1 ฐานข้อมูลภายในอุปกรณ์คอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงานเสียหายหรือข้อมูลถูกทำลาย

2.2 ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

2.3เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดการทำงาน

แนวทางการป้องกันความเสียหายจากภัยพิบัติ

1. ภัยพิบัติจากภายนอก

1.1 ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสมแมลงสัตว์กัดแทะ เป็นต้น

1.1.1 การป้องกันและการดำเนินการอัคคีภัย

(1) หน่วยงานในสังกัดกำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่างๆ

(2) หน่วยงานในสังกัดอบรมแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิงการหนีไฟขั้นต้นให้แก่ข้าราชการตำรวจทุกราย

(3) หน่วยงานในสังกัดติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน

(4) หน่วยงานในสังกัดจัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

1.1.2 การป้องกันอุทกภัยและอุณหภูมิที่ไม่เหมาะสม

(1) หน่วยงานในสังกัดเปิดเครื่องปรับอากาศ สำหรับเครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ในช่วงเวลาที่ใช้งาน และตรวจสอบการทำงานให้ใช้งานได้อย่างสม่ำเสมอ

(2) หน่วยงานในสังกัดตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

(3) หน่วยงานในสังกัดต้องจัดให้เครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงานและเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ไม่อยู่ในบริเวณที่น้ำท่วมถึง

1.2 การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงานที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

1.2.1 หน่วยงานในสังกัดจัดให้มีควบคุมการเข้าออกห้องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน และการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปยุ่งเกี่ยวกับอุปกรณ์คอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน หากจำเป็นให้มีเจ้าหน้าที่ของหน่วย เป็นผู้รับผิดชอบควบคุมดูแล

1.2.2 หน่วยงานในสังกัดจัดให้มีการรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน

1.2.3 หน่วยงานที่รับผิดชอบดำเนินการติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

1.3 ระบบการสื่อสารของเครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงานที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง

1.3.1 ให้หน่วยงานในสังกัดตรวจสอบระบบเครือข่ายทั้งภายใน (LAN, Wifi) และภายนอก (Internet) อาคารให้สามารถใช้งานได้ตลอดเวลา

1.3.2 ให้ติดต่อเจ้าหน้าที่ SIT Contact and service Center ได้ 3 ช่องทาง

(1) โทรศัพท์ 02 033 1988

(2) Email : service.ib@somapait.com

(3) Line name: SIT.CSC-OSO โดยการแจ้งผ่านระบบ Line ให้แจ้งตามรูปแบบดังต่อไปนี้

- ชื่อ-สกุล(ยศ)
- หน่วยงาน
- เบอร์โทรติดต่อ
- ระบบและปัญหาที่พบ
- ภาพหรือวีดิโอเมื่อพบปัญหา
- URL:
- IP:
- User ID:

1.3.3 หน่วยงานโทรศัพท์แจ้งปัญหาไปยังฝ่ายจัดการระบบศูนย์เทคโนโลยีและสารสนเทศสำนักงานตรวจคนเข้าเมืองที่หมายเลขโทรศัพท์ 06-6074-9815 เพื่อแจ้งข้อขัดข้อง

1.3.4 หน่วยงานโทรศัพท์แจ้งปัญหาไปยังองค์การโทรศัพท์แห่งประเทศไทย (TOT) หมายเลขโทรศัพท์ 0-2159-9555 เพื่อให้ตรวจสอบระบบสายสัญญาณภายใน และ อุปกรณ์กระจายสัญญาณเครือข่ายภายในหน่วยงาน

1.4 ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

1.4.1 หน่วยงานในสังกัดติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC)

1.4.2 หน่วยงานในสังกัดกำชับผู้ใช้งานให้เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ ตรวจสอบ
ระบบสำรองไฟฟ้า (UPS) และปิดระบบสำรองไฟฟ้า(UPS) ทุกวันศุกร์ เพื่อยืดอายุการใช้งาน

1.4.3 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้บันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่างๆ

1. 5 การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศรวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

1.5.1 หน่วยงานในสังกัดติดตั้ง Firewall หรือ โปรแกรมที่มีฟังก์ชั่น Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

1.5.2 หน่วยงานในสังกัดติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่มีการใช้งาน

1.5.3 ให้ผู้ใช้งานระบบปฏิบัติดังนี้

(1) ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(2) ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น

(3) จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

(4) เปลี่ยนรหัสผ่านโดยทันที เมื่อทราบว่ารหัสผ่านของตนอาจ ถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(5) ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย 8 อักขระ

(6)รหัสผ่านโดยใช้เทคนิคส่วนตัวที่ง่ายต่อการจำรหัสผ่านที่ได้กำหนดไว้

(7) ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

(8) ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น 123, abcd เป็นต้น หรือเป็นกลุ่มของตัวอักขระที่เหมือนกัน เช่น 11111, aaa, bbb เป็นต้น

(9) เปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุกระยะ 2 เดือน ส่วนในกรณีของผู้ดูแลระบบ ให้เปลี่ยนรหัสผ่านใหม่ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุกระยะ 1 เดือน

(10) เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(11) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

(12) ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เช่น บันทึกไว้ในหน้าจอล็อกอิน (ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง จะได้ไม่ต้องใส่รหัสผ่านอีกครั้ง)

(13) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(14) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสาหรับระบบงานต่าง ๆ ที่ตนใช้งาน

1.5.4 หน่วยงานในสังกัดติดตั้งโปรแกรมให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ DDOS

1.6 ไวรัสคอมพิวเตอร์

1.6.1 หน่วยงานในสังกัดติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัส อยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

1.6.2ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

(1) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

(2) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

(3) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

1.6.3 ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ใช้ความระมัดระวังในการเปิด E-mail

(1) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

(2) ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

1.6.4 ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต

(1) ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ

(2) ไม่ควรเปิด website ที่แนะนามาทาง E-mail

(3) ไม่ดาวน์โหลดไฟล์จาก website ที่ไม่น่าเชื่อถือ

(4) ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ

(5) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

1.7 ระบบเสียหายจากภัยสงคราม/เหตุจลาจลและการเกิดสถานการณ์ความไม่สงบ สงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ในการป้องกันหากไม่สามารถย้ายสถานที่หรือป้องกันสถานที่ได้ จึงให้หน่วยงานในสังกัดดำเนินการ Backup ข้อมูลไว้มากกว่า 1 Backup และแยกสถานที่จัดเก็บ และถ้าเกิดความเสียหายเกิดขึ้นกับข้อมูล ก็สามารถนำข้อมูลที่มีการ Backup ไว้ และอุปกรณ์คอมพิวเตอร์ สำรองมาใช้แทน หากเกิดความเสียหายร้ายแรงควรมีศูนย์คอมพิวเตอร์สำรองเพิ่ม

2. ภัยพิบัติจากภายใน

2.1 ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

2.1.1 หน่วยงานในสังกัดติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน และลูกข่ายเพื่อให้สามารถตรวจสอบได้

2.1.2 หน่วยงานในสังกัดติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสเสมอ

2.1.3 ผู้ใช้งานอุปกรณ์คอมพิวเตอร์หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

2.1.4 ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ควรหลีกเลี่ยงการใช้อุปกรณ์บันทึกข้อมูลภายนอก (Flash Drive, Handy Drive ,Thumb Drive, USB Drive) เพื่อป้องกันไวรัส

2.2 ข้าราชการตำรวจขาดความรู้ในการใช้เครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์และซอฟท์แวร์ ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดการทำงาน

2.2.1 หน่วยงานในสังกัดให้ความรู้แก่ข้าราชการตำรวจและหน่วยงานผ่านช่องทางต่างๆเช่น website, หนังสือเวียน จัดฝึกอบรม เป็นต้น

2.2.2 หน่วยงานในสังกัดตั้งรหัสผ่านแก่อุปกรณ์เครือข่ายของหน่วยงานเพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่ หรือบุคลากรที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

1.กรณีเครื่องลูกข่าย

1.1 ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบเทคโนโลยีสารสนเทศได้ตามปกติให้ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ผู้นั้นแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือดูแลทราบ หรือกรณีมีเหตุอันทำให้เจ้าหน้าที่ผู้เกี่ยวข้องไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ ทุกหน่วยงานในสังกัดทราบ

1.2 กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ดึงสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องโดยเร็ว

1.3 ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็น อันตรายต่อหน่วย งานภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง ให้ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ดำเนินการดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

1.4 ให้เจ้าหน้าที่ที่เกี่ยวข้อง แจ้งเหตุขัดข้องนั้นให้ผู้บังคับบัญชาทราบโดยเร็ว

2.กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

2.1 ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็วแล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

2.2 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย โดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

2.3 ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

2.4 รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

2.5 ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ Server และระบบเครือข่ายโดยเร็วที่สุด

2.6 ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรองหรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

2.7 หน่วยงานผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

3.กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

3.1 เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆ ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

3.2 สแกนและกำจัดไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัส

3.3 แจ้งเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อตรวจสอบ

3.4 การบันทึกข้อมูลด้วยมือพร้อมตรวจสอบข้อมูลบุคคลต้องห้ามแบ[OFFLINE

4.หลักปฏิบัติของข้าราชการตำรวจในสังกัดในการป้องกันอัคคีภัยเพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และเพื่อให้ปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติ ดังนี้

4.1 ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

4.2 ศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

4.3 ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉินมิให้ปิดตายหรือมีสิ่งกีดขวางและสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉิน เพื่อให้ไปถึงทางได้แม้ว่าไฟดับหรือปกคลุมไปด้วยควัน

4.4 เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้จากนั้นออกจากอาคารแล้วแจ้งหน่วยดับเพลิงทันที

4.5 เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

4.6 หากเพลิงไหม้ในห้องทำงาน ให้ออกจากห้อง ปิดประตู แล้วแจ้งฝ่ายอาคารและ สถานที่เพื่อแจ้งหน่วยดับเพลิงทันที

4.7 หากเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนออกจากอาคารให้วางมือบนประตูหากประตูมีความเย็นอยู่ ค่อยๆ เปิดประตู แล้วไปยังทางหนีไฟฉุกเฉินที่ใกล้ที่สุด

4.8 หากเพลิงไหม้อยู่บริเวณใกล้ประตู จะมีความร้อน ห้ามเปิดประตูโดยเด็ดขาด ให้รีบแจ้งหน่วยดับเพลิงและแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเพลิงไหม้ หาผ้าเปียกปิดทางเข้าของควันปิดพัดลมและเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

4.9 เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

4.10 ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

5. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับส่งมาก ดังนั้น สิ่งที่มักจะเกิดขึ้นและยากต่อการหลีกเลี่ยงคือ ผลกระทบต่างๆที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลสำคัญ รวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า จึงให้ผู้ใช้งานคอมพิวเตอร์ปฏิบัติดังนี้

5.1 เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาเปิดใช้งานทั้งเครื่องคอมพิวเตอร์ที่เก็บข้อมูลหลักของหน่วยงาน และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC)

5.2 เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม

การกู้คืนระบบเครื่องคอมพิวเตอร์โดยปกติระบบเครื่องคอมพิวเตอร์ ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

1. จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน
2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน 48 ชั่วโมง
4.ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้เป็นการชั่วคราว

ผู้รับผิดชอบ

1.ระดับนโยบาย

งานเทคโนโลยีสารสนเทศ กองบังคับการตรวจคนเข้าเมือง 1

2.ระดับปฏิบัติ

เจ้าหน้าที่ผู้ดูแลระบบของกองกำกับการ 3 กองบังคับการตรวจคนเข้าเมือง 1 รับผิดชอบ รักษาความปลอดภัยระบบฐานข้อมูล ระบบเทคโนโลยีสารสนเทศ และอุปกรณ์คอมพิวเตอร์ให้ สามารถใช้งานได้เป็นปกติ

การติดตามและรายงานผล

หน่วยงานในสังกัดกำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไข ให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณี

พันตำรวจโทหญิง ผู้เสนอแผน
(ชลธิชา มิสกุล)
สารวัตรกองกำกับการ 3 กองบังคับการตรวจคนเข้าเมือง 1

พันตำรวจโทหญิง ผู้เห็นชอบแผน
(วิภาวดี เจริญเนติศาสตร์)
รองผู้กำกับการ 3 กองบังคับการตรวจคนเข้าเมือง 1

พันตำรวจเอกหญิง ผู้อนุมัติแผน
(พรชนก เพชรกาฬ)
ผู้กำกับการ 3 กองบังคับการตรวจคนเข้าเมือง 1
สำนักงานตรวจคนเข้าเมือง