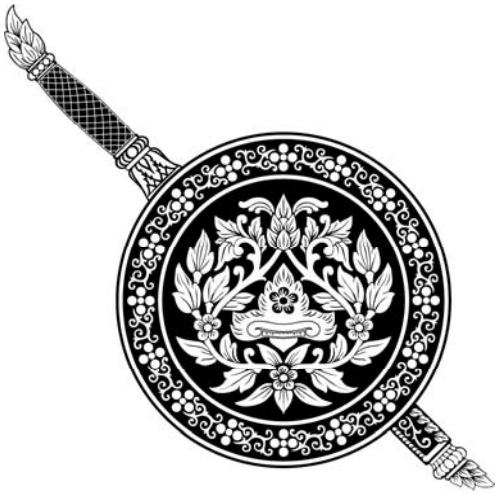

แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ
เมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan)
ของตำรวจภูธรจังหวัดสกลนคร
ปีงบประมาณ พ.ศ.๒๕๕๗-๒๕๕๘

งานเทคโนโลยีสารสนเทศ
ตำรวจภูธรจังหวัดสกลนคร

คำนำ

ตำรวจภูธรจังหวัดสกลนคร ได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่มีความสำคัญยิ่งต่อการบริหารระบบราชการ จำเป็นต้องได้รับการดูแลรักษาให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา ดังนั้น เพื่อลดความเสี่ยงต่าง ๆ อันอาจจะเกิดขึ้นกับระบบสารสนเทศจึงได้จัดทำแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการบำรุงรักษาและป้องกันแก้ไขปัญหาอันอาจส่งผลกระทบต่อข้อมูลและสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ โปรแกรมระบบฐานข้อมูล ระบบเครือข่ายของตำรวจภูธรจังหวัดสกลนคร

งานเทคโนโลยีสารสนเทศ
ตำรวจภูธรจังหวัดสกลนคร

แผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

๑. <u>หลักการและเหตุผล</u>

ตำรวจภูธรจังหวัดสกลนคร ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงาน และให้บริการประชาชนให้ได้รับความสะดวก ในขณะเดียวกัน ระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ส่งผลกระทบต่อการดำเนินงานของตำรวจภูธรจังหวัดสกลนคร ตำรวจภูธรภาค ๔ และสำนักงานตำรวจแห่งชาติ

เพื่อป้องกันและแก้ไขปัญหาดังกล่าว ตำรวจภูธรจังวัดสกลนคร โดยงานเทคโนโลยีสารสนเทศ ตำรวจภูธรจังหวัดสกลนคร จึงได้จัดทำแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) ของตำรวจภูธรจังหวัดสกลนคร ประจำปีงบประมาณ พ.ศ.๒๕๕๗ - ๒๕๕๘ เป็นกรอบแนวทางในดูแลรักษาระบบฯ ให้สามารถใช้งานได้อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด

๒. <u>วัตถุประสงค์</u>

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๕ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของตำรวจภูธรจังหวัดสกลนคร ตำรวจภูธรภาค ๔ และสำนักงานตำรวจแห่งชาติ

๓. <u>การประเมินสถานการณ์ความเสี่ยง</u>

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศ ของตำรวจภูธรจังหวัดสกลนคร พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

๓.๑ เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศ ในเบื้องต้น จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรม สัมมนา ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด

๓.๒ เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้

๑) ติดตั้ง firewall ทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องให้บริการ(server) และเครื่องลูกข่าย(client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย

๒) แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านเครือข่าย internet รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากไวรัสต่างๆ ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

๓.๓ เกิดจากระบบไฟฟ้าขัดข้อง หรือความเสียหายจากเพลิงไหม้ โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (server) ในกรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บ และสำรองข้อมูลไว้อย่างปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงมีระบบควบคุม ป้องกันเพลิงไหม้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามจุดต่างๆในอาคารและทำป้ายบอกจุดติดตั้งเพื่อดับเพลิง

๓.๔ เกิดจากโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์ ในส่วนของห้องคอมพิวเตอร์แม่ข่าย ได้กำหนดห้ามผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออกสามารถใส่กุญแจเพื่อป้องกันไม่ให้บุคคลภายนอกเข้ามาในห้องควบคุมโดยไม่ได้รับอนุญาต ในอนาคตคาดว่าจะมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๔. <u>การเตรียมการเบื้องต้น</u>

๔.๑ การสำรองข้อมูล (Back up) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย หรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยมีแนวทาง โดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่าย และการสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลเป็นประจำทุกสัปดาห์

๔.๒ การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟแวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้ โดยมีวิธีการดังนี้

๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมป้องกันไวรัส
- อัพเดตข้อมูลไวรัส
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ ที่เชื่อมต่อทาง USB พอร์ต หรือแผ่นซีดี

- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จัก หรือน่าสงสัย
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๓) ใช้ความระมัดระวังในการเปิด E-mail

- อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- ลบ E-mail ทิ้งทันที่ถ้าไม่ทราบแหล่งที่มา

๔) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet

- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ
- ไม่ควรเข้าไปเปิด website ที่แนะนำมาทาง E-mail ที่ไม่ทราบแหล่งที่มา
- ไม่ ดาวน์โหลด ไฟล์ จาก website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๔.๓ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าได้ประมาณ ๒๐-๓๐ นาที

๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๔.๔ มีระบบป้องกันไฟไหม้ เนื่องจากยังขาดงบประมาณในการสนับสนุนการปรับปรุงห้องคอมพิวเตอร์แม่ข่าย จึงยังไม่มีระบบป้องกันไฟไหม้ที่เหมาะสม แต่ในเบื้องต้น มีอุปกรณ์ดับเพลิงติดตั้งในทุกอาคาร เพื่อการควบคุมเพลิงในเบื้องต้น

๔.๕ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

๑) มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป ที่ประตูเข้าออก มีการติดตั้งสายูและกุญแจล็อค ในอนาคตคาดว่าจะได้ติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๔) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๕) การเรียกใช้ระบบสารสนเทศจากหน่วยงานต่างๆ ทั้งในส่วนกลาง และส่วนภูมิภาค ผู้ใช้ระบบจะต้องมีการบันทึกชื่อผู้ใช้ (user name) และรหัสผ่าน (password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ตามสิทธิ์และอำนาจหน้าที่ความรับผิดชอบ

๖) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัย คุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๔.๖ การจัดเตรียมอุปกรณ์ที่จำเป็น ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

๑) แผ่นติดตั้งระบบปฏิบัติการ/ ระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ

๒) อุปกรณ์จัดเก็บข้อมูลและระบบงานที่สำคัญ

๓) แผ่นโปรแกรม antivirus/spyware

๔) แผ่น driver อุปกรณ์ต่างๆ

๕) ระบบสำรองไฟฉุกเฉิน

๖) อุปกรณ์สำรองต่างๆ (hardware) ของเครื่องคอมพิวเตอร์

๕. <u>มาตรการความปลอดภัยด้วยรหัสผ่าน</u>

มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบสารสนเทศ ไม่สามารถเข้าถึง แก้ไข เปลี่ยนแปลงข้อมูล หรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง โดย

๕.๑ กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ ให้แก้ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยวข้อง ผู้ที่รับผิดชอบสามารถเข้าในระบบได้ตามความรับผิดชอบ (Access) โดยมีลำดับขั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละระดับฐานข้อมูล ดังนี้

๑) บุคคลที่สามารถเรียกดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถแก้ไข ปรับปรุงข้อมูลได้

๒) บุคคลที่สามารถเรียกดูข้อมูลและแก้ไข ปรับปรุงข้อมูลในส่วนที่ผู้ใช้รับผิดชอบต่อความถูกต้องของข้อมูลในฐานข้อมูลนั้น

๓) บุคคลที่สามารถเรียกดู แก้ไข ปรับปรุงข้อมูลระดับฐานข้อมูล ในกรณีที่ผู้ใช้มีข้อผิดพลาดในการปรับปรุงข้อมูล ผู้รับผิดชอบของหน่วยงานเจ้าของหน่วยงานเป็นผู้ดูแล แก้ไข ข้อมูลในส่วนนี้ซึ่งการเข้าใช้ฐานข้อมูล ในแต่ละระบบ จะมีการกำหนดสิทธิการเข้าถึงฐานข้อมูล ตามหน้าที่ความรับผิดชอบของผู้ใช้ฐานข้อมูล เพื่อรักษาความปลอดภัยของฐานข้อมูล โดยมีการกำหนด Log in และ Password ในการเข้าถึงข้อมูลและผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงและเปลี่ยนแปลงแก้ไขข้อมูลได้ ผู้ใช้ระบบทั่วไปที่ผู้บังคับบัญชาที่เป็นหน่วยงานเจ้าของระบบ เป็นผู้อนุมัติให้ดำเนินการได้ โดยจะแบ่งเป็นการดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถเปลี่ยนแปลงแก้ไขได้ และการที่สามารถปรับปรุงข้อมูลได้ ทั้งนี้ เพื่อเป็นการรักษาความปลอดภัยของฐานข้อมูล

๕.๒ กำหนดระยะเวลาการใช้งานระบบสารสนเทศ ของผู้ใช้ระบบ (User) โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้ เมื่อพ้นระยะเวลาที่กำหนดไว้

๕.๓ การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า ๖ ตัวอักษร และควรใช้ ตัวเลข อักขระพิเศษประกอบและสำหรับผู้ใช้งานระบบสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน โดยการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรให้ซ้ำกับรหัสเดิมในครั้งสุดท้าย ซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ถ้ามีผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที เพื่อป้องกันความปลอดภัยของการใช้ระบบสารสนเทศ

๖. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๖.๑ กรณีเครื่องลูกข่าย

๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่ศูนย์ทราบ หรือกรณีมีเหตุอันทำให้ฝ่ายเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ฝ่ายเทคโนโลยีสารสนเทศ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย(สาย LAN) ออกจากเครื่องนั้นโดยเร็ว

๓) ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อกลุ่มงาน/หน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๖.๒ กรณีเครื่องบริการ (server) และอุปกรณ์เครือข่าย

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณา

ตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้ น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔) รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๕) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๖) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗) ผู้ดูแลระบบ ต้องรีบรายงานบังคับบัญชาตามลำดับชั้นจนถึงผู้บังคับการตำรวจภูธรจังหวัดอุดรธานี ทราบโดยเร็ว

๖.๓ กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

๑) ติดตั้งโปรแกรม Anti-virus

๒) ใช้งานโปรแกรม Anti-virus

๖.๔ กรณีเครื่องคอมพิวเตอร์ลูกข่ายที่ใช้งานระบบ POLIS ไม่ได้ ให้โทรศัพท์แจ้งศูนย์ Hotline ของบริษัท ทีโอที จำกัด (มหาชน)

๖.๕ กรณีเมนบอร์ดหรือฮาร์ดดิสก์

กรณีเมนบอร์ดเสียหาย

๑) ทำการจัดหา เมนบอร์ด Main board หรือ Mather board มาเปลี่ยน (อาจใช้วิธีการพิเศษในการจัดหามาก่อนแล้วจัดซื้อตามที่หลัง) จากนั้นถอด เมนบอร์ดเดิมที่ชำรุดออกแล้วติดตั้งเมนบอร์ดใหม่แทน แล้วทำการบูตระบบใช้งานตามปกติ

กรณีฮาร์ดดิสค์เสียหาย

๑) จัดหาฮาร์ดดิสค์มาเปลี่ยน

๒) ติดตั้งระบบปฏิบัติการ และระบบเครือข่าย

๓) นำ BACKUP ที่ได้จัดทำไว้จาก มาทำ RECOVER เพื่อนำข้อมูลเดิมกลับมาใช้เหมือนเดิม

๔) ทำการรันเครื่องทำงานตามเดิม

๗. <u>แผนทำระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม</u>

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติ ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๕) นำ BACKUP ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยเจ้าหน้าที่กู้ระบบ และ/หรือ ทีมงานจากบริษัทฯ ที่จัดจ้างบำรุงรักษาระบบสารสนเทศ (ถ้ามี) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๖) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

๘. <u>ผู้รับผิดชอบ</u>

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

๘.๑ ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

๘.๑.๑ รองผู้บังคับการตำรวจภูธรจังหวัดสกลนคร ที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ (CIO)

๘.๑.๒ ผู้กำกับการฝ่ายอำนวยการ ตำรวจภูธรจังหวัดสกลนคร

๘.๒ ระดับปฏิบัติ

๘.๒.๑ สารวัตร และรองสารวัตรฝ่ายอำนวยการ ตำรวจภูธรจังหวัดสกลนคร ที่รับผิดชอบงานเทคโนโลยีสารสนเทศ

รับผิดชอบ กำกับดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษาทบทวนวางแผน ติดตาม การบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ ตำรวจภูธรจังหวัดสกลนคร

๘.๒.๒ เจ้าหน้าที่ผู้รับผิดชอบงานเทคโนโลยีสารสนเทศตำรวจภูธรจังหวัดสกลนคร ทุกนาย

รับผิดชอบดูแลบำรุงรักษา ระบบเครื่อง ระบบเครือข่าย และระบบความปลอดภัยทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่างๆ ของระบบคอมพิวเตอร์และระบบเครือข่าย ตลอดจนรักษาความปลอดภัยของระบบฐานข้อมูล รวมทั้งการทำสำเนาฐานข้อมูล

๙. <u>การติดตามและรายงาน</u>

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบ รายงานผลการดำเนินการ หรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหา ตลอดจนผลการแก้ไขปัญหาให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้

๑๐. <u>ผู้เสนอ/อนุมัติแผน</u>

พ.ต.อ. ผู้เสนอแผน
(บุญเลิศ ราชพรหมมา)
ผกก.ฝอ.ภ.จว.สกลนคร

พ.ต.อ. ผู้อนุมัติแผน
(ธนันท์ชัย สุขา)
รอง ผบก.ฯ ปรท.ผบก ภ.จว.สกลนคร