
# แผนป้องกันและแก้ไขปัญหาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของ ตำรวจภูธรภาค ๖ ประจำปีงบประมาณ พ.ศ.๒๕๖๑-๒๕๖๕

ฝ่ายอำนวยการ ๖ กองบังคับการอำนวยการ
ตำรวจภูธรภาค ๖

# คำนำ

ในปัจจุบันระบบเทคโนโลยีสารสนเทศได้มีการพัฒนาและเผยแพร่ข้อมูลข่าวสารอย่างรวดเร็ว และเป็นการสื่อสารแบบสองทิศทาง อีกทั้งยังมีความสำคัญอย่างยิ่งต่อการบริหารระบบราชการ ซึ่งฝ่ายอำนวยการ ๖ กองบังคับการอำนวยการตำรวจภูธรภาค ๖ เป็นศูนย์กลางในการเก็บรวบรวมข้อมูลต่างๆ ด้วยระบบคอมพิวเตอร์ ในการดำเนินงานและรักษาความปลอดภัยของระบบข้อมูล ได้ตระหนักถึงการดูแลรักษาระบบสารสนเทศของหน่วยให้มีความมั่นคงปลอดภัยและลดความเสี่ยงต่างๆ ที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนั้นเพื่อให้ระบบสารสนเทศของตำรวจภูธรภาค ๖ สามารถใช้งานได้อย่างมีประสิทธิภาพและประสิทธิผล จึงได้จัดทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน (Information Technology Contingency Plan) ของตำรวจภูธรภาค ๖ ประจำปีงบประมาณ พ.ศ.๒๕๖๑-๒๕๖๕ ขึ้น เพื่อใช้เป็นกรอบแนวทางในการบำรุงรักษาป้องกัน และแก้ไขปัญหาที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงานในสังกัดต่อไป

ฝ่ายอำนวยการ ๖ กองบังคับการอำนวยการ
ตำรวจภูธรภาค ๖

# สารบัญ

# แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน
# (IT Contingency Plan) ของตำรวจภูธรภาค ๖
# ปีงบประมาณ พ.ศ.๒๕๖๑-๒๕๖๕

**หลักการและเหตุผล**

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการปฏิบัติงานราชการ ทั้งในส่วนของการบริหารจัดการ การจัดเก็บและรวบรวมข้อมูล รวมไปถึงการประมวลผลระบบงานที่สำคัญ ซึ่งข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากรในหน่วยงานตำรวจภูธรภาค ๖ ได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์ต่างๆ เสียหายได้

ตำรวจภูธรภาค ๖ จึงได้ทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) ของตำรวจภูธรภาค ๖ ปีงบประมาณ พ.ศ.๒๕๖๑-๒๕๖๕ เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศรวมถึงระบบอุปกรณ์ต่างๆ

**วัตถุประสงค์**

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
๒. เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบการบริหารจัดการข้อมูลสารสนเทศ รวมทั้งเป็นการเผยแพร่ความรู้เกี่ยวกับการแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศให้ผู้ที่เกี่ยวข้องได้นำไปใช้ประโยชน์
๓. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร
๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์กร
๕. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ
๖. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

**ภัยพิบัติ**

ภัยที่เกิดจากธรรมชาติและจากการกระทำของมนุษย์ที่มีระดับความรุนแรงและผลกระทบที่ต่างกันไป ซึ่งอาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของตำรวจภูธรภาค ๖ สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

๑. ภัยพิบัติจากภายนอก...

**๑. ภัยพิบัติจากภายนอก**

๑.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ แผ่นดินไหว

๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดแย้ง

๑.๔ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๑.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๑.๖ ไวรัสคอมพิวเตอร์

๑.๗ ระบบเสียหายจากภัยสงคราม เหตุจลาจล การประท้วงและการเกิดสถานการณ์ความไม่สงบ

**๒. ภัยพิบัติจากภายใน**

๒.๑ ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๒.๓ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดการทำงาน

## <u>แนวทางการป้องกันความเสียหายจากภัยพิบัติ</u>

**๑. ภัยพิบัติจากภายนอก**

**๑.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย** ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ แผ่นดินไหว

๑.๑.๑ <u>การป้องกันและการดำเนินการอัคคีภัย</u>

(๑) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่างๆ

(๒) ประชาสัมพันธ์แผนป้องกันและระงับอัคคีภัย การหนีไฟขั้นต้นให้แก่ข้าราชการตำรวจทุกราย

(๓) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย

(๔) จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

(๕) ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๑.๑.๒ <u>การป้องกันอุทกภัย</u>...

๑.๑.๒ <u>การป้องกันอุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม</u>

(๑) เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น สำหรับเครื่องแม่ข่ายตลอด ๒๔ ชั่วโมง และตรวจสอบการทำงานให้ใช้งานได้อย่างสม่ำเสมอ

(๒) ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

(๓) เครื่องคอมพิวเตอร์แม่ข่ายต้องไม่อยู่ในบริเวณที่น้ำท่วมถึง

(๔) ตรวจสอบข้อมูลเรื่องน้ำท่วมที่เคยเกิดในละแวกพื้นที่ใกล้เคียง เพื่อคาดการณ์และเตรียมตัวได้ถูก

(๕) บันทึกหมายเลขโทรศัพท์สำหรับเหตุฉุกเฉิน

(๖) เก็บของมีค่าไว้ในที่ปลอดภัย และบันทึกรายการทรัพย์สินหรือถ่ายรูปไว้เป็นหลักฐาน

๑.๑.๓ <u>การป้องกันและการดำเนินการแผ่นดินไหว</u>

(๑) ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย

(๒) สังเกตพฤติกรรมของสัตว์ ซึ่งสัตว์หลายชนิดจะมีการรับรู้ ท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้า เช่น หนู งู สุนัข แมลงสาบ เป็นต้น

(๓) จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย

**๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล**

๑.๒.๑ ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำเข้าไป

๑.๒.๒ จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่ายมีการตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

**๑.๓ ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง**

๑.๓.๑ การตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ตลอดเวลา

๑.๓.๒ ต้องจัดให้มีเครือข่ายสำรอง สำหรับใช้ในกรณีที่เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้

**๑.๔ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ**

๑.๔.๑ แยกไฟระบบคอมพิวเตอร์แม่ข่ายออกจากสายไฟหลักที่ผ่านสะพานไฟเข้าสู่หน่วยงาน

๑.๔.๒ ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์

๑.๔.๓ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ

๑.๔.๔ เมื่อเกิด...

๑.๔.๔ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้บันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์รวมทั้งอุปกรณ์ต่างๆ

๑.๔.๕ ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

**๑.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล**

๑.๕.๑ สแกนหาจุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยใช้ซอฟท์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

๑.๕.๒ ติดตั้ง Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

๑.๕.๓ จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๑.๕.๔ ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ

๑.๕.๕ กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต ดังนี้

(๑) ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น

(๒) เปลี่ยนรหัสผ่านโดยทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๓) ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

(๔) เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(๕) เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

(๖) ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เช่น บันทึกไว้ในหน้าจอล็อกอิน

(๗) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

**๑.๖ ไวรัสคอมพิวเตอร์**

๑.๖.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๑.๖.๒ ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

(๑) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

(๒) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

(๓) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๑.๖.๓ ใช้ความ...

๑.๖.๓ ใช้ความระมัดระวังในการเปิด E-mail

(๑) ไม่เปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา

(๒) ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๑.๖.๔ ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต

(๑) ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ

(๒) ไม่ควรเปิด website ที่แนะนำมาทาง E-mail

(๓) ไม่ดาวน์โหลดไฟล์จาก website ที่ไม่น่าเชื่อถือ

(๔) ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ

(๕) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

**๑.๗ ระบบเสียหายจากภัยสงคราม/เหตุจลาจล การประท้วงและการเกิดสถานการณ์ความไม่สงบ**

เนื่องจากเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ ในการป้องกันหากไม่สามารถย้ายสถานที่หรือป้องกันสถานที่ได้ ควรมีการ Back Up ข้อมูลไว้มากกว่า ๑ Back Up และแยกสถานที่จัดเก็บ และถ้าเกิดความเสียหายเกิดขึ้นกับข้อมูล ก็สามารถนำข้อมูลที่มีการ Back Up ไว้ และอุปกรณ์คอมพิวเตอร์ สำรองมาใช้แทน หากเกิดความเสียหายร้ายแรงควรมีศูนย์คอมพิวเตอร์สำรองเพิ่ม

**๒. ภัยพิบัติจากภายใน**

**๒.๑ ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย**

๒.๑.๑ การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน

๒.๑.๒ การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนดทุกสัปดาห์ โดยจะสำรองข้อมูลโครงสร้างข้อมูล 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 ข้าราชการตำรวจ...

**๒.๓ ข้าราชการตำรวจขาดความรู้ในการใช้เครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน**

๒.๓.๑ ให้ความรู้แก่ข้าราชการตำรวจและหน่วยงานผ่านช่องทางต่างๆ เช่น website, หนังสือเวียน เป็นต้น

๒.๓.๒ ใส่กุญแจปิดประตูห้อง Server เพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่ หรือบุคลากรที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

## ขั้นตอนปฏิบัติในมาตรการที่สำคัญ

**๑. การสำรองข้อมูล (Back Up)**

การสำรองข้อมูลมีวัตถุประสงค์เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ ดังนี้

๑.๑ การสำรองข้อมูลอัตโนมัติโดยระบบเครื่องประมวลผลแม่ข่าย โดยสำรองข้อมูลไว้ในสื่อบันทึก ๑ ชุด

๑.๒ การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตาม ระยะเวลาที่กำหนดเป็นประจำทุกสัปดาห์ โดยสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในสื่อบันทึก

**๒. การกู้ข้อมูล (Recovery)**

โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) และอุปกรณ์กระจายสัญญาณ (Switching & HUB) ต้องอยู่ในสภาพพร้อมใช้งาน และรองรับการให้บริการเครื่องลูกข่ายได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ จำเป็นต้องกู้ระบบคืนให้เร็วที่สุดเท่าที่จะทำได้ ซึ่งเป็นวิธีการที่ทำให้ระบบทำงานของเครื่องคอมพิวเตอร์และฐานข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยกำหนดให้เจ้าหน้าที่เทคโนโลยีสารสนเทศ ฝ่ายอำนวยการ ๖ กองบังคับการอำนวยการตำรวจภูธรภาค ๖ ดำเนินการดังนี้

๒.๑ ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูลที่ได้สำรองไว้ในสื่อบันทึกทุกสัปดาห์

๒.๒ ทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้สำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียทุกสัปดาห์

**ขั้นตอนการแก้ไขปัญหา**

๑. ทำการ Recovery เมื่อทราบว่าระบบเสียหายหรือหยุดทำงาน ข้อมูลที่ต้อง Recovery ทันที คือ

- ฐานข้อมูลระบบรายงานผลการดำเนินงานตามแผนยุทธศาสตร์ และแผนปฏิบัติราชการ
- ระบบประมวลผลเผยแพร่ข้อมูลข่าวสารและสารสนเทศ
- ฐานข้อมูลเพื่อการบริหารงานภายใน (Back Office) ได้แก่ ฐานข้อมูลระบบเอกสารอิเล็กทรอนิกส์ (E-cop/new) , โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Anti Virus) , โปรแกรมระบบปฏิบัติการการจัดการเครือข่าย (Network Software) และเว็บไซต์ของตำรวจภูธรภาค ๖ และทุกหน่วยในสังกัด

๒. กรณีไม่สามารถ...

๒. กรณีไม่สามารถดำเนินการได้เอง ให้ใช้ทีมกู้ระบบจากภายนอก เช่น จ้างผู้ให้บริการแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ กู้ระบบกลับคืนโดยเร็ว โดยนำ BACKUP TAPE / CD-ROM / HARDDISK ที่สำรองข้อมูลไว้กลับมา

## ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

**๑. กรณีเครื่องลูกข่าย**

๑.๑ ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบเทคโนโลยีสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้องหรือดูแลทราบ หรือ กรณีมีเหตุอันทำให้เจ้าหน้าที่ผู้เกี่ยวข้องไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

๑.๒ กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ดึงสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องโดยเร็ว

๑.๓ ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง ให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๑.๔ ให้เจ้าหน้าที่ที่เกี่ยวข้อง แจ้งเหตุขัดข้องนั้นให้ผู้บังคับบัญชาทราบโดยเร็ว

**๒. กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย**

๒.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒.๒ ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๒.๓ ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๒.๔ รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๒.๕ ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ Server และระบบเครือข่ายโดยเร็วที่สุด เช่น บริษัท ทีโอที จำกัดมหาชน หรือศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานตำรวจแห่งชาติ

๒.๖ ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง

๒.๗ ตรวจสอบอุปกรณ์ภายนอกต่างๆ เช่น เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์กระจายสัญญาณ ปลั๊กไฟฟ้า เช่น เครื่องยังทำงานอยู่หรือไม่ ปุ่มทำงานปิดหรือเปิดอยู่ ปลั๊กไฟฟ้า สาย Lan หลุดหลวมหรือไม่ แล้วแก้ไขตามจุด

๒.๘ ตรวจสอบการเชื่อมต่อของสัญญาณเครือข่ายว่ารับสัญญาณและกระจายสัญญาณออกไปได้หรือไม่ โดยใช้คำสั่ง ping ตามด้วยเลข IP

๒.๙ ทำการ restart ปิดสวิตซ์การทำงานของอุปกรณ์ไว้สักครู่ และเปิดใหม่

๒.๑๐ ผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

๓. กรณีเครื่อง...

**๓. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ให้ดำเนินการ ดังนี้**

๓.๑ เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆ ดึงสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

๓.๒ สแกนและกำจัดไวรัสหรือกักไวรัส (Quarantine) ด้วยโปรแกรมป้องกันไวรัส

๓.๓ แจ้งเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อตรวจสอบ

**๔. หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัยเพื่อป้องกันมิให้เกิดอัคคีภัยในอาคาร และบุคลากรสามารถปฏิบัติตนได้ถูกต้อง เมื่อเกิดอัคคีภัย** จึงกำหนดหลักปฏิบัติ ดังนี้

๔.๑ ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

๔.๒ ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

๔.๓ ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบทางออกฉุกเฉิน มิให้ปิดตายหรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเอง ไปยังทางออกฉุกเฉิน เพื่อให้ไปถึงทางได้ แม้ว่าไฟดับหรือปกคลุมไปด้วยควัน

๔.๔ เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้จากนั้นออกจากอาคารแล้วแจ้งหน่วยดับเพลิงทันที

๔.๕ เมื่อได้ยินเสียงสัญญาณเตือนเพลิงไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

๔.๖ หากเพลิงไหม้ในห้องทำงานให้ออกจากห้อง ปิดประตู แล้วแจ้งเจ้าหน้าที่รักษาความปลอดภัย (รปภ.ภ.๖) เพื่อแจ้งหน่วยดับเพลิงทันที

๔.๗ หากเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนออกจากอาคารให้วางมือบนประตู หาก ประตูมีความเย็นอยู่ ค่อยๆ เปิดประตู แล้วไปยังทางหนีไฟฉุกเฉินที่ใกล้ที่สุด

๔.๘ หากเพลิงไหม้อยู่บริเวณใกล้ประตู จะมีความร้อน ห้ามเปิดประตูโดยเด็ดขาด ให้รีบแจ้งหน่วยดับเพลิง และแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเพลิงไหม้ หาผ้าเปียก ปิดทางเข้าของควัน ปิดพัดลม และเครื่องปรับอากาศ ส่งสัญญาณขอความช่วยเหลือที่หน้าต่าง

๔.๙ เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

๔.๑๐ ห้ามใช้ลิฟต์ขณะเกิดเพลิงไหม้

๔.๑๑ ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔.๑๒ ปิดสวิตซ์อุปกรณ์ และถอดปลั๊กไฟฟ้าออก เพื่อตัดระบบการจ่ายไฟ พร้อมทั้งรีบขนย้ายอุปกรณ์คอมพิวเตอร์ ไปไว้ในที่ปลอดภัย

๔.๑๓ ตรวจสอบความเสียหายและจัดทำบัญชีอุปกรณ์คอมพิวเตอร์ทุกอย่างไว้ แล้วรายงานผู้บังคับบัญชาทราบโดยเร็ว

**๕. ระบบป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้า**

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้าที่ได้รับส่งมาก ดังนั้น สิ่งที่มักจะเกิดขึ้นและยากต่อการหลีกเลี่ยงคือ ผลกระทบต่างๆ ที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลสำคัญ รวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า ประกอบด้วย

๕.๑ เปิดใช้งาน...

๕.๑ เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาเปิดใช้งานทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

๕.๒ เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

**๖. การป้องกันน้ำท่วม**

๖.๑ เตรียมอุปกรณ์สื่อสาร สำรองแบตเตอรี่โทรศัพท์ ไฟฉายพร้อมถ่าน กรณีฉุกเฉินให้ใช้วิทยุสื่อสารคลื่นความถี่หลัก

๖.๒ ย้ายสิ่งของขึ้นที่สูง ส่วนของใช้ขนาดใหญ่ หาอิฐหรือไม่หนุนให้สูงขึ้นจากพื้น

๖.๓ ปิดอุปกรณ์ไฟฟ้าทุกชนิดภายในอาคาร ตัดระบบไฟฟ้า ห้ามสัมผัสเครื่องใช้ไฟฟ้า

๖.๔ ระวังสัตว์อันตรายที่มากับน้ำ เช่น งู ตะขาบ

๖.๕ เดินอย่างระมัดระวัง เนื่องจากอาจมีอันตรายจากโคลนที่ทำให้ลื่น หรือเศษวัสดุของมีคมที่ลอยมากับน้ำ

๖.๖ ห้ามบริโภคทุกอย่างที่สัมผัสกับน้ำ

๖.๗ ห้ามเดินตามเส้นทางที่น้ำไหล เนื่องจากกระแสน้ำแรงอาจพัดพาไปได้ หากจำเป็นต้องเดินผ่านที่น้ำไหลให้ลองใช้ไม้จุ่มเพื่อวัดระดับน้ำก่อนทุกครั้ง

๖.๘ ห้ามขับรถในพื้นที่ที่กำลังเกิดน้ำท่วม

๖.๙ ห้ามเข้าใกล้อุปกรณ์ไฟฟ้า เสาไฟฟ้า สายไฟฟ้า เนื่องจากหากมีไฟฟ้ารั่ว อาจถูกไฟดูดได้

๖.๑๐ รายงานให้ผู้บังคับบัญชาทราบโดยเร็ว

๖.๑๑ ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

**๗. การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น และการเตรียมความพร้อม กรณีเกิดแผ่นดินไหว**

๗.๑ เตรียมไฟฉาย อุปกรณ์ยังชีพ เช่น ยารักษาโรค

๗.๒ ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง

๗.๓ มีการประสานงานกับหน่วยกู้ภัย เมื่อเกิดแผ่นดินไหว

๗.๔ สำรวจสถานที่อพยพที่ปลอดภัย

๗.๕ จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและสิ่งของที่จำเป็น

๗.๖ รายงานให้ผู้บังคับบัญชาทราบโดยเร็ว

๗.๗ ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

## <u>แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม</u>

การคืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑. จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน

๒. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง

๔. นำสื่อที่ได้...

๔. นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็วภายใน ๔๘ ชั่วโมง

๕. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่นๆ ที่เกี่ยวข้อง

**ผู้รับผิดชอบ**

**๑. ระดับนโยบาย**

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

**๒. ระดับปฏิบัติ**

เจ้าหน้าที่ผู้ดูแลระบบของหน่วย รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

**การติดตามและรายงานผล**

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็น ประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณี ตามที่ระบุไว้

พ.ต.อ. ผู้เสนอแผน
(สารนัย คงเมือง)
รอง ผบก.ฯ รรท.ผบก.อก.ภ.๖

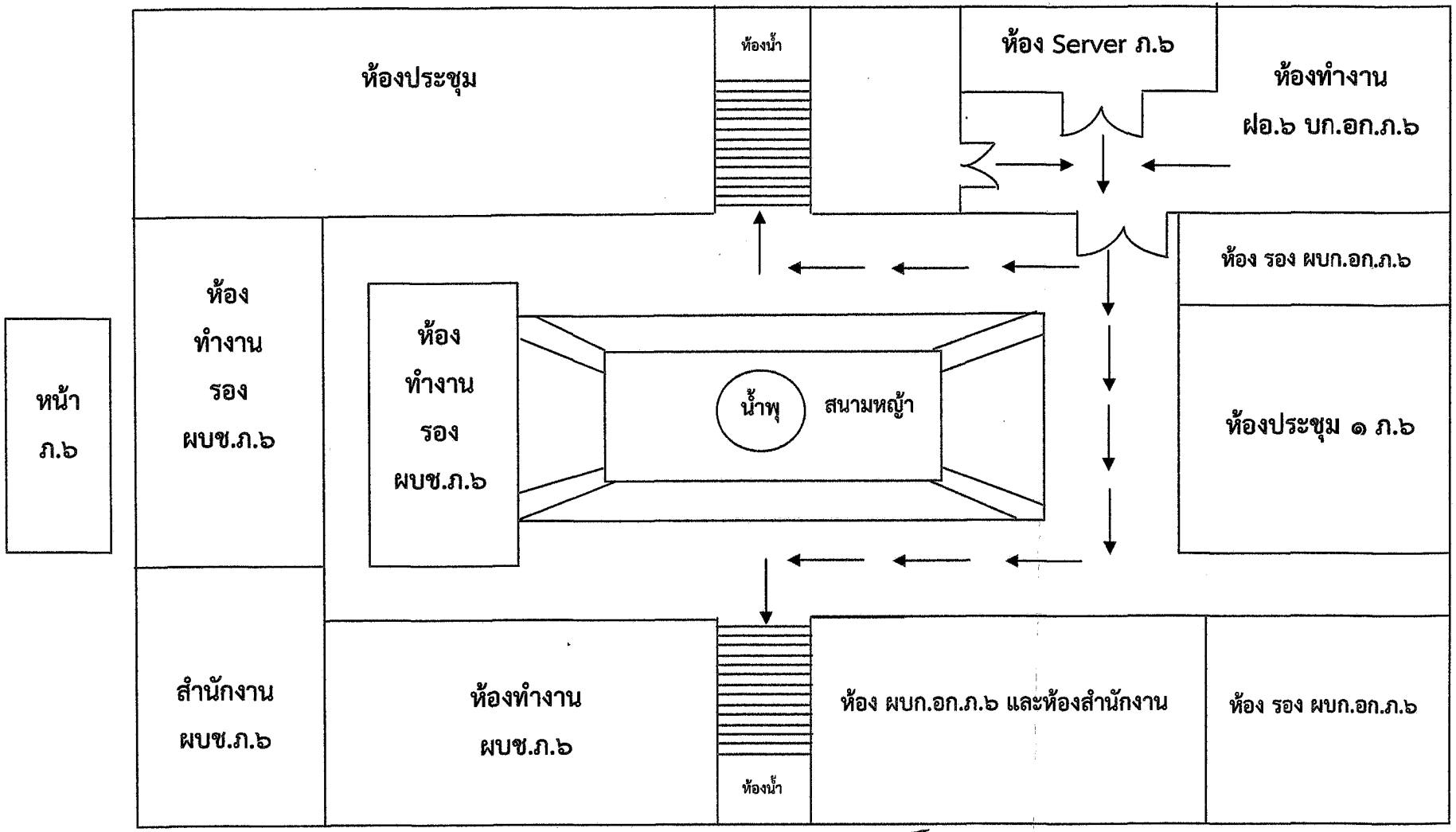
พล.ต.ต. ผู้เห็นชอบแผน
(วันชัย สุวรรณศิริเขต)
รอง ผบช.ภ.๖/CIO ของ ภ.๖

พล.ต.ท. ผู้อนุมัติแผน
(ทวิชชาติ พละศักดิ์)
ผบช.ภ.๖

**ผนวก ก.**

# แผนผังขนย้ายอุปกรณ์ระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน

(บริเวณอาคาร ภ.๖ ชั้น ๒)




ตรวจแล้วถูกต้อง

พ.ต.อ

(ไพฑูรย์ สุขุมวัฒนะ)

ผกก.ฝอ.๖ บก.อก.ภ.๖