แผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ จังหวัดมุกดาหาร (IT Contingency Plan) ประจำปีงบประมาณ พ.ศ. ๒๕๖๑ - ๒๕๖๔

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
สำนักงานจังหวัดมุกดาหาร
โทร. ๐-๔๒๖๑-๑๓๓๐ มท. ๔๙๐๒๔

แผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศจังหวัดมุกดาหาร
ประจำปีงบประมาณ พ.ศ.๒๕๖๑ - ๒๕๖๔

---

๑. หลักการและเหตุผล

ปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการปฏิบัติงานราชการ ทั้งในส่วนของการบริหารจัดการ การจัดเก็บและรวบรวมข้อมูล รวมไปถึงการประมวลผลระบบงานที่สำคัญ จังหวัดมุกดาหารจึงได้ให้ความสำคัญกับการป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ เพื่อวิเคราะห์ความเสี่ยงป้องกันการโจมตีทางไซเบอร์ โดยได้จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินให้ระบบใช้งานได้ตามปกติ เพื่อเป็นคู่มือให้กับส่วนราชการ/หน่วยงานที่เกี่ยวข้องในจังหวัดถือปฏิบัติ รวมทั้ง เป็นการสนับสนุนการนำข้อมูลไปใช้วิเคราะห์เพื่อการบริหารงานของผู้บริหารระดับจังหวัด

ปีงบประมาณ พ.ศ.๒๕๖๑ สำนักงาน ก.พ.ร. ได้กำหนดแนวทางการประเมินผู้บริหารองค์การ ประเด็นส่งเสริมการใช้ดิจิทัลและขีดความสามารถที่มีอยู่และพัฒนาขึ้นทุก ๖ เดือน โดยกำหนดให้มีการวิเคราะห์ความเสี่ยงป้องกันการโจมตีทางไซเบอร์ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินให้ระบบใช้งานได้ตามปกติ เป็นตัวชี้วัดสำหรับประเมินผู้บริหารองค์กร (ผู้ว่าราชการจังหวัด)

๒. นิยามศัพท์

๒.๑ การบริหารความเสี่ยง หมายถึง การบริหารจัดการและการเก็บรวบรวมข้อมูลอย่างเป็นระบบเพื่อไม่ให้ข้อมูลที่จัดเก็บเกิดการสูญหายอันเนื่องมาจากภัยพิบัติที่เกิดขึ้น

๒.๒ ภัยพิบัติ หมายถึง ภัยที่เกิดจากธรรมชาติและจากการกระทำของมนุษย์ที่มีระดับความรุนแรงและผลกระทบที่ต่างกันไป กล่าวคือ

๒.๒.๑ ภัยที่เกิดจากธรรมชาติ เป็นภัยที่เกิดจากสภาพทางภูมิศาสตร์และที่ตั้ง ได้แก่ อุทกภัย วาตภัย ภัยหนาว ภัยแล้ง ไฟป่า และแผ่นดินไหว เป็นต้น

๒.๒.๒ ภัยที่เกิดจากการกระทำของมนุษย์ เป็นภัยที่ปรากฏเป็นรูปธรรมและภัยที่เป็นนามธรรม ได้แก่ อัคคีภัย ภัยจากการคมนาคมขนส่ง ภัยจากการทำงาน ภัยจากสารเคมีและวัตถุอันตราย ภัยจากโรคระบาดสัตว์และพืช รวมทั้งภัยจากเทคโนโลยีสารสนเทศอื่นๆ

๓. วัตถุประสงค์

๓.๑ เพื่อเตรียมความพร้อมและสามารถรองรับสถานการณ์หรือภัยพิบัติฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศของจังหวัด

๓.๒ เพื่อให้มีแผนบริหารความเสี่ยงและแผนแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศที่สามารถควบคุมและลดผลกระทบจากความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓.๓ เพื่อเป็นแนวทางในการกำกับดูแล ตรวจสอบการบริหารจัดการข้อมูลสารสนเทศ รวมทั้งเป็นการเผยแพร่ความรู้เกี่ยวกับการบริหารความเสี่ยงและการแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศให้กับหน่วยงานที่เกี่ยวข้องนำไปใช้ประโยชน์

๓.๔ เพื่อให้การดำเนินงานเป็นไปตามตัวชี้วัดของสำนักงาน ก.พ.ร.

๓.๕ เพื่อให้เกิดการรับรู้ ตระหนักรู้ และเข้าใจถึงความเสี่ยงที่อาจจะเกิดขึ้น และวิธีการจัดการที่เหมาะสม

๔. สภาพปัญหาที่เกิดขึ้น

จากการประชุมคณะทำงานเพื่อทบทวนแผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านข้อมูลระบบสารสนเทศจังหวัดมุกดาหาร (พ.ศ.๒๕๖๑ - ๒๕๖๔) ครั้งที่ ๑/๒๕๖๑ เมื่อวันพฤหัสบดีที่ ๑๙ เมษายน ๒๕๖๑ เวลา ๑๐.๐๐ น. ณ ห้องประชุมดอกช้างน้าว ชั้น ๒ ศาลากลางจังหวัดมุกดาหาร คณะทำงานได้ร่วมกันวิเคราะห์สภาพปัญหาปัจจุบันที่เกิดขึ้นและวิธีการแก้ไขปัญหา สรุปดังนี้

๔.๑ หลายหน่วยงานมีสภาพปัญหาที่คล้ายคลึงกันคือปัญหาจากไวรัสคอมพิวเตอร์ที่ส่วนใหญ่มาจากการแลกเปลี่ยนข้อมูลผ่าน Handy Drive การเชื่อมต่ออินเตอร์เน็ต หรือการเปิดจดหมายอิเลกทรอนิกส์ที่มีไวรัสคอมพิวเตอร์แฝงเข้ามา ซึ่งแต่ละหน่วยได้มีวิธีการจัดการที่แตกต่างกันไป เช่น การติดตั้งโปรแกรมกำจัดไวรัส การตรวจสอบและควบคุมการเข้าใช้งานโดยการล็อกอินเข้าสู่ระบบ และการจำกัดสิทธิ์การใช้งานโปรแกรมบางประเภท เช่น โปรแกรมดาวน์โหลด (Bit Load) เป็นต้น

๔.๒ มีการสำรองข้อมูลอย่างสม่ำเสมอ เช่น สำรองข้อมูลโดยเจ้าหน้าที่ผู้ปฏิบัติงานในแต่ละวัน/สัปดาห์ สำรองข้อมูลไว้กับเครื่องแม่ข่าย และสำรองข้อมูลไว้ในระบบคลาวด์ (Cloud computing)

๔.๓ การตรวจสอบและดูแลรักษาอุปกรณ์และเครื่องคอมพิวเตอร์ ได้มีบางหน่วยงานที่มีการจ้างบริษัทที่ปรึกษาเข้ามาดูแลรับผิดชอบ แต่ส่วนใหญ่จะดำเนินการเองโดยการติดตั้งโปรแกรมป้องกัน/กำจัดไวรัสและได้ทำการปรับปรุงข้อมูล (Update) ให้เป็นปัจจุบันอยู่เสมอ รวมทั้ง การขอรับการสนับสนุนจากหน่วยงานข้างเคียงหากไม่สามารถดำเนินการได้

๕. การระบุความเสี่ยงและวิเคราะห์ความเสี่ยง

จากการพิจารณาและวิเคราะห์ความเสี่ยงด้านระบบข้อมูลสารสนเทศที่อาจจะเกิดขึ้น สามารถแยกความเสี่ยงด้านต่างๆ สรุปดังนี้

๕.๑ ความเสี่ยงที่เกิดจากภัยพิบัติทางธรรมชาติ เช่น วาตภัย และอุทกภัย

๕.๒ ความเสี่ยงที่เกิดจากการกระทำของมนุษย์ เช่น เกิดจากการปฏิบัติงาน กระแสไฟฟ้าขัดข้อง และอัคคีภัย

๕.๓ ความเสี่ยงที่เกิดจากโปรแกรมหรืออุปกรณ์คอมพิวเตอร์เช่น การโจมตีจากไวรัสคอมพิวเตอร์หรือการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ หรือการเคลื่อนย้ายอุปกรณ์หรือการติดตั้งอุปกรณ์ในจุดที่ไม่เหมาะสม เป็นต้น

๕.๔ ความเสี่ยงที่เกิดจากระบบเครือข่าย ทั้งระบบอินทราเน็ตและอินเทอร์เน็ต รวมถึงความเสี่ยงจากการบุกรุกเครือข่าย

๕.๕ ความเสี่ยงด้านระบบข้อมูลสารสนเทศ เช่น ข้อมูลถูกทำลายหรือมีการแก้ไขเปลี่ยนแปลง เป็นต้น

๖. หลักในการปฏิบัติ

๖.๑ เป้าหมายการปฏิบัติ

๖.๑.๑ ส่วนราชการ/หน่วยงานที่เกี่ยวข้องสามารถสนับสนุนและประสานการปฏิบัติด้านข้อมูลสารสนเทศอย่างเป็นระบบและรวดเร็ว

๖.๑.๒ สามารถป้องกันและลดความเสียหายที่อาจเกิดขึ้น ทั้งที่เป็นผลที่เกิดจากเหตุการณ์ภัยพิบัติโดยตรงและผลกระทบที่จะตามมาได้อย่างทันท่วงที

๖.๒ หลักการปฏิบัติ

๖.๒.๑ ความรวดเร็วในการแก้ไขปัญหา การประเมินสถานการณ์ในกรณีที่เกิดเหตุภัยพิบัติในเขตพื้นที่รับผิดชอบให้พิจารณาเหตุการณ์ว่าเป็นภัยพิบัติประเภทใดแล้วรายงานให้จังหวัดทราบทันที

๑) การสั่งการ เพื่อแก้ไขปัญหาให้หน่วยงานและบุคคลที่เกี่ยวข้องกับการปฏิบัติยึดถือการปฏิบัติงานโดยเคร่งครัดตามคำสั่งจังหวัด โดยจังหวัดจะจัดตั้งศูนย์ปฏิบัติการจังหวัดขึ้น เพื่อทำหน้าที่อำนวยการประสานการปฏิบัติ และมอบหมายให้หน่วยงาน/บุคคลดำเนินการแก้ไขปัญหา (แล้วแต่กรณี) และในกรณีที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทยเข้าควบคุมการปฏิบัติงานให้โอนอำนาจการสั่งการไปให้ผู้ที่ได้รับมอบหมายเพื่อสั่งการตามลำดับชั้นต่อไป

๒) ในกรณีศูนย์ปฏิบัติการจังหวัดพิจารณาเห็นว่าเหตุการณ์ที่เกิดขึ้นเกินขีดความสามารถในการดำเนินการ ให้ประสานขอรับการสนับสนุนจากหน่วยงานอื่นที่เกี่ยวข้องเข้าร่วมปฏิบัติการตามความจำเป็นและตามความเหมาะสม

๓) ในกรณีที่ไม่สามารถแก้ไขปัญหาได้ด้วยตนเองให้ศูนย์ปฏิบัติการจังหวัดประสานขอรับการสนับสนุนไปยังศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

๔) การติดต่อสื่อสารระหว่างศูนย์ปฏิบัติการจังหวัดกับหน่วยปฏิบัติและหน่วยร่วมปฏิบัติการในพื้นที่ให้เป็นไปตามแผนป้องกันภัยฝ่ายพลเรือนของจังหวัดมุกดาหาร

๕) เพื่อความสะดวกในการปฏิบัติงานให้กันประชาชนและผู้ที่ไม่เกี่ยวข้องออกจากบริเวณที่เกิดเหตุ เช่น กรณีอัคคีภัย เป็นต้น

๖.๒.๒ ในกรณีที่ปรากฏว่าภัยที่เกิดขึ้นเป็นภัยที่เกิดจากระบบเทคโนโลยี ให้ถือว่าการรักษาระบบข้อมูลสารสนเทศเพื่อการบริหารเป็นสิ่งสำคัญที่สุดและหากจำเป็นให้ทำการขนย้ายวัสดุอุปกรณ์และระบบข้อมูลสารสนเทศออกจากบริเวณเกิดภัย

๖.๒.๓ ความสม่ำเสมอในการตรวจสอบระบบ โปรแกรม Anti Virus และ Firewall

๖.๒.๔ ต้องใช้วัสดุอุปกรณ์ที่ได้มาตรฐานและกำหนดมาตรฐานในการควบคุมดูแลในกรณีที่มีการเก็บรักษาข้อมูลสารสนเทศที่อาจก่อให้เกิดผลกระทบต่อการดำเนินงานด้านข้อมูลสารสนเทศของจังหวัด

๗. ขั้นตอนในการปฏิบัติ

๗.๑ การเตรียมการก่อนเกิดภัย

๗.๑.๑ จัดให้มีการฝึกอบรมให้ความรู้แก่เจ้าหน้าที่ เพื่อให้ทราบถึงพิบัติภัยและวิธีป้องกันในการเก็บรักษาข้อมูลสารสนเทศหากเกิดภัยพิบัติขึ้นในพื้นที่

๗.๑.๒ จัดทำทำเนียบส่วนราชการให้เป็นปัจจุบัน เพื่อความสะดวกในกรณีเกิดเหตุภัยพิบัติฉุกเฉินในพื้นที่

๗.๑.๓ จัดให้มีการฝึกอบรมเพื่อเตรียมการดูแลรักษาเครื่องมืออุปกรณ์และข้อมูลที่มีการจัดเก็บโดยชี้แจงให้ทราบขั้นตอนและวิธีการปฏิบัติในขณะเกิดเหตุภัยพิบัติ

๗.๑.๔ จัดให้มีวัสดุอุปกรณ์และเครื่องคอมพิวเตอร์ที่เหมาะสม และเตรียมสถานที่สำรองในการติดตั้ง หากมีภัยพิบัติเกิดขึ้น

๗.๑.๕ ให้ตรวจสอบวัสดุ/อุปกรณ์ที่ใช้ในการเก็บรักษาข้อมูลสารสนเทศให้มีความพร้อมทุกสถานการณ์

๗.๑.๖ ให้ศูนย์ปฏิบัติการจังหวัดเป็นหน่วยรับผิดชอบในการจัดทำแผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ รวมทั้งจัดหาเครื่องมือวัสดุอุปกรณ์และสถานที่สำรองในการป้องกันและบรรเทาภัยพิบัติไว้ให้พร้อม **(แผนภูมิที่ ๑)**

๗.๒ การปฏิบัติเมื่อเกิดภัย

๗.๒.๑ ภายในเขตศาลากลางจังหวัดให้แจ้งสำนักงานป้องกันและบรรเทาสาธารณภัยจังหวัด จัดชุดเจ้าหน้าที่ออกปฏิบัติงานตามแผนทันที **(แผนภูมิที่ ๒)**

๗.๒.๒ นอกเขตศาลากลางจังหวัดให้แจ้งส่วนราชการ/หน่วยงานที่เกี่ยวข้อง และองค์กรปกครองส่วนท้องถิ่นที่ตั้งนอกพื้นที่ศาลากลางจังหวัด เช่น เทศบาลเมืองมุกดาหาร เป็นต้น

๗.๒.๓ รายงานเหตุการณ์ให้ผู้ว่าราชการจังหวัด รองผู้ว่าราชการจังหวัด (CIO) หัวหน้าสำนักงานจังหวัด หรือหัวหน้าศูนย์ปฏิบัติการจังหวัด หมายเลขโทรศัพท์ ๐-๔๒๖๑-๑๓๓๐

๗.๒.๔ กรณีเกิดเหตุในระดับอำเภอให้จัดชุดเจ้าหน้าที่ออกปฏิบัติงานทันทีตามแผนของอำเภอแล้วรายงานเหตุการณ์ให้ผู้ว่าราชการจังหวัด รองผู้ว่าราชการจังหวัด (CIO) หัวหน้าสำนักงานจังหวัด หรือหัวหน้าศูนย์ปฏิบัติการจังหวัด หมายเลขโทรศัพท์ ๐-๔๒๖๑-๑๓๓๐ **(แผนภูมิที่ ๓)**

๗.๓ การฟื้นฟูบูรณะ

๗.๓.๑ หน่วยงานที่ประสบภัยพิบัติประเมินค่าความเสียหาย

๗.๓.๒ ปรับปรุงแก้ไขให้สถานการณ์ให้กลับคืนสู่สภาพปกติ กู้ข้อมูล (Restore) ในกรณีที่เห็นว่าหน่วยงานสามารถดำเนินการได้เอง

๗.๒.๓ กรณีที่ไม่สามารถดำเนินการได้ให้รายงานความเสียหายและประมาณการค่าความเสียหายให้จังหวัดทราบเพื่อขอรับการสนับสนุนงบประมาณต่อไป

๗.๔ แผนการดำเนินงาน IT Contingency Plan

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	ผลการดำเนินงาน	ผู้รับผิดชอบ
๑.เครื่องคอมพิวเตอร์แม่ข่ายโดนไวรัสคอมพิวเตอร์โจมตี	๑.ป้องกันไม่ให้ไวรัสคอมพิวเตอร์โจมตีเครื่องคอมพิวเตอร์แม่ข่ายได้	๑.มีการติดตั้งโปรแกรม Nod ๓๒ Anti Virus หรือโปรแกรมป้องกันไวรัสคอมพิวเตอร์ และตั้งเวลาให้ทำการ Update และตรวจสอบไวรัส ภายในเครื่องโดยอัตโนมัติ ๒.นำ Linux Server มาใช้งาน	เจ้าหน้าที่กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด	๑.กำจัดไวรัสคอมพิวเตอร์โดยการการสแกน และ Update โปรแกรมสแกนไวรัส	๑.ใช้โปรแกรม Nod๓๒ Anti Virus หรือโปรแกรมป้องกันไวรัสคอมพิวเตอร์อื่นๆ	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด
		๒. มีการกำหนดสิทธิให้เครื่องคอมพิวเตอร์ลูกข่ายที่เข้ามาใช้บริการใช้ได้เฉพาะเว็บเพจ เท่านั้น	เจ้าหน้าที่กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด	๒.กรณีที่ไวรัสคอมพิวเตอร์ทำลายระบบจนไม่สามารถให้บริการต่อไปได้ จะทำการล้างระบบเครื่องคอมพิวเตอร์แม่ข่าย แล้วติดตั้งระบบปฏิบัติการใหม่ และนำข้อมูลที่ Backup ไว้เข้าสู่ระบบ ๓. มีการทดสอบการ Backup	๒. ได้ทำสำเนาข้อมูลทั้งหมดของระบบไว้ ๒ ชุด แยกเก็บต่างที่กัน - ห้องสื่อสาร ๑ ชุด - สำนักงานศึกษาธิการจังหวัด ๓. จัดทำคู่มือการติดตั้งระบบใหม่ และวิธีการนำเข้าข้อมูล	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด
		๓.มีการตรวจสอบสถานะการทำงานของเครื่องแม่ข่ายทุกสัปดาห์	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด			

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	ผลการดำเนินงาน	ผู้รับผิดชอบ
๒. Hard Disk คอมพิวเตอร์แม่ข่ายเสียหาย ไม่สามารถให้บริการได้	๑.ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายภายในห้องที่มีความเหมาะสมทั้งอุณหภูมิ และที่ตั้ง	๑.ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายภายในห้องที่มีอุณหภูมิพอเหมาะ ควบคุมไม่ให้อุณหภูมิสูงเกินไป	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด	๑.มีจานบันทึกข้อมูล (Hard Disk) สำรอง ๑ ชุด ๒. Handy drive ๓. CD ๔. Cloud Computing	๑.มีการติดตั้งจานบันทึกข้อมูล (Hard Disk) สำรองเมื่อเครื่องคอมพิวเตอร์แม่ข่ายหลักไม่สามารถให้บริการได้ และสามารถนำข้อมูลที่ทำสำเนาไว้มานำเข้าระบบเพื่อให้บริการได้ภายในเวลาไม่เกิน ๓ ชั่วโมง	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด
		๒.ตรวจเช็ค ทำความสะอาดป้องกันไม่ให้มีฝุ่นละอองจนทำให้เครื่องเสียหาย	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด			
		๓.ติดตั้งอุปกรณ์สำรองไฟฟ้าเพื่อป้องกันไฟฟ้าตกหรือกระชาก	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด			

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	ผลการดำเนินงานปี	ผู้รับผิดชอบ
๓. เกิดไฟไหม้เครื่องคอมพิวเตอร์แม่ข่าย หรือภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย	๑.ป้องกันไม่ให้เกิดเพลิงไหม้	๑.มีการติดตั้งอุปกรณ์ตัดวงจรไฟฟ้า กรณีไฟฟ้ารั่วหรือลัดวงจร	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด	๑.จัดหาเครื่องคอมพิวเตอร์แม่ข่ายสำรอง ๒.จัดหาเครื่อง PC สำรอง	นำข้อมูลที่ทำสำเนาไว้มานำเข้าระบบเพื่อให้ระบบใช้งานได้	๑.กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด ๒.สำนักงานป้องกันและบรรเทาสาธารณภัยจังหวัด ๓.สำนักงานที่ดินจังหวัด
	๒.ป้องกันไม่ให้ไฟฟ้าลัดวงจร	๒.ติดตั้งอุปกรณ์ตรวจจับควันภายในอาคาร ติดตั้งระบบส่งสัญญาณแจ้งเหตุเตือนภัย, ติดตั้งอุปกรณ์ดับเพลิง/น้ำยาเคมีดับเพลิง	สำนักงานจังหวัด			
		๓.ป้องกันไม่ให้มีผู้ที่ไม่เกี่ยวข้องเข้าไปในห้องเครื่องคอมพิวเตอร์แม่ข่าย	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด			
๔.เครื่องแม่ข่ายถูกโจรกรรม	๑. มีระบบควบคุมการเข้าใช้ห้องเครื่องคอมพิวเตอร์แม่ข่าย ๒. มีระบบกล้องโทรทัศน์วรจรปิด	๑.ป้องกันไม่ให้มีผู้ที่ไม่เกี่ยวข้องเข้าไปในห้องเครื่องคอมพิวเตอร์แม่ข่าย และมีการลงลายมือชื่อทุกครั้งก่อนเข้า-ออก	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด	๑.จัดหาเครื่องคอมพิวเตอร์แม่ข่ายสำรอง	๑.นำข้อมูลที่ทำสำเนาไว้มานำเข้าระบบเพื่อให้ระบบใช้งานได้	๑.กลุ่มงานอำนวยการ (สื่อสาร) นักงานจังหวัด ๒.สำนักงานศึกษาธิการจังหวัด

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	ผลการดำเนินงาน	ผู้รับผิดชอบ
๕.ข้อมูลสูญหาย	๑.ทำการสำเนาข้อมูล	๑.ได้ทำสำเนาข้อมูลทั้งหมดของระบบไว้ ๒ ชุด แยกเก็บต่างที่กัน คือ ห้องสื่อสาร ๑ ชุด, สำนักศึกษาธิการจังหวัด ๑ ชุด ๒.จัดทำคู่มือการติดตั้งระบบใหม่ และวิธีการนำเข้าข้อมูล	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานศึกษาธิการจังหวัด	๑.ทำการกู้คืนข้อมูล	๑.ทดสอบนำเข้าข้อมูลจากฐานข้อมูล ๒.ข้อมูลที่สำเนาไว้ในอุปกรณ์อื่น (Hard Disk, เทป, แผ่นซีดี)	๑.กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด ๒.สำนักงานสาธารณสุขจังหวัด
๖. การเชื่อมโยงเครือข่ายล้มเหลว	ตรวจสอบการเชื่อมโยงเครือข่ายเป็นประจำทุกวัน	- มอบหมายเจ้าหน้าที่ผู้ดูแลเครื่องแม่ข่ายให้ตรวจสอบการเรียกใช้ระบบทุกวัน - จัดเวรรักษาการณ์ศาลากลางจังหวัด ๒๔ ชม. - จัดเวรรักษาการสำนักงานจังหวัด ๒๔ ชม.	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด	จัดหาเครือข่ายสำรอง MOI หรือ GIN หรือ CAT หรือ TOT	ใช้เครือข่ายสำรอง MOI หรือ GIN หรือ CAT หรือ TOT	๑.กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด ๒.สำนักงานสาธารณสุขจังหวัด

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	ผลการดำเนินงาน	ผู้รับผิดชอบ
๗. ไฟไหม้ศาลากลางจังหวัด (ห้องสถานีสื่อสารจังหวัด)	๑.ป้องกันไม่ให้เกิดเพลิงไหม้ ป้องกันไม่ให้ไฟฟ้าลัดวงจร	๑.ติดตั้งอุปกรณ์ตัดวงจรไฟฟ้ากรณีไฟฟ้ารั่วหรือลัดวงจร ๒.ติดตั้งอุปกรณ์ดับเพลิงชนิดถังเคมี/น้ำยาเคมีดับเพลิง	สำนักงานจังหวัด สนง.สาธารณสุขจังหวัด สนง.ป้องกันและบรรเทาฯ	๑.ปิดระบบสารสนเทศเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพวง ๒.ขนย้ายระบบสารสนเทศ เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพวง ไปไว้ที่ สนง.ป้องกันและบรรเทาฯ	๑.ทดสอบการปิดระบบสารสนเทศ คอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง ๒.สำเนาข้อมูลไว้ในอุปกรณ์อื่น (Hard Disk,เทป, แผ่นซีดี)	๑.กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด ๒.สนง.ป้องกันและบรรเทาจังหวัด ๓.สำนักงานศึกษาธิการจังหวัด
	๑.ป้องกันการวางเพลิงจากบุคคล	๑.ป้องกันไม่ให้มีผู้ที่ไม่เกี่ยวข้องเข้าไปในห้องเครื่องคอมพิวเตอร์แม่ข่าย ๒.มีการจัดตั้งเวรรักษาการณ์อาคารศาลากลางจังหวัด ๒๔ ชั่วโมง ๓. มีการบันทึกข้อมูลบุคคลที่เข้า-ออกสถานีสื่อสาร จ.มห.	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด	๑.จัดหาเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ต่อพ่วงที่จำเป็นทดแทน ในกรณีไม่สามารถขนย้ายได้ทัน หรืออุปกรณ์เสียหาไม่สามารใช้การได้	๑.นำข้อมูลที่ทำสำเนาไว้นำเข้าระบบเพื่อให้ระบบใช้งานได้โดยเร็วที่สุด	๑.กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด ๒.สนง.ป้องกันและบรรเทาจังหวัด

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	ผลการดำเนินงาน	ผู้รับผิดชอบ
๘. สถานการณ์ฉุกเฉินที่เกิดจากการชุมนุมประท้วง บุกรุกศาลากลางจังหวัด (ห้องสถานีสื่อสารจังหวัด)	๑.ป้องกันไม่ให้ผู้ชุมนุมบุกรุกศาลากลาง (ห้องสถานีสื่อสารจังหวัด)	๑. จัดเวรยามรักษาการณ์อาคารศาลากลางจังหวัด ๒. จัดเจ้าหน้าที่รักษาการณ์สถานีสื่อสาร สำนักงานจังหวัด	ทุกส่วนราชการ	๑. ปิดระบบสารสนเทศเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์ต่อพวง ๒. ขนย้ายระบบสารสนเทศ เครื่องแม่ข่ายคอมพิวเตอร์ และอุปกรณ์ต่อพวง ไว้ที่ สนง.ป้องกันและบรรเทาจังหวัด	๑.ทดสอบการปิดระบบสารสนเทศ คอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง ๒.สำเนาข้อมูลไว้ในอุปกรณ์ Hard Disk และแผ่นซีดี	ทุกส่วนราชการ
๙.น้ำท่วมห้องคอมพิวเตอร์แม่ข่าย (สถานีสื่อสารจังหวัด)	๑.ป้องกันไม่ให้เกิดน้ำท่วมขัง	๑.ตรวจสอบอุปกรณ์ระบายน้ำ/อุปกรณ์น้ำประปา ในห้องคอมพิวเตอร์แม่ข่าย ๒.ตรวจสอบหน้าต่างให้สามารถป้องกันฝน/น้ำ	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด	๑. ปิดระบบสารสนเทศเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์ต่อพวง	๑.ทดสอบการปิดระบบสารสนเทศ คอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง ๒.สำเนาข้อมูลไว้ในอุปกรณ์ Hard Disk และแผ่นซีดี	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด
๑๐.เว็บไซต์จังหวัด/หน่วยงานถูกโจมตีทางไซเบอร์	๑.ป้องกันไม่ให้มีการโจมตีทางไซเบอร์	๑.ติดตั้งระบบ Firewall ๒.เปลี่ยนรหัสเข้าเว็บไซต์ทุกสามเดือน ๓.ตรวจสอบข้อผิดพลาดของเว็บไซต์ทุกสัปดาห์	กลุ่มงานอำนวยการ (สื่อสาร) สำนักงานจังหวัด	๑.ปิดระบบเว็บไซต์ ๒.ตัดการเชื่อมต่อกับระบบเครือข่าย ๓.หาช่องโหว่ของเว็บไซต์	๑.ทดสอบการปิดระบบสารสนเทศ คอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง ๒.สำเนาข้อมูลไว้ในอุปกรณ์ Hard Disk และแผ่นซีดี	ทุกส่วนราชการ

๗.๕ กระบวนการแก้ไขปัญหาจากภัยพิบัติในกรณีที่สำคัญ

<u>กรณีที่ ๑ : เครื่องคอมพิวเตอร์แม่ข่ายโดนไวรัสคอมพิวเตอร์โจมตี</u>

๑. การสรุปเหตุเบื้องต้น โดยเครื่องคอมพิวเตอร์จะมีการทำงานที่ผิดปกติไป

๑.๑ เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ เช่น ไม่สามารถ log in เข้าระบบได้ (กรณีการเข้าระบบถูกทำลายด้วยวิธีการลบ แก้ไข หรือปรับเปลี่ยนข้อมูล)

๑.๒ ไฟล์งานในเครื่องคอมพิวเตอร์หายไป โดยการสังเกตจากข้อความที่แจ้งเตือน

๑.๓ โปรแกรมไม่สามารถทำงานได้ (Run ไม่ขึ้น)

๑.๔ อาจมีข้อความ (System Message) ที่แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้

๒. การแจ้งเหตุ โดยทำการ

๒.๑ จดบันทึก สรุป อาการที่ผิดปกติ

๒.๒ คัดลอก (Print Screen) หน้าจอที่ผิดปกติ

๓. การประเมินสถานการณ์โดยการแจ้งผู้รับผิดชอบหรือเจ้าหน้าที่ที่ประจำ ณ จุดเกิดเหตุ

๔. แนวทางการปฏิบัติกรณีระบบมีปัญหาต้องติดตั้งระบบใหม่ สำหรับศูนย์ปฏิบัติการจังหวัดมุกดาหาร มีขั้นตอนการติดตั้งระบบดังนี้

๔.๑ การติดตั้งโปรแกรมระบบปฏิบัติการใหม่

๔.๒ การตั้งค่าระบบการให้บริการของเครื่องคอมพิวเตอร์แม่ข่าย

๔.๓ การดึงข้อมูลจากระบบสำรองข้อมูลเข้ามาในระบบฐานข้อมูลเดิม

<u>กรณีที่ ๒ : Hard Disk คอมพิวเตอร์แม่ข่ายเสียหาย ไม่สามารถใช้งานได้</u>

๑. การสรุปเหตุเบื้องต้น โดยสังเกตว่า

๑.๑ เกิดเสียงดังผิดปกติหรือเสียงการหมุนแผ่น Hard Disk เสียงดังผิดปกติ

๑.๒ อุปกรณ์มีอาการสั่น

๑.๓ ไฟสถานะดับ/กระพริบ ไม่เป็นปกติ

๑.๔ ให้สังเกตว่าหน้าจอคอมพิวเตอร์ (Monitor) มีข้อความเตือน (Message Warning)

๒. การแจ้งเหตุ โดยให้ดำเนินการ ดังนี้

๒.๑ จดบันทึกและสรุปอาการที่ผิดปกติ

๒.๒ คัดลอก (Print Screen) หน้าจอที่ผิดปกติ

๓. การประเมินสถานการณ์โดยการแจ้งผู้รับผิดชอบหรือเจ้าหน้าที่ที่ประจำ ณ จุดเกิดเหตุ

๔. แนวทางการปฏิบัติ ทำการสำรองข้อมูล (Back Up) จัดเก็บไว้ในจานบันทึกข้อมูลแบบภายนอก (External harddisk) หรือเขียนใส่แผ่นซีดีรอม

<u>กรณีที่ ๓ : เกิดไฟไหม้ตัวเครื่องแม่ข่ายหรือภายในห้องเครื่องคอมพิวเตอร์แม่ข่าย (ห้องสื่อสาร)</u>

๑. การสรุปเบื้องต้น โดยสังเกตจาก

๑.๑ ตรวจดูอุณหภูมิ ควัน กลิ่น ที่ผิดปกติ ที่เกิดขึ้นในห้องคอมพิวเตอร์แม่ข่าย

๑.๒ สัญญาณของเครื่องตรวจจับอุณหภูมิ หรือควัน กลิ่น ที่ผิดปกติ

๒. การแจ้งเหตุ โดยดำเนินการ ดังนี้

๒.๑ กดสัญญาณเตือนภัย (กรณีสัญญาเตือนภัยไม่ทำงานอัตโนมัติ) เพื่อการอพยพเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่ายที่สำคัญ

๒.๒ ระบบแจ้งเหตุเตือนภัยส่งสัญญาณแจ้งเหตุโดยอัตโนมัติ

๓. การประเมินสถานการณ์ โดยการแจ้งเจ้าหน้าที่เวรรักษาความปลอดภัย อส. หรือตำรวจเพื่อประสานแจ้งหน่วยดับเพลิงในกรณีควบคุมเพลิงไม่ได้

๔. แนวทางการปฏิบัติ

๔.๑ ทำการตัดวงจรไฟฟ้าและใช้อุปกรณ์ดับเพลิงเคมีที่ติดตั้งไว้ภายในอาคารศาลากลางจังหวัดทำการดับเพลิงในกรณีที่สามารถควบคุมเพลิงได้ และประสานแจ้งหน่วยดับเพลิงในกรณีควบคุมเพลิงไม่ได้

๔.๒ ทำการกันผู้ที่ไม่เกี่ยวข้องให้ออกจากที่เกิดเหตุโดยด่วน

๔.๓ นำเครื่องคอมพิวเตอร์แม่ข่ายสำรองมาติดตั้งให้บริการแทนโดยเร็วที่สุด

<u>กรณีที่ ๔ : เครื่องคอมพิวเตอร์แม่ข่ายถูกโจรกรรม</u>

๑. การสรุปเหตุเบื้องต้น โดยสังเกตจาก

๑.๑ สังเกตเหตุอันผิดปกติ เช่น มีร่องรอยการงัดแงะ

๑.๒ สรุปสถานการณ์เพื่อประสานงานผู้เกี่ยวข้องต่อไป

๒. การแจ้งเหตุ โทรศัพท์แจ้งเหตุผู้ที่เกี่ยวข้องโดยตรง เช่น ตำรวจ เจ้าหน้าที่เวรรักษาความปลอดภัยประจำอาคารศาลากลางจังหวัดมุกดาหารโดยด่วน

๓. การประเมินสถานการณ์

๓.๑ จัดให้มีเวรยามเจ้าหน้าที่เวรรักษาความปลอดภัยบริเวณทางขึ้นศาลากลางจังหวัดมุกดาหาร

๓.๒ กรณีห้องเครื่องคอมพิวเตอร์แม่ข่าย มอบหมายให้มีเจ้าหน้าที่ดูแลรับผิดชอบกุญแจโดยตรง เช่น นายช่างไฟฟ้า เป็นต้น

๓.๓ จัดให้มีการทำการตรวจตราการปิดประตูทุกครั้งก่อนปิดห้อง

๔. แนวทางการปฏิบัติ

๔.๑ ให้ติดต่อเจ้าหน้าที่ หรือเจ้าหน้าที่ที่เกี่ยวข้อง ประสานงานโดยการนำข้อมูลสำรองมาทำการติดตั้งให้บริการทดแทน

๔.๒ ทำการทดสอบระบบหลังการติดตั้ง โดยเริ่มระบบเพื่อตรวจสอบการทำงาน

๔.๓ ทำการตรวจสอบข้อมูลว่า ข้อมูลมีความถูกต้อง ครบถ้วน สมบูรณ์ ทันสมัย

๔.๔ ติดตามผลการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย

<u>กรณีที่ ๕ : ข้อมูลสูญหาย</u>

๑. การสรุปเบื้องต้น

๑.๑ เกิดความผิดปกติทางกายภาพ เช่น ดิสก์สูญหาย หรือเสียหาย

๑.๒ เกิดจากการทำงานของระบบ

๑) ไม่สามารถเข้าถึงข้อมูลได้

๒) โปรแกรมระบบฐานข้อมูลไม่ทำงาน

๓) อุปกรณ์คอมพิวเตอร์บางตัวไม่ทำงาน หรือติดต่อกับฮาร์ดดิสก์ (Hard Disk) ไม่ได

๔) มีข้อความแจ้งเหตุที่ผิดปกติ

๒. การแจ้งเหตุ โดยทำการจดบันทึก / สรุป และทำการ Print Screen ข้อความที่ผิดปกติ

๓. การประเมินสถานการณ์ (Incident Evaluation) แจ้งเหตุให้เจ้าหน้าที่ที่เกี่ยวข้องทราบ

๔. แนวทางการปฏิบัติ (Response Operation)

๔.๑ นำฮาร์ดดิสก์ (Hard Disk) สำรองมาทำการติดตั้ง

๔.๒ ทดสอบการเชื่อมโยง

๔.๓ ทดสอบการทำงานของระบบโดยรวม

๔.๔ กรณีที่ต้องปรับข้อมูล ต้องทำการปรับข้อมูลตามช่วงวันที่ที่ต้องการ

๔.๕ นำข้อมูลสำรอง (Back Up) ในช่วงที่ต้องการมากู้คืนข้อมูล

๔.๖ ทำการตรวจสอบความถูกต้องของข้อมูลว่า ข้อมูลมีความสมบูรณ์ ครบถ้วน น่าเชื่อถือได้

๔.๗ มอบหมายให้มีเจ้าหน้าที่ที่รับผิดชอบทำการสำรองข้อมูล

๔.๘ การสำรองข้อมูลอย่างสม่ำเสมอ

๔.๙ ทำการสำรวจผลการสำรองข้อมูล

๔.๑๐ ทำการสำรองข้อมูลเต็มรูปแบบ (Full Back UP) ของทุกๆ เดือน

๔.๑๑ ตรวจสอบการทำงานของฐานข้อมูลหลังจากดำเนินการเสร็จ

<u>กรณีที่ ๖ : การเชื่อมโยงเครือข่ายล้มเหลว</u>

๑. การสรุปเหตุเบื้องต้น

๑.๑ เครื่องคอมพิวเตอร์ในศูนย์ปฏิบัติการจังหวัดมุกดาหารและผู้บริหารระดับสูงของจังหวัดไม่สามารถเรียกดูข้อมูลจากเครื่องคอมพิวเตอร์แม่ข่ายของศูนย์ปฏิบัติการจังหวัดมุกดาหารได้

๑.๒ เครื่องคอมพิวเตอร์จากศูนย์ปฏิบัติการกระทรวงมหาดไทยไม่สามารถเรียกดูข้อมูลจากศูนย์ปฏิบัติการจังหวัดมุกดาหารได้

๑.๓ เครื่องคอมพิวเตอร์ในศูนย์ปฏิบัติการจังหวัดมุกดาหาร Ping ไปที่กระทรวงมหาดไทยไม่ได้

๒. การแจ้งเหตุ ให้เจ้าหน้าที่ของศูนย์ปฏิบัติการจังหวัดมุกดาหารตรวจสอบระบบเครือข่ายภายใน (LAN) และเครือข่ายทางด่วนข้อมูลของกระทรวงมหาดไทย (ATM Network) พร้อมสรุปเหตุขัดข้อง

๓. การประเมินสถานการณ์ เจ้าหน้าที่ของศูนย์ปฏิบัติการจังหวัดมุกดาหาร ต้องตรวจสอบและแจ้งสาเหตุที่ขัดข้องให้ชัดเจนว่าอยู่ในกรณีใด

๔. แนวทางการปฏิบัติ

๔.๑ เจ้าหน้าที่ช่างประจำศูนย์ปฏิบัติการจังหวัดมุกดาหาร วิเคราะห์ ตรวจสอบ หาสาเหตุขัดข้องของอุปกรณ์เชื่อมโยงเครือข่าย

๑) แก้ไขด้วย Software กรณีขัดข้องเทคนิคการตั้งค่าอุปกรณ์ (Configuration)

๒) แก้ไขโดยใช้อุปกรณ์ Hardware สับเปลี่ยน กรณีอุปกรณ์เครือข่ายเสีย

๔.๒ หลังการตรวจสอบแก้ไขเสร็จเรียบร้อยแล้ว ให้ทำการทดลองระบบและตรวจสอบผลการใช้งาน

๔.๓ บันทึกผลการตรวจสอบและการแก้ไขปัญหา

๘. แนวทางปฏิบัติเพื่อป้องกันหรือลดความเสี่ยงด้านระบบข้อมูลสารสนเทศ

๘.๑ การบำรุงรักษา

๑) มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และมีการดูแลอย่างถูกต้องและต่อเนื่อง

๒) ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

๓) การใช้แผ่นซีดีหรือ Handy drive ควรตรวจสอบไวรัสก่อนใช้ทุกครั้ง

๔) ควรทำความสะอาดเครื่องคอมพิวเตอร์เสมอ และมีการตรวจสอบดูแลคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอ

๕) ควรใช้คำสั่งในโปรแกรม Windows ในการบำรุงรักษาเครื่องเป็นประจำ เช่น การอัพเดท หรือการปรับปรุงการทำงานตามคำแนะนำของ Windows เป็นต้น

๖) ติดตั้ง Firewall เพื่อเป็นการป้องกันเบื้องต้น เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าสู่ระบบเครือข่าย

๗) ฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงาน รวมทั้งการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ

๘.๒ การรักษาความปลอดภัย

๑) กำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์และในกรณีที่พบว่า มีการใช้งานหรือมีการเปลี่ยนแปลงในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที

๒) ทำการทดสอบระบบซอฟท์แวร์เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานอย่างสม่ำเสมอ

๓) ติดตั้งโปรแกรมระบบรักษาความปลอดภัย เช่น การติดตั้ง Firewall

๔) กำหนดเจ้าหนาที่รับผิดชอบในการดำเนินการไว้อย่างชัดเจน

๘.๓ มาตรการในการป้องกันไวรัส

๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอย่างสม่ำเสมอ ดังนี้

- ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม
- สร้างแผ่น Emergency Disk เพื่อใช้ในการกู้ระบบ
- อัพเดตข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัพเดต
- เปิดใช้งาน Auto Protect
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

๒) การป้องกันจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

- ทำการสแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น .pif หรือไฟล์ที่มีนามสกุลไม่คุ้นเคย
- หลีกเลี่ยงการใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา

๘.๔ การจัดการด้านกายภาพและสิ่งแวดล้อม

๑) พิจารณาตำแหน่งของห้องคอมพิวเตอร์แม่ข่ายและติดตั้งระบบเทคโนโลยีสารสนเทศไว้ที่เครื่องคอมพิวเตอร์แม่ข่าย รวมถึงการกำหนดที่ตั้งของเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้า สายสัญญาณต่างๆ โดยหลีกเลี่ยงการติดตั้งระบบไว้ในจุดที่มีความเสี่ยง รวมทั้งมีอุปกรณ์ป้องกันภัยพิบัติในเบื้องต้น เช่น เครื่องปรับอากาศ ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย ถังดับเพลิง เป็นต้น

๒) ควบคุมการเข้าออกห้องปฏิบัติการระบบข้อมูลสารสนเทศ โดยกำหนดเป็นพื้นที่เขตหวงห้ามเฉพาะและการกำหนดสิทธิ์การเข้าออกให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

๓) จัดห้องคอมพิวเตอร์แม่ข่ายให้เป็นสัดส่วนเฉพาะเพื่อความสะดวกในการปฏิบัติงานและยังทำให้การควบคุมและการเข้าถึงอุปกรณ์คอมพิวเตอร์ต่างๆ มีประสิทธิภาพมากขึ้น โดยอาจจัดแยกส่วนอุปกรณ์ที่จำเป็นในการเข้าถึงข้อมูล เช่น การสำรองข้อมูลไว้กรณีฉุกเฉินเมื่อข้อมูลเกิดการเสียหาย

๔) วางระบบป้องกันไฟที่เหมาะสม โดยจัดให้มีถังดับเพลิงที่พร้อมใช้งานได้ตลอดเวลา

๕) จัดให้มีระบบป้องกันไฟฟ้ากระชากเพื่อไม่ให้คอมพิวเตอร์ได้รับความเสียหาย รวมทั้งการติดตั้งระบบสายดินที่ได้มาตรฐานหรือจัดให้มีระบบไฟฟ้าสำรอง

๖) มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยการตั้งอุณหภูมิเครื่องปรับอากาศและค่าความชื้นให้มีระดับเหมาะสมระบบคอมพิวเตอร์

๘.๕ การสำรองข้อมูลและกู้คืนข้อมูล

๑) เพื่อให้มีความพร้อมในการใช้งานและป้องกันการสูญหายของข้อมูล ในส่วนของศูนย์ปฏิบัติการจังหวัดจึงได้ทำการสำรองข้อมูลไว้ดังนี้

- การ Backup ข้อมูลโดยฝากเก็บข้อมูลไว้ที่ Server ของสำนักงานสาธารณสุขจังหวัดมุกดาหารและ Server ของศูนย์ปฏิบัติการจังหวัด (POC) โดยข้อมูลจะ Backup อัตโนมัติไปที่ Server ทั้ง ๒ แห่ง ณ เวลา ๐๐.๐๐ น. ทุกวัน ส่วนกรณีของเว็บไซต์จังหวัดมุกดาหารจะ Backup ที่ศูนย์เทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงมหาดไทย

- การ Backup ข้อมูลที่ศูนย์ปฏิบัติการจังหวัดมุกดาหาร โดยทำการ Backup ข้อมูลลงในซีดีรอมที่เครื่องแม่ข่ายทุกสัปดาห์ **(แผนภูมิที่ ๔)**

๒) มีการมอบหมายเจ้าหน้าที่รับผิดชอบการสำรองข้อมูล

๓) กำหนดให้มีการทดสอบข้อมูลสำรองอย่างน้อยเดือนละ ๑ ครั้ง เพื่อตรวจสอบข้อมูลและโปรแกรมต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและสามารถใช้งานได้

๔) จัดเก็บรักษาข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัยและติดฉลากไว้อย่างชัดเจน

๕) หากเกินขีดความสามารถให้ขอรับการสนับสนุนจากศูนย์ปฏิบัติการจังหวัดหรือศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

๘.๖ การตรวจสอบการเข้าสู่ระบบ

๑) การกำหนดสิทธิให้แก่ผู้ใช้งาน

- กำหนดสิทธิการเข้าถึงข้อมูลสารสนเทศและระบบคอมพิวเตอร์ เช่น กำหนดสิทธิในการเข้าใช้ระบบให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ

- กำหนดระยะเวลาการใช้งานของ user พร้อม password และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

- กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างรอบคอบและมีชั้นความลับ

- ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่นจะต้องขออนุญาตจากผู้มีอำนาจหน้าที่เพื่อให้การอนุมัติทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นในการเข้าใช้งาน

๒) ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน

- กำหนดให้รหัสผ่านมีความยาวตามมาตรฐานสากล

- ควรใช้อักขระพิเศษประกอบ เช่น @ ; < > เป็นต้น

- สำหรับผู้ใช้งานทั่วไปควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน ส่วนผู้ดูแลระบบควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๓ เดือน

- ในการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรจะกำหนดรหัสผ่านใหม่ซ้ำชื่อเดิม

- กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

- ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่าน โดยบุคคลอื่นผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

๘.๗ การจัดการด้านบุคลากร

- กำหนดโครงสร้างบุคลากรด้านเทคโนโลยีสารสนเทศและการบริหารจัดการในลักษณะกระจายภารกิจและความรับผิดชอบ รวมทั้งการแต่งตั้งเจ้าหน้าที่ที่มีความรู้ความสามารถและมีประสบการณ์ด้านคอมพิวเตอร์ ซึ่งสามารถถ่ายทอดความรู้ให้แก่ผู้ใช้งานได้อย่างมีประสิทธิภาพ

- หากมีการเปลี่ยนแปลงผู้ดูแลระบบหรือเจ้าหน้าที่ผู้รับผิดชอบจะต้องแจ้งให้ผู้บังคับบัญชาทราบเพื่อประโยชน์ในการบริหารงาน

- การจัดจ้างบุคคลภายนอก (Outsourcing) เพื่อดำเนินการและควบคุมกำกับดูแลหรือเป็นที่ปรึกษาจากบริษัทที่มีความชำนาญเฉพาะทางและมีเครื่องมือและเทคโนโลยีที่ทันสมัยและเอื้อต่อการพัฒนาระบบฐานข้อมูลสารสนเทศ

- จัดส่งเจ้าหน้าที่เข้ารับการฝึกอบรมความรู้ทางเทคโนโลยีสารสนเทศเป็นระยะ

๘.๘ การป้องกันปัญหาที่เกิดจากกระแสไฟฟ้า โดยยึกหลักปฏิบัติของเจ้าหน้าที่เพื่อป้องกันความเสียหายที่เกิดจากกระแสไฟฟ้า ดังนี้

๑) เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งาน ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

๒) เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

๘.๙ การปฏิบัติการรักษาความปลอดภัยสถานที่

ให้ถือปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗ บทที่ ๕ เรื่อง การรักษาความปลอดภัยเกี่ยวกับสถานที่ **(ผนวก ก)** โดยเคร่งครัด

๙. ผู้รับผิดชอบแผน

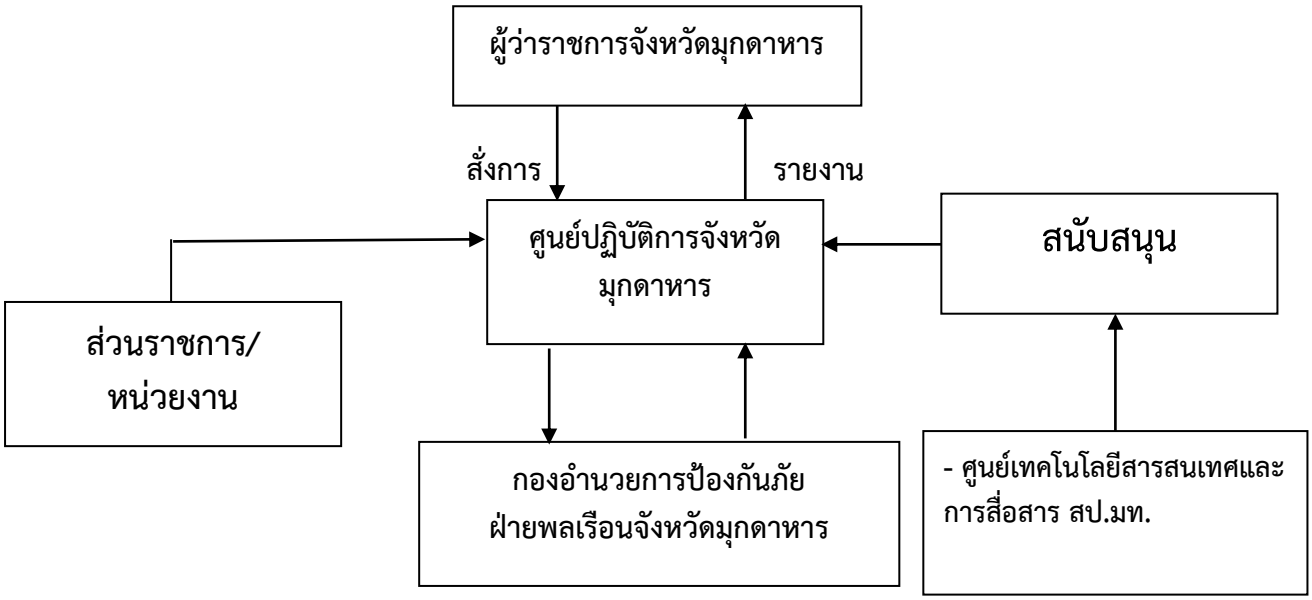
ให้หัวหน้ากลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สำนักงานจังหวัดมุกดาหาร เจ้าหน้าที่ผู้ปฏิบัติงานในศูนย์ปฏิบัติการจังหวัด (นายช่างไฟฟ้า) และเจ้าหน้าที่ผู้ปฏิบัติงานด้านระบบข้อมูลสารสนเทศของส่วนราชการ/หน่วยงานประจำจังหวัดมุกดาหาร ถือปฏิบัติและประสานงานให้เป็นไปตามแผนฯ หากมีปัญหาอุปสรรคหรือข้อขัดข้องใดเกิดขึ้นให้รายงานผู้บังคับบัญชาได้ทราบตามลำดับชั้นต่อไป

(ลงชื่อ) ผู้เสนอแผน
(นายอนุรัตน์ ธรรมประจำจิต)
หัวหน้าสำนักงานจังหวัดมุกดาหาร

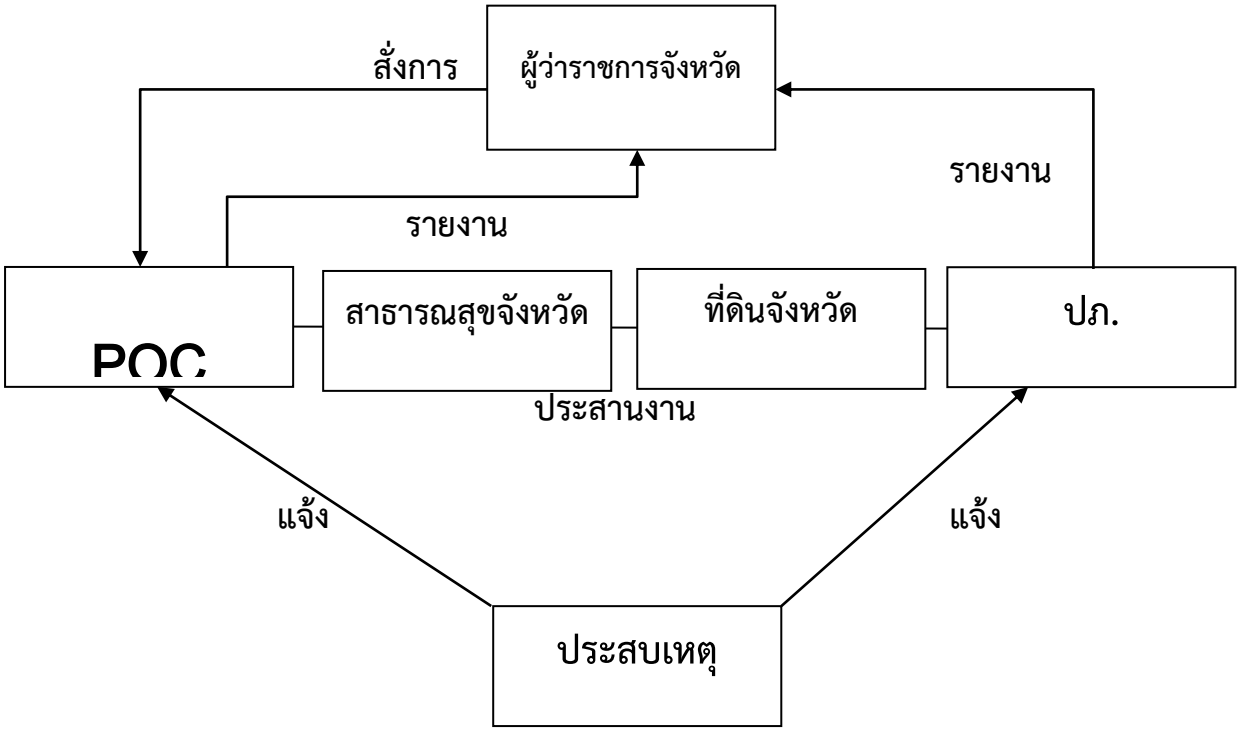
(ลงชื่อ) ผู้เห็นชอบแผน
(นายปานทอง สระคูพันธ์)
รองผู้ว่าราชการจังหวัดมุกดาหาร
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) จังหวัดมุกดาหาร

(ลงชื่อ) ผู้อนุมัติแผน
(นายไพฑูรย์ รักษ์ประเทศ)
ผู้ว่าราชการจังหวัดมุกดาหาร

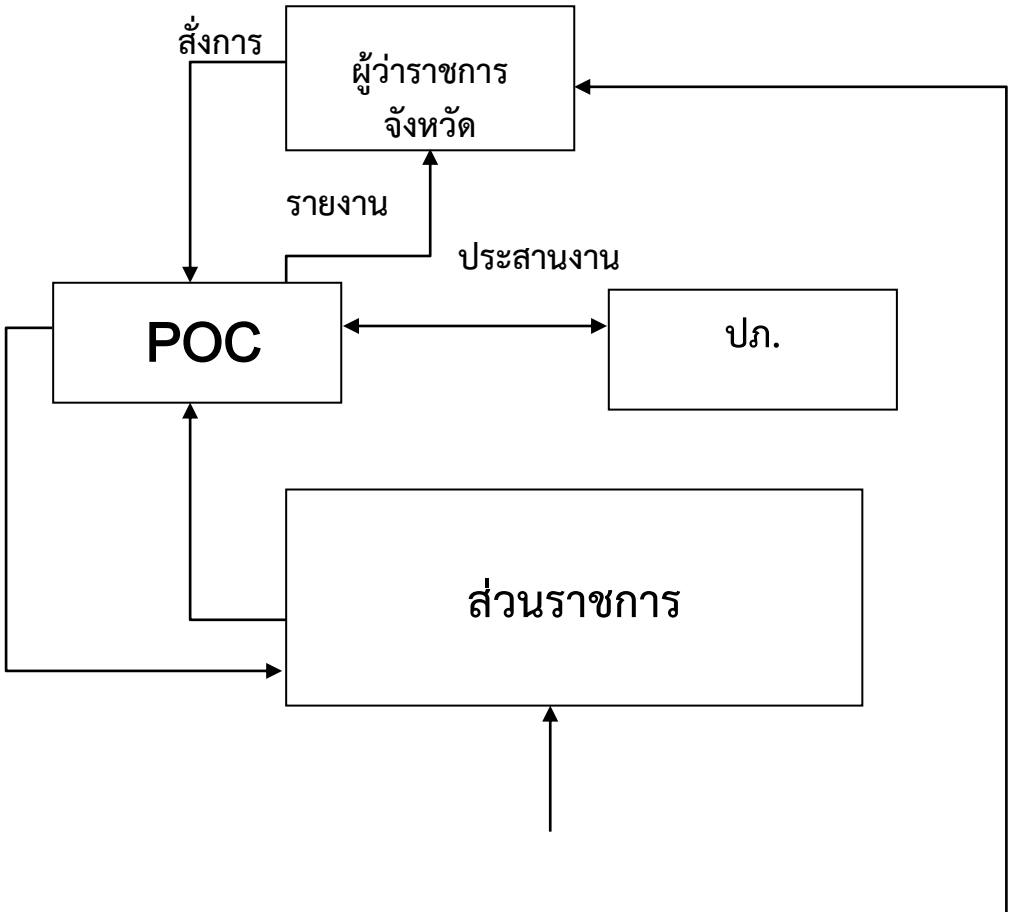
<u>แผนภูมิที่ ๑</u> การเตรียมความพร้อมก่อนเกิดภัยพิบัติ



<u>แผนภูมิที่ ๒</u> **การปฏิบัติการเมื่อเกิดภัย (กรณีเหตุเกิดบริเวณศาลากลางจังหวัดฯ)**



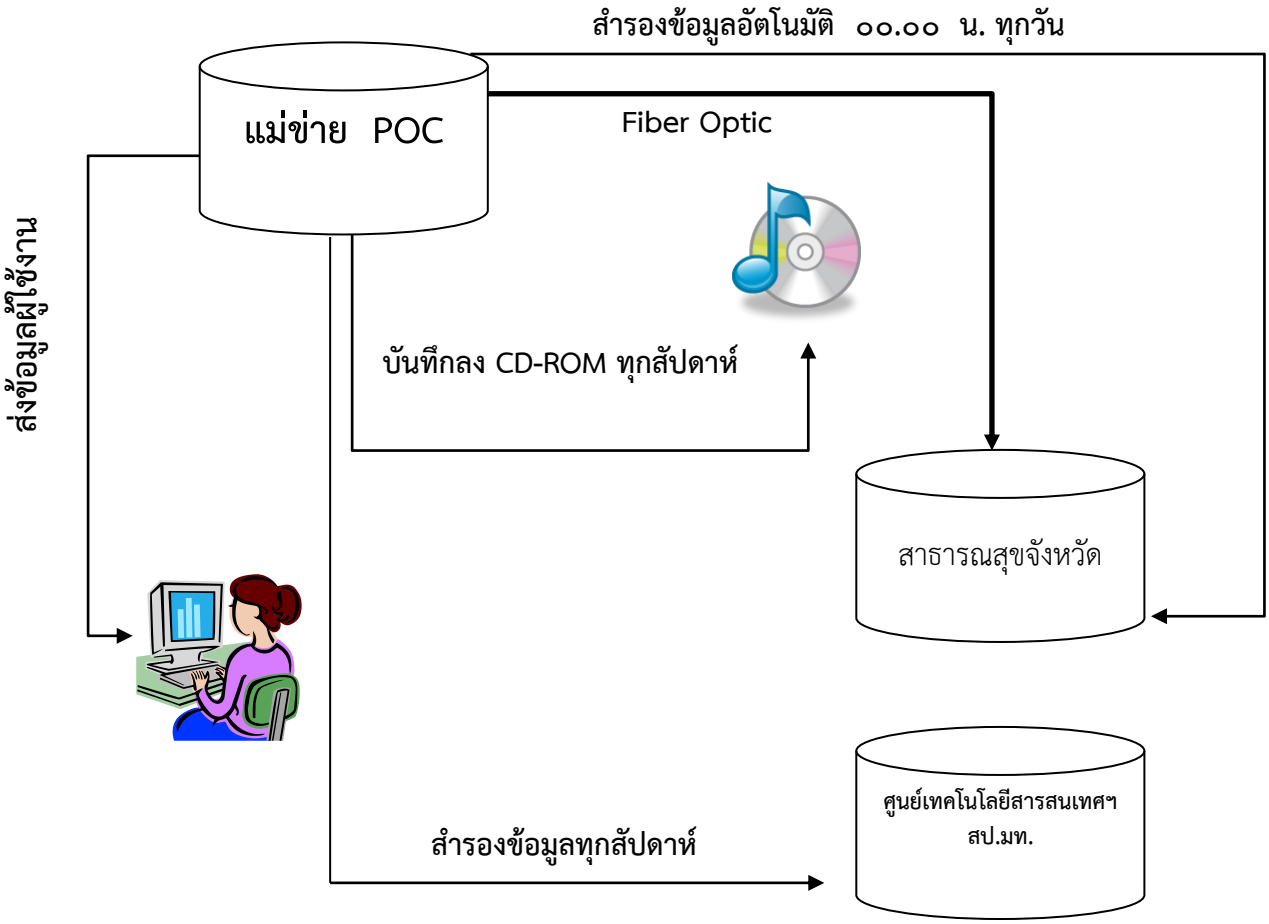
<u>แผนภูมิที่ ๓</u> **การปฏิบัติการเมื่อเกิดภัย (กรณีเกิดเหตุนอกเขตศาลากลางจังหวัดฯ)**



จุดเกิดเหตุ

-๒๑-

<u>แผนภูมิที่ ๔</u> การปฏิบัติการเมื่อเกิดภัย (การ Backup ข้อมูลที่ศูนย์ปฏิบัติการจังหวัดมุกดาหาร)



ผนวก ก

ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗
บทที่ ๕ การรักษาความปลอดภัยเกี่ยวกับสถานที่

.....

๓๘. คำจำกัดความ

การรักษาความปลอดภัยเกี่ยวกับสถานที่ คือมาตรการที่กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่ที่สงวน อาคาร และสถานที่ของส่วนราชการ ตลอดจนวัสดุ อุปกรณ์ เจ้าหน้าที่และเอกสารในอาคารสถานที่ดังกล่าวให้พ้นจากการโจรกรรม การจารกรรมและการก่อวินาศกรรมหรือเหตุอื่นใดอันอาจทำให้เสียสมรรถภาพในการปฏิบัติภารกิจของส่วนราชการได้

๓๙. ความมุ่งหมาย การรักษาความปลอดภัยเกี่ยวกับสถานที่มีความมุ่งหมายเพื่อ

๓๙.๑ กำหนดมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ของส่วนราชการ

๓๙.๒ เป็นแนวทางในการวางแผนรักษาความปลอดภัยเกี่ยวกับสถานที่ของส่วนราชการที่ตั้งขึ้นใหม่หรือขยายออกไป และเป็นแนวทางในการประเมินค่าแห่งการรักษาความปลอดภัยเกี่ยวกับสถานที่ที่มีอยู่แล้ว

๓๙.๓ เป็นแนวทางให้ส่วนราชการดำเนินมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่ตามความเหมาะสมกับระดับความสำคัญของสถานที่นั้นๆ

๓๙.๔ ช่วยเจ้าหน้าที่รับผิดชอบในการพิทักษ์รักษาสถานที่และวัตถุต่าง ๆ ที่มีค่าสูงของชาติให้ปฏิบัติงานได้อย่างมีประสิทธิภาพ

๔๐. ข้อพิจารณาในการวางมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่

๔๐.๑ ปัจจัยสำคัญที่จะต้องพิจารณาในการวางมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ ได้แก่ ความสำคัญของภารกิจของส่วนราชการนั้น ๆ สภาพของสถานที่ลักษณะทางภูมิศาสตร์ สถานการณ์ทางเศรษฐกิจอุดมการณ์ทางการเมืองของประชาชนในพื้นที่นั้นๆ และพฤติการณ์ของฝ่ายที่อาจเป็นศัตรู ตลอดจนการสนับสนุนช่วยเหลือที่จะพึงได้รับจากส่วนราชการอื่น ๆ

๔๐.๒ ระดับการรักษาความปลอดภัยของสถานที่หนึ่ง ๆ ย่อมมีความแตกต่างกันแล้วแต่ความสำคัญของภารกิจของภารกิจ สิ่งที่เป็นความลับ ทรัพย์สิน และอาคารสถานที่ จึงต้องแยกพิจารณาการวางมาตรการการป้องกันแต่ละอาคารสถานที่ เช่น อาคารสถานที่บางแห่ง พื้นที่ทั้งหมดอาจต้องการมาตรการการรักษาความปลอดภัยเพียงแบบเดียว แต่สถานที่อีกแห่งหนึ่งมีกิจการเฉพาะอย่าง หรือพื้นที่ภายในเฉพาะแห่งที่ต้องการมาตรการการรักษาความปลอดภัยมากแบบเป็นพิเศษ เช่น การจัดแยกกิจการให้อยู่ต่างหาก และการเพิ่มมาตรการการป้องกันให้มากขึ้นเป็นต้น

๔๐.๓ ในการออกแบบก่อสร้างที่สงวน อาคารสถานที่หรือเครื่องกีดขวางทางราชการที่มีความสำคัญหรือความลับจะต้องพิทักษ์รักษา ให้สถาปนิก และ/หรือวิศวกรผู้ออกแบบพิจารณาให้ด้านการรักษาความปลอดภัยด้วย โดยหารือกับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของส่วนราชการนั้นๆ หรือองค์การรักษาความปลอดภัย ทั้งนี้ให้อยู่ในความรับผิดชอบของหัวหน้าส่วนราชการ

๔๑. ภยันตรายที่ควรพิจารณาเกี่ยวกับสถานที่มีภยันตรายที่ควรพิจารณาดังนี้

๔๑.๑ ภยันตรายที่เกิดจากปรากฏการณ์ธรรมชาติและอุปัทวเหตุ เช่น พายุ น้ำท่วม ฟ้าผ่า และเพลิงไหม้ เป็นต้น

๔๑.๒ ภยันตรายเกิดจากการกระทำของมนุษย์แบ่งออกเป็น ๒ ประเภท คือ

๔๑.๒.๑ การกระทำโดยเปิดเผย เช่น การโจรกรรม การจลาจล การก่อความไม่สงบ และการโจมตีของข้าศึก เป็นต้น

๔๑.๒.๒ การกระทำโดยทางลับ เช่น การจารกรรม และการก่อวินาศกรรม เป็นต้น

๔๒. การสำรวจหรือการตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่ ในการสำรวจหรือการตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่ราชการต่าง จะต้องปฏิบัติตามขั้นตอนดังต่อไปนี้

ขั้นที่ ๑ ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของส่วนราชการวางแนวทางในการสำรวจหรือการตรวจสอบ โดยวิเคราะห์สภาพแวดล้อม หลักฐานในการปฏิบัติและข้อบกพร่องที่มีมาแล้ว

ขั้นที่ ๒ สำรวจบริเวณพื้นที่ และอาคารสถานที่โดยละเอียด

ขั้นที่ ๓ จัดทำรายงานการสำรวจหรือการตรวจสอบ โดยชี้ให้เห็นข้อบกพร่องของมาตรการการป้องกันที่ใช้อยู่ในปัจจุบันที่จะทำให้เกิดการละเมินการรักษาความปลอดภัยแล้วเสนอแนะให้หัวหน้าส่วนราชการพิจารณาแก้ไขมาตรการและวางระเบียบปฏิบัติในการรักษาความปลอดภัยในเรื่องต่างๆ ดังต่อไปนี้

๔๒.๑ เขตรั้วและการจำกัดช่องทางเข้าออก

๔๒.๒ การใช้เครื่องกีดขวาง

๔๒.๓ การให้แสงสว่าง

๔๒.๔ การจัดเจ้าหน้าที่รักษาความปลอดภัยสถานที่

๔๒.๕ การติดต่อสื่อสารและระบบสัญญาณแจ้งภัย

๔๒.๖ การควบคุมการเข้าออกของบุคคลภายนอก

๔๒.๗ การควบคุมการจราจร

๔๒.๘ การควบคุมการเข้าออกของเจ้าหน้าที่ภายใน

๔๒.๙ การกำหนดพื้นที่ที่มีการรักษาความปลอดภัย

๔๒.๑๐ ที่เก็บอาวุธ กระสุน วัตถุระเบิด หรือวัสดุลับของทางราชการ ซึ่งจะต้องพิทักษ์รักษาเป็นพิเศษ

๔๒.๑๑ การป้องกันอัคคีภัย

๔๒.๑๒ การตรวจตราเป็นประจำหรือการตรวจสอบตามห้วงระยะเวลา เพื่อค้นหาข้อบกพร่องและสั่งการตามที่เห็นสมควร

๔๓. มาตรการการรักษาความปลอดภัย เกี่ยวกับสถานที่ให้ส่วนราชการจัดให้มีการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้เหมาะสม โดยพิจารณาให้มาตรการดังต่อไปนี้

๔๓.๑ เครื่องกีดขวาง คือ เครื่องมือที่ใช้ป้องกัน ขัดขวาง หรือหน่วงเหนี่ยวบุคคลสัตว์หรือยานพาหนะที่ไม่มีสิทธิเข้าไปในพื้นที่รักษาความปลอดภัย โดยใช้เครื่องกีดขวางเป็นแนวเขตของพื้นที่ก่อให้เกิดภาพทาง

จิตวิทยา และทางวัตถุทำให้กล้าเข้าหรือหน่วงเหนี่ยวการล่วงล้ำเพื่อให้ยามรักษาการณ์มีโอกาสตรวจพบ หยุดยั้งหรือจับกุมได้ อีกทั้งเป็นการประหยัดจำนวนเจ้าหน้าที่ยามรักษาการณ์ และเป็นการบังคับให้บุคคลหรือยานพาหนะที่จะผ่านเข้าออก ต้องผ่านเฉพาะตามทางเข้าออกที่กำหนดให้เพื่อสะดวกในการควบคุมและตรวจสอบเครื่องกีดขวางโดยทั่วไปแบ่งเป็น ๒ ชนิด คือ

๔๓.๑.๑ เครื่องกีดขวางตามธรรมชาติ เช่น ทะเล แม่น้ำ ลำคลอง หน้าผา ฯลฯ ที่ได้ดังแปลงให้เป็นประโยชน์ในการกั้น

๔๓.๑.๒ เครื่องกีดขวางที่ประดิษฐ์ขึ้น รั้วทึบ รั้วโปร่ง เครื่องกั้น ถนน ลวด หีบเพลง กำแพง ลูกกรงเหล็ก ฯลฯ

๔๓.๒ การให้แสงสว่าง การให้แสงสว่างก็เพื่อจะให้มองเห็นบริเวณรั้วและเขตหวงห้ามต่างๆ โดยชัดเจนในเวลามืด จะได้มองเห็นผู้ที่บุกรุกเข้ามาในสถานที่ การให้แสงสว่างมี ๒ วิธีคือ

๔๓.๒.๑ การใช้แสงส่องโดยตรง คือการพุ่งแสงสว่างส่องไปยังจุดใดจุดหนึ่งที่ต้องการ เช่น ตัวอาคาร รั้ว หรือประตู เป็นต้น

๔๓.๒.๒ การใช้แสงส่องกระจายรอบตัว ทำให้มีความสว่างทั่วบริเวณ ดวงไฟควรอยู่ในระดับสูงพอที่จะช่วยให้มองเห็นเครื่องกีดขวางต่างๆ ได้ชัดเจน ในกรณีที่รั้วเป็นแบบทึบก็ต้องให้มีแสงสว่างส่องให้เห็นได้ทั้งสองด้านและต้องให้รัศมีแสงสว่างของดวงหนึ่ง ๆ ทับเลยเข้าไปในรัศมีของดวงข้างเคียงเพื่อมิให้มีพื้นที่อับแสงระหว่างรัศมีดวงไฟ

๔๓.๓ เจ้าหน้าที่รักษาความปลอดภัยสถานที่ คือ เจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบในการรักษาความปลอดภัย ประกอบด้วยเจ้าหน้าที่เวรรักษาความปลอดภัยประจำวันยามรักษาการณ์และเจ้าหน้าที่อื่น เจ้าหน้าที่รักษาความปลอดภัยสถานที่จัดขึ้นด้วยความมุ่งหมายเพื่อให้การรักษาความปลอดภัยเกี่ยวกับสถานที่มีประสิทธิภาพยิ่งขึ้นเพราะไม่ว่าจะมีเครื่องกีดขวางชนิดใดหากไม่มีการเฝ้ารักษาแล้ว ก็อาจมีการเล็ดลอดเข้าไปได้

๔๓.๓.๑ <u>หน้าที่</u> เจ้าหน้าที่เวรรักษาความปลอดภัยประจำวันมีหน้าที่กำกับดูแลการปฏิบัติของยามรักษาการณ์และหน้าที่อื่นที่ได้รับมอบหมายจากหัวหน้าส่วนราชการนั้นๆ ยามรักษาการณ์มีหน้าที่ป้องกันบริเวณเขตหวงห้ามทั้งหมด ตลอดจนวัสดุและสิ่งอุปกรณ์ทั้งปวงทำการตรวจสอบบุคคล
ยานพาหนะและสิ่งของต่างๆ โดยเฉพาะเกี่ยวกับการป้องกันอัคคีภัย อุบัติเหตุและภยันตรายอื่น ๆ

๔๓.๓.๒ <u>จำนวน</u> การกำหนดเจ้าหน้าที่รักษาความปลอดภัยสถานที่ให้พิจารณาปัจจัยดังต่อไปนี้

๔๓.๓.๒.๑ จุดอ่อนของอาคารสถานที่ต่าง ๆ

๔๓.๓.๒.๒ จำนวนช่องทางเข้าออก

๔๓.๓.๒.๓ ลักษณะของงานและทรัพย์สินที่พึงได้รับการพิทักษ์รักษา

๔๓.๓.๒.๔ จำนวนผู้เยี่ยมเยียน

๔๓.๓.๒.๕ จำนวนบริเวณเขตหวงห้าม

๔๓.๓.๒.๖ จำนวนยานพาหนะที่ผ่านเข้าออก

๔๓.๓.๒.๗ จำนวนเจ้าหน้าที่ในส่วนราชการนั้น ๆ

๔๓.๓.๒.๘ เวลาพักผ่อนของเจ้าหน้าที่รักษาความปลอดภัย

๔๓.๓.๓ <u>ที่ตั้ง</u> ที่ทำการของเจ้าหน้าที่รักษาความปลอดภัยสถานที่ ควรต้องอยู่ในบริเวณที่สามารถปฏิบัติหน้าที่ได้สะดวก ภายในที่ตั้งควรมีที่เก็บอาวุธ เครื่องมือเครื่องใช้และเครื่องมือสื่อสาร ในที่ตั้งจะต้องมีเจ้าหน้าที่รักษาความปลอดภัยสถานที่ประจำอยู่อย่างน้อยหนึ่งคนตลอดเวลา

๔๓.๓.๔ <u>การติดต่อสื่อสาร</u> ในกรณีที่มียามรักษาการณ์ ควรมีโทรศัพท์ตั้งไว้ ณ จุดอันเหมาะสมที่สุดในเส้นทางของยามรักษาการณ์ และควรกำหนดประมวลลับสำหรับใช้พิสูจน์ฝ่ายระหว่างกันขึ้น ยาม

รักษาการณ์จะต้องรายงานตรงตามกำหนดเวลาเสมอด้วย นอกจากโทรศัพท์ควรกำหนดวิธีการหรือเครื่องมือสื่อสารอื่นสำรองไว้ในกรณีที่โทรศัพท์ขัดข้อง

๔๓.๓.๕ <u>ระบบสัญญาณแจ้งภัย</u> ระบบสัญญาแจ้งภัยคือ วิธีการใช้เครื่องมือทางเทคนิคสำหรับตรวจและแจ้งให้ทราบ ในเมื่อมีการเข้าใกล้หรือการล่วงล้ำเข้ามาในพื้นที่รักษาความปลอดภัย ระบบสัญญาณแจ้งภัยนี้อาจเป็นเครื่องมือเทคนิคทางอิเล็กทรอนิกส์ ทางไฟฟ้า หรือทางเครื่องกล เช่น แผ่นโลหะ เส้นลวดคลื่นแสง คลื่นเสียง กับดัก เป็นต้น ที่จะทำให้เกิดสัญญาณเมื่อมีผู้บุกรุก โดยใช้ติดกับประตู หน้าต่าง ตู้เก็บเอกสาร ห้องนิรภัย กำแพง รั้ว พื้น ฯลฯ

๔๓.๓.๖ <u>การฝึกอบรม</u> เจ้าหน้าที่รักษาความปลอดภัยสถานที่ควรได้รับการฝึกอบรมและมีความรู้ในเรื่องต่างๆ ดังนี้

๔๓.๓.๖.๑ การป้องกันการจารกรรมและการก่อวินาศกรรม

๔๓.๓.๖.๒ บริเวณสถานที่ทั้งหมด จุดสำคัญของสถานที่นั้น รวมทั้งที่ตั้งสวิตซ์ไฟฟ้าที่สำคัญๆ เครื่องมือเครื่องใช้ในการดับเพลิง ตลอดจนภยันตรายต่างๆ ที่อาจเกิดขึ้นแก่สถานที่ราชการนั้นๆ

๔๓.๓.๖.๓ การติดต่อสื่อสารในหน่วยรักษาความปลอดภัย

๔๓.๓.๖.๔ วิธีต่อสู้ป้องกันตัวตามความเหมาะสม

๔๓.๓.๖.๕ ระบบที่ใช้สำหรับแสดงตนซึ่งสถานที่นั้นได้กำหนดไว้

๔๓.๓.๗ <u>เครื่องแบบและอาวุธของยามรักษาการณ์</u> ยามรักษาการณ์ควรแต่งเครื่องแบบและในขณะปฏิบัติหน้าที่ถ้ามีอาวุธก็ต้องเป็นอาวุธที่ถูกต้องตามกฎหมาย พร้อมทั้งมีความรู้ความ สามารถในเรื่องการใช้อาวุธเป็นอย่างดี

๔๓.๔ <u>การควบคุมบุคคลและยานพาหนะ</u>

๔๓.๔.๑ <u>การควบคุมบุคคล</u> พึงปฏิบัติดังต่อไปนี้

๔๓.๔.๑.๑ จัดให้มีบัตรผ่านสำหรับบุคคลภายในเพื่อใช้แสดงว่าเป็นผู้ที่ได้รับอนุญาตให้ผ่านเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัยได้ การออกแบบบัตรผ่านควรมีลักษณะมิให้ปลอมแปลงได้ง่ายและควรเปลี่ยนรูปแบบตามห้วงระยะเวลาที่เห็นสมควร อย่างน้อยให้มีรายละเอียดแสดงชื่อส่วนราชการ ชื่อ รูปถ่าย ส่วนสูง น้ำหนัก และลายมือชื่อของผู้ถือบัตร ลายมือชื่อผู้ออกบัตร หมายเลขประจำตัวบัตร วัน เดือน ปี ที่ออกบัตร วันเดือนปีที่บัตรหมดอายุ กับจะต้องควบคุมการจัดทำและการจ่ายบัตรโดยกวดขัน

๔๓.๔.๑.๒ จัดมีป้ายแสดงตนสำหรับบุคคลภายในและภายนอก เพื่อแสดงว่าเป็นคคลที่ได้รับอนุญาตให้เข้าไปในพื้นที่ใดได้ในฐานะอะไร ก่อนที่บุคคลดังกล่าวจะเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัยของส่วนราชการนั้น ๆ ให้ติดป้ายแสดงตนไว้ในที่ที่เห็นได้ชัด เช่น ที่อกเสื้อ

๔๓.๔.๑.๓ จัดให้มีการบันทึกหลักฐานสำหรับบุคคลภายนอก เช่นผู้มาประชุม ติดต่อหรือเยี่ยม ตลอดจนช่างก่อสร้าง ซ่อมแซม ผู้นำส่งหรือรับสิ่งของจากส่วนราชการหรือหน่วยงานเป็นต้น โดยให้มีรายละเอียด คือ วันและเวลาที่ผ่านเข้า ชื่อ สัญชาติ ตำบลที่อยู่ ชื่อสถานที่ทำงาน ชื่อและหน่วยงานของผู้รับการติดต่อหรือเยี่ยม เหตุผลที่มาติดต่อหรือเยี่ยม วันและเวลาที่กลับออกไป ฯลฯ ในกรณีที่มีการก่อสร้าง ซ่อมแซม หรือรับส่งสิ่งของจากส่วนราชการ หรือหน่วยงานให้หัวหน้าส่วนราชการหรือหน่วยงานนั้นวางมาตรการควบคุมโดยใกล้ชิดตลอดเวลา

๔๓.๔.๔.๔ จัดให้มีที่พักผู้มาติดต่อหรือเยี่ยมไว้เป็นพิเศษต่างหาก ไม่ควรอนุญาตให้ผู้มาเยี่ยมเข้าไปยังที่ทำงาน นอกจากบุคคลที่มาติดต่อราชการที่เกี่ยวข้องโดยแท้จริง ในการนี้ผู้รับการเยี่ยมจะต้องรับผิดชอบในตัวผู้เยี่ยมตลอดเวลา ตั้งแต่รับตัวมาจากเจ้าหน้าที่รักษาความปลอดภัยสถานที่จนส่งตัวคืน สำหรับคนรถของผู้มาติดต่อหรือเยี่ยมหรือผู้ที่โดยสารมาด้วย คงให้รออยู่ ณ บริเวณที่จอดรถ

๔๓.๔.๒ การควบคุมยานพาหนะ พึงปฏิบัติดังต่อไปนี้

๔๓.๔.๒.๑ มีเจ้าหน้าที่ตรวจสอบยานพาหนะเข้าออกของสถานที่ตั้ง ทำหน้าที่ตรวจสอบบุคคลและสิ่งของต่างๆ บนยานพาหนะและควบคุมบรรดายานพาหนะที่อนุญาตให้ผ่านเข้าไปในสถานที่ต้องนั้น โดยให้ใช้เส้นทางและที่จอดรถที่อนุญาตเท่านั้น

๔๓.๔.๒.๒ ทำบันทึกหลักฐานยานพาหนะเข้าออกตามหัวข้อเหล่านี้ คือ

๔๓.๔.๒.๒.๑ วันและเวลาที่ยานพาหนะผ่านเข้า

๔๓.๔.๒.๒.๒ ชื่อคนขับและชื่อผู้โดยสาร

๔๓.๔.๒.๒.๓ เลขทะเบียนยานพาหนะ

๔๓.๔.๒.๒.๔ ลักษณะและจำนวนสิ่งของที่บรรทุกยานพาหนะที่นำเข้า-ออก

๔๓.๔.๒.๒.๕ วัตถุประสงค์และสถานที่ที่ยานพาหนะจะเข้าไป

๔๓.๔.๒.๒.๖ วัน และเวลาที่ยานพาหนะผ่านออก

๔๓.๔.๒.๓ จัดที่จอดรถให้อยู่ห่างจากตัวอาคารที่สำคัญและหรือสิ่งของที่ติดเพลิงง่ายประมาณไม่น้อยกว่า ๖ เมตร

๔๓.๕ พื้นที่ที่มีการรักษาความปลอดภัย คือ พื้นที่ที่มีการกำหนดขอบเขตโดยแน่ชัด ซึ่งมีข้อจำกัดและการควบคุมการเข้าออกเป็นพิเศษ มีความมุ่งหมายเพื่อจะพิทักษ์สิ่งที่เป็นความลับ บุคคล ทรัพย์สิน วัสดุและสิ่งอุปกรณ์ของทางราชการให้ปลอดภัย โดยกำหนดมาตรการการรักษาความปลอดภัยในแต่ละเขตให้มีระดับแตกต่างกันตามความสำคัญ การกำหนดพื้นที่ที่มีการรักษาความปลอดภัย พึงปฏิบัติดังต่อไปนี้

๔๓.๕.๑ กำหนดให้มี “พื้นที่ควบคุม” ซึ่งเป็นพื้นที่ที่อยู่ติดต่อหรือที่อยู่โดยรอบ “พื้นที่หวงห้าม” ภายในเขต “พื้นที่ควบคุม” นี้ต้องมีระเบียบการควบคุมบุคคลและยานพาหนะเพื่อช่วยกลั่นกรองเสียชั้นหนึ่งก่อนที่จะให้เข้าถึง “พื้นที่หวงห้าม”

๔๓.๕.๒ กำหนดให้มี “พื้นที่หวงห้าม” ซึ่งเป็นพื้นที่ที่มีการพิทักษ์รักษาสิ่งที่เป็นความลับตลอดจนบุคคลสำคัญทรัพย์สินหรือวัสดุที่สำคัญของทางราชการ “พื้นที่หวงห้าม” นี้อาจแยกออกเป็น”เขตหวงห้ามเฉพาะ” กับ “เขตหวงห้ามเด็ดขาด”

“เขตหวงห้ามเฉพาะ” คือเขตพื้นที่ซึ่งมีสิ่งที่เป็นความลับตลอดจนบุคคลหรือสิ่งที่มีความสำคัญซึ่งจะต้องพิทักษ์รักษาและการเข้าไปในเขตพื้นที่นี้โดยปราศจากการควบคุม อาจทำให้สามารถเข้าถึงความลับบุคคล และสิ่งอุปกรณ์สำคัญดังกล่าว บุคคลที่ได้รับอนุญาตให้เข้าไปใน “เขตหวงห้ามเฉพาะ” จะต้องได้รับความไว้วางใจตามชั้นความลับที่เหมาะสมกับ “เขตหวงห้ามเฉพาะ” นั้น ๆหรือมิฉะนั้นก็ต้องจัดเจ้าหน้าที่ควบคุมและกำหนดระเบียบการควบคุมภายในขึ้น ตัวอย่าง “เขตหวงห้ามเฉพาะ” เช่น ที่เก็บอาวุธที่เก็บเชื้อเพลิง ชุมสายโทรศัพท์ กองบังคับการของทหาร และห้องปฏิบัติการลับห้องปฏิบัติงานของหัวหน้าส่วนราชการที่เห็นสมควรเป็นต้น

“เขตหวงห้ามเด็ดขาด” คือ เขตพื้นที่ซึ่งมีสิ่งที่เป็นความลับตลอดจนบุคคลหรือสิ่งที่มีความสำคัญยิ่ง ซึ่งจะต้องพิทักษ์รักษาการเข้าไปในเขตพื้นที่นี้อาจทำให้สามารถเข้าถึงความลับบุคคลและสิ่งที่มีความสำคัญยิ่งในการรักษาความปลอดภัยดังกล่าวโดยตรง บุคคลที่ได้รับอนุญาตให้เข้าไปใน “เขตหวงห้ามเด็ดขาด” จะต้องได้รับความไว้วางใจตามชั้นความลับที่เหมาะสมกับ “เขตหวงห้ามเด็ดขาด” นั้นๆเท่านั้น ตัวอย่าง “เขตหวงห้ามเด็ดขาด” เช่น ศูนย์ปฏิบัติการสื่อสาร ห้องปฏิบัติการลับ ห้องปฏิบัติงานของผู้บังคับบัญชาชั้นสูงห้องหรือสถานที่ขณะที่ใช้ในการประชุมลับและห้องนิรภัยเป็นต้น

๔๓.๖ การป้องกันอัคคีภัย

๔๓.๖.๑ การวางมาตรการการป้องกันอัคคีภัย หัวหน้าหน้าส่วนราชการกำหนดมาตรการป้องกันอัคคีภัย โดยมีเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยเป็นผู้วางแผนและกำกับดูแลให้เป็นไปตาม

กฎหมายว่าด้วยการป้องกันและระงับอัคคีภัย กฎกระทรวง และมติคณะรัฐมนตรี ตลอดจนคำสั่งของทางราชการต่าง ๆ ที่เกี่ยวกับเรื่องนี้

๔๓.๖.๒ เจ้าหน้าที่ดับเพลิงในเวลาราชการให้จัดข้าราชการเป็นเจ้าหน้าที่ดับเพลิง โดยแบ่งเป็นสองกลุ่ม คือ กลุ่มที่หนึ่งมีหน้าที่ดับเพลิง และอีกกลุ่มหนึ่งมีหน้าที่ขนย้ายเอกสารและควบคุมรับผิดชอบเอกสารและวัสดุ โดยให้แต่ละกลุ่มมีจำนวนเพียงพอสำหรับงานนั้นๆ สำหรับนอกเวลาราชการให้เป็นหน้าที่ของเจ้าหน้าที่เวรรักษาความปลอดภัยประจำวัน และยามรักษาการณ์เป็นผู้รับผิดชอบ

๔๓.๖.๓ การจัดเตรียมเครื่องอุปกรณ์ในการดับเพลิง ให้มีสัญญาณแจ้งเหตุเพลิงไหม้ติดตั้งไว้และเตรียมเครื่องมือเครื่องใช้ในการดับเพลิงขั้นต้นไว้ให้พร้อม เช่น น้ำ ทราย กระป๋องน้ำ เชือกบันได ขวาน ไม้มือเสือ ตลอดจนเครื่องดับเพลิงให้เหมาะกับประเภทสื่อที่ทำให้เกิดเพลิงไหม้ไว้ทุกประเภท สำหรับเครื่องดับเพลิงเคมีให้ติดตั้งไว้ในที่ที่หยิบฉวยใช้งานได้ง่ายและมีจำนวนเพียงพอ โดยหมั่นตรวจสอบให้อยู่ในภาพที่ใช้การได้อยู่เสมอ และแจ้งให้ทุกคนรู้แหล่งน้ำสำหรับใช้ดับเพลิงที่ใกล้ที่สุด ที่ตั้งและหมายเลขโทรศัพท์ของหน่วยดับเพลิงที่ติดต่อได้สะดวกและรวดเร็วที่สุด

๔๓.๖..๔ การฝึกอบรมให้อบรมเจ้าหน้าที่ให้มีความระมัดระวังเพื่อป้องกันอัคคีภัยและฝึกซ้อมให้มีความรู้ ความชำนาญในการดับเพลิงขั้นต้น เจ้าหน้าที่ควรมีความรู้ในเรื่องต่าง ๆ เหล่านี้คือ

๔๓.๖.๔.๑ ประเภทของไฟ

๔๓.๖.๔.๒ เครื่องมือเครื่องใช้ในการดับเพลิง

๔๓.๖.๔.๓ การติดต่อสื่อสาร การคมนาคม แผนผังอาคารและบริเวณโดยรอบ

๔๓.๖.๔.๔ ที่ตั้งและหมายเลขโทรศัพท์ของหน่วยดับเพลิง

๔๓.๖.๔.๕ แผนการดับเพลิงของส่วนราชการ

๔๔. การวางแผนรักษาความปลอดภัยเกี่ยวกับสถานที่ ในการวางแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ต้องพิจารณาจากผลการประมาณการและหรือข้อมูลตามหัวข้อดังต่อไปนี้เป็นหลัก คือ

๔๔.๑ สถานการณ์โดยทั่วไปและสภาพแวดล้อมโดยรอบพื้นที่

๔๔.๒ ข่าวสาร สิ่งบอกเหตุ และการเตือนภัย

๔๔.๓ ภารกิจและหน้าที่ของหน่วยงาน

๔๔.๔ จำนวนเจ้าหน้าที่ที่ปฏิบัติงานและเจ้าหน้าที่รักษาความปลอดภัย

๔๔.๕ งบประมาณที่จะใช้ในการวางมาตรการการรักษาความปลอดภัย

๔๔.๖ การสนับสนุนจากหน่วยเหนือและหน่วยงานอื่น ๆ

๔๔.๗ การติดต่อสื่อสารภายในหน่วยกับหน่วยเหนือและหน่วยงานอื่น ๆ

๔๔.๘ รายงานการสำรวจหรือการตรวจสอบการรักษาความปลอดภัย

.....

ที่ มห ๐๐๑๗.๒/ว ๒๕๘๐

ศาลากลางจังหวัดมุกดาหาร
ถนนวิวิธสุรการ มห ๔๙๐๐๐

๓ พฤษภาคม ๒๕๖๑

เรื่อง แนวทางการประเมินผู้บริหารองค์การ

เรียน หัวหน้าส่วนราชการทุกส่วนราชการ หัวหน้าหน่วยงานรัฐวิสาหกิจทุกหน่วยงาน นายอำเภอทุกอำเภอ นายกองค์การบริหารส่วนจังหวัดมุกดาหาร และนายกเทศมนตรีเมืองมุกดาหาร

สิ่งที่ส่งมาด้วย แผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านข้อมูลระบบสารสนเทศ จังหวัดมุกดาหาร (พ.ศ.๒๕๖๑ - ๒๕๖๔) จำนวน ๑ เล่ม

ด้วยสำนักงาน ก.พ.ร. ได้กำหนดแนวทางการประเมินผู้บริหารองค์การ (ผู้ว่าราชการจังหวัด) ประเด็นที่ ๗ ส่งเสริมการใช้ดิจิทัลและขีดความสามารถที่มีอยู่และพัฒนาขึ้นทุก ๖ เดือน (ข้อ ๔) มีการวิเคราะห์ความเสี่ยงป้องกันการโจมตีทางไซเบอร์ และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินให้ระบบใช้งานได้ตามปกติ

จังหวัดมุกดาหารพิจารณาแล้วเห็นว่า เพื่อเป็นประโยชน์สำหรับการวิเคราะห์ความเสี่ยงและการป้องกันการโจมตีทางไซเบอร์ที่อาจจะเกิดขึ้นกับระบบข้อมูลสารสนเทศเทศของจังหวัดและหน่วยงาน ดังนั้น จึงขอให้ส่วนราชการถือปฏิบัติตามแผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านข้อมูลระบบสารสนเทศจังหวัดมุกดาหาร (พ.ศ.๒๕๖๑ - ๒๕๖๔) ทั้งนี้ สามารถดาวน์โหลดสิ่งที่ส่งมาด้วยได้ที่เว็บไซต์จังหวัดมุกดาหาร www.mukdahan.go.th/plan_it2561

จึงเรียนมาเพื่อทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นายไพฑูรย์ รักษ์ประเทศ)
ผู้ว่าราชการจังหวัดมุกดาหาร

สำนักงานจังหวัด
กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด
โทร./โทรสาร ๐-๔๒๖๑-๑๓๓๐, มท. ๔๙๑๒๔
E-mail : mukdahan_poc@hotmail.com