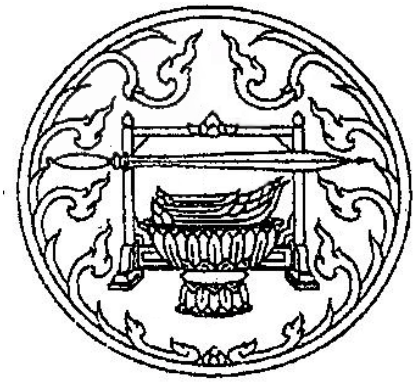

แผนป้องกันและแก้ไขปัญหาภัยพิบัติฉุกเฉินด้านระบบข้อมูลสารสนเทศ
(IT Contingency Plan)

ประจำปี 2553
จังหวัดราชบุรี

กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร
สำนักงานจังหวัดราชบุรี

แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ
ระบบข้อมูลสารสนเทศศูนย์ปฏิบัติการจังหวัดราชบุรี ประจำปี 2553

****

แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ มีการวิเคราะห์ความเสี่ยงในรูปแบบต่างๆ ที่อาจเกิดขึ้น รวมทั้งมีมาตรการในการบริหารจัดการความเสี่ยง เพื่อให้การบริหารและจัดการกับระบบสารสนเทศและเครือข่ายคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ในกรณีที่เกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติขึ้น มีรายละเอียดดังนี้

การวิเคราะห์ความเสี่ยงด้านระบบสารสนเทศ

จากการพิจารณาและวิเคราะห์ความเสี่ยงด้านระบบข้อมูลสารสนเทศที่อาจจะเกิดขึ้น สามารถแยกได้ดังนี้

1. ความเสี่ยงที่เกิดจากภัยพิบัติทางธรรมชาติ เช่น วาตภัย อุทกภัย แผ่นดินไหว
2. ความเสี่ยงที่เกิดจากการกระทำของมนุษย์ เช่น เกิดจากการปฏิบัติงาน กระแสไฟฟ้าขัดข้องหรืออัคคีภัย
3. ความเสี่ยงที่เกิดจากโปรแกรม หรืออุปกรณ์คอมพิวเตอร์ ที่เกิดจากการโจมตีจากไวรัสคอมพิวเตอร์หรือการใช้โปรแกรมที่ไม่มีลิขสิทธิ์ การเคลื่อนย้ายอุปกรณ์หรือการติดตั้งอุปกรณ์ในจุดที่ไม่เหมาะสม
4. ความเสี่ยงที่เกิดจากระบบเครือข่าย ทั้งระบบอินทราเน็ตและอินเตอร์เน็ต รวมถึงความเสี่ยงจากการบุกรุกเครือข่าย
5. ความเสี่ยงด้านระบบข้อมูลสารสนเทศ เช่น ข้อมูลถูกทำลายหรือมีการแก้ไขเปลี่ยนแปลง

การประเมินสถานการณ์ความเสี่ยงด้านระบบสารสนเทศ

ความเสี่ยงที่อาจเป็นอันตรายต่อระบบข้อมูลสารสนเทศ มีดังนี้

1. เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน hardware และ software อันอาจทำให้ระบบข้อมูลสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบข้อมูลสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบข้อมูลสารสนเทศ ในเบื้องต้น จึงได้จัดให้เจ้าหน้าที่เข้ารับการอบรม สัมมนา ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด
2. เกิดจากไวรัสคอมพิวเตอร์ (Computer Virus) สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้

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

2.2 แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านเครือข่าย internet รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจากไวรัสต่างๆ ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

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

4. เกิดจากโจรกรรม การขโมยอุปกรณ์คอมพิวเตอร์ ในส่วนของห้องคอมพิวเตอร์แม่ข่าย ได้กำหนดห้ามผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ผู้รับผิดชอบนำพาเข้าไป

แนวทางปฏิบัติเพื่อป้องกันหรือลดความเสี่ยงด้านระบบข้อมูลสารสนเทศ

1. การบำรุงรักษา

1.1 มีการแก้ไขปัญหาเครื่องคอมพิวเตอร์เบื้องต้นได้โดยผู้ดูแลระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมถึงมีการรับประกันความเสียหายจากผู้ขาย และมีการดูแลอย่างถูกต้องและต่อเนื่อง

1.2 ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

1.3 การใช้แผ่น CD หรือ Handy Drive ควรตรวจสอบไวรัสก่อนใช้ทุกครั้ง

1.4 ควรดูแลทำความสะอาดเครื่องคอมพิวเตอร์และเครื่องแม่ข่ายอย่างสม่ำเสมอ

1.5 การติดตั้ง Firewall เพื่อเป็นการป้องกันเบื้องต้นไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าสู่ระบบเครือข่ายได้

1.6 การฝึกอบรมผู้ดูแลระบบและผู้ใช้ระบบให้มีความรู้ความเข้าใจในระบบงาน รวมทั้งการรักษาความปลอดภัยในการใช้ระบบสารสนเทศ

2. การรักษาความปลอดภัย

2.1 กำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยของคอมพิวเตอร์ และในกรณีที่พบว่ามีการใช้งานหรือมีการเปลี่ยนแปลงในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไขและรายงานให้ผู้บังคับบัญชาทราบทันที

2.2 ทำการทดสอบระบบซอฟต์แวร์เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานอย่างสม่ำเสมอ

2.3 ติดตั้งโปรแกรมระบบรักษาความปลอดภัย เช่น การติดตั้ง Firewall

2.4 กำหนดเจ้าหน้าที่รับผิดชอบในการดำเนินการไว้อย่างชัดเจน

3. มาตรการในการป้องกันไวรัส

3.1 ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอย่างสม่ำเสมอ

3.2 ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ

3.3 ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ 1 ครั้ง

3.4 หลีกเลี่ยงการใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา

4. การจัดการด้านกายภาพและสิ่งแวดล้อม

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

4.2 ควบคุมการเข้าออกห้องปฏิบัติการระบบข้อมูลสารสนเทศ กำหนดเป็นพื้นที่เขตหวงห้ามเฉพาะ และการกำหนดสิทธิการเข้าออกให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

4.3 จัดห้องคอมพิวเตอร์แม่ข่ายให้เป็นสัดส่วนเฉพาะ เพื่อความสะดวกในการปฏิบัติงานและยังทำให้การควบคุมและการเข้าถึงอุปกรณ์คอมพิวเตอร์ต่างๆ มีประสิทธิภาพมากขึ้น โดยจัดแยกส่วนอุปกรณ์ที่จำเป็นในการเข้าถึงข้อมูล เช่น การสำรองข้อมูลไว้กรณีฉุกเฉินเมื่อข้อมูลเกิดความเสียหาย

4.4 วางระบบป้องกันไฟที่เหมาะสม โดยจัดให้มีถังดับเพลิงที่พร้อมใช้งานได้ตลอดเวลา

4.5 จัดให้มีระบบป้องกันไฟฟ้ากระชากและไฟฟ้าดับ เพื่อไม่ให้คอมพิวเตอร์ได้รับความเสียหาย รวมทั้งติดตั้งระบบสายดินที่ได้มาตรฐานหรือจัดให้มีระบบไฟฟ้าสำรอง

4.6 มีการควบคุมสภาพแวดล้อมให้มีอุณหภูมิและความชื้นที่เหมาะสม โดยการตั้งอุณหภูมิเครื่องปรับอากาศและค่าความชื้นให้มีระดับเหมาะสมกับระบบคอมพิวเตอร์

5. การสำรองข้อมูลและกู้คืนข้อมูล

5.1 เพื่อให้มีความพร้อมในการใช้งานและป้องกันการสูญหายของข้อมูล ในส่วนของจังหวัดได้ทำการ Backup ข้อมูลไว้ที่เครื่องแม่ข่ายของจังหวัดและเครื่องแม่ข่ายของบริษัท

5.2 การ Backup ข้อมูลที่จังหวัด เจ้าหน้าที่จะทำการ Backup ข้อมูลลงใน CD-ROM ที่เครื่องแม่ข่ายทุกเดือน

5.3 มีคำสั่งแต่งเจ้าหน้าที่รับผิดชอบงานรักษาความปลอดภัยข้อมูลไว้อย่างชัดเจน

5.4 กำหนดให้มีการทดสอบข้อมูลสำรองอย่างน้อยเดือนละ 1 ครั้ง เพื่อตรวจสอบว่าข้อมูลและโปรแกรมต่างๆ ที่ได้สำรองไว้มีความถูกต้องครบถ้วนและสามารถใช้งานได้

5.5 จัดเก็บรักษาข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัยและติดฉลากไว้อย่างชัดเจน

5.6 หากเกินขีดความสามารถให้ขอรับการสนับสนุนจากจังหวัด หรือศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย

6. การตรวจสอบการเข้าสู่ระบบ

6.1 การกำหนดสิทธิให้แก่ผู้ใช้งาน

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

6.2 ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน

- สำหรับผู้ใช้งานทั่วไป ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 6 เดือน ส่วนผู้ดูแลระบบ ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 3 เดือน

- ในการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรจะกำหนดรหัสผ่านใหม่ซ้ำชื่อเดิม
- ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

7. การจัดการด้านบุคลากร

7.1 กำหนดโครงสร้างบุคลากรด้านเทคโนโลยีสารสนเทศและการบริหารจัดการ ในลักษณะกระจายภารกิจและความรับผิดชอบ รวมทั้งการแต่งตั้งเจ้าหน้าที่ที่มีความรู้ความสามารถและมีประสบการณ์ด้านคอมพิวเตอร์ ซึ่งสามารถถ่ายทอดความรู้ให้แก้ผู้ใช้งานได้อย่างมีประสิทธิภาพ

7.2 หากมีการเปลี่ยนแปลงผู้ดูแลระบบหรือเจ้าหน้าที่ผู้รับผิดชอบจะต้องแจ้งให้ผู้บังคับบัญชาทราบ เพื่อประโยชน์ในการบริหารงาน

7.3 การจัดจ้างบุคคลภายนอก (Outsourcing) เพื่อดำเนินการและควบคุม กำกับดูแล หรือเป็นที่ปรึกษาจากบริษัทที่มีความชำนาญเฉพาะทาง และมีเครื่องมือและเทคโนโลยีที่ทันสมัยและเอื้อต่อการพัฒนาระบบข้อมูลสารสนเทศ

7.4 จัดส่งเจ้าหน้าที่เข้ารับการฝึกอบรมความรู้ทางเทคโนโลยีสารสนเทศเป็นระยะๆ

8. การป้องกันปัญหาที่เกิดจากกระแสไฟฟ้า

หลักปฏิบัติของเจ้าหน้าที่เพื่อป้องกันความเสียหายที่เกิดจากกระแสไฟฟ้ามีดังนี้

8.1 เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งาน ทั้งเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

8.2 เมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

9. การปฏิบัติการรักษาความปลอดภัยสถานที่

ให้ถือปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2517 บทที่ 5 เรื่อง การรักษาความปลอดภัยเกี่ยวกับสถานที่ (ผนวก ก) โดยเคร่งครัด

แนวทางการแก้ไขปัญหาตามแผน IT Contingency Plan
จังหวัดราชบุรี

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

ภัยพิบัติ	แนวทางปฏิบัติเมื่อเกิดเหตุ (IT Contingency Plan)	แนวทางการฟื้นฟูระบบ (Recovery Plan)	หน่วยงานรับผิดชอบ
6. เครื่องคอมพิวเตอร์แม่ข่ายโดนไวรัสคอมพิวเตอร์โจมตี	- กำจัดไวรัสคอมพิวเตอร์ โดยใช้โปรแกรม Anti Virus Nod32 ที่กระทรวงมหาดไทยมีให้ - กรณีที่ไวรัสคอมพิวเตอร์ทำลายระบบจนไม่สามารถให้บริการต่อไปได้ ต้องทำการล้างระบบคอมพิวเตอร์แม่ข่าย แล้วติดตั้งระบบใหม่ และนำข้อมูลจากสำเนาข้อมูล (Backup) ที่จัดเก็บไว้	- ติดตั้งโปรแกรม Anti Virus Nod32 ป้องกันไวรัสคอมพิวเตอร์ และตั้งเวลาให้ทำการ update และตรวจสอบไวรัส ภายในเครื่องอัตโนมัติ	กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร สำนักงานจังหวัดราชบุรี

ผนวก ก
ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.2517
บทที่ 5
การรักษาความปลอดภัยเกี่ยวกับสถานที่

.....

38. คำจำกัดความ

การรักษาความปลอดภัยเกี่ยวกับสถานที่ คือมาตรการที่กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่ที่สงวน อาคาร และสถานที่ของส่วนราชการ ตลอดจนวัสดุ อุปกรณ์ เจ้าหน้าที่และเอกสารในอาคารสถานที่ดงกล่าวให้พ้นจากการโจรกรรม การจารกรรมและการก่อวินาศกรรมหรือเหตุอื่นใดอันอาจทาให้เสียสมรรถภาพในการปฏิบัติภารกิจของส่วนราชการได้

39. ความมุ่งหมาย การรักษาความปลอดภัยเกี่ยวกับสถานที่มีความมุ่งหมายเพื่อ

39.1 กำหนดมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ของส่วนราชการ

39.2 เป็นแนวทางในการวางแผนรักษาความปลอดภัยเกี่ยวกับสถานที่ของส่วนราชการที่ตั้งขึ้นใหม่หรือขยายออกไป และเป็นแนวทางในการประเมินค่าแห่งการรักษาความปลอดภัยเกี่ยวกับสถานที่ที่มีอยู่แล้ว

39.3 เป็นแนวทางให้ส่วนราชการดาเนินมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่ตามความเหมาะสมกับระดับความสำคัญของสถานที่นั้นๆ

39.4 ช่วยเจ้าหน้าที่รับผิดชอบในการพิทักษ์รักษาสถานที่และวัตถุต่าง ๆ ที่มีค่าสูงของชาติให้ปฏิบัติงานได้อย่างมีประสิทธิภาพ

40. ข้อพิจารณาในการวางมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่

40.1 ปัจจัยสำคัญที่จะต้องพิจารณาในการวางมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ได้แก่ความสำคัญของภารกิจของส่วนราชการนั้น ๆ สภาพของสถานที่ลักษณะทางภูมิศาสตร์ สถานการณ์ทางเศรษฐกิจอุดมการณ์ทางการเมืองของประชาชนในพื้นที่นั้น ๆ และพฤติการณ์ของฝ่ายที่อาจเป็นศัตรูตลอดจนการสนับสนุนช่วยเหลือที่จะพึงได้รับจากส่วนราชการอื่น ๆ

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

40.3 ในการออกแบบก่อสร้างที่สงวน อาคารสถานที่หรือเครื่องกีดขวางทางราชการที่มีความสำคัญหรือความลับจะต้องพิทักษ์รักษา ให้สถาปนิก และ/หรือวิศวกรผู้ออกแบบพิจารณาให้ด้านการรักษาความปลอดภัยด้วย โดยหารือกับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของส่วนราชการนั้น ๆ หรือองค์การรักษาความปลอดภัย ทั้งนี้ให้อยู่ในความรับผิดชอบของหัวหน้าส่วนราชการ

41. ภยันตรายที่ควรพิจารณาเกี่ยวกับสถานที่มีภยันตรายที่ควรพิจารณาดังนี้

41.1 ภยันตรายที่เกิดจากปรากฏการณ์ธรรมชาติและอุบัติเหตุ เช่น พายุ น้ำท่วม ฟ้าผ่า และเพลิงไหม้เป็นต้น

41.2 ภยันตรายเกิดจากการกระทำของมนุษย์แบ่งออกเป็น 2 ประเภท คือ

41.2.1 การกระทำโดยเปิดเผย เช่น การโจรกรรม การจลาจล การก่อความไม่สงบ และการโจมตีของข้าศึก เป็นต้น

41.2.2 การกระทำโดยทางลับ เช่น การจารกรรม และการก่อวินาศกรรม เป็นต้น

42. การสำรวจหรือการตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่ ในการสำรวจหรือการตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่ราชการต่าง จะต้องปฏิบัติตามขั้นตอนดังต่อไปนี้

ขั้นที่ 1 ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของส่วนราชการวางแนวทางในการสำรวจหรือการตรวจสอบ โดยวิเคราะห์สภาพแวดล้อม หลักฐานในการปฏิบัติและข้อบกพร่องที่มีมาแล้ว

ขั้นที่ 2 สำรวจบริเวณพื้นที่ และอาคารสถานที่โดยละเอียด

ขั้นที่ 3 จัดทารายงานการสำรวจหรือการตรวจสอบ โดยชี้ให้เห็นข้อบกพร่องของมาตรการการป้องกันที่ใช้อยู่ในปัจจุบันที่จะทาให้เกิดการละเมินการรักษาความปลอดภัยแล้วเสนอแนะให้หัวหน้าส่วนราชการพิจารณาแก้ไขมาตรการและวางระเบียบปฏิบัติในการรักษาความปลอดภัยในเรื่องต่างๆ ดังต่อไปนี้

42.1 เขตรั้วและการจำกัดช่องทางเข้าออก

42.2 การใช้เครื่องกีดขวาง

42.3 การให้แสงสว่าง

42.4 การจัดเจ้าหน้าที่รักษาความปลอดภัยสถานที่

42.5 การติดต่อสื่อสารและระบบสัญญาณแจ้งภัย

42.6 การควบคุมการเข้าออกของบุคคลภายนอก

42.7 การควบคุมการจราจร

42.8 การควบคุมการเข้าออกของเจ้าหน้าที่ภายใน

42.9 การกำหนดพื้นที่ที่มีการรักษาความปลอดภัย

42.10 ที่เก็บอาวุธ กระสุน วัตถุระเบิด หรือวัสดุลับของทางราชการ ซึ่งจะต้องพิทักษ์รักษาเป็นพิเศษ

42.11 การป้องกันอัคคีภัย

42.12 การตรวจตราเป็นประจาหรือการตรวจสอบตามห้วงระยะเวลา เพื่อค้นหาข้อบกพร่องและสั่งการตามที่เห็นสมควร

43. มาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้ส่วนราชการจัดให้มีการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้เหมาะสม โดยพิจารณาให้มาตรการดังต่อไปนี้

43.1 เครื่องกีดขวาง คือ เครื่องมือที่ใช้ป้องกัน ขัดขวาง หรือหน่วงเหนี่ยวบุคคลสัตว์หรือยานพาหนะที่ไม่มีสิทธิเข้าไปในพื้นที่รักษาความปลอดภัย โดยใช้เครื่องกีดขวางเป็นแนวเขตของพื้นที่ก่อให้เกิดภาพทางจิตวิทยา และทางวัตถุทาให้กล้าเข้าหรือหน่วงเหนี่ยวการล่วงล้าเพื่อให้ยามรักษาการณ์มีโอกาสตรวจพบ หยุดยั้งหรือจับกุมได้ อีกทั้งเป็นการประหยัดจานวนเจ้าหน้าที่ยามรักษาการณ์ และเป็น

43.1.1 เครื่องกีดขวางตามธรรมชาติ เช่น ทะเล แม่น้ำ ลาคลอง หน้าผา ฯลฯ ที่ได้ดัดแปลงให้เป็นประโยชน์ในการกั้น

43.1.2 เครื่องกีดขวางที่ประดิษฐ์ขึ้น รั้วทึบ รั้วโปร่ง เครื่องกั้น ถนน ลวด หีบเพลง กำแพง ลูกกรงเหล็ก ฯลฯ

43.2 การให้แสงสว่าง การให้แสงสว่างก็เพื่อจะให้มองเห็นบริเวณรั้วและเขตหวงห้ามต่าง ๆ โดยชัดเจนในเวลามืด จะได้มองเห็นผู้ที่บุกรุกเข้ามาในสถานที่ การให้แสงสว่างมี 2 วิธีคือ

43.2.1 การใช้แสงส่องโดยตรง คือการพุ่งแสงสว่างส่องไปยังจุดใดจุดหนึ่งที่ต้องการ เช่น ตัวอาคาร รั้ว หรือประตู เป็นต้น

43.2.2 การใช้แสงส่องกระจายรอบตัว ทาให้มีความสว่างทั่วบริเวณ ดวงไฟควรอยู่ในระดับสูงพอที่จะช่วยให้มองเห็นเครื่องกีดขวางต่าง ๆ ได้ชัดเจน ในกรณีที่รั้วเป็นแบบทึบก็ต้องให้มีแสงสว่างส่องให้เห็นได้ทั้งสองด้านและต้องให้รัศมีแสงสว่างของดวงหนึ่ง ๆ ทับเลยเข้าไปในรัศมีของดวงข้างเคียงเพื่อมิให้มีพื้นที่อับแสงระหว่างรัศมีดวงไฟ

43.3 เจ้าหน้าที่รักษาความปลอดภัยสถานที่ คือ เจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบในการรักษาความปลอดภัย ประกอบด้วยเจ้าหน้าที่เวรรักษาความปลอดภัยประจาวันยามรักษาการณ์และเจ้าหน้าที่อื่น เจ้าหน้าที่รักษาความปลอดภัยสถานที่จัดขึ้นด้วยความมุ่งหมายเพื่อให้การรักษาความปลอดภัยเกี่ยวกับสถานที่มีประสิทธิภาพยิ่งขึ้น เพราะไม่ว่าจะมีเครื่องกีดขวางชนิดใดหากไม่มีการเฝ้ารักษาแล้ว ก็อาจมีการเล็ดลอดเข้าไปได้

43.3.1 หน้าที่ เจ้าหน้าที่เวรรักษาความปลอดภัยประจาวันมีหน้าที่กำกับดูแลการปฏิบัติของยามรักษาการณ์และหน้าที่อื่นที่ได้รับมอบหมายจากหัวหน้าส่วนราชการนั้น ๆ ยามรักษาการณ์มีหน้าที่ป้องกันบริเวณเขตหวงห้ามทั้งหมด ตลอดจนวัสดุและสิ่งอุปกรณ์ทั้งปวงทาการตรวจสอบบุคคล ยานพาหนะและสิ่งของต่าง ๆ โดยเฉพาะเกี่ยวกับการป้องกันอัคคีภัย อุบัติเหตุและภยันตรายอื่น ๆ

43.3.2 จำนวน การกำหนดเจ้าหน้าที่รักษาความปลอดภัยสถานที่ให้พิจารณาปัจจัยดังต่อไปนี้

43.3.2.1 จุดอ่อนของอาคารสถานที่ต่าง ๆ

43.3.2.2 จำนวนช่องทางเข้าออก

43.3.2.3 ลักษณะของงานและทรัพย์สินที่พึงได้รับการพิทักษ์รักษา

43.3.2.4 จำนวนผู้เยี่ยมเยียน

43.3.2.5 จำนวนบริเวณเขตหวงห้าม

43.3.2.6 จำนวนยานพาหนะที่ผ่านเข้าออก

43.3.2.7 จำนวนเจ้าหน้าที่ในส่วนราชการนั้น ๆ

43.3.2.8 เวลาพักผ่อนของเจ้าหน้าที่รักษาความปลอดภัย

43.3.3 ที่ตั้ง ที่ทำการของเจ้าหน้าที่รักษาความปลอดภัยสถานที่ ควรต้องอยู่ในบริเวณที่สามารถปฏิบัติหน้าที่ได้สะดวก ภายในที่ตั้งควรมีที่เก็บอาวุธ เครื่องมือเครื่องใช้และเครื่องมือสื่อสาร ในที่ตั้งจะต้องมีเจ้าหน้าที่รักษาความปลอดภัยสถานที่ประจาอยู่อย่างน้อยหนึ่งคนตลอดเวลา

43.3.4 การติดต่อสื่อสาร ในกรณีที่มียามรักษาการณ์ ควรมีโทรศัพท์ตั้งไว้ ณ จุดอันเหมาะสมที่สุดในเส้นทางของยามรักษาการณ์ และควรกำหนดประมวลลับสาหรับใช้พิสูจน์ฝ่ายระหว่างกันขึ้น ยามรักษาการณ์จะต้องรายงานตรงตามกำหนดเวลาเสมอด้วย นอกจากโทรศัพท์ควรกำหนดวิธีการหรือเครื่องมือสื่อสารอื่นสารองไว้ในกรณีที่โทรศัพท์ขัดข้อง

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

43.3.6 การฝึกอบรม เจ้าหน้าที่รักษาความปลอดภัยสถานที่ควรได้รับการฝึกอบรมและ มีความรู้ในเรื่องต่าง ๆ ดังนี้

43.3.6.1 การป้องกันการจารกรรมและการก่อวินาศกรรม

43.3.6.2 บริเวณสถานที่ทั้งหมด จุดสำคัญของสถานที่นั้น รวมทั้งที่ตั้งสวิตซ์ไฟฟ้าที่สำคัญ ๆ เครื่องมือเครื่องใช้ในการดับเพลิง ตลอดจนภยันตรายต่าง ๆ ที่อาจเกิดขึ้นแก่สถานที่ราชการนั้น ๆ

43.3.6.3 การติดต่อสื่อสารในหน่วยรักษาความปลอดภัย

43.3.6.4 วิธีต่อสู้ป้องกันตัวตามความเหมาะสม

43.3.6.5 ระบบที่ใช้สาหรับแสดงตนซึ่งสถานที่นั้นได้กำหนดไว้

43.3.7 เครื่องแบบและอาวุธของยามรักษาการณ์ ยามรักษาการณ์ควรแต่งเครื่องแบบ และในขณะปฏิบัติหน้าที่ถ้ามีอาวุธก็ต้องเป็นอาวุธที่ถูกต้องตามกฎหมาย พร้อมทั้งมีความรู้ความ สามารถในเรื่องการใช้อาวุธเป็นอย่างดี

43.4 การควบคุมบุคคลและยานพาหนะ

43.4.1 การควบคุมบุคคล พึงปฏิบัติดังต่อไปนี้

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

43.4.1.2 จัดมีป้ายแสดงตนสำหรับบุคคลภายในและภายนอก เพื่อแสดงว่าเป็นบุคคลที่ได้รับอนุญาตให้เข้าไปในพื้นที่ใดได้ในฐานะอะไร ก่อนที่บุคคลดังกล่าวจะเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัยของส่วนราชการนั้น ๆ ให้ติดป้ายแสดงตนไว้ในที่ที่เห็นได้ชัด เช่น ที่อกเสื้อ

43.4.1.3 จัดให้มีการบันทึกหลักฐานสาหรับบุคคลภายนอก เช่นผู้มาประชุม ติดต่อ หรือเยี่ยม ตลอดจนช่างก่อสร้าง ซ่อมแซม ผู้นาส่งหรือรับสิ่งของจากส่วนราชการหรือหน่วยงานเป็นต้น โดยให้มีรายละเอียด คือ วันและเวลาที่ผ่านเข้า ชื่อ สัญชาติ ตำบลที่อยู่ ชื่อสถานที่ทางาน ชื่อและหน่วยงานของผู้รับการติดต่อหรือเยี่ยม เหตุผลที่มาติดต่อหรือเยี่ยม วันและเวลาที่กลับออกไป ฯลฯ ใน

43.4.1.4 จัดให้มีที่พักผู้มาติดต่อหรือเยี่ยมไว้เป็นพิเศษต่างหาก ไม่ควรอนุญาตให้ผู้มาเยี่ยมเข้าไปยังที่ทางาน นอกจากบุคคลที่มาติดต่อราชการที่เกี่ยวข้องโดยแท้จริง ในการนี้ผู้รับการเยี่ยมจะต้องรับผิดชอบในตัวผู้เยี่ยมตลอดเวลา ตั้งแต่รับตัวมาจากเจ้าหน้าที่รักษาความปลอดภัยสถานที่จนส่งตัวคืน สาหรับคนรถของผู้มาติดต่อหรือเยี่ยมหรือผู้ที่โดยสารมาด้วย คงให้รออยู่ ณ บริเวณที่จอดรถ

43.4.2 การควบคุมยานพาหนะ พึงปฏิบัติดังต่อไปนี้

43.4.2.1 มีเจ้าหน้าที่ตรวจสอบยานพาหนะเข้าออกของสถานที่ตั้ง ทำหน้าที่ตรวจสอบบุคคลและสิ่งของต่าง ๆ บนยานพาหนะและควบคุมบรรดายานพาหนะที่อนุญาตให้ผ่านเข้าไปในสถานที่ต้องนั้น โดยให้ใช้เส้นทางและที่จอดรถที่อนุญาตเท่านั้น

43.4.2.2 ทำบันทึกหลักฐานยานพาหนะเข้าออกตามหัวข้อเหล่านี้ คือ

43.4.2.2.1 วันและเวลาที่ยานพาหนะผ่านเข้า

43.4.2.2.2 ชื่อคนขับและชื่อผู้โดยสาร

43.4.2.2.3 เลขทะเบียนยานพาหนะ

43.4.2.2.4 ลักษณะและจำนวนสิ่งของที่บรรทุกยานพาหนะที่นำเข้าและนำออก

43.4.2.2.5 วัตถุประสงค์และสถานที่ที่ยานพาหนะจะเข้าไป

43.4.2.2.6 วัน และเวลาที่ยานพาหนะผ่านออก

43.4.2.3 จัดที่จอดรถให้อยู่ห่างจากตัวอาคารที่สาคัญและหรือสิ่งของที่ติดเพลิงง่ายประมาณไม่น้อยกว่า 6 เมตร

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

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

43.5.2 กำหนดให้มี “พื้นที่หวงห้าม” ซึ่งเป็นพื้นที่ที่มีการพิทักษ์รักษาสิ่งที่เป็นความลับตลอดจนบุคคลสำคัญ ทรัพย์สินหรือวัสดุที่สำคัญของทางราชการ “พื้นที่หวงห้าม” นี้อาจแยกออกเป็น” เขตหวงห้ามเฉพาะ” กับ “เขตหวงห้ามเด็ดขาด”

“เขตหวงห้ามเฉพาะ” คือเขตพื้นที่ซึ่งมีสิ่งที่เป็นความลับตลอดจนบุคคลหรือสิ่งที่มีความสำคัญ ซึ่งจะต้องพิทักษ์รักษาและการเข้าไปในเขตพื้นที่นี้โดยปราศจากการควบคุม อาจทำให้สามารถเข้าถึงความลับ บุคคล และสิ่งอุปกรณ์สำคัญดังกล่าว บุคคลที่ได้รับอนุญาตให้เข้าไปใน “เขตหวงห้ามเฉพาะ” จะต้องได้รับความไว้วางใจตามชั้นความลับที่เหมาะสมกับ “เขตหวงห้ามเฉพาะ” นั้น ๆหรือมิฉะนั้นก็ต้องจัดเจ้าหน้าที่ควบคุมและกำหนดระเบียบการควบคุมภายในขึ้น ตัวอย่าง “เขตหวงห้าม

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

43.6 การป้องกันอัคคีภัย

43.6.1 การวางมาตรการการป้องกันอัคคีภัย หัวหน้าหน้าส่วนราชการกำหนดมาตรการป้องกันอัคคีภัย โดยมีเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยเป็นผู้วางแผนและกากับดูแลให้เป็นไปตามกฎหมายว่าด้วยการป้องกันและระงับอัคคีภัย กฎกระทรวง และมติคณะรัฐมนตรี ตลอดจนคำสั่งของทางราชการต่าง ๆ ที่เกี่ยวกับเรื่องนี้

43.6.2 เจ้าหน้าที่ดับเพลิง ในเวลาราชการให้จัดข้าราชการเป็นเจ้าหน้าที่ดับเพลิง โดยแบ่งเป็นสองกลุ่ม คือ กลุ่มที่หนึ่งมีหน้าที่ดับเพลิง และอีกกลุ่มหนึ่งมีหน้าที่ขนย้ายเอกสารและควบคุมรับผิดชอบเอกสารและวัสดุ โดยให้แต่ละกลุ่มมีจานวนเพียงพอสาหรับงานนั้น ๆ สาหรับนอกเวลาราชการให้เป็นหน้าที่ของเจ้าหน้าที่เวรรักษาความปลอดภัยประจาวัน และยามรักษาการณ์เป็นผู้รับผิดชอบ

43.6.3 การจัดเตรียมเครื่องอุปกรณ์ในการดับเพลิง ให้มีสัญญาณแจ้งเหตุเพลิงไหม้ติดตั้งไว้และเตรียมเครื่องมือเครื่องใช้ในการดับเพลิงขั้นต้นไว้ให้พร้อม เช่น น้ำ ทราย กระป๋องน้ำ เชือกบันได ขวาน ไม้มือเสือ ตลอดจนเครื่องดับเพลิงให้เหมาะกับประเภทสื่อที่ทาให้เกิดเพลิงไหม้ไว้ทุกประเภท สำหรับเครื่องดับเพลิงเคมีให้ติดตั้งไว้ในที่ที่หยิบฉวยใช้งานได้ง่ายและมีจานวนเพียงพอ โดยหมั่นตรวจสอบให้อยู่ในภาพที่ใช้การได้อยู่เสมอ และแจ้งให้ทุกคนรู้แหล่งน้ำสำหรับใช้ดับเพลิงที่ใกล้ที่สุด ที่ตั้งและหมายเลขโทรศัพท์ของหน่วยดับเพลิงที่ติดต่อได้สะดวกและรวดเร็วที่สุด

43.6..4 การฝึกอบรม ให้อบรมเจ้าหน้าที่ให้มีความระมัดระวังเพื่อป้องกันอัคคีภัยและฝึกซ้อมให้มีความรู้ ความชำนาญในการดับเพลิงชั้นต้น เจ้าหน้าที่ควรมีความรู้ในเรื่องต่าง ๆ เหล่านี้คือ

43.6.4.1 ประเภทของไฟ

43.6.4.2 เครื่องมือเครื่องใช้ในการดับเพลิง

43.6.4.3 การติดต่อสื่อสาร การคมนาคม แผนผังอาคารและบริเวณโดยรอบ

43.6.4.4 ที่ตั้งและหมายเลขโทรศัพท์ของหน่วยดับเพลิง

43.6.4.5 แผนการดับเพลิงของส่วนราชการ

44. **การวางแผนรักษาความปลอดภัยเกี่ยวกับสถานที่** ในการวางแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ต้องพิจารณาจากผลการประมาณการและหรือข้อมูลตามหัวข้อดังต่อไปนี้เป็นหลัก คือ

44.1 สถานการณ์โดยทั่วไปและสภาพแวดล้อมโดยรอบพื้นที่

44.2 ข่าวสาร สิ่งบอกเหตุ และการเตือนภัย

44.3 ภารกิจและหน้าที่ของหน่วยงาน

44.4 จำนวนเจ้าหน้าที่ที่ปฏิบัติงานและเจ้าหน้าที่รักษาความปลอดภัย

44.5 งบประมาณที่จะใช้ในการวางมาตรการการรักษาความปลอดภัย

44.6 การสนับสนุนจากหน่วยเหนือและหน่วยงานอื่น ๆ
44.7 การติดต่อสื่อสารภายในหน่วยกับหน่วยเหนือและหน่วยงานอื่น ๆ
44.8 รายงานการสำรวจหรือการตรวจสอบการรักษาความปลอดภัย

.....