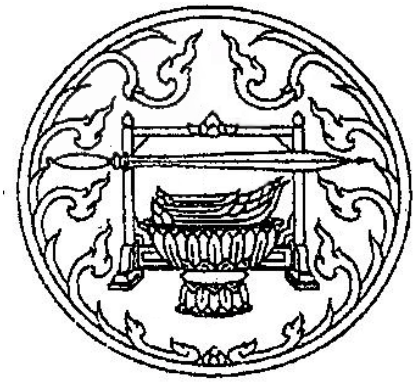


แผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ
(IT Contingency Plan)

ประจำปี ๒๕๕๖
จังหวัดราชบุรี

กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร
สำนักงานจังหวัดราชบุรี

แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ
ระบบข้อมูลสารสนเทศศูนย์ปฏิบัติการจังหวัดราชบุรี ประจำปี ๒๕๕๖

****

แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ มีการวิเคราะห์ความเสี่ยงในรูปแบบต่างๆ ที่อาจเกิดขึ้น รวมทั้งมีมาตรการในการบริหารจัดการความเสี่ยง เพื่อให้การบริหารและจัดการกับระบบสารสนเทศและเครือข่ายคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ในกรณีที่เกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติขึ้น มีรายละเอียดดังนี้

ขั้นตอนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงที่มีประสิทธิภาพมีขั้นตอนการดำเนินการ ดังนี้

๑. การกำหนดวัตถุประสงค์ที่ต้องการบรรลุ เพื่อกำหนดหลักการและทิศทางในกระบวนการบริหารความเสี่ยงมีลักษณะที่เฉพาะเจาะจง สามารถทำให้บุคลากรทุกระดับในองค์กรเข้าใจตรงกันวัดผลได้ชัดเจน ทั้งในเชิงปริมาณหรือเชิงคุณภาพภายใต้ศักยภาพ ทรัพยากรและสิ่งแวดล้อมที่มีอยู่ทิศทางเดียวกับวิสัยทัศน์ขององค์กรในระยะเวลาที่กำหนด

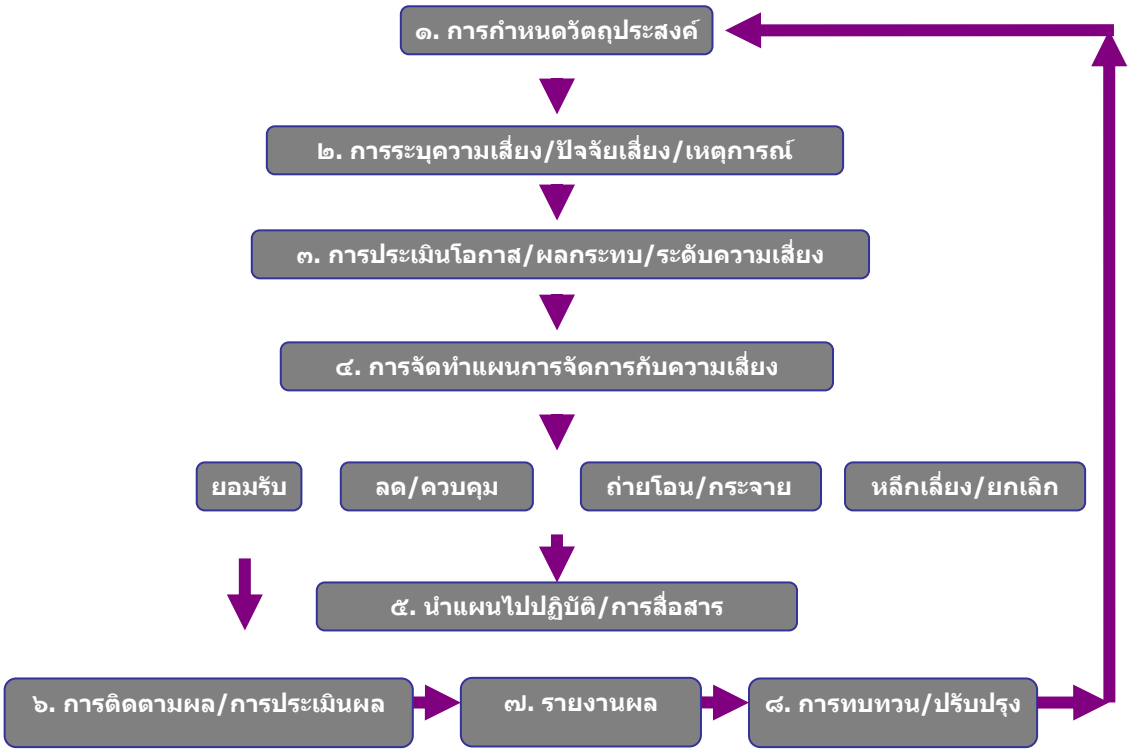
๒. การระบุความเสี่ยงทั้งปัจจัยภายในและภายนอกที่เป็นเหตุการณ์หรืออุปสรรคใดที่อาจเกิดขึ้นและส่งผลกระทบต่อการบรรลุวัตถุประสงค์ที่องค์กรได้ตั้งไว้

๓. ประเมินโอกาส (Likelihood) ผลกระทบ (Impact) และระดับความเสี่ยง (Risk Exposure)ประเมินแต่ละปัจจัยเสี่ยงว่ามีโอกาสที่จะเกิดได้มากน้อยเพียงใดแล้วส่งผลกระทบต่อองค์กรรุนแรงเพียงใดนำมาจัดลำดับว่าปัจจัยเสี่ยงใดมีความสำคัญมากน้อยกว่ากัน เพื่อกำหนดมาตรการตอบโต้ได้อย่างเหมาะสม

๔. การวางแผนจัดการกับความเสี่ยง โดยการพิจารณากำหนดแนวทาง /มาตรการจัดการกับความเสี่ยง เพื่อให้ระดับความเสี่ยงลดลงจนอยู่ในระดับที่สามารถควบคุมมิให้เกิดผลกระทบที่ทำให้องค์กรไม่บรรลุเป้าหมาย ภายใต้พื้นฐานการเปรียบเทียบระหว่างต้นทุนที่จะเกิดขึ้นมีความคุ้มค่าต่อองค์กรหรือไม่

๕. การสื่อสารแผน/ติดตามทบทวน มีการติดตาม รายงาน ประเมินผลการดำเนินการตามมาตรการจัดการความเสี่ยงโดยมีการสื่อสารที่มีประสิทธิภาพทำให้บุคลากรผู้ปฏิบัติทุกระดับเข้าใจบทบาทหน้าที่นำไปใช้อย่างถูกต้อง มีประสิทธิภาพผู้บริหารทราบปัญหาที่เกิดขึ้นจากการปฏิบัติและข้อผิดพลาดที่อาจเกิดขึ้นจากการดำเนินการนำมาทบทวนปรับปรุงแก้ไขให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไปภายในระยะเวลาที่กำหนดอย่างมีประสิทธิภาพ

ขั้นตอนการบริหารความเสี่ยง



การวิเคราะห์ความเสี่ยงด้านระบบสารสนเทศ

จากการพิจารณาและวิเคราะห์ความเสี่ยงด้านระบบข้อมูลสารสนเทศที่อาจจะเกิดขึ้น สามารถแยกได้ดังนี้

๑. ความเสี่ยงที่เกิดจากภัยพิบัติทางธรรมชาติ เช่น วาตภัย อุทกภัย แผ่นดินไหว

๒. ความเสี่ยงที่เกิดจากการกระทำของมนุษย์ เช่น เกิดจากการปฏิบัติงาน กระแสไฟฟ้าขัดข้อง หรืออัคคีภัย

๓. ความเสี่ยงที่เกิดจากโปรแกรม หรืออุปกรณ์คอมพิวเตอร์ ที่เกิดจากการโจมตีจากไวรัสคอมพิวเตอร์หรือการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ การเคลื่อนย้ายอุปกรณ์หรือการติดตั้งอุปกรณ์ในจุดที่ไม่เหมาะสม

๔. ความเสี่ยงที่เกิดจากระบบเครือข่าย ทั้งระบบอินทราเน็ตและอินเตอร์เน็ต รวมถึงความเสี่ยงจากการบุกรุกเครือข่าย

๕. ความเสี่ยงด้านระบบข้อมูลสารสนเทศ เช่น ข้อมูลถูกทำลายหรือมีการแก้ไขเปลี่ยนแปลง

การประเมินสถานการณ์ความเสี่ยงด้านระบบสารสนเทศ

ความเสี่ยงที่อาจเป็นอันตรายต่อระบบข้อมูลสารสนเทศ มีดังนี้

๑. เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน hardware และ software อัน

๒. เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้

๒.๑ ติดตั้ง firewall ทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก และมีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องให้บริการ (Server) และเครื่องลูกข่าย (Client) ซึ่งทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบเครือข่าย

๒.๒ แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านเครือข่าย internet รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากไวรัสต่างๆ ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

๓. เกิดจากระบบไฟฟ้าขัดข้อง หรือความเสียหายจากเพลิงไหม้ โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (server) ในกรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บ และสำรองข้อมูลไว้อย่างปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงมีระบบควบคุม ป้องกันเพลิงไหม้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามภายในศูนย์ปฏิบัติการ

๔. เกิดจากโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์ ในส่วนของห้องคอมพิวเตอร์แม่ข่าย ได้กำหนดห้ามผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ผู้รับผิดชอบนำพาเข้าไป

๕. เกิดจากการบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล โดยดำเนินการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

แนวทางปฏิบัติเพื่อป้องกันหรือลดความเสี่ยงด้านระบบข้อมูลสารสนเทศ

๑. การบำรุงรักษา

๑.๑ มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และมีการดูแลอย่างถูกต้องและต่อเนื่อง

๑.๒ ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

๑.๓ การใช้แผ่น CD หรือ Handy Drive ควรตรวจสอบไวรัสก่อนใช้ทุกครั้ง

๑.๔ ควรดูแลทำความสะอาดเครื่องคอมพิวเตอร์และเครื่องแม่ข่ายอย่างสม่ำเสมอ

๑.๕ การติดตั้ง Firewall เพื่อเป็นการป้องกันเบื้องต้นไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าสู่ระบบเครือข่ายได้

๑.๖ การฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงาน รวมทั้งการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ

๒. การรักษาความปลอดภัย

๒.๑ กำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์ และในกรณีที่พบว่ามีการใช้งานหรือมีการเปลี่ยนแปลงในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที

๒.๒ ทำการทดสอบระบบซอฟต์แวร์เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานอย่างสม่ำเสมอ

๒.๓ ติดตั้งโปรแกรมระบบรักษาความปลอดภัย เช่น การติดตั้ง Firewall

๒.๔ กำหนดเจ้าหน้าที่รับผิดชอบในการดำเนินการไว้อย่างชัดเจน

๓. มาตรการในการป้องกันไวรัส

๓.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ

๓.๒ ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ

๓.๓ ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

๓.๔ หลีกเลี่ยงการใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา

๔. การจัดการด้านกายภาพและสิ่งแวดล้อม

๔.๑ พิจารณาตำแหน่งของห้องคอมพิวเตอร์แม่ข่ายและติดตั้งระบบข้อมูลสารสนเทศไว้ที่เครื่องคอมพิวเตอร์แม่ข่าย รวมถึงการกำหนดที่ตั้งของเครื่องคอมพิวเตอร์ การเดินสายไฟฟ้า สายสัญญาณต่างๆ โดยหลีกเลี่ยงการติดตั้งระบบไว้ในจุดที่มีความเสี่ยง รวมทั้งมีอุปกรณ์ป้องกันภัยพิบัติในเบื้องต้น เช่น เครื่องปรับอากาศ ตู้ Rack เพื่อเก็บเครื่องคอมพิวเตอร์แม่ข่าย ถังดับเพลิง เป็นต้น

๔.๒ ควบคุมการเข้าออกห้องปฏิบัติการระบบข้อมูลสารสนเทศ กำหนดเป็นพื้นที่เขตหวงห้ามเฉพาะ และการกำหนดสิทธิการเข้าออกให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

๔.๓ จัดห้องคอมพิวเตอร์แม่ข่ายให้เป็นสัดส่วนเฉพาะ เพื่อความสะดวกในการปฏิบัติงานและยังทำให้การควบคุมและการเข้าถึงอุปกรณ์คอมพิวเตอร์ต่างๆ มีประสิทธิภาพมากขึ้น โดยจัดแยกส่วนอุปกรณ์ที่จำเป็นในการเข้าถึงข้อมูล เช่น การสำรองข้อมูลไว้กรณีฉุกเฉินเมื่อข้อมูลเกิดความเสียหาย

๔.๔ วางระบบป้องกันไฟที่เหมาะสม โดยจัดให้มีถังดับเพลิงที่พร้อมใช้งานได้ตลอดเวลา

๔.๕ จัดให้มีระบบป้องกันไฟฟ้ากระชากและไฟฟ้าดับ เพื่อไม่ให้คอมพิวเตอร์ได้รับความเสียหาย รวมทั้งติดตั้งระบบสายดินที่ได้มาตรฐานหรือจัดให้มีระบบไฟฟ้าสำรอง

๔.๖ มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยการตั้งอุณหภูมิเครื่องปรับอากาศและค่าความชื้นให้มีระดับเหมาะสมกับระบบคอมพิวเตอร์

๕. การสำรองข้อมูลและกู้คืนข้อมูล

๕.๑ เพื่อให้มีความพร้อมในการใช้งานและป้องกันการสูญหายของข้อมูล ในส่วนของจังหวัดได้ทำการ Backup ข้อมูลไว้ที่เครื่องแม่ข่ายของจังหวัดและเครื่องแม่ข่ายของบริษัท

๕.๒ การ Backup ข้อมูลที่จังหวัด เจ้าหน้าที่จะทำการ Backup ข้อมูลลงใน CD-ROM ที่เครื่องแม่ข่ายทุกเดือน

๕.๓ มีคำสั่งแต่งเจ้าหน้าที่รับผิดชอบงานรักษาความปลอดภัยข้อมูลไว้อย่างชัดเจน

๕.๔ กำหนดให้มีการทดสอบข้อมูลสำรองอย่างน้อยเดือนละ ๑ ครั้ง เพื่อตรวจสอบว่าข้อมูลและโปรแกรมต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและสามารถใช้งานได้

๕.๕ จัดเก็บรักษาข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัยและติดฉลากไว้อย่างชัดเจน

๕.๖ หากเกินขีดความสามารถให้ขอรับการสนับสนุนจากจังหวัด หรือศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

๖. การตรวจสอบการเข้าสู่ระบบ

๖.๑ การกำหนดสิทธิให้แก่ผู้ใช้งาน

- การกำหนดสิทธิการเข้าถึงข้อมูลสารสนเทศและระบบคอมพิวเตอร์ เช่น กำหนดสิทธิในการเข้าใช้ระบบให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ
- กำหนดระยะเวลาการใช้งานของ User พร้อม Password และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่น จะต้องขออนุญาตจากผู้มีอำนาจหน้าที่เพื่อให้การอนุมัติทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นในการเข้าใช้งาน

๖.๒ ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน

- สำหรับผู้ใช้งานทั่วไป ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน ส่วนผู้ดูแลระบบ ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๓ เดือน
- ในการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรจะกำหนดรหัสผ่านใหม่ซ้ำชื่อเดิม
- ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

๗. การจัดการด้านบุคลากร

๗.๑ กำหนดโครงสร้างบุคลากรด้านเทคโนโลยีสารสนเทศและการบริหารจัดการ ในลักษณะกระจายภารกิจและความรับผิดชอบ รวมทั้งการแต่งตั้งเจ้าหน้าที่ที่มีความรู้ความสามารถและมีประสบการณ์ด้านคอมพิวเตอร์ ซึ่งสามารถถ่ายทอดความรู้ให้แก่ผู้ใช้งานได้อย่างมีประสิทธิภาพ

๗.๒ หากมีการเปลี่ยนแปลงผู้ดูแลระบบหรือเจ้าหน้าที่ผู้รับผิดชอบจะต้องแจ้งให้ผู้บังคับบัญชาทราบ เพื่อประโยชน์ในการบริหารงาน

๗.๓ การจัดจ้างบุคคลภายนอก (Outsourcing) เพื่อดำเนินการและควบคุม กำกับดูแล หรือเป็นที่ปรึกษาจากบริษัทที่มีความชำนาญเฉพาะทาง และมีเครื่องมือและเทคโนโลยีที่ทันสมัยและเอื้อต่อการพัฒนาระบบข้อมูลสารสนเทศ

๗.๔ จัดส่งเจ้าหน้าที่เข้ารับการฝึกอบรมความรู้ทางเทคโนโลยีสารสนเทศเป็นระยะๆ

๘. การป้องกันปัญหาที่เกิดจากกระแสไฟฟ้า

หลักปฏิบัติของเจ้าหน้าที่เพื่อป้องกันความเสียหายที่เกิดจากกระแสไฟฟ้ามีดังนี้

๘.๑ เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งาน ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

๘.๒ เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

๙. การปฏิบัติการรักษาความปลอดภัยสถานที่

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

๑๐.แผนทำระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม

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

๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๕) นำ BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยใช้ทีมกู้ระบบ (ผู้ดูแลระบบ และทีมงานจากบริษัทฯ ที่จัดจ้างบำรุงรักษาระบบสารสนเทศ) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง

๖) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

แนวทางการแก้ไขปัญหาตามแผน IT Contingency Plan
จังหวัดราชบุรี

ภัยพิบัติ	แนวทางปฏิบัติเมื่อเกิดเหตุ (IT Contingency Plan)	แนวทางการฟื้นฟูระบบ (Recovery Plan)	หน่วยงานรับผิดชอบ
๑. น้ำท่วม	- เจ้าหน้าที่ที่รับผิดชอบ ประเมินสถานการณ์ - Shutdown Server และปิดอุปกรณ์ (หากทำได้) - ขนย้ายอุปกรณ์ไปยังสถานที่ที่ปลอดภัย	- เช่าใช้บริการเครื่องแม่ข่ายจากเอกชน - Restore ข้อมูลที่ได้สำรองไว้ - ทบทวนมาตรการรักษาความปลอดภัยของสถานที่ให้รัดกุมยิ่งขึ้น	กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี
๒. ไฟไหม้	- อพยพคนออกจากอาคารที่เกิดเหตุ - แจ้งเจ้าหน้าที่ดับเพลิงในกรณีที่ควบคุมเพลิงไม่ได้ - หากไม่ร้ายแรง ให้เจ้าหน้าที่ผู้รับผิดชอบ พยายามเคลื่อนย้ายข้อมูลที่มีความสำคัญออกก่อน	- เช่าใช้บริการเครื่องแม่ข่ายจากเอกชน - Restore ข้อมูลที่ได้สำรองไว้ - ทบทวนมาตรการรักษาความปลอดภัยของสถานที่ให้รัดกุมยิ่งขึ้น	กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี
๓. เครื่องแม่ข่ายขัดข้อง หรือมีอุปกรณ์ชำรุด	- เจ้าหน้าที่ผู้รับผิดชอบตรวจสอบหาสาเหตุ - ใช้เครื่องสำรอง เพื่อทำงานทดแทน	- ดำเนินการซ่อมเครื่องที่ชำรุดให้ใช้งานได้โดยเร็ว - Restore ข้อมูลที่ได้สำรองไว้ - ทบทวนมาตรการรักษาความปลอดภัยของสถานที่ให้รัดกุมยิ่งขึ้น	กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี
๔. การเชื่อมโยงเครือข่ายล้มเหลว	- กรณีวงจรสัญญาณเครือข่ายภายนอกขัดข้อง ให้แจ้งผู้ให้บริการ ดำเนินการแก้ไข - กรณีอุปกรณ์ / เครือข่ายภายในขัดข้อง ให้เจ้าหน้าที่รีบดำเนินการแก้ไข	- ดำเนินการแก้ไขซ่อมแซมอุปกรณ์ที่ชำรุด - บันทึกประวัติความเสียหาย สาเหตุ และระยะเวลาที่ใช้ในการแก้ไขปัญหา เพื่อเป็นข้อมูลในปีต่อไป	กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี
๕. ฮาร์ดดิสก์เสียหาย	- ใช้ฮาร์ดดิสก์สำรองใส่ทดแทน - ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายในห้องที่มีอุณหภูมิพอเหมาะ ควบคุมไม่ให้อุณหภูมิสูงเกินไป - ติดตั้งอุปกรณ์สำรองไฟฟ้า เพื่อป้องกันไฟฟ้ากระชาก	- จัดซื้อฮาร์ดดิสก์สำรองไว้ใช้งาน - ทำการสำรองข้อมูล (Backup) ตามแนวทางปฏิบัติที่กำหนดไว้ - ทบทวนมาตรการรักษาความปลอดภัยของสถานที่ และเครื่องแม่ข่ายให้รัดกุมยิ่งขึ้น	กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี

ภัยพิบัติ	แนวทางปฏิบัติเมื่อเกิดเหตุ (IT Contingency Plan)	แนวทางการฟื้นฟูระบบ (Recovery Plan)	หน่วยงานรับผิดชอบ
๖. เครื่องคอมพิวเตอร์แม่ข่ายโดนไวรัสคอมพิวเตอร์โจมตี	- กำจัดไวรัสคอมพิวเตอร์ โดยใช้โปรแกรม Anti Virus Nod๓๒ ที่กระทรวงมหาดไทยมีให้ - กรณีที่ไวรัสคอมพิวเตอร์ทำลายระบบจนไม่สามารถให้บริการต่อไปได้ ต้องทำการล้างระบบคอมพิวเตอร์แม่ข่าย แล้วติดตั้งระบบใหม่ และนำข้อมูลจากสำเนาข้อมูล (Backup) ที่จัดเก็บไว้	- ติดตั้งโปรแกรม Anti Virus Nod๓๒ ป้องกันไวรัสคอมพิวเตอร์ และตั้งเวลาให้ทำการ update และตรวจสอบไวรัส ภายในเครื่องอัตโนมัติ	กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี
๗. แผ่นดินไหว	- รีบเคลื่อนย้ายอุปกรณ์ออกภายนอกตัวอาคาร - ผู้ดูแลระบบนำข้อมูลสำรองเคลื่อนย้ายไปด้วยหากสามารถทำได้	- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้	กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี
๘. ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง	- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ ให้แจ้งผู้บังคับบัญชาทราบ	- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบตรวจสอบความชำรุดเสียหาย ซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อผู้เกี่ยวข้อง	กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี

การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

๑. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑.๑ หัวหน้าสำนักงานจังหวัดราชบุรี

๑.๒ หัวหน้ากลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี

๒. รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย ประสานงานหน่วยงานที่เกี่ยวข้อง และ ได้แก่

๒.๑ นายสำเริง บุญจง	นายช่างไฟฟ้าชำนาญงาน
๒.๒ นายสัจจะ แสงจันทร์	นายช่างไฟฟ้าชำนาญงาน
๒.๓ นางสาวปัทมาภรณ์ เกตุหอม	นักวิชาการคอมพิวเตอร์ชำนาญการ

แผนการซักซ้อมกรณีเกิดปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ**ที่อาจเกิดกับระบบฐานข้อมูลและสารสนเทศ**

๑. แผนการซักซ้อมกรณีเกิดเพลิงไหม้ มีขั้นตอนการดำเนินการดังนี้

กรณีเพลิงไหม้ไม่รุนแรง

๑) ทำการปิดระบบไฟฟ้าหลักของอาคาร

๒) นำอุปกรณ์ดับเพลิง ฉีดพ่นเพื่อระงับไม่ให้ไฟไหม้ลุกลาม

๓) เมื่อสามารถระงับเพลิงไหม้แล้ว ให้ทำการตรวจสอบความเสียหายของอุปกรณ์ พร้อมทำการกู้คืนระบบให้สามารถทำงานได้ตามปกติ

กรณีเพลิงไหม้แบบลุกลาม

๑) ทำการปิดระบบไฟฟ้าหลักของอาคาร

๒) นำอุปกรณ์ดับเพลิง ฉีดพ่นเพื่อระงับไม่ให้ไฟไหม้ลุกลาม

๓) เมื่อสามารถระงับเพลิงไหม้แล้ว ให้ทำการตรวจสอบความเสียหายของอุปกรณ์ พร้อมทำการกู้คืน

๔) หากตรวจพบอุปกรณ์เกิดความเสียหายและไม่สามารถกู้คืนระบบได้ ให้ทำการประสานงานกับบริษัทผู้รับผิดชอบดูแลอุปกรณ์ที่เสียหาย เพื่อดำเนินการแก้ไขให้สามารถใช้งานได้ตามปกติ

๒. แผนการซักซ้อมสถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

๑) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้บังคับบัญชาทราบ

๒) หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

๓. แผนซักซ้อมสถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

กรณีโจรกรรม

๑) ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

๒) สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

๓) ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆ ได้โดยเร็ว

กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

๑) แจ้งผู้บังคับบัญชาทราบ

๒) ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

๔. แผนการซักซ้อมกรณีตรวจพบการถูกเจาะระบบฐานข้อมูลและสารสนเทศ

กรณีการป้องกันไวรัสล้มเหลว

๑) กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

๒) วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

๓) ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

๔) ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

๕) กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่ในสำนักงานจังหวัดทราบ หรือกรณีมีเหตุอันทำให้ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานที่ใช้ระบบเครือข่ายของสำนักงานจังหวัดทราบ

กรณีการป้องกันผู้บุกรุกล้มเหลว

๑) กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall

๒) ผู้ดูแลระบบแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

๓) ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

แผนปฏิบัติในการบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

๑. การเตรียมการเบื้องต้น

๑) รายละเอียดระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของจังหวัดราชบุรีสามารถดำเนินงานได้อย่างต่อเนื่อง จึงได้มีการเตรียมการจัดทำรายละเอียดของระบบสารสนเทศต่างๆ เพื่อใช้ในการตรวจสอบความถูกต้อง รายละเอียด และที่มาของอุปกรณ์ต่างๆ (ภาคผนวก ก)

๒) การสำรองข้อมูล (Back up) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้น เมื่อข้อมูลถูกทำลายหรือเสียหาย โดยสามารถนำข้อมูลสำเนากลับมาใช้งานได้ มีการตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย

๓) การกู้ข้อมูล (Recovery)

(๑) ทำการทดสอบ Recovery ข้อมูล โครงสร้างและโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้ทำการสำรองไว้

(๒) ทำการทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูลและระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้ทำการสำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

๔) การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย ผู้ใช้งานต้องระมัดระวังในการใช้งานคอมพิวเตอร์ โดยเฉพาะเมื่อเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้ มีวิธีป้องกันดังนี้

(๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
- ติดตั้งโปรแกรมป้องกันไวรัส
- อัพเดตข้อมูลไวรัสอยู่เสมอ
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ
- ใช้โปรแกรมตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

(๒) ระวังภัยเมื่อเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ เช่น แผ่นดิสก์ แผ่นซีดี เป็นต้น
- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์หรือดาวน์โหลดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จัก หรือน่าสงสัย
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

(๓) ใช้ความระมัดระวังในการเปิด E-mail
- อย่าเปิดไฟล์ E-mail ถ้าไม่ทราบแหล่งที่มา
- ลบ E-mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

(๔) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet
- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ
- ไม่ควรเข้า Website ที่แนะนำจาก E-mail ที่ไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๕) การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ

(๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) โดยทั่วไประยะเวลาในการสำรองไฟฟ้าประมาณ ๒๐ – ๓๐ นาที

(๒) เปิดเครื่องสำรองไฟฟ้า ตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์

(๓) เครื่องสำรองไฟฟ้าควรอยู่ในสภาพพร้อมใช้งานเสมอ

(๔) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และทำการปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๖) มีระบบป้องกันไฟไหม้ เนื่องจากไม่ได้รับงบประมาณในการปรับปรุงห้องคอมพิวเตอร์แม่ข่าย จึงยังไม่มีระบบป้องกันไฟไหม้ที่เหมาะสม แต่ในเบื้องต้นมีอุปกรณ์ดับเพลิงติดตั้งในอาคาร และได้กำหนดแนวทางปฏิบัติดังนี้

(๑) ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

(๒) ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

(๓) ควรหาทางออกฉุกเฉินสองทางที่ใกล้ห้องทำงาน ตรวจสอบดูทางออกฉุกเฉินไม่ปิดตาย และสามารถใช้เป็นเส้นทางจากภายใน อาคารได้อย่างปลอดภัย

(๔) เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้ เปิดสัญญาณเตือนเพลิงไหม้ จากนั้นออกจากอาคารแล้วโทรศัพท์แจ้งหน่วยดับเพลิง

(๕) ถ้าเพลิงไหม้ในห้องทำงาน ให้หนีออกมาแล้วปิดประตูห้อง รีบแจ้งหน่วยดับเพลิงทันที

(๖) ถ้าเพลิงไหม้เกิดขึ้นภายนอกห้องทำงาน ก่อนจะหนีออกมาให้วางมือบนประตู หากประตูมีความเย็นอยู่ ค่อยๆ ปิดประตู แล้วหนีไปยังทางหนีไฟฉุกเฉินทันที

(๗) เมื่อต้องเผชิญกับควันไฟที่ปกคลุม ให้ใช้วิธีคลานหนีไปทางฉุกเฉิน เพราะอากาศบริสุทธิ์จะอยู่ด้านล่าง

๗) การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ เป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

(๑) มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นจะต้องได้รับอนุญาตจากเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศผู้รับผิดชอบ อนึ่ง ที่ประตูเข้าออกควรเพิ่มอุปกรณ์สายโซ่และกุญแจล็อค การเข้าถึงห้องเซิร์ฟเวอร์โดยการล็อคกุญแจ และมีเจ้าหน้าที่เครื่องคอมพิวเตอร์คอยควบคุมดูแลตลอด หากเจ้าหน้าที่ภายในหรือเจ้าหน้าที่บริษัทภายนอก มีความจำเป็นต้องเข้าใช้งานจะต้องลงรายละเอียดการขอเข้าใช้ห้อง โดยมีแบบฟอร์มบันทึกการใช้งาน เช่น บันทึกชื่อผู้ขอเข้าใช้, ชื่อบริษัท, เบอร์โทรศัพท์ติดต่อกลับ และบันทึกรายละเอียดการใช้งานทุกครั้ง

(๒) ติดตั้ง Firewall ป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ของจังหวัดราชบุรี

(๓) ติดตั้งระบบ Antivirus ป้องกันไวรัส/เวิร์ม และสแปมเมล์ ที่มาจากเครือข่ายภายนอกได้ส่วนหนึ่ง ซึ่งเป็นการแบ่งเบาภาระในการบำรุงรักษาเครื่องคอมพิวเตอร์ ระบบเครือข่ายภายในที่เกิดปัญหาต่างๆ

(๔) ติดตั้งการทำงานระบบ Load Balance เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ต

(๕) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตว่ามีปริมาณมากผิดปกติหรือไม่ หรือมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้หาสาเหตุและการป้องกันต่อไป

(๖) การเรียกใช้ระบบสารสนเทศของหน่วยงานต่างๆ ผู้ใช้ระบบจะต้องบันทึกผู้ใช้ (User Name) และรหัสผ่าน (Password) เพื่อตรวจสอบระบบก่อนอนุญาตให้ใช้งานได้

๘) การจัดเตรียมอุปกรณ์ที่จำเป็น ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี ได้จัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็น ดังนี้

(๑) แผ่น boot disk

(๒) แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

(๓) แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

(๔) แผ่นโปรแกรม Antivirus/Spyware

(๕) แผ่น driver อุปกรณ์ต่างๆ

(๖) ระบบสำรองไฟฉุกเฉิน

๙) การบำรุงรักษาเครื่อง เนื่องจากเครื่องคอมพิวเตอร์ที่ใช้งานอยู่เป็นระยะเวลานาน มักจะเกิดปัญหาเครื่องทำงานช้าลง การเปิดโปรแกรมต่างๆ ไม่ทำงาน ทั้งนี้เนื่องจากการสะสมของไฟล์ที่เรียกว่าขยะ ทำให้การค้นหาไฟล์ที่ต้องการนานขึ้น อีกทั้งยังเป็นช่องทางหนึ่งที่ไวรัสคอมพิวเตอร์ต่างๆ จะแทรกเข้ามาในเครื่องก่อให้เกิดความเสียหาย ซึ่งมีวิธีป้องกันดังนี้

(๑) ทำการ Disk Cleanup ซึ่งเป็นการใช้งานโปรแกรมของ Windows เอง เป็นตัวจัดการไฟล์ขยะที่อยู่ในระบบ ลบทิ้งออกไปทำให้เนื้อที่ของ Hard disk เพิ่มขึ้น การประมวลผลของระบบก็จะเร็วขึ้น

(๒) การ Check Disk เป็นการเช็คสภาพ Hard disk ว่ายังใช้งานได้ดีอยู่หรือไม่ และยังสามารถกันส่วนที่เสียหายไม่ให้เป็นอุปสรรคต่อการใช้งาน (Bad Sectors)

(๓) การทำ Defragment เป็นการจัดเรียงข้อมูลไม่ให้กระจัดกระจาย ยากต่อการสืบค้นข้อมูลและการเปิดโปรแกรมเพื่อใช้งาน

๒. กรณีเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย

๑) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๒) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๓) รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๔) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๕) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งบริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๓. กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัสคอมพิวเตอร์ ให้ดำเนินการดังนี้

๑) ติดตั้งโปรแกรม NOD๓๒

๒) ใช้งานโปรแกรม NOD๓๒

๔. การดำเนินการตามแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ (IT Contingency Plan) และการวิเคราะห์ ทบทวนสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ

การที่จังหวัดราชบุรีได้นำระบบฐานข้อมูลและระบบสารสนเทศมาใช้ในการปฏิบัติงาน และให้บริการส่วนราชการ และประชาชน ซึ่งหากระบบเกิดความเสียหายจะส่งผลต่อการปฏิบัติงานต่างๆ ดังนั้นจึงต้องให้ความสำคัญในการบริหารความเสี่ยงด้านระบบฐานข้อมูลและสารสนเทศ และได้ดำเนินการจัดทำแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ (IT Contingency Plan) ตั้งแต่ปี ๒๕๕๒ โดยทบทวนในปี ๒๕๕๔ และปฏิบัติตามแผนฯ อย่างต่อเนื่อง ซึ่งได้กำหนดไว้ ๓ ขั้นตอน ดังนี้

(๑) ปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ และรายงานผล

(๒) วิเคราะห์ ทบทวนสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ

(๓) หาแนวทางการป้องกันสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ และแนวทางแก้ไข เมื่อเกิดสถานการณ์ที่ส่งผลให้ระบบสารสนเทศเสียหาย เพื่อใช้เป็นข้อมูลในการปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(๔) โดยในปี ๒๕๕๔ ได้ดำเนินการวิเคราะห์ ทบทวนสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศและหาแนวทางการป้องกันสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ และแนวทางแก้ไข เมื่อเกิดสถานการณ์ที่ส่งผลให้ระบบสารสนเทศเสียหาย เพื่อใช้เป็นข้อมูบในการปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ผนวก ก

รายละเอียดระบบสารสนเทศ

จังหวัดราชบุรี

ลำดับที่	ระบบงาน	คำอธิบาย	การจัดเก็บข้อมูล	บริษัทผู้พัฒนา / ดูแล	หมายเหตุ
๑	ระบบศูนย์ข้อมูลกลาง กระทรวงมหาดไทยและจังหวัด	- เป็น Web Based Application สามารถบันทึก แก้ไข เรียกดู สืบค้น ข้อมูล ๔๕ กลุ่มเรื่อง ๓๒ ตัวชี้วัด	ฐานข้อมูล Oracle ๑๑ g	กระทรวงมหาดไทย	- ส่วนราชการต่างๆ บันทึกข้อมูลเข้าสู่ Server ที่กระทรวงมหาดไทย แล้วผู้ดูแลระบบโยนข้อมูลมาไว้ที่ Server จังหวัด
๒	ระบบบริการข้อมูลข่าวสาร (Web Site)	- เป็น Web Based Application สามารถทั้งบันทึก แก้ไข เรียกดู สืบค้น หรือ แสดงผลจาก Web Site เผยแพร่แก่สาธารณะ, สามารถค้นหาข้อมูลต่างๆ	ฐานข้อมูล Oracle	สำนักงานจังหวัดราชบุรี	
๓	ระบบฐานข้อมูลบุคคล (PPIS)	- เป็นซอฟต์แวร์ที่พัฒนาโดย กพ. จัดเก็บข้อมูลต่างๆ ของข้าราชการ เช่น ข้อมูลส่วนบุคคล (ชื่อ-สกุล, เลขบัตรประชาชน, การศึกษา ฯลฯ) , เงินเดือน ,เครื่องราชฯ	ฐานข้อมูล Windows Server ๒๐๐๓	สำนักงาน ก.พ.	- ส่วนราชการต่างๆ บันทึกข้อมูลเข้าสู่ Server ที่จังหวัด
๔	ระบบ GFMIS	- เป็นระบบการจัดสรรงบประมาณ, ระบบบริหาร/ติดตามการใช้งบประมาณ ระบบบัญชีแยกประเภทแบบเกณฑ์คงค้าง, ระบบบัญชีบริหาร/บัญชีต้นทุน, ระบบบัญชีเจ้าหนี้ , ระบบบัญชีทรัพย์สินถาวร, ระบบบริหารเงินสด ระบบบริหารทรัพยากรบุคคล	ฐานข้อมูล Oracle ๑๑g	กรมบัญชีกลาง	
๕	ระบบ Authentication	- เป็นระบบที่ใช้แสดงตัวตนในการเข้าใช้อินเตอร์เน็ต ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งผู้ที่จะใช้งานเครือข่ายอินเตอร์เน็ตในศาลากลาง จะต้องมี User ID และ Password มิเช่นนั้น จะไม่สามารถใช้งานอินเตอร์เน็ตได้ ดังนั้น ทุกครั้งที่เชื่อมต่อเข้าใช้งาน จึงต้องใช้ User ID และ Password	Hardware	สำนักงานจังหวัดราชบุรี	
๖	ระบบ GIS	- เป็นระบบที่จัดเก็บและแสดงสถานการณ์หรือข้อมูลสำคัญต่างๆ อาทิเช่น สถานที่สำคัญ, พื้นที่เฝ้าระวังเตือนภัย, แหล่งทรัพยากรธรรมชาติ, เส้นทางการเดินทาง หรือปริมาณความหนาแน่นของข้อมูลด้านต่างๆ	ฐานข้อมูล Oracle	สำนักงานจังหวัดราชบุรี	

ผนวก ข

การดำเนินการตามแผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ (IT Contingency Plan) และการวิเคราะห์ทบทวนสถานการณ์ความไม่แน่นอน ภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ

รายละเอียดการดำเนินการตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับงานสารสนเทศ (IT Contingency Plan) และแนวทางในการดำเนินการในปีงบประมาณ ๒๕๕๖

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการตามแผนปี ๒๕๕๕	แนวทางในการดำเนินการในปี ๒๕๕๖
๑	การฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Back up and Recovery)	(๑) สำรองข้อมูล (Back up)	- ทำการสำรองข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์แม่ข่าย เป็นประจำสัปดาห์ - ในส่วนขอข้อมูลในระบบงานต่างๆ จะมีการสำรองเป็นประจำทุกสัปดาห์	- ทำการสำรองข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์แม่ข่าย เป็นประจำสัปดาห์ - ในส่วนขอข้อมูลในระบบงานต่างๆ จะมีการสำรองเป็นประจำทุกสัปดาห์
		(๒) การกู้คืนข้อมูลจากความเสียหาย (Recovery)	- ทำการทดสอบการกู้คืนข้อมูล (Recovery) ทุกๆ ๖ เดือน หรืออย่างน้อยปีละ ๑ ครั้ง	- ทำการทดสอบการกู้คืนข้อมูล (Recovery) ทุกๆ ๖ เดือน หรืออย่างน้อยปีละ ๑ ครั้ง
๒	การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์	(๑) ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย	- ห้ามบุคคลที่ไม่มีหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นจะต้องได้รับอนุญาตจากเจ้าหน้าที่ และที่ประตูมีการป้องกันการเข้าถึงห้องเซิร์ฟเวอร์ โดยการล็อคกุญแจ	- ติดตั้งระบบสแกนลายนิ้วมือเพื่อเข้าออกห้องเซิร์ฟเวอร์
		(๒) การป้องกันการบุกรุก	- ติดตั้ง Firewall ป้องกันไม่ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของจังหวัดราชบุรี - ติดตั้งการทำงานระบบ Load Balance เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ต	

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการตามแผนปี ๒๕๕๕	แนวทางในการดำเนินการในปี ๒๕๕๖
			- มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตว่ามีปริมาณมากผิดปกติหรือไม่ หรือมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้หาสาเหตุและการป้องกันต่อไป	- มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของเจ้าหน้าที่ภายในศาลากลางจังหวัดราชบุรี โดยในการเก็บข้อมูลจราจรนั้น จะสามารถระบุรายละเอียดผู้เข้าใช้บริการระบบเครือข่ายเป็นรายบุคคลได้ โดยมีการตรวจสอบเป็นประจำและสม่ำเสมอ
๓	มีระบบรักษาความมั่นคงปลอดภัย (Security) ของระบบฐานข้อมูล	(๑) ป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย ผู้ใช้งานต้องระมัดระวังในการใช้งานคอมพิวเตอร์ โดยเฉพาะเมื่อเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบ	- ติดตั้ง Antivirus เพื่อป้องกันไว้รัสที่มาจากเครือข่ายภายนอกได้ส่วนหนึ่ง ซึ่งเป็นการแบ่งเบาภาระในการบำรุงรักษาเครื่องคอมพิวเตอร์ ระบบเครือข่ายภายใน ที่เกิดปัญหาต่างๆ - ปี ๒๕๕๕ จังหวัดราชบุรีได้ดำเนินการบำรุงรักษาเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงและการแก้ไขปัญหาระบบ เพื่อให้ผู้ปฏิบัติงานสามารถใช้ระบบสารสนเทศผ่านระบบเครือข่ายได้อย่างมีประสิทธิภาพ และเพื่อควบคุมดูแล บำรุงรักษา ระบบคอมพิวเตอร์ในองค์กรสามารถใช้งานได้ตลอดเวลา โดยแผนการบำรุงรักษาระบบเครื่องคอมพิวเตอร์มีการดำเนินการดังนี้	- ปี ๒๕๕๖ จังหวัดราชบุรีมีแผนการบำรุงรักษาเครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วงและการแก้ไขปัญหาระบบ เพื่อให้ผู้ปฏิบัติงานสามารถใช้ระบบสารสนเทศผ่านระบบเครือข่ายได้อย่างมีประสิทธิภาพ และเพื่อควบคุมดูแล บำรุงรักษา ระบบคอมพิวเตอร์ในองค์กรสามารถใช้งานได้ตลอดเวลา โดยแผนการบำรุงรักษาระบบเครื่องคอมพิวเตอร์มีการดำเนินการดังนี้ ๑. การทำความสะอาด และบำรุงรักษาอุปกรณ์คอมพิวเตอร์ ๒. ตรวจสอบการทำงานของระบบปฏิบัติการ เช่น ลบข้อมูลที่ไม่จำเป็น (Disk Cleanup) และทำการจัดเรียงข้อมูล (Defragmenter) และทำการปรับปรุงช่อง

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการตามแผนปี ๒๕๕๕	แนวทางในการดำเนินการในปี ๒๕๕๖
			๑. การทำความสะอาด และบำรุงรักษาอุปกรณ์คอมพิวเตอร์ ๒. ตรวจสอบการทำงานของระบบปฏิบัติการ เช่น ลบข้อมูลที่ไม่จำเป็น (Disk Cleanup) และทำการจัดเรียงข้อมูล (Defragmenter) และทำการปรับปรุงช่องโหว่ของระบบปฏิบัติการ ๓. ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัส ๔. ถ่ายทอดความรู้และแนะนำการใช้งาน ๕. ให้คำปรึกษาวิธีการใช้ระบบงาน	โหว่ของระบบปฏิบัติการ ๔. ถ่ายทอดความรู้และแนะนำการใช้งาน ๕. ให้คำปรึกษาวิธีการใช้ระบบงาน
		(๒) การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ	- ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) โดยทั่วไประยะเวลาในการสำรองไฟฟ้าประมาณ ๒๐ – ๓๐ นาที - เปิดเครื่องสำรองไฟฟ้าตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์	- ติดตาม ตรวจสอบ บำรุงรักษา อุปกรณ์ให้สามารถใช้งานได้ดีอยู่สม่ำเสมอ - เปิดเครื่องสำรองไฟฟ้าตลอดเวลาในการใช้งานเครื่องคอมพิวเตอร์ - เครื่องสำรองไฟฟ้าอยู่ในสภาพพร้อมใช้งานเสมอ - เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และทำการปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่างๆ - ตรวจสอบปริมาณการใช้งานไม่ให้เกิดโหลด

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการตามแผนปี ๒๕๕๕	แนวทางในการดำเนินการในปี ๒๕๕๖
			- เครื่องสำรองไฟฟ้าอยู่ในสภาพพร้อมใช้งานเสมอ - เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และทำการปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ	
		(๓) มีระบบป้องกันไฟไหม้	- มีอุปกรณ์ดับเพลิงติดตั้งในอาคารศาลากลางจังหวัดราชบุรีหลายจุด	- มีอุปกรณ์ดับเพลิงติดตั้งในอาคารศาลากลางจังหวัดราชบุรีหลายจุด
๔	มีการกำหนดสิทธิ์ให้ผู้ใช้ในแต่ละระดับ (Access rights)	มาตรการพื้นฐานในการสร้างความปลอดภัยให้กับระบบสารสนเทศในการกำหนดรหัสผ่าน มีหลักการดังนี้ (๑) กำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละระดับฐานข้อมูล ดังนี้ - บุคคลที่สามารถละเรียกดูข้อมูลได้เพียงอย่างเดียว จะไม่สามารถแก้ไข ปรับปรุงข้อมูลได้	- มีการกำหนดสิทธิในการเข้าใช้เครื่องคอมพิวเตอร์แม่ข่าย - มีการกำหนดสิทธิในการเข้าใช้ระบบงานต่างๆ - ปฏิบัติตามมาตรการพื้นฐานในการสร้างความปลอดภัยให้กับระบบสารสนเทศในการกำหนดรหัสผ่าน - จังหวัดราชบุรีดำเนินการจัดทำระบบยืนยันตัวบุคคลการใช้อินเตอร์เน็ต ศูนย์ราชการจังหวัดราชบุรี เพื่อรองรับ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และได้ทำการกำหนด Username / Password ให้กับ	- จังหวัดราชบุรีได้ทำการกำหนด Username / Password ให้กับผู้ใช้งานระบบ Internet และระบบงานต่างๆ ซึ่งในส่วนของ Username / Password ที่ใช้ในการ Log in เข้าใช้งานระบบงานต่างๆ นั้น จังหวัดราชบุรีได้ทำการจำกัดสิทธิ์การเข้าใช้ระบบงานตามสถานะของผู้ใช้งาน โดยจะสามารถเข้าใช้งานได้ตามหน้าที่หรือหน่วยงานรับผิดชอบเท่านั้น ไม่สามารถเข้าใช้งานในส่วนอื่นๆ ที่ไม่เกี่ยวข้อง สำหรับผู้ใช้งาน ระบบ Internet ได้มีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ด้วย - มีการให้ความรู้แก่ผู้ใช้ระบบงานถึงข้อ

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการตามแผนปี ๒๕๕๕	แนวทางในการดำเนินการในปี ๒๕๕๖
		- บุคคลที่สามารถเรียกดูข้อมูลและสามารถแก้ไขปรับปรุงข้อมูลได้เฉพาะในส่วนที่ตนรับผิดชอบ - บุคคลที่สามารถเรียกดู และสามารถแก้ไขปรับปรุงข้อมูลในระดับฐานข้อมูล กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบของหน่วยงานเจ้าของระบบงานมอบหมายในการเข้าใช้ฐานข้อมูล แต่ละระบบจะมีการกำหนดสิทธิการเข้าถึงฐานข้อมูลตามหน้าที่ความรับผิดชอบชองผู้ใช้ฐานข้อมูล เพื่อรักษาความปลอดภัยของฐานข้อมูลด้วยการกำหนดชื่อผู้ใช้ Log in และรหัสผ่าน Password (๒) กำหนดระยะเวลาการใช้งานระบบสารสนเทศของผู้ใช้ระบบ (User) โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้เมื่อพ้นระยะเวลาที่กำหนดไว้	ผู้ใช้งาน ระบบ Internet เพื่อให้เป็นไปตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่ใช้ในการ Log in เข้าใช้งานระบบงานต่างๆ นั้น จังหวัดราชบุรีได้ทำการจำกัดสิทธิ์การเข้าใช้ระบบงานตามสถานะของผู้ใช้งาน โดยจะสามารถเข้าใช้งานได้ตามหน้าที่หรือหน่วยงานรับผิดชอบเท่านั้น ไม่สามารถเข้าใช้งานในส่วนอื่นๆ ที่ไม่เกี่ยวข้อง	พึงระวังในการเก็บรักษา Username / Password เพื่อป้องกันผู้อื่นนำไปใช้

ลำดับที่	ประเด็น	มาตรการ	การดำเนินการตามแผนปี ๒๕๕๕	แนวทางในการดำเนินการในปี ๒๕๕๖
		(๓) การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า ๖ ตัวอักษร และควรใช้ตัวเลข อัขระพิเศษประกอบ ผู้ใช้งานระบบสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน การเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรซ้ำกับรหัสเดิม ผู้ใช้จะต้องเก็บรหัสผ่านไว้เป็นความลับ หากผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนใหม่ทันที		

ผนวก ค

ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ

พ.ศ.๒๕๑๗

บทที่ ๕ การรักษาความปลอดภัยเกี่ยวกับสถานที่

ผนวก ค

ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๑๗

บทที่ ๕

การรักษาความปลอดภัยเกี่ยวกับสถานที่

.....

๓๘. คำจำกัดความ

การรักษาความปลอดภัยเกี่ยวกับสถานที่ คือมาตรการที่กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่ที่สงวน อาคาร และสถานที่ของส่วนราชการ ตลอดจนวัสดุ อุปกรณ์ เจ้าหน้าที่และเอกสารในอาคารสถานที่ดงกล่าวให้พ้นจากการโจรกรรม การจารกรรมและการก่อวินาศกรรมหรือเหตุอื่นใดอันอาจทาให้เสียสมรรถภาพในการปฏิบัติภารกิจของส่วนราชการได้

๓๙. ความมุ่งหมาย การรักษาความปลอดภัยเกี่ยวกับสถานที่มีความมุ่งหมายเพื่อ

๓๙.๑ กำหนดมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ของส่วนราชการ

๓๙.๒ เป็นแนวทางในการวางแผนรักษาความปลอดภัยเกี่ยวกับสถานที่ของส่วนราชการที่ตั้งขึ้นใหม่หรือขยายออกไป และเป็นแนวทางในการประเมินค่าแห่งการรักษาความปลอดภัยเกี่ยวกับสถานที่ที่มีอยู่แล้ว

๓๙.๓ เป็นแนวทางให้ส่วนราชการดาเนินมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่ตามความเหมาะสมกับระดับความสำคัญของสถานที่นั้นๆ

๓๙.๔ ช่วยเจ้าหน้าที่รับผิดชอบในการพิทักษ์รักษาสถานที่และวัตถุต่าง ๆ ที่มีค่าสูงของชาติให้ปฏิบัติงานได้อย่างมีประสิทธิภาพ

๔๐. ข้อพิจารณาในการวางมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่

๔๐.๑ ปัจจัยสำคัญที่จะต้องพิจารณาในการวางมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ได้แก่ความสำคัญของภารกิจของส่วนราชการนั้น ๆ สภาพของสถานที่ลักษณะทางภูมิศาสตร์ สถานการณ์ทางเศรษฐกิจอุดมการณ์ทางการเมืองของประชาชนในพื้นที่นั้น ๆ และพฤติการณ์ของฝ่ายที่อาจเป็นศัตรูตลอดจนการสนับสนุนช่วยเหลือที่จะพึงได้รับจากส่วนราชการอื่น 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 โดยหารือกับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของส่วนราชการนั้น ๆ หรือองค์การรักษาความปลอดภัย ทั้งนี้ให้อยู่ในความรับผิดชอบของหัวหน้าส่วนราชการ

๔๑. ภยันตรายที่ควรพิจารณาเกี่ยวกับสถานที่มีภยันตรายที่ควรพิจารณาดังนี้

๔๑.๑ ภยันตรายที่เกิดจากปรากฏการณ์ธรรมชาติและอุบัติเหตุ เช่น พายุ น้ำท่วม ฟ้าผ่า และเพลิงไหม้เป็นต้น

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 จัดทารายงานการสำรวจหรือการตรวจสอบ โดยชี้ให้เห็นข้อบกพร่องของมาตรการการป้องกันที่ใช้อยู่ในปัจจุบันที่จะทาให้เกิดการละเมินการรักษาความปลอดภัยแล้วเสนอแนะให้หัวหน้าส่วนราชการพิจารณาแก้ไขมาตรการและวางระเบียบปฏิบัติในการรักษาความปลอดภัยในเรื่องต่างๆ 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 การตรวจตราเป็นประจาหรือการตรวจสอบตามห้วงระยะเวลา เพื่อค้นหาข้อบกพร่องและสั่งการตามที่เห็นสมควร

๔๓. มาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้ส่วนราชการจัดให้มีการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้เหมาะสม โดยพิจารณาให้มาตรการดังต่อไปนี้

๔๓.๑ เครื่องกีดขวาง คือ เครื่องมือที่ใช้ป้องกัน ขัดขวาง หรือหน่วงเหนี่ยวบุคคลสัตว์หรือยานพาหนะที่ไม่มีสิทธิเข้าไปในพื้นที่รักษาความปลอดภัย โดยใช้เครื่องกีดขวางเป็นแนวเขตของพื้นที่

๔๓.๑.๑ เครื่องกีดขวางตามธรรมชาติ เช่น ทะเล แม่น้ำ ลาคลอง หน้าผา ฯลฯ ที่ได้ดัดแปลงให้เป็นประโยชน์ในการกั้น

๔๓.๑.๒ เครื่องกีดขวางที่ประดิษฐ์ขึ้น รั้วทึบ รั้วโปร่ง เครื่องกั้น ถนน ลวด หีบเพลง กำแพง ลูกกรงเหล็ก ฯลฯ

๔๓.๒ การให้แสงสว่าง การให้แสงสว่างก็เพื่อจะให้มองเห็นบริเวณรั้วและเขตหวงห้ามต่าง ๆ โดยชัดเจนในเวลามืด จะได้มองเห็นผู้ที่บุกรุกเข้ามาในสถานที่ การให้แสงสว่างมี ๒ วิธีคือ

๔๓.๒.๑ การใช้แสงส่องโดยตรง คือการพุ่งแสงสว่างส่องไปยังจุดใดจุดหนึ่งที่ต้องการ เช่น ตัวอาคาร รั้ว หรือประตู เป็นต้น

๔๓.๒.๒ การใช้แสงส่องกระจายรอบตัว ทาให้มีความสว่างทั่วบริเวณ ดวงไฟควรอยู่ในระดับสูงพอที่จะช่วยให้มองเห็นเครื่องกีดขวางต่าง ๆ ได้ชัดเจน ในกรณีที่รั้วเป็นแบบทึบก็ต้องให้มีแสงสว่างส่องให้เห็นได้ทั้งสองด้านและต้องให้รัศมีแสงสว่างของดวงหนึ่ง ๆ ทับเลยเข้าไปในรัศมีของดวงข้างเคียงเพื่อมิให้มีพื้นที่อับแสงระหว่างรัศมีดวงไฟ

๔๓.๓ เจ้าหน้าที่รักษาความปลอดภัยสถานที่ คือ เจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบในการรักษาความปลอดภัย ประกอบด้วยเจ้าหน้าที่เวรรักษาความปลอดภัยประจาวันยามรักษาการณ์และเจ้าหน้าที่อื่น เจ้าหน้าที่รักษาความปลอดภัยสถานที่จัดขึ้นด้วยความมุ่งหมายเพื่อให้การรักษาความปลอดภัยเกี่ยวกับสถานที่มีประสิทธิภาพยิ่งขึ้น เพราะไม่ว่าจะมีเครื่องกีดขวางชนิดใดหากไม่มีการเฝ้ารักษาแล้ว ก็อาจมีการเล็ดลอดเข้าไปได้

๔๓.๓.๑ หน้าที่ เจ้าหน้าที่เวรรักษาความปลอดภัยประจาวันมีหน้าที่กำกับดูแลการปฏิบัติของยามรักษาการณ์และหน้าที่อื่นที่ได้รับมอบหมายจากหัวหน้าส่วนราชการนั้น ๆ ยามรักษาการณ์มีหน้าที่ป้องกันบริเวณเขตหวงห้ามทั้งหมด ตลอดจนวัสดุและสิ่งอุปกรณ์ทั้งปวงทาการตรวจสอบบุคคล ยานพาหนะและสิ่งของต่าง ๆ โดยเฉพาะเกี่ยวกับการป้องกันอัคคีภัย อุบัติเหตุและภยันตรายอื่น ๆ

๔๓.๓.๒ จำนวน 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 ที่ตั้ง ที่ทำการของเจ้าหน้าที่รักษาความปลอดภัยสถานที่ ควรต้องอยู่ในบริเวณที่สามารถปฏิบัติหน้าที่ได้สะดวก ภายในที่ตั้งควรมีที่เก็บอาวุธ เครื่องมือเครื่องใช้และเครื่องมือสื่อสาร ในที่ตั้งจะต้องมีเจ้าหน้าที่รักษาความปลอดภัยสถานที่ประจาอยู่อย่างน้อยหนึ่งคนตลอดเวลา

๔๓.๓.๔ การติดต่อสื่อสาร ในกรณีที่มียามรักษาการณ์ ควรมีโทรศัพท์ตั้งไว้ ณ จุดอันเหมาะสมที่สุดในเส้นทางของยามรักษาการณ์ และควรกำหนดประมวลลับสาหรับใช้พิสูจน์ฝ่ายระหว่างกันขึ้น ยามรักษาการณ์จะต้องรายงานตรงตามกำหนดเวลาเสมอด้วย นอกจากโทรศัพท์ควรกำหนดวิธีการหรือเครื่องมือสื่อสารอื่นสารองไว้ในกรณีที่โทรศัพท์ขัดข้อง

๔๓.๓.๕ ระบบสัญญาณแจ้งภัย ระบบสัญญาแจ้งภัยคือ วิธีการใช้เครื่องมือทางเทคนิคสำหรับตรวจและแจ้งให้ทราบ ในเมื่อมีการเข้าใกล้หรือการล่วงล้าเข้ามาในพื้นที่รักษาความปลอดภัย ระบบสัญญาณแจ้งภัยนี้อาจเป็น เครื่องมือเทคนิคทางอิเล็กทรอนิกส์ ทางไฟฟ้า หรือทางเครื่องกล เช่น แผ่นโลหะ เส้นลวดคลื่นแสง คลื่นเสียง กับดักเป็นต้น ที่จะทาให้เกิดสัญญาณเมื่อมีผู้บุกรุก โดยใช้ติดกับประตู หน้าต่าง ตู้เก็บเอกสาร ห้องนิรภัย กำแพง รั้ว พื้น ฯลฯ

๔๓.๓.๖ การฝึกอบรม เจ้าหน้าที่รักษาความปลอดภัยสถานที่ควรได้รับการฝึกอบรมและมีความรู้ในเรื่องต่าง ๆ ดังนี้

๔๓.๓.๖.๑ การป้องกันการจารกรรมและการก่อวินาศกรรม

๔๓.๓.๖.๒ บริเวณสถานที่ทั้งหมด จุดสำคัญของสถานที่นั้น รวมทั้งที่ตั้งสวิตช์ไฟฟ้าที่สำคัญ ๆ เครื่องมือเครื่องใช้ในการดับเพลิง ตลอดจนภยันตรายต่าง ๆ ที่อาจเกิดขึ้นแก่สถานที่ราชการนั้น ๆ

๔๓.๓.๖.๓ การติดต่อสื่อสารในหน่วยรักษาความปลอดภัย

๔๓.๓.๖.๔ วิธีต่อสู้ป้องกันตัวตามความเหมาะสม

๔๓.๓.๖.๕ ระบบที่ใช้สาหรับแสดงตนซึ่งสถานที่นั้นได้กำหนดไว้

๔๓.๓.๗ เครื่องแบบและอาวุธของยามรักษาการณ์ ยามรักษาการณ์ควรแต่งเครื่องแบบและในขณะปฏิบัติหน้าที่ถ้ามีอาวุธก็ต้องเป็นอาวุธที่ถูกต้องตามกฎหมาย พร้อมทั้งมีความรู้ความ สามารถในเรื่องการใช้อาวุธเป็นอย่างดี

๔๓.๔ การควบคุมบุคคลและยานพาหนะ

๔๓.๔.๑ การควบคุมบุคคล พึงปฏิบัติดังต่อไปนี้

๔๓.๔.๑.๑ จัดให้มีบัตรผ่านสาหรับบุคคลภายในเพื่อใช้แสดงว่าเป็นผู้ที่ได้รับอนุญาตให้ผ่านเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัยได้ การออกแบบบัตรผ่านควรมีลักษณะมิให้ปลอมแปลงได้ง่ายและควรเปลี่ยนรูปแบบตามห้วงระยะเวลาที่เห็นสมควร อย่างน้อยให้มีรายละเอียดแสดงชื่อส่วนราชการ ชื่อ รูปถ่ายส่วนสูง น้าหนัก และลายมือชื่อของผู้ถือบัตร ลายมือชื่อผู้ออกบัตร หมายเลขประจาตัวบัตร วัน เดือน ปี ที่ออกบัตร วันเดือนปีที่บัตรหมดอายุ กับจะต้องควบคุมการจัดทาและการจ่ายบัตรโดยกวดขัน

๔๓.๔.๑.๒ จัดมีป้ายแสดงตนสำหรับบุคคลภายในและภายนอก เพื่อแสดงว่าเป็นบุคคลที่ได้รับอนุญาตให้เข้าไปในพื้นที่ใดได้ในฐานะอะไร ก่อนที่บุคคลดังกล่าวจะเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัยของส่วนราชการนั้น ๆ ให้ติดป้ายแสดงตนไว้ในที่ที่เห็นได้ชัด เช่น ที่อกเสื้อ

๔๓.๔.๑.๓ จัดให้มีการบันทึกหลักฐานสาหรับบุคคลภายนอก เช่นผู้มาประชุม ติดต่อ หรือเยี่ยม ตลอดจนช่างก่อสร้าง ซ่อมแซม ผู้นาส่งหรือรับสิ่งของจากส่วนราชการหรือหน่วยงานเป็น

๔๓.๔.๑.๔ จัดให้มีที่พักผู้มาติดต่อหรือเยี่ยมไว้เป็นพิเศษต่างหาก ไม่ควรอนุญาตให้ผู้มาเยี่ยมเข้าไปยังที่ทางาน นอกจากบุคคลที่มาติดต่อราชการที่เกี่ยวข้องโดยแท้จริง ในการนี้ผู้รับการเยี่ยมจะต้องรับผิดชอบในตัวผู้เยี่ยมตลอดเวลา ตั้งแต่รับตัวมาจากเจ้าหน้าที่รักษาความปลอดภัยสถานที่จนส่งตัวคืน สาหรับคนรถของผู้มาติดต่อหรือเยี่ยมหรือผู้ที่โดยสารมาด้วย คงให้รออยู่ ณ บริเวณที่จอดรถ

๔๓.๔.๒ การควบคุมยานพาหนะ พึงปฏิบัติดังต่อไปนี้

๔๓.๔.๒.๑ มีเจ้าหน้าที่ตรวจสอบยานพาหนะเข้าออกของสถานที่ตั้ง ทำหน้าที่ตรวจสอบบุคคลและสิ่งของต่าง ๆ 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 ลักษณะและจำนวนสิ่งของที่บรรทุกยานพาหนะที่นำเข้าและนำออก

๔๓.๔.๒.๒.๕ วัตถุประสงค์และสถานที่ที่ยานพาหนะจะเข้าไป

๔๓.๔.๒.๒.๖ วัน และเวลาที่ยานพาหนะผ่านออก

๔๓.๔.๒.๓ จัดที่จอดรถให้อยู่ห่างจากตัวอาคารที่สาคัญและหรือสิ่งของที่ติดเพลิงง่ายประมาณไม่น้อยกว่า 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” ซึ่งเป็นพื้นที่ที่มีการพิทักษ์รักษาสิ่งที่เป็นความลับตลอดจนบุคคลสำคัญ ทรัพย์สินหรือวัสดุที่สำคัญของทางราชการ “พื้นที่หวงห้าม” นี้อาจแยกออกเป็น” เขตหวงห้ามเฉพาะ” กับ “เขตหวงห้ามเด็ดขาด”

“เขตหวงห้ามเฉพาะ” คือเขตพื้นที่ซึ่งมีสิ่งที่เป็นความลับตลอดจนบุคคลหรือสิ่งที่มีความสำคัญ ซึ่งจะต้องพิทักษ์รักษาและการเข้าไปในเขตพื้นที่นี้โดยปราศจากการควบคุม อาจทำให้สามารถเข้าถึงความลับ บุคคล และสิ่งอุปกรณ์สำคัญดังกล่าว บุคคลที่ได้รับอนุญาตให้เข้าไปใน “เขตหวง

"เขตหวงห้ามเด็ดขาด" คือ เขตพื้นที่ซึ่งมีสิ่งที่เป็นความลับตลอดจนบุคคลหรือสิ่งที่มีความสำคัญยิ่ง ซึ่งจะต้องพิทักษ์รักษาการเข้าไปในเขตพื้นที่นี้อาจทาให้สามารถเข้าถึงความลับบุคคลและสิ่งที่มีความสำคัญยิ่งในการรักษาความปลอดภัยดังกล่าวโดยตรง บุคคลที่ได้รับอนุญาตให้เข้าไปใน "เขตหวงห้ามเด็ดขาด" จะต้องได้รับความไว้วางใจตามชั้นความลับที่เหมาะสมกับ "เขตหวงห้ามเด็ดขาด" นั้นๆเท่านั้น ตัวอย่าง "เขตหวงห้ามเด็ดขาด" เช่น ศูนย์ปฏิบัติการสื่อสาร ห้องปฏิบัติการลับ ห้องปฏิบัติงานของผู้บังคับบัญชาชั้นสูงห้องหรือสถานที่ขณะที่ใช้ในการประชุมลับและห้องนิรภัยเป็นต้น

๔๓.๖ การป้องกันอัคคีภัย

๔๓.๖.๑ การวางมาตรการการป้องกันอัคคีภัย หัวหน้าหน้าส่วนราชการกำหนดมาตรการป้องกันอัคคีภัย โดยมีเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยเป็นผู้วางแผนและกากับดูแลให้เป็นไปตามกฎหมายว่าด้วยการป้องกันและระงับอัคคีภัย กฎกระทรวง และมติคณะรัฐมนตรี ตลอดจนคำสั่งของทางราชการต่าง ๆ ที่เกี่ยวกับเรื่องนี้

๔๓.๖.๒ เจ้าหน้าที่ดับเพลิง ในเวลาราชการให้จัดข้าราชการเป็นเจ้าหน้าที่ดับเพลิง โดยแบ่งเป็นสองกลุ่ม คือ กลุ่มที่หนึ่งมีหน้าที่ดับเพลิง และอีกกลุ่มหนึ่งมีหน้าที่ขนย้ายเอกสารและควบคุมรับผิดชอบเอกสารและวัสดุ โดยให้แต่ละกลุ่มมีจานวนเพียงพอสาหรับงานนั้น ๆ สาหรับนอกเวลาราชการให้เป็นหน้าที่ของเจ้าหน้าที่เวรรักษาความปลอดภัยประจาวัน และยามรักษาการณ์เป็นผู้รับผิดชอบ

๔๓.๖.๓ การจัดเตรียมเครื่องอุปกรณ์ในการดับเพลิง ให้มีสัญญาณแจ้งเหตุเพลิงไหม้ติดตั้งไว้ และเตรียมเครื่องมือเครื่องใช้ในการดับเพลิงชั้นต้นไว้ให้พร้อม เช่น น้ำ ทราย กระป๋องน้ำ เชือก บันได ขวาน ไม้มือเสือ ตลอดจนเครื่องดับเพลิงให้เหมาะกับประเภทสื่อที่ทาให้เกิดเพลิงไหม้ไว้ทุกประเภท สำหรับเครื่องดับเพลิงเคมีให้ติดตั้งไว้ในที่ที่หยิบฉวยใช้งานได้ง่ายและมีจานวนเพียงพอ โดยหมั่นตรวจสอบให้อยู่ในภาพที่ใช้การได้อยู่เสมอ และแจ้งให้ทุกคนรู้แหล่งน้ำสำหรับใช้ดับเพลิงที่ใกล้ที่สุด ที่ตั้งและหมายเลขโทรศัพท์ของหน่วยดับเพลิงที่ติดต่อได้สะดวกและรวดเร็วที่สุด

๔๓.๖..๔ การฝึกอบรม ให้อบรมเจ้าหน้าที่ให้มีความระมัดระวังเพื่อป้องกันอัคคีภัยและฝึกซ้อมให้มีความรู้ ความชำนาญในการดับเพลิงชั้นต้น 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

.....