บันทึกข้อความ

ส่วนราชการ ภ.จว.พิจิตร โทร. ๐-๕๖๖๑-๓๘๖๒

ที่ ๐๐๒๑.๖๑๒/ ๒๘๘ **วันที่** ๒๑ พฤษภาคม ๒๕๕๗

เรื่อง ส่งแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน(IT Contingency Plan)

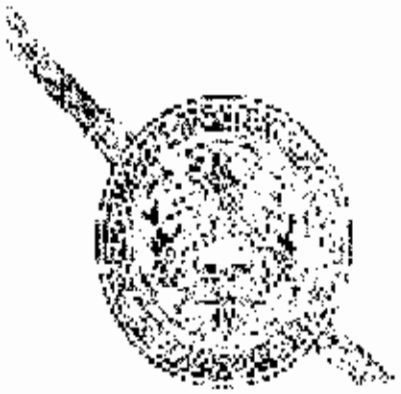
เรียน ผบช.ภ.๖

ตามหนังสือ ภ.๖ ที่ ๐๐๒๑.๑๙๑/๒๗๕๙ ลง ๒๙ เม.ย.๕๗ เรื่อง รายละเอียดตัวชี้วัดย่อยที่ ๖.๒ ระดับความสำเร็จของการพัฒนาองค์การ ด้านทุนสารสนสนเทศ ประจำปีงบประมาณ พ.ศ.๒๕๕๗ ซึ่งตามสั่งการให้แต่ละ ภ.จว. จัดทำแผนปฏิบัติการของหน่วย แล้วส่งให้ ภ.๖ ทราบ นั้น

ภ.จว.พิจิตร ได้ดำเนินการจัดทำแผนฯ เสร็จเรียบร้อย จึงขอส่งแผนฯ ดังกล่าวพร้อมนี้ด้วยแล้ว จำนวน ๑ ชุด

จึงเรียนมาเพื่อโปรดทราบ

พล.ต.ต.
(กฤษณะ ศิริปิยะวัฒน์)
ผบก.ภ.จว.พิจิตร



แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน
(IT Contingency Plan) ของ ตำรวจภูธรจังหวัดพิจิตร
ปีงบประมาณ พ.ศ.๒๕๕๗-๒๕๕๘

งานเทคโนโลยีสารสนเทศและการสื่อสาร

ตำรวจภูธรจังหวัดพิจิตร

คำนำ

ระบบเทคโนโลยีสารสนเทศ ของ ตำรวจภูธรจังหวัดพิจิตร มีความสำคัญยิ่งต่อการบริหารระบบราชการ ซึ่ง งานเทคโนโลยีสารสนเทศ และการสื่อสาร ตำรวจภูธรจังหวัดพิจิตร มีหน้าที่รับผิดชอบในการดำเนินการตรวจสอบควบคุมมาตรฐานการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ ของตำรวจภูธรจังหวัดพิจิตร ได้ตระหนักถึงการดูแลรักษาระบบสารสนเทศของตำรวจภูธรจังหวัดพิจิตร ให้มีความมั่นคงปลอดภัยและลดความเสี่ยงต่าง ๆ ที่จะเกิดขึ้นกับระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของตำรวจภูธรจังหวัดพิจิตร สามารถใช้งานได้อย่างมีประสิทธิภาพและประสิทธิผล จึงได้จัดทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน(IT Contingency Plan) ของตำรวจภูธรจังหวัดพิตร ปีงบบประมาณ พ.ศ.๒๕๕๗-๒๕๕๘ เพื่อเป็นกรอบแนวทางในการบำรุงรักษา ป้องกันและแก้ไขปัญหาที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงานในสังกัด ตำรวจภูธรจังหวัดพิจิตร

งานเทคโนโลยีสารสนเทศและการสื่อสาร
ตำรวจภูธรจังหวัดพิจิตร

สารบัญ

เนื้อหา หน้า

แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน
(IT Contingency Plan) ของตำรวจภูธรจังหวัดพิจิตร
ปีงบประมาณ พ.ศ.๒๕๕๗ - ๒๕๕๘

หลักการและเหตุผล

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากรในหน่วยงาน ตำรวจภูธรจังหวัดพิจิตร ได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์ต่าง ๆ เสียหายได้

ตำรวจภูธรจังหวัดพิจิตร จึงได้จัดทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน(IT Contingency Plan) ของสำนักงานตำรวจแห่งชาติ ปีงบประมาณ พงศ.๒๕๕๗-๒๕๕๘ เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ รวมถึงระบบอุปกรณ์ต่าง ๆ

วัตถุประสงค์

๑. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ขององค์กร

๒. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๔. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๕. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ขององค์กร

ภัยพิบัติ

ภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติสามารถจำแนกได้เป็นสองกลุ่มหลัก ๆ ได้แก่

๑. ภัยพิบัติจากภายนอก

๑.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่ายได้แก่ อัคคีภัย อุทกภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ ระบบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง

๑.๔ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๑.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๑.๖ ไวรัสคอมพิวเตอร์

๑.๗ ระบบเสียหายจากภัยสงคราม เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

๒. ภัยพิบัติจากภายใน

๒.๑ ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๒.๓ เจ้าหน้าที่หรือบุคลากรของหน่วยขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดทำงาน

แนวทางการป้องกันความเสียหายจากภัยพิบัติ

๑. ภัยพิบัติจากภายนอก

๑.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

๑.๑.๑ <u>การป้องกันและการดำเนินการอัคคีภัย</u>

(๑) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่าง ๆ

(๒) อบรมแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิง การหนีไฟขั้นต้นให้แก่ข้าราชการตำรวจทุกราย

(๓) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทครอนิกส์ สำหรับห้องคอมพิวเตอร์แม่ข่าย

(๔) จัดทำเครื่องหมายกระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

๑.๑.๒ <u>การป้องกันอุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม</u>

(๑) เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น สำหรับเครื่องแม่ข่ายตลอด ๒๔ ชั่วโมง และตรวจสอบการทำงานให้ใช้งานได้อย่างสม่ำเสมอ

(๒) ตรวจสอบการรั่วซึมของหลังคาเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

(๓) เครื่องคอมพิวเตอร์แม่ข่ายต้องไม่อยู่บริเวณที่น้ำท่วมถึง

๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๒.๑ ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลอื่นที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำเข้าไป

๑.๒.๒ จัดให้มีระบบรักษษความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตน(Finger Scan) และมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

๑.๒.๓ ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๑.๓ ระบบสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง

๑.๓.๑ การตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ตลอดเวลา

๑.๓.๒ ต้องจัดให้มีเครือข่ายสำรอง สำหรับใช้ในกรณีที่เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้

๑.๔ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๑.๔.๑ แยกไฟระบบคอมพิวเตอร์แม่ข่ายออกจากสายไฟหลักที่ผ่านสะพานไฟเข้าสู่หน่วยงาน

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

๑.๔.๓ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ ตรวจสอบระบบสำรองไฟฟ้า(UPS) ทุกวันศุกร์

๑.๔.๔ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้บันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่าง ๆ

๑.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๑.๕.๑ สแกนหาจุดอ่อน และอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยใช้ซอฟท์แวร์ เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

๑.๕.๒ ติดตั้ง Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตและอินทราเน็ตสามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

๑.๕.๓ ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตขององค์กร และกลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

๑.๕.๔ จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราบเน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๑.๕.๕ ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่มีการใช้งาน

๑.๕.๖ กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติ ดังนี้

(๑) ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

(๒) ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น

(๓) จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

(๔) เปลี่ยนรหัสผ่านโดยทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๕) ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย ๘ อักขระ

(๖) ตั้งรหัสผ่านโดยใช้เทคนิคส่วนตัวที่ง่ายต่อการจำรหัสผ่านที่ได้กำหนดไว้

(๗) ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

(๘) ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓,abcd เป็นต้น หรือเป็นกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑๑,aaa,bbb เป็นต้น

(๙) เปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๖ เดือน ส่วนในกรณีของผู้ดูแลระบบ ให้เปลี่ยนรหัสผ่านใหม่ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุก ๆ ๓ เดือน

(๑๐) เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(๑๑) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันที ครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

(๑๒) ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เช่น บันทึกไว้ในหน้าจอล็อกอิน(ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อคอินในภายหลัง จะได้ไม่ต้องใส่รหัสผ่านอีกครั้ง)

(๑๓) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

๑.๕.๗ ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอก โดยนำระบบ DMZ มากรอง IP ที่จะเข้ามายังระบบเครือข่าย

๑.๕.๘ ติดตั้งระบบอุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ DDOS

๑.๖ ไวรัสคอมพิวเตอร์

๑.๖.๑ ติดตั้งโปรแกรมป้องกันไวรัส และอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๑.๖.๒ ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ

(๑) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

(๒) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

(๓) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๑.๖.๓ ใช้ความระมัดระวังในการเปิด E-mail

(๑) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

(๒) ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๑.๖.๔ ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จากอินเทอร์เน็ต

(๑) ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่าง ๆ

(๒) ไม่ควรเปิด website ที่แนะนำมาทาง E-mail

(๓) ไม่ดาวน์โหลดไฟล์จาก website ที่ไม่น่าเชื่อถือ

(๔) ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่าง ๆ อย่างสม่ำเสมอ

(๕) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๑.๗ ระบบเสียหายจากภัยสงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

เนื่องจากเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ ในการป้องกันหากไม่สามารถย้ายสถานที่หรือป้องกันสถานที่ได้ ควรมีการ Back Up ข้อมูลไว้มากกว่า ๑ Back Upและแยกสถานที่จัดเก็บ และ ถ้าเกิดความเสียหายเกิดขึ้นกับข้อมูล ก็สามารถนำข้อมูลที่มีการ Back Up ไว้ และอุปกรณ์คอมพิวเตอร์ สำรองมาใช้แทน หากเกิดความเสียหายร้ายแรงควรมีศูนย์คอมพิวเตอร์สำรองเพิ่ม

๒. ภัยพิบัติจากภายใน

๒.๑ ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๑.๑ การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน

๒.๑.๒ การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนด ทุกสัปดาห์ โดยจะสำรองข้อมูล โครงสร้างข้อมูล Source Code และบันทึกข้อมูลลงในสื่อบันทึก

๒.๑.๓ ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้สำรองไว้ในสื่อบันทึก ทุกสัปดาห์

๒.๑.๔ ทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้สำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

๒.๑.๕ จัดเจ้าหน้าที่ในการบำรุงรักษาสื่อบันทึกข้อมูลของเครื่องคอมพิวเตอร์แม่ข่าย เพื่อลดความเสียหายของข้อมูล

๒.๒ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๒.๒.๑ ติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องแม่ข่ายและลูกข่ายเพื่อให้สามารถตรวจสอบได้

๒.๒.๒ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ

๒.๒.๓ หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๒.๓ ข้าราชการตำรวจขาดความรู้ในการใช้เครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๒.๓.๑ ให้ความรู้แก่ข้าราชการตำรวจและหน่วยงานผ่านช่องทางต่าง ๆ เช่น Website, หนังสือเวียน เป็นต้น

๒.๓.๒ ใส่กุญแจตู้อุปกรณ์เครือข่าย เพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่ หรือบุคลากรที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

ขั้นตอนการปฏิบัติในมาตรการที่สำคัญ

๑. การสำรองข้อมูล(Back up)

๑.๑ การสำรองข้อมูลอัตโนมัติโดยระบบเครื่องประมวลผลแม่ข่าย โดยสำรองข้อมูลไว้ในสื่อบันทึก ๑ ชุด

๑.๒ การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตาม ระยะเวลาที่กำหนดเป็นประจำทุกสัปดาห์ โดยสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในสื่อบันทึก

๒. การกู้ข้อมูล(Recovery)

๒.๑ ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูลที่ได้สำรองไว้ในสื่อบันทก ทุกสัปดาห์

๒.๒ ทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้สำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสีย ทุกสัปดาห์

ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๑.กรณีเครื่องลูกข่าย

๑.๑ ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบเทคโนโลยีสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือดูแลทราบ หรือกรณีเหตุอันทำให้เจ้าหน้าที่ผู้เกี่ยวข้องไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานสังกัดทราบ

๑.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ดึงสายเชื่อมโยงระบบเครือข่าย(LAN) ออกจากเครื่องโดยเร็ว

๑.๓ ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง ให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๑.๔ ให้เจ้าหน้าที่ที่เกี่ยวข้อง แจ้งเหตุขัดข้องนั้นให้หัวหน้า หรือผู้บังคับบัญชาทราบโดยเร็ว

๒. กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

๒.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๒.๒ ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๒.๓ ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๒.๔ รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๒.๕ ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ Sever และระบบ เครือข่ายโดยเร็วที่สุด

๒.๖ ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบ นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๒.๗ ผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

๓. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการ ดังนี้

๓.๑ เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้น ๆ ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

๓.๒ สแกนและกำจัดไวรัส หรือกักไวรัส(Quarantine) ด้วยโปรแกรมป้องกันไวรัส

๓.๓ แจ้งเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อตรวจสอบ

๔. หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัยเพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้อย่างถูกต้อง เมื่อเกิดอัคคีภัย จึงกำหนดหลักปฏิบัติ ดังนี้

๔.๑ ไม่กระทำการใด ๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

๔.๒ ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

๔.๓ ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉิน มิให้ปิดตายหรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉิน เพื่อให้ไปถึงทางได้ แม้ว่าไฟดับหรือปกคลุมไปด้วยควัน

๔.๔ เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้ จากนั้นออกจากอาคารแล้วแจ้งหน่วยดับเพลิงทันที

๔.๕ เมื่อได้ยินเสียงสัญญาณเตือนไฟไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

๔.๖ หากเพลิงไหม้ในห้องทำงาน ให้ออกจากห้อง ปิดประตู แล้วแจ้งฝ่ายอาคารและ สถานที่เพื่อแจ้งหน่วยดับเพลิงทันที

๔.๗ หากเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนออกจากอาคารให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อย ๆ เปิดประตู แล้วไปยังทางหนีไฟฉุกเฉินที่ใกล้ที่สุด

๔.๘ หากเพลิงไหม้อยู่บริเวณใกล้ประตู จะมีความร้อน ห้ามเปิดประตูโดยเด็ดขาด ให้รีบแจ้งหน่วยดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเพลิงไหม้ หากผ้าเปียก ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

๔.๙ เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

๔.๑๐ ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

๕. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับส่งมาก ดังนั้น สิ่งที่มักจะเกิดขึ้นและยากต่อการหลีกเลี่ยงคือ ผลกระทบต่าง ๆ ที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลสำคัญ รวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ประกอบด้วย

๕.๑ เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ(UPS) ตลอดระยะเวลาเปิดใช้งานทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

๕.๒ เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม

การคืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ 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 ระบบอื่น ๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบ

๑. ระดับนโยบาย

รองผู้บังคับการตำรวจภูธรจังหวัดพิจิตร(ฝ่ายบริหาร)ซึ่งเป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ของตำรวจภูธรจังหวัดพิจิตร รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจน ติดตาม กำกับดูแล ควบคุมการตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

๒. ระดับปฏิบัติ

สารวัตรฝ่ายอำนวยการ ๒ ตำรวจภูธรจังหวัดพิจิตร รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการ หรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้

ร.ต.อ. ผู้เสนอแผน

(วสุเทพ ใจอินทร์)

สว.ฝอ.ภ.จว.พิจิตร

พล.ต.ต. ผู้อนุมัติแผน

(กฤษณะ ศิริปิยะวัฒน์)

ผบก.ภ.จว.พิจิตร