มาตรฐานการรักษาความปลอดภัย
หน่วยงานของรัฐฝ่ายพลเรือน

จัดทำโดย สำนักข่าวกรองแห่งชาติ

คำนำ

สำนักข่าวกรองแห่งชาติ ในฐานองค์การรักษาความปลอดภัยฝ่ายพลเรือน ได้จัดทำมาตรฐานการรักษาความปลอดภัย สำหรับหน่วยงานของรัฐในสังกัดฝ่ายพลเรือน เพื่อเป็นบรรทัดฐานในการกำหนดมาตรการการรักษาความปลอดภัยให้เหมาะสม สอดคล้อง กับสภาพแวดล้อม ภารกิจหน้าที่ ความสำคัญ และความจำเป็นของแต่ละหน่วยงาน

มาตรฐานการรักษาความปลอดภัย หมายถึงระดับที่ควรจะเป็นของมาตรการต่างๆ ที่กำหนดขึ้นเพื่อให้หน่วยงานของรัฐนำไปเป็นแนวทางปฏิบัติ เพื่อพิทักษ์รักษา บุคคล ข้อมูลข่าวสารลับ และสถานที่ ให้พ้นจากการโจรกรรม การจารกรรม การบ่อนทำลาย การก่อวินาศกรรม และการก่อการร้าย รวมถึงการลดความเสียหายที่อาจจะเกิดขึ้นจากการละเมิดการรักษาความปลอดภัย

มาตรฐานการรักษาความปลอดภัย กำหนดแนวทางปฏิบัติไว้ 5 ด้าน คือ

1. มาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล หมายถึง มาตรการที่กำหนดขึ้น เมื่อหน่วยงานนำไปเป็นแนวปฏิบัติสามารถสรรหาบุคคลที่มีคุณสมบัติเหมาะสมและเชื่อแน่ว่า เป็นบุคคลที่ไม่เป็นภัยต่อความมั่นคงเข้ามาปฏิบัติหน้าที่ในหน่วยงาน

2. มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ หมายถึง มาตรการที่กำหนดขึ้น เมื่อหน่วยงานนำไปเป็นแนวปฏิบัติ จะทำให้คุ้มครองข้อมูลข่าวสารลับไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลงหรือรั่วไหลไปสู่บุคคลที่ไม่เกี่ยวข้องได้

3. มาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ หมายถึง มาตรการที่กำหนดขึ้น เมื่อหน่วยงานนำไปเป็นแนวปฏิบัติจะทำให้พิทักษ์รักษาอาคาร สถานที่ วัสดุอุปกรณ์ตลอดจนเจ้าหน้าที่และข้อมูลข่าวให้รอดพ้นจากภัยอันตราย

4. มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ หมายถึงมาตรการที่กำหนดขึ้น เมื่อหน่วยงานนำไปปฏิบัติจะคุ้มครองข้อมูลข่าวสารลับที่อยู่ในระบบอิเล็กทรอนิกส์ ให้พ้นจากการสูญหาย ถูกทำลาย เปลี่ยนแปลงหรือรั่วไหลได้

5. มาตรฐานการรักษาความปลอดภัยในการประชุมลับ หมายถึงมาตรการที่กำหนดขึ้น หน่วยงานนำไปปฏิบัติจะพิทักษ์รักษาสิ่งที่เป็นความลับในการประชุมไม่ให้รั่วไหล รวมถึงคุ้มครองบุคคลและสถานที่ในการประชุมลับ

สำนัก10 สำนักข่าวกรองแห่งชาติ

ธันวาคม 2553

สารบัญ

ส่วนที่ 1
มาตรฐานการรักษาความปลอดภัย

1. หลักการและเหตุผล

ประเทศไทยต้องเผชิญกับความเปลี่ยนแปลงจากภัยคุกคามหลายรูปแบบ ทั้งภัยธรรมชาติ ภัยที่เกิดจากการกระทำของมนุษย์โดยทางตรงและทางอ้อม ซึ่งสร้างความเสียหายต่อชีวิต ทรัพย์สินของประชาชน หน่วยงานของรัฐ และส่งผลกระทบต่อการปฏิบัติหน้าที่ราชการ รวมทั้งทรัพย์สินของทางราชการ แม้หน่วยงานของรัฐหลายแห่ง ได้กำหนดกลยุทธ์ในการป้องกันแล้ว แต่ปัญหาดังกล่าวยังไม่หมดไป ซึ่งอาจเกิดขึ้นใหม่ได้อีก โดยมีเหตุปัจจัยสถานการณ์แวดล้อมแตกต่างกันไป

จากสถานการณ์ดังกล่าวข้างต้น เพื่อให้การดำเนินการรักษาความปลอดภัยอย่างเป็นระบบ และได้มาตรฐาน นับเป็นกลยุทธ์ที่สำคัญอย่างยิ่งที่จะช่วยป้องกันภัยคุกคามและบรรเทาความเสียหายที่อาจเกิดขึ้นได้อย่างมีประสิทธิผล เพื่อเป็นการตอบสนองต่อหลักการรักษาความปลอดภัย สำนักข่าวกรองแห่งชาติ สำนักนายกรัฐมนตรี ในฐานะองค์การรักษาความปลอดภัยฝ่ายพลเรือน ได้เล็งเห็นถึงความสำคัญและความจำเป็น จึงกำหนดมาตรฐานการรักษาความปลอดภัยขึ้น เพื่อให้หน่วยงานของรัฐฝ่ายพลเรือน นำไปเป็นแนวทางปฏิบัติในการวางมาตรการการรักษาความปลอดภัยขั้นพื้นฐานในหน่วยงานของรัฐต่อไป

2. วัตถุประสงค์

เพื่อกำหนดแนวทางการปฏิบัติเกี่ยวกับการรักษาความปลอดภัยหน่วยงานของรัฐให้เป็นไปในแนวทางเดียวกัน ดังนี้

2.1 มีความรู้ความเข้าใจในเรื่องการรักษาความปลอดภัย และความจำเป็นที่ต้องจัดทำระบบการรักษาความปลอดภัย

2.2 ดำเนินการและปฏิบัติตามคำแนะนำของมาตรฐานการรักษาความปลอดภัยที่กำหนดไว้

2.3 ควบคุม กำกับและดูแลระบบการรักษาความปลอดภัย ตลอดจนทบทวนปรับปรุงให้เหมาะสมกับสถานการณ์และสิ่งแวดล้อม ให้มีประสิทธิภาพอยู่เสมอ

3. การบริหารจัดการด้านการรักษาความปลอดภัย

3.1 หัวหน้าหน่วยงานของรัฐมีหน้าที่รับผิดชอบและจัดให้มีระบบการรักษาความปลอดภัยในหน่วยงานของตน

3.2 หัวหน้าหน่วยงานของรัฐ อาจมอบอำนาจหน้าที่ให้แก่ผู้ใต้บังคับบัญชาให้ปฏิบัติหน้าที่ เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย เพื่อทำหน้าที่ดำเนินการควบคุม กำกับดูแล ตลอดจนให้คำปรึกษาเกี่ยวกับการรักษาความปลอดภัยด้าน บุคคล ข้อมูลข่าวสารลับ และสถานที่ ของหน่วยงานนั้น ๆ โดยมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร และรับรองความไว้วางใจให้เข้าถึงชั้นความลับ

3.3 หน่วยงานของรัฐ มีหน้าที่รับผิดชอบจัดการอบรมเจ้าหน้าที่ของหน่วยงานให้ทราบถึงความจำเป็นและมาตรการของการรักษาความปลอดภัย รวมทั้งจัดให้มี การอบรมและทบทวน เพิ่มเติมอยู่เสมอ ตามห้วงระยะเวลาที่เหมาะสม

3.4 กรณีหน่วยงานของรัฐมอบหมาย หรือทำสัญญาจ้างให้ภาคเอกชนดำเนินการอย่างหนึ่งอย่างใดซึ่งเกี่ยวข้องกับการรักษาความปลอดภัย ให้ภาคเอกชนนั้นถือปฏิบัติตามมาตรฐานการรักษาความปลอดภัยนี้ด้วย

4. การจัดทำแผนการรักษาความปลอดภัย

หน่วยงานของรัฐต้องจัดทำแผนการปฏิบัติด้านการรักษาความปลอดภัย ทั้งในเวลาปกติ และเวลาฉุกเฉิน เพื่อพิทักษ์รักษา และคุ้มครองป้องกันสิ่งที่เป็นความลับของทางราชการ เจ้าหน้าที่ของรัฐ หน่วยงานของรัฐ และทรัพย์สินมีค่าของแผ่นดินให้พ้นจากการโจรกรรม การบ่อนทำลาย การจารกรรม และการก่อวินาศกรรม หรือการกระทำอื่นใดที่มีผลกระทบต่อความมั่นคงและผลประโยชน์แห่งรัฐ แผนการรักษาความปลอดภัยที่มีประสิทธิภาพจำเป็นต้องดำเนินการเกี่ยวกับการรักษาความปลอดภัยด้านบุคคล ข้อมูลข่าวสารลับ และสถานที่ ให้สอดคล้องกับความสำคัญของหน่วยงานและสภาพแวดล้อมของแต่ละส่วนราชการ โดยต้องมีการปรับปรุงทบทวนแก้ไขให้เหมาะสมอยู่เสมอ และสอดคล้องกับมติคณะกรรมการนโยบายรักษาความปลอดภัยแห่งชาติ (กรช.) เมื่อ 1 กันยายน 2553 ให้หน่วยงานของรัฐเคร่งครัดในการตรวจสอบและจัดระเบียบการควบคุมการรักษาความปลอดภัยให้เป็นไปตามระเบียบการรักษาความปลอดภัยที่กำหนด แล้วส่งให้องค์การรักษาความปลอดภัยพิจารณา

บทที่ 1

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล

การรักษาความปลอดภัยเกี่ยวกับบุคคล เป็นมาตรการที่กำหนดขึ้นสำหรับใช้ปฏิบัติต่อผู้ที่อยู่ระหว่างรอบรรจุ หรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ หรือผู้ที่จะได้รับความไว้วางใจให้เข้าถึงสิ่งที่เป็นความลับของทางราชการ หรือให้ปฏิบัติหน้าที่ราชการที่สำคัญ เพื่อเลือกเฟ้น และตรวจสอบ ให้ได้ผู้ที่มีคุณสมบัติเหมาะสมให้เป็นที่เชื่อแน่ว่าต้องเป็นผู้ที่ไม่เป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ

หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการปฏิบัติ หรือมอบหมายให้มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล ดังนี้

1. ดำเนินการตรวจสอบประวัติและพฤติการณ์บุคคล

1.1 ผู้ที่อยู่ระหว่างรอบรรจุหรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ

1.2 ผู้ที่เป็นลูกจ้างทดลองปฏิบัติงาน หรือฝึกงานก่อนบรรจุเข้าปฏิบัติงาน

1.3 เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์และผู้ที่ขอกลับเข้ารับราชการใหม่

1.4 เจ้าหน้าที่ของรัฐหรือบุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน้าที่ หรือตำแหน่งสำคัญของหน่วยงาน หรือเกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการ ทรัพย์สิน มีค่าของแผ่นดิน

1.5 ผู้ได้รับทุนการศึกษาทั้งในประเทศหรือต่างประเทศแล้วมีข้อผูกพันให้เข้าปฏิบัติงานให้แก่หน่วยงานของรัฐเมื่อสำเร็จการศึกษา

1.6 บุคคลภายนอกที่เข้ามาปฏิบัติงานให้หน่วยงานของรัฐ

1.7 กรณีตรวจพบบุคคลที่มีพฤติการณ์ หรือปรากฏข่าวสารที่น่าจะเป็นภัยต่อความมั่นคง และผลประโยชน์แห่งรัฐ หรือบุคคลที่เกี่ยวข้องกับชั้นความลับของทางราชการ หัวหน้าหน่วยงานของรัฐ อาจขอให้องค์การรักษาความปลอดภัยตรวจสอบเพิ่มเติมได้

2. หน่วยงานของรัฐต้องจัดให้มีการรับรองความไว้วางใจบุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการ โดยมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร และต้องผ่านการตรวจสอบประวัติและพฤติการณ์

3. เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหน่วยงานของรัฐ ต้องบันทึกชื่อบุคคลที่ได้รับการรับรองความไว้วางใจไว้ในทะเบียนความไว้วางใจของหน่วยงาน

4. หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการอบรมชี้แจงเกี่ยวกับระเบียบการรักษาความปลอดภัยแก่บุคคลที่ได้รับการบรรจุใหม่ ผู้ที่ไม่เคยได้รับการอบรม หรือผู้ที่จะได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับความลับของทางราชการ รวมถึงการให้ความรู้ในวิทยาการด้านต่าง ๆ และต้องอบรมทบทวนตามระยะเวลาที่เหมาะสม เพื่อกระตุ้นจิตสำนึกและวินัยในด้านการรักษาความปลอดภัย

บทที่ 2

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ

เป็นการคุ้มครองข้อมูลข่าวสารลับไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง หรือรั่วไหล การเปิดเผยข้อมูลข่าวสารลับต่อบุคคลผู้ไม่มีอำนาจหน้าที่ต้องอยู่ภายใต้เงื่อนไข โดยมีข้อยกเว้นที่ชัดเจนสอดคล้องกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544

ข้อมูลข่าวสารลับ ที่กล่าวถึงในมาตรฐานการรักษาความปลอดภัยข้อมูลข่าวสารลับนี้ หมายถึง ข้อมูลข่าวสารที่มีคำสั่งไม่ให้เปิดเผยตามมาตรา 14 หรือ มาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 และอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน มีการกำหนดให้มีชั้นความลับชั้นลับ ลับมาก หรือลับที่สุด โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกัน ซึ่งเป็นข้อมูลข่าวสารในรูปเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม หรือการบันทึกภาพ ส่วนข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ จะมีการกำหนดมาตรฐานและคู่มือการปฏิบัติไว้เป็นการเฉพาะ

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการปฏิบัติดังนี้

1. หัวหน้าหน่วยงานของรัฐต้องมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร และให้การรับรองความไว้วางใจแก่บุคคลที่เกี่ยวข้องกับการดำเนินการต่อข้อมูลข่าวสารลับ ดังนี้

1.1 นายทะเบียนข้อมูลข่าวสารลับ และผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับทำหน้าที่ดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ

1.2 ผู้มีอำนาจในการกำหนดชั้นความลับ

1.3 คณะกรรมการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ ประกอบด้วย คณะกรรมการตรวจสอบข้อมูลข่าวสารลับ คณะกรรมการทำลายข้อมูลข่าวสารลับ

1.4 อนุญาตให้ส่งข้อมูลข่าวสารลับ ทั้งภายในและภายนอกประเทศด้วยวิธีทางโทรคมนาคม ไปรษณีย์ลงทะเบียนตอบรับ ฯลฯ

2. การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ ต้องดำเนินการตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ที่กำหนดไว้อย่างเคร่งครัด

2.1 การกำหนดชั้นความลับและแสดงเหตุผล

หน่วยงานของรัฐที่มีข้อมูลข่าวสารลับ ต้องมีการกำหนดชั้นความลับให้ข้อมูลข่าวสารนั้น โดยต้องระบุเหตุผลย่อ (ให้สอดคล้องกับข้อมูลข่าวสารที่ไม่ต้องเปิดเผยตามมาตรา14 และ15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540) ของการกำหนดชั้นความลับนั้นไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับ ต้องแสดงชั้นความลับให้เห็นชัดเจน ข้อมูลข่าวสารลับสามารถ ปรับลด เพิ่ม ยกเลิก ชั้นความลับได้ โดยหน่วยงานเจ้าของเรื่องเดิม ผู้มีอำนาจกำหนดชั้นความลับของข้อมูลข่าวสารลับนั้น

2.2 การจัดทำข้อมูลข่าวสารลับ

2.2.1 กำหนดจำนวนเจ้าหน้าที่ที่เกี่ยวข้องและจำกัดให้ทราบเท่าที่จำเป็น

2.2.2 มีการคุมชุดข้อมูลข่าวสารลับ

2.3 หน่วยงานของรัฐที่ครอบครองข้อมูลข่าวสารลับ สามารถ สำเนา แปล เข้ารหัส หรือถอดรหัสข้อมูลข่าวสารลับเองได้ โดยต้องบันทึกรายละเอียดไว้ที่ต้นฉบับและฉบับที่ดำเนินการสำเนา แปล เข้าหรือถอดรหัสด้วย

2.4 การโอนข้อมูลข่าวสารลับภายในหน่วยงาน หรือ ระหว่างหน่วยงาน ต้องได้รับการอนุมัติจากหัวหน้าหน่วยงานของรัฐ และบันทึกการโอนไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับ

2.5 การส่ง การรับ ข้อมูลข่าวสารลับ

2.5.1 การส่งข้อมูลข่าวสารลับภายในหน่วยงาน ต้องใช้ใบปกข้อมูลข่าวสารลับปิดทับข้อมูลข่าวสารลับ และการส่งออกนอกหน่วยงานต้องบรรจุซอง หรือภาชนะทึบแสงสองชั้นอย่างมั่นคง และแยกทะเบียนข้อมูลข่าวสารลับ ออกจากทะเบียน รับ- ส่งข้อมูลข่าวสารที่ไม่มีชั้นความลับ

2.5.2 การรับข้อมูลข่าวสารลับ ต้องให้นายทะเบียนข้อมูลข่าวสารลับหรือผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ ลงชื่อในใบตอบรับแล้วส่งคืนใบตอบรับนั้นแก่ผู้นำส่งหรือจัดส่งคืนภายหลัง และลงทะเบียนข้อมูลข่าวสารลับก่อนที่จะดำเนินการต่อไป

2.6 การเก็บรักษาข้อมูลข่าวสารลับ หน่วยงานของรัฐต้องเก็บรักษาไว้ในที่ปลอดภัย และควรกำหนดระเบียบการเก็บรักษาข้อมูลข่าวสารลับของหน่วยงานตนเองเพิ่มเติม

2.7 การยืมข้อมูลข่าวสารลับของหน่วยงานอื่น ต้องได้รับอนุญาตจากหน่วยงานเจ้าของเรื่อง ยกเว้นเป็นการขอยืมภายในหน่วยงานเจ้าของเรื่องและต้องบันทึกการยืมไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับ

2.8 การทำลายข้อมูลข่าวสารลับทุกชั้นความลับ ต้องส่งให้หอจดหมายเหตุแห่งชาติพิจารณาก่อนทำลาย ยกเว้นข้อมูลข่าวสารลับ ชั้นลับที่สุด ที่เสี่ยงต่อการรั่วไหลอันก่อให้เกิดอันตรายแก่ประโยชน์แห่งรัฐ หัวหน้าหน่วยงานของรัฐอาจพิจารณาทำลายเองได้

2.9 หากข้อมูลข่าวสารลับสูญหาย ผู้ทราบข้อเท็จจริงต้องรายงานให้หัวหน้าหน่วยงานของรัฐที่ตนสังกัดและหน่วยงานเจ้าของเรื่องเดิมทราบ เพื่อดำเนินการตรวจสอบและสอบสวนข้อเท็จจริง และจดแจ้งการสูญหายไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับ

2.10 การเปิดเผยข้อมูลข่าวสารลับของหน่วยงาน ให้ปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544

2.10.1 การเปิดเผยข้อมูลข่าวสารลับโดยหัวหน้าหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐ ตาม ม.20 (1) แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

2.10.2 การเปิดเผยข้อมูลข่าวสารลับกรณีคำวินิจฉัยของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร

3. หน่วยงานของรัฐต้องจัดให้มีแผนการปฏิบัติต่อข้อมูลข่าวสารลับในเวลาปกติและเวลาฉุกเฉิน เพื่อป้องกันการเข้าถึงของบุคคลที่ไม่มีอำนาจหน้าที่ โดยจัดทำแผนดังนี้

3.1 แผนเคลื่อนย้ายข้อมูลข่าวสารลับ

3.2 แผนการพิทักษ์รักษา

3.3 แผนการทำลาย

บทที่ 3

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

เพื่อเป็นการคุ้มครองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง หรือรั่วไหล มีความมั่นคงปลอดภัยและเชื่อถือได้ หน่วยงานของรัฐควรพิจารณาถึงหลักการในการรักษาความปลอดภัย เกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ดังนี้

1. การควบคุมการเข้าถึง

กำหนดตัวบุคคล การรหัส จำกัดสิทธิของเจ้าหน้าที่ผู้ใช้งาน ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และกำหนดพื้นที่ที่มีการรักษาความปลอดภัย

2. การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

2.1 การจัดทำ

2.1.1 การจัดทำต้องดำเนินการโดยเจ้าหน้าที่ผู้มีสิทธิในการเข้าถึงข้อมูลข่าวสารลับ และผ่านการตรวจสอบประวัติและพฤติการณ์

2.1.2 ชุดอุปกรณ์คอมพิวเตอร์ที่ใช้จัดทำข้อมูลข่าวสารลับ ไม่ควรใช้เครื่องที่เชื่อมต่อกับระบบเครือข่ายอิเล็กทรอนิกส์ (อินเตอร์เน็ต)

2.1.3 สถานที่ที่ใช้จัดทำข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ควรเป็นพื้นที่ที่มีการรักษาความปลอดภัย

2.1.4 การสำเนา การแปล การแจกจ่าย การโอน ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ต้องมีการควบคุมการดำเนินการ

2.2 การจัดเก็บ

2.2.1 ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ทุกชั้นความลับ ต้องเข้ารหัส และจัดเก็บในเครื่องคอมพิวเตอร์แม่ข่ายหรือจัดเก็บในสื่ออิเล็กทรอนิกส์ที่มีระบบการรักษาความปลอดภัยในการเข้าใช้งานเครื่องคอมพิวเตอร์

2.2.2 สถานที่จัดเก็บเครื่องคอมพิวเตอร์แม่ข่าย และสื่ออิเล็กทรอนิกส์ควรเป็นพื้นที่ที่มีการรักษาความปลอดภัย

2.2.3 ควรมีระบบสำรองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์และเครื่องคอมพิวเตอร์แม่ข่ายสำรอง โดยแยกจัดเก็บในสถานที่ปลอดภัย

2.3 การ รับ-ส่ง

2.3.1 ข้อมูลข่าวสารลับที่ รับ-ส่ง ทางระบบโทรคมนาคม จะต้องดำเนินการเข้ารหัสแล้วเท่านั้น

2.3.2 กำหนดระเบียบปฏิบัติการ รับ-ส่ง ข้อมูลข่าวสารลับทางระบบโทรคมนาคม

2.3.3 จัดทำทะเบียนเจ้าหน้าที่ควบคุมการรหัสและเจ้าหน้าที่การรหัส

2.4 การทำลาย

2.4.1 ขั้นตอนการขออนุมัติทำลายข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ใช้หลักการเดียวกับข้อมูลข่าวสารลับที่เป็นเอกสาร

2.4.2 วิธีการทำลายข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ใช้ชุดคำสั่งในระบบปฏิบัติการหรือโปรแกรมซึ่งทำหน้าที่ลบแฟ้มข้อมูลโดยไม่สามารถกู้กลับคืนได้

บทที่ 4

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่

มาตรฐานที่กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่ที่สงวน อาคาร และสถานที่ของหน่วยงานของรัฐ ตลอดจนวัสดุอุปกรณ์ เจ้าหน้าที่ของรัฐ และข้อมูลข่าวสาร ในอาคารสถานที่ดังกล่าวให้พ้นจากการโจรกรรม การจารกรรม การก่อวินาศกรรม การก่อการร้าย หรือเหตุอื่นใด อันอาจทำให้เสียสมรรถภาพในการปฏิบัติภารกิจของหน่วยงาน ซึ่งจะส่งผลให้เกิดความเสียหายต่อหน่วยงานของรัฐ

หน่วยงานของรัฐต้องดำเนินการสำรวจ ตรวจสอบ และจัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่

การกำหนดมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ ให้ดำเนินการดังนี้

1. หน่วยงานของรัฐต้องกำหนดพื้นที่รักษาความปลอดภัยตามความเหมาะสม กำหนดขอบเขตที่แน่ชัดว่าพื้นที่ใดเป็นพื้นที่ควบคุม หรือพื้นที่หวงห้าม เพื่อควบคุมการเข้า-ออก ของบุคคล และยานพาหนะ

2. วางระบบป้องกันทางวัตถุเพื่อเป็นเครื่องหน่วงเหนี่ยว กีดขวาง ป้องกันบุคคล หรือยานพาหนะที่ไม่มีสิทธิเข้าไปในพื้นที่ที่มีการรักษาความปลอดภัย เช่น รั้ว เครื่องกีดขวาง ช่องทาง เข้า-ออก รวมถึงระบบการให้แสงสว่างในยามวิกาล

3. การควบคุมบุคคลและยานพาหนะ

3.1 การควบคุมบุคคล เพื่อตรวจสอบให้ทราบว่าเป็นบุคคลที่ได้รับอนุญาตให้ผ่านเข้าพื้นที่ โดยจัดทำบัตรผ่าน บัตรแสดงตน และบันทึกหลักฐานการผ่าน เข้า ออก นั้น

3.2 การควบคุมยานพาหนะ เพื่อให้ทราบว่ายานพาหนะใดได้รับอนุญาตให้ผ่านเข้าในบริเวณพื้นที่ได้ และยังรวมถึงการควบคุมบุคคล และสิ่งของต่าง ๆ บนยานพาหนะด้วย

4. ระบบรักษาการณ์ หน่วยงานของรัฐต้องจัดให้มีเจ้าหน้าที่รักษาความปลอดภัยประจำวัน เจ้าหน้าที่ยามรักษาการณ์ ฯลฯ วางระบบการติดต่อสื่อสารและสัญญาณแจ้งภัย สำหรับตรวจและเตือนให้ทราบเมื่อมีภัย รวมถึงการติดตั้งอุปกรณ์เสริมมาตรการการรักษาความปลอดภัยทางเครื่องมือเครื่องใช้อิเล็กทรอนิกส์หรืออื่น ๆ เพื่อให้การรักษาความปลอดภัยมีประสิทธิภาพมากยิ่งขึ้น

5. ระบบป้องกันและระงับอัคคีภัย หัวหน้าหน่วยงานของรัฐต้องจัดให้มีมาตรการป้องกันและระงับอัคคีภัยที่มีประสิทธิภาพ

บทที่ 5

มาตรฐานการรักษาความปลอดภัยในการประชุมลับ

หัวหน้าหน่วยงานของรัฐต้องจัดให้มีมาตรการการรักษาความปลอดภัยในการประชุมลับ โดยกำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับบุคคล ข้อมูลข่าวสารลับ และสถานที่ เพื่อพิทักษ์รักษาสิ่งที่เป็นความลับของทางราชการที่ปรากฏในการประชุมลับไม่ให้มีการรั่วไหล ถูกจารกรรม รบกวน หรือขัดขวางการประชุม รวมทั้งคุ้มครองบุคคลและสถานที่ที่เกี่ยวข้องกับการประชุมลับนั้นจากการก่อวินาศกรรม ทั้งนี้ ให้นำมาตรฐานของการรักษาความปลอดภัยแต่ละเรื่องมาปรับใช้โดยอนุโลม

บทที่ 6

มาตรฐานการปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

หัวหน้าหน่วยงานของรัฐต้องกำหนดแนวทางปฏิบัติ เมื่อเกิดการละเมิดการรักษาความปลอดภัย เพื่อลดระดับความเสียหายกรณีเกิดการละเมิด ฝ่าฝืน หรือละเลยไม่ปฏิบัติตามมาตรการการรักษาความปลอดภัยที่กำหนดไว้ จะโดยเจตนาหรือไม่ก็ตาม อันเป็นเหตุให้ความลับของทางราชการรั่วไหล หรือเป็นเหตุให้เจ้าหน้าที่ของรัฐ วัสดุอุปกรณ์ ทรัพย์สินของรัฐได้รับความเสียหาย และป้องกันไม่ให้เกิดซ้ำ ค้นหาข้อบกพร่อง สาเหตุ เพื่อนำมาปรับปรุงแก้ไขมาตรการการรักษาความปลอดภัยให้รัดกุมยิ่งขึ้น

ส่วนที่ 2

บทที่ 7

คู่มือการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล

บุคคลเป็นปัจจัยสำคัญที่สุดในการปฏิบัติตามมาตรการการรักษาความปลอดภัยทุกด้านให้สำเร็จและมีประสิทธิภาพ อย่างไรก็ดี บุคคลอาจเป็นต้นเหตุที่ก่อให้เกิดความเสียหายต่อระบบการรักษาความปลอดภัยได้เช่นกัน ฉะนั้น การรักษาความปลอดภัยเกี่ยวกับบุคคลจึงกำหนดขึ้น เพื่อคัดกรอง ตรวจสอบบุคคลที่จะเข้าปฏิบัติงานให้กับหน่วยงานของรัฐ เพื่อให้ได้ผู้ที่มีคุณสมบัติเหมาะสม และมีความประพฤติที่ไม่เสียหาย หรือเป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ

1. การตรวจสอบประวัติและพฤติการณ์บุคคล

บุคคลที่ต้องได้รับการตรวจสอบประวัติและพฤติการณ์ คือ ผู้ได้รับการบรรจุเป็นเจ้าหน้าที่ใหม่ของรัฐ เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์ ผู้ที่ขอกลับเข้ารับราชการ นักเรียน นักศึกษา นิสิตผู้รับทุนของหน่วยงานของรัฐที่มีข้อผูกพันว่าจะได้รับการบรรจุเข้าทำงานในหน่วยงานของรัฐนั้น ๆ บุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน่วยงานของรัฐ เช่น พนักงานที่จัดจ้างจากบริษัทภายนอก บุคคลที่ได้รับการแต่งตั้งให้ดำรงตำแหน่งสำคัญ ตามความเหมาะสมของภารกิจในหน่วยงานของรัฐ บุคคลที่มีพฤติการณ์หรือปรากฏข่าวสาร หรือติดต่อกับบุคคล หรือองค์กรที่อาจเป็นภัยต่อความมั่นคงของประเทศ เจ้าหน้าที่ของรัฐที่เข้าถึงเรื่อง**ลับที่สุด ลับมาก ลับ หรือการรหัส**

การตรวจสอบประวัติและพฤติการณ์บุคคล หน่วยงานของรัฐนั้น ๆ ดำเนินการตรวจสอบเองได้ โดยขอคำแนะนำจากองค์การรักษาความปลอดภัย เพื่อให้ได้บุคคล ที่มีคุณสมบัติครบถ้วนตรงตามวัตถุประสงค์ของหน่วยงานและตามกฎหมายหรือระเบียบข้อบังคับ

แนวทางการตรวจสอบประวัติและพฤติการณ์บุคคล

1. การตรวจสอบเบื้องต้น

1.1 ตรวจสอบบุคคลที่อยู่ระหว่างรอบรรจุหรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ ผู้ที่เป็นลูกจ้างทดลองปฏิบัติงาน หรือฝึกงานก่อนบรรจุเข้าปฏิบัติงาน เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์ ผู้ที่พ้นจากภารกิจ หรือตำแหน่งหน้าที่แล้วแต่ต้องกลับเข้าทำงานที่เกี่ยวข้องกับชั้นความลับของทางราชการ ผู้ที่ขอกลับเข้ารับราชการใหม่

เจ้าหน้าที่ของรัฐหรือบุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน้าที่ หรือตำแหน่งสำคัญของหน่วยงาน หรือเกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการหรือทรัพย์สินมีค่าของแผ่นดิน ผู้ได้รับทุนการศึกษาทั้งในประเทศหรือต่างประเทศแล้วมีข้อผูกพันให้เข้าปฏิบัติงานให้แก่หน่วยงานของรัฐเมื่อสำเร็จการศึกษา และบุคคลภายนอกที่เข้ามาปฏิบัติงานให้หน่วยงานของรัฐ

1.2 วิธีการตรวจสอบเบื้องต้น ให้มีการปฏิบัติดังนี้

1.2.1 ให้ผู้ถูกตรวจสอบประวัติและพฤติการณ์บุคคลกรอกรายละเอียดในแบบประวัติบุคคล (รปภ.1) ให้ครบ ภายใต้การควบคุมดูแลของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วยงานของรัฐ หรือเจ้าหน้าที่ผู้ที่ได้รับมอบหมายจากเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย

1.2.2 ให้หน่วยงานของรัฐทำหนังสือถึงหัวหน้าสถานีตำรวจนครบาลหรือหัวหน้าสถานีตำรวจภูธรที่ผู้ถูกตรวจสอบประวัติและพฤติการณ์บุคคลมีภูมิลำเนาอยู่ เพื่อพิมพ์ลายนิ้วมือส่งให้กองทะเบียนประวัติอาชญากร สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ ตรวจสอบพิมพ์ลายนิ้วมือและประวัติอาชญากร

1.2.3 ในกรณีที่ปรากฏความผิดหรือมีผลของคดี ให้หน่วยงานของรัฐพิจารณาผลการตรวจสอบว่าจะสั่งบรรจุเข้ารับราชการ หรือสั่งเลิกบรรจุหรือเลิกจ้าง

1.2.4 ในกรณีที่หัวหน้าหน่วยงานของรัฐสั่งบรรจุเข้ารับราชการ ให้หน่วยงานของรัฐส่งแบบประวัติบุคคล (รปภ.1) และผลการตรวจสอบพิมพ์ลายนิ้วมือและประวัติอาชญากรให้องค์การรักษาความปลอดภัยดำเนินการต่อไป ตามมาตรการที่องค์การรักษาความปลอดภัยแต่ละฝ่ายกำหนดไว้

2. การตรวจสอบโดยละเอียด

2.1 การตรวจสอบบุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการชั้นลับที่สุด ลับมาก หรือการรหัส บุคคลที่มีพฤติการณ์ หรือปรากฏข่าวสาร หรือติดต่อกับบุคคล หรือองค์การทั้งภายในและภายนอกประเทศ ที่จะเป็นภัย หรือเสี่ยงต่อความมั่นคงและผลประโยชน์แห่งรัฐ บุคคลที่จะได้รับมอบหมายให้ทำหน้าที่หรือแต่งตั้งให้ดำรงตำแหน่งที่สำคัญในหน่วยงานของรัฐ ต้องได้รับการตรวจสอบโดยละเอียด

2.2 วิธีการตรวจสอบโดยละเอียด

ในการตรวจสอบประวัติและพฤติการณ์บุคคลตามข้อ 2.1 หน่วยงานของรัฐอาจขอให้องค์การรักษาความปลอดภัย ดำเนินการแทน โดยให้ทำเป็นหนังสือถึง

องค์การรักษาความปลอดภัยฝ่ายที่เกี่ยวข้องเพื่อดำเนินการตรวจสอบ โดยแจ้งเหตุผลและวัตถุประสงค์ของการตรวจสอบให้องค์การรักษาความปลอดภัยดำเนินการตามมาตรการที่กำหนดไว้ และให้ระบุในหนังสือนั้นไว้ด้วยว่าบุคคลนั้นปัจจุบันดำรงตำแหน่งใด จะขอให้ดำรงตำแหน่งใด หรือเคยได้รับความไว้วางใจ ชั้นใด เมื่อใด เคยผ่านการตรวจสอบแล้วด้วยหรือไม่ หน่วยงานของรัฐใดตรวจสอบ เมื่อใด และจะให้เข้าถึงชั้นความลับใด รวมถึงการรหัสด้วยหรือไม่

3. ในระหว่างที่รอฟังผลการตรวจสอบประวัติและพฤติการณ์บุคคล ถ้าจำเป็นต้องรีบบรรจุหรือจ้างบุคคลเข้าปฏิบัติงาน ก็ให้บรรจุหรือจ้างก่อนได้ โดยมีเงื่อนไขว่าถ้าผลการตรวจสอบปรากฏว่าผู้นั้นมีความประพฤติหรือมีประวัติและพฤติการณ์ไม่เหมาะสม ให้หน่วยงานของรัฐสั่งเลิกบรรจุหรือเลิกจ้างได้

4. ถึงแม้ว่าหัวหน้าหน่วยงานของรัฐจัดให้มีการตรวจสอบประวัติและพฤติการณ์ของผู้ใต้บังคับบัญชาแล้วนั้น เพื่อให้การรักษาความปลอดภัยมีประสิทธิภาพอยู่เสมอ หากพบว่า เจ้าหน้าที่ของรัฐผู้ใดมีพฤติการณ์ที่น่าสงสัยหรือมีการกระทำอันก่อให้เกิดความไม่น่าไว้วางใจซึ่งอาจเป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ ให้ย้ายผู้นั้นออกจากตำแหน่งหน้าที่นั้นโดยเร็วและพิจารณาดำเนินการต่อไป โดยให้รายงานองค์การรักษาความปลอดภัยทราบ หรือขอให้ตรวจสอบประวัติพฤติการณ์ใหม่

2. การรับรองความไว้วางใจบุคคลเพื่อให้เข้าถึงสิ่งที่เป็นความลับของทางราชการ

หัวหน้าหน่วยงานของรัฐเป็นผู้พิจารณารับรองความไว้วางใจให้เจ้าหน้าที่ของรัฐหรือบุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการ หรือปฏิบัติหน้าที่สำคัญ โดยให้ปฏิบัติดังนี้

2.1 บุคคลที่ได้รับการรับรองความไว้วางใจ ต้องผ่านการตรวจสอบประวัติและพฤติการณ์ โดยได้รับการอนุมัติจากหัวหน้าหน่วยงานของรัฐและให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยบันทึกในแบบการรับรองความไว้วางใจ (รปภ.4)

2.2 บุคคลใดที่ได้รับการรับรองความไว้วางใจ ต้องผ่านการอบรม หรือชี้แจงในเรื่องการรักษาความปลอดภัย เพื่อให้สามารถปฏิบัติหน้าที่ที่ได้รับมอบหมายให้ถูกต้องและมีจิตสำนึกในการรักษาความปลอดภัย

2.3 บุคคลที่ได้รับความไว้วางใจ จะต้องลงนามในบันทึกรับรองการรักษาความลับ (รปภ.6) เมื่อเข้ารับตำแหน่งหน้าที่ และเมื่อพ้นตำแหน่งหน้าที่ให้ลงนามในบันทึก

รับรองการรักษาความลับ (รปภ.7) เพื่อสัญญาว่าจะรักษาความลับของทางราชการ และไม่นำไปเปิดเผยให้ผู้ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับทราบ

การรับรองความไว้วางใจบุคคลให้เข้าถึงความลับชั้นต่าง ๆ หรือหน้าที่สำคัญไม่มีข้อจำกัดในเรื่องตำแหน่ง ระดับ ยศ แต่อย่างใด กรณีเกิดความจำเป็นหัวหน้าหน่วยงานของรัฐพิจารณาเห็นว่าบุคคลผู้นั้นมีความเหมาะสม โดยดำเนินกรรมวิธีการรับรองความไว้วางใจตามที่ระเบียบกำหนดไว้

2.4 เมื่อมีความจำเป็นเร่งด่วน หัวหน้าหน่วยงานของรัฐอาจรับรองความไว้วางใจบุคคล ก่อนทราบผลการตรวจสอบประวัติและพฤติการณ์ ในกรณีดังนี้

2.4.1 บุคคลที่มีความจำเป็นต้องรีบแต่งตั้งหรือว่าจ้าง

2.4.2 บุคคลปฏิบัติหน้าที่เฉพาะภารกิจเป็นการชั่วคราวที่เกี่ยวกับความลับของทางราชการ

3. การทะเบียนความไว้วางใจ

เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหน่วยงานของรัฐ จะต้องลงทะเบียนความไว้วางใจ (รปภ.5) ของเจ้าหน้าที่ในหน่วยงานของตนที่ได้รับความไว้วางใจ โดยยึดถือใบรับรองความไว้วางใจ (รปภ.4) เป็นหลักฐาน และมีการตรวจสอบข้อมูลให้ถูกต้องตามความเป็นจริงอยู่เสมอ

เมื่อพบบุคคลใดมีพฤติการณ์ที่น่าสงสัย ต้องตรวจสอบประวัติและพฤติการณ์เพิ่มเติม หากปรากฏพฤติการณ์เป็นที่ไม่น่าไว้วางใจ ให้ยกเลิกหรือลดระดับความไว้วางใจ พร้อมบันทึกการเปลี่ยนแปลงในทะเบียนความไว้วางใจทุกครั้ง

กรณีที่พ้นจากตำแหน่งหรือหน้าที่ที่เกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการในชั้นลับที่สุด ลับมาก และลับ ต้องคัดชื่อบุคคลนั้นออกจากทะเบียนความไว้วางใจ (รปภ.5) ด้วย และให้บุคคลนั้นส่งคืนข้อมูลข่าวสารและหลักฐานต่าง ๆ ในความรับผิดชอบทั้งหมด และเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยประจำหน่วยงานของรัฐต้องชี้แจงให้ทราบถึงความรับผิดชอบในการรักษาความลับของทางราชการ พร้อมกับให้บุคคลนั้นลงลายมือชื่อในบันทึกรับรองการรักษาความลับ เมื่อพ้นตำแหน่งหรือหน้าที่ (รปภ.7) ไว้เป็นหลักฐาน

4. การอบรมเรื่องการรักษาความปลอดภัย

การมีจิตสำนึกและวินัยในการรักษาความปลอดภัย มีความสำคัญอย่างยิ่งต่อการรักษาความปลอดภัยในหน่วยงานของรัฐ ดังนั้นหน่วยงานของรัฐ จึงควรจัดให้มีการปฏิบัติดังนี้

4.1 หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการอบรมชี้แจงระเบียบเกี่ยวกับการรักษาความปลอดภัยแก่เจ้าหน้าที่ของรัฐ บุคคลที่จะปฏิบัติหน้าที่เกี่ยวข้องกับความลับของทางราชการ และบุคคลที่ต้องเข้ามาปฏิบัติงานในพื้นที่ควบคุม ให้มีความรู้ความเข้าใจเกี่ยวกับเรื่องการรักษาความปลอดภัย

4.2 ต้องมีการอบรม ทบทวนเกี่ยวกับการรักษาความปลอดภัย และเพิ่มเติมวิทยาการใหม่ตามห้วงเวลาที่เหมาะสม เพื่อกระตุ้นจิตสำนึกและวินัยในการรักษาความปลอดภัย

4.3 หน่วยงานของรัฐอาจประสานขอความร่วมมือ และคำแนะนำในการจัดอบรมให้ความรู้จากองค์การรักษาความปลอดภัยได้

บทที่ 8

คู่มือการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ

เพื่อเป็นการป้องกันข้อมูลข่าวสารลับหน่วยงานของรัฐไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง หรือรั่วไหล และป้องกันการเข้าถึงของผู้ที่ไม่มีอำนาจหน้าที่ หน่วยงานของรัฐควรปฏิบัติดังนี้

1. หัวหน้าหน่วยงานของรัฐต้องมีคำสั่งแต่งตั้งให้บุคคลปฏิบัติหน้าที่ต่าง ๆ เป็นลายลักษณ์อักษร ดังนี้

1.1 นายทะเบียนข้อมูลข่าวสารลับ และผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ มีหน้าที่ดังนี้

1.1.1 ดำเนินการทางทะเบียนข้อมูลข่าวสารลับ และจัดให้มีทะเบียนข้อมูลข่าวสารลับ ซึ่งประกอบด้วย ทะเบียนรับ (ทขล.1) ทะเบียนส่ง (ทขล.2) ทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3)

1.1.2 จัดเก็บแบบทะเบียนต่าง ๆ และข้อมูลข่าวสารลับที่อยู่ในความควบคุมดูแลให้ปลอดภัย

1.1.3 เก็บรักษาบัญชีลายมือชื่อนายทะเบียนข้อมูลข่าวสารลับ และผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ ของหน่วยงานของรัฐที่ติดต่อเกี่ยวข้องกันเป็นประจำ

1.1.4 ประสานผู้ควบคุมทะเบียนความไว้วางใจ (เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย) ในการกำหนดบุคคลที่จะเข้าถึงชั้นความลับ และบันทึกชื่อไว้ในทะเบียนความไว้วางใจ ที่กำหนดในประกาศสำนักนายกรัฐมนตรี (ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.2552)

1.1.5 ปฏิบัติงานอื่นที่เกี่ยวข้องกับข้อมูลข่าวสารลับ หรือได้รับมอบหมายจากหัวหน้าหน่วยงานของรัฐ

1.2 ผู้มีอำนาจในการกำหนดชั้นความลับ

1.3 คณะกรรมการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ ประกอบด้วย คณะกรรมการตรวจสอบ และคณะกรรมการทำลายข้อมูลข่าวสารลับ ซึ่งมีนายทะเบียนข้อมูลข่าวสารลับเป็นประธาน และเจ้าหน้าที่ไม่น้อยกว่า 2 คน เป็นกรรมการ คณะกรรมการทั้งสองชุดดังกล่าวเป็นคนละชุดกันยกเว้นประธานกรรมการ

คณะกรรมการตรวจสอบความถูกต้องในการปฏิบัติตามระเบียบ การมีอยู่ของข้อมูลข่าวสารลับตามทะเบียนข้อมูลข่าวสาร อย่างน้อยทุก 6 เดือน และข้อมูลข่าวสารลับที่ไม่ประสงค์จะเก็บรักษา และข้อมูลข่าวสารลับที่ครบอายุการเก็บรักษาตาม มาตรา14 และมาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

2. การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ หัวหน้าหน่วยงานของรัฐอาจมอบหมายการกำหนดชั้นความลับให้ผู้ใต้บังคับบัญชาได้ โดยมีคำสั่งมอบหมายเป็นลายลักษณ์อักษร

2.1 การกำหนดชั้นความลับและแสดงเหตุผล

2.1.1 การกำหนดชั้นความลับต้องคำนึงถึงข้อมูลข่าวสารที่ไม่ต้องเปิดเผยตามมาตรา14 ,15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 และปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ที่กำหนดให้พิจารณาถึงองค์ประกอบในการกำหนดชั้นความลับดังต่อไปนี้

1) ความสำคัญของเนื้อหา
2) แหล่งที่มาของข้อมูล
3) วิธีการนำไปใช้ประโยชน์
4) จำนวนบุคคลที่รับทราบ
5) ผลกระทบหากมีการเปิดเผย
6) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติในการกำหนดชั้นความลับของข้อมูลข่าวสาร

2.1.2 การแสดงชั้นความลับต้องให้เห็นเด่นชัด ทั้งข้อมูลข่าวสารที่มีสภาพเป็นกระดาษ เอกสารม้วน หรือพับ จานบันทึก แถบบันทึก หรือข้อมูลข่าวสารลับที่อยู่ในรูปแบบอื่น ๆ

2.1.3 การปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ต้องกระทำโดยผู้กำหนดชั้นความลับของหน่วยงานเจ้าของเรื่อง และต้องแจ้งให้หน่วยงานของรัฐอื่นที่ได้รับการแจกจ่ายทราบ เพื่อแก้ไขชั้นความลับด้วยทุกครั้ง

2.2 การจัดทำข้อมูลข่าวสารลับ ควรดำเนินการ ดังนี้

2.2.1 กำหนดจำนวนเจ้าหน้าที่ที่เกี่ยวข้อง และจำกัดให้ทราบเท่าที่จำเป็น ซึ่งบุคคลผู้นั้นต้องได้รับความไว้วางใจไม่ต่ำกว่าชั้นความลับของข้อมูลข่าวสารลับนั้น

2.2.2 การจัดทำต้องทำในสถานที่ที่ปลอดภัย

2.2.3 กระดาษหรือวัสดุ ที่อยู่ในกระบวนการจัดทำข้อมูลข่าวสารลับ เช่น กระดาษร่าง กระดาษคาร์บอน ให้ทำลายทันทีที่จัดทำเสร็จเรียบร้อย ถ้าเป็นการจัดทำที่ใช้ระบบเทคโนโลยีสารสนเทศ จะต้องมีการลบ หรือทำลาย จนไม่สามารถนำไปใช้ประโยชน์ได้ หากไม่ทำลายต้องเก็บรักษาในที่ปลอดภัย เช่นเดียวกับการเก็บรักษาข้อมูลข่าวสารลับ

2.2.4 ข้อมูลข่าวสารลับที่มีสภาพเป็นเอกสาร ให้แสดงชื่อหน่วยงานส่วนย่อยและหน่วยงานเจ้าของเรื่อง เลขที่ชุดของจำนวนชุดทั้งหมด เลขที่หน้าของจำนวนหน้าทั้งหมด ไว้ทุกหน้าของข้อมูลข่าวสารลับ ในส่วนที่เห็นได้ชัดเจน เช่น มุมขวาด้านบนของเอกสาร เพื่อสะดวกในการตรวจสอบว่าข้อมูลข่าวสารลับชุดใดได้แจกจ่ายให้แก่ผู้ใด การบันทึกจำนวนหน้าเพื่อให้ทราบว่าข้อมูลข่าวสารลับนั้นเป็นหน้าใดของจำนวนทั้งหมดกี่หน้า หากมีการสูญหายไปหน้าใดหน้าหนึ่ง จะได้ทราบและสามารถติดตามหาผู้ละเมิดและหาทางลดหรือแก้ไขความเสียหายที่เกิดขึ้นได้

2.3 หน่วยงานของรัฐที่ครอบครองข้อมูลข่าวสารลับใดอยู่ หมายรวมถึงฉบับที่ตนเป็นเจ้าของเรื่อง หรือฉบับที่ได้รับการแจกจ่ายมาจากหน่วยงานอื่น ให้รับผิดชอบในการจัดทำสำเนาเพิ่มเติม หรือการแปล ได้เอง โดยให้บันทึกจำนวนที่สำเนาเพิ่ม และทำบัญชีรายการแจกจ่ายไว้ด้วย เพื่อการควบคุมและตรวจสอบกรณีเกิดการละเมิดการรักษาความลับหรือเมื่อข้อมูลข่าวสารลับรั่วไหล

2.4 การโอนข้อมูลข่าวสารลับจะกระทำได้ต่อเมื่อผู้โอน และผู้รับโอนได้รับอนุมัติจากหัวหน้าหน่วยงานของรัฐ และต้องดำเนินการโดยมีหลักฐานเป็นลายลักษณ์อักษร เมื่อดำเนินการแล้วทั้งผู้โอน และผู้รับโอน ต้องรายงานให้หัวหน้าหน่วยงานของตนทราบ

การโอนข้อมูลข่าวสารลับระหว่างหน่วยงานของรัฐ หรือการโอนข้อมูลข่าวสารลับภายในหน่วยงานเดียวกัน ควรปฏิบัติดังนี้

1. เจ้าหน้าที่ผู้โอน และผู้รับโอนต้องจัดทำบันทึกการโอน และบุคคลดังกล่าวต้องได้รับความไว้วางใจไม่ต่ำกว่าชั้นความลับของข้อมูลข่าวสารลับนั้น

2. นายทะเบียนข้อมูลข่าวสารลับ ต้องจดแจ้งการโอนในทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3)

2.5 การส่ง การรับ ข้อมูลข่าวสารลับ ดำเนินการดังนี้

การส่งข้อมูลข่าวสารลับ

2.5.1 การส่งข้อมูลข่าวสารลับภายในหน่วยงานให้ใช้ใบปกข้อมูลข่าวสารลับปิดทับข้อมูลข่าวสารลับ เพื่อให้ผู้ไม่มีหน้าที่เกี่ยวข้องได้เห็นข้อความภายใน และเป็นการเตือนให้รักษาความลับของทางราชการ ผู้ส่งต้องกระทำโดยเจ้าหน้าที่ผู้รับผิดชอบและได้รับความไว้วางใจไม่ต่ำกว่าชั้นความลับของข้อมูลข่าวสารลับนั้น

2.5.2 การส่งข้อมูลข่าวสารลับออกนอกบริเวณหน่วยงาน หมายความรวมถึงการส่งให้แก่หน่วยงานอื่น และการส่งให้หน่วยงานเดียวกันแต่ไม่ได้อยู่บริเวณเดียวกัน ควรปฏิบัติดังนี้

1) ข้อมูลข่าวสารลับต้องบรรจุซองทึบแสงสองชั้น และให้แนบใบตอบรับไว้ที่หน้าซองชั้นในของข้อมูลข่าวสารลับนั้น

2) บนซองชั้นใน ให้จ่าหน้า

- ระบุเลขที่หนังสือนำส่ง
- ชื่อหรือตำแหน่งผู้รับ
- หน่วยงานผู้ส่ง
- ทำเครื่องหมายแสดงชั้นความลับทั้งด้านหน้าและด้านหลัง

3) ผู้ปิดผนึกซอง ต้องเป็นผู้มีอำนาจหน้าที่ การปิดผนึก และลงลายมือชื่อของผู้ปิดผนึกไว้บนรอยปิดผนึกของซอง และใช้แถบกาวชนิดใสปิดทับ เพราะแถบกาวใสจะช่วยให้สามารถตรวจสอบร่องรอยการลอบเปิดซอง หรือห่อชั้นในได้ง่าย

4) บนซองชั้นนอก ให้จ่าหน้าเหมือนซองชั้นใน แต่ไม่ต้องแสดงชั้นความลับ

การรับข้อมูลข่าวสารลับ

ใบตอบรับ ที่แนบไว้หน้าซองชั้นใน ไม่ต้องระบุชั้นความลับ และชื่อเรื่องระบุเฉพาะเลขที่หนังสือ วัน เดือน ปี จำนวนหน้า และหมายเลขฉบับ นายทะเบียนข้อมูลข่าวสารลับ หรือผู้ช่วยนายทะเบียนฯ (ผู้รับ) จะส่งคืนใบตอบรับตามสายงานของการส่งหนังสือ หากให้เจ้าหน้าที่นำสารถือข้อมูลข่าวสารลับไปเองให้รอรับใบตอบรับคืนด้วย

สำหรับข้อมูลข่าวสารลับที่มีการระบุชื่อผู้รับ ให้บุคคลตามที่ระบุชื่อเป็นผู้เปิดซองนั้น หรือภายในหน่วยงานกำหนดแนวปฏิบัติ จะมอบอำนาจให้นายทะเบียนข้อมูลข่าวสารลับเปิดซองข้อมูลข่าวสารลับ เฉพาะระบุตำแหน่ง หรือเฉพาะข้อมูลข่าวสารชั้นลับ เป็นต้น

2.6 การเก็บรักษาข้อมูลข่าวสารลับ

2.6.1 ข้อมูลข่าวสารลับที่มีสภาพเป็นเอกสาร ให้เจ้าหน้าที่ผู้ครอบครองควบคุมดูแล เก็บข้อมูลข่าวสารลับเหล่านั้นไว้ในแฟ้มข้อมูลข่าวสารลับ และเก็บแฟ้มข้อมูลข่าวสารลับไว้ในตู้เก็บข้อมูลข่าวสารลับโดยแยกเป็นเฉพาะเรื่อง

2.6.2 ตู้เก็บข้อมูลข่าวสารลับควรเป็นตู้เหล็ก ปิดล็อคด้วยกุญแจที่มั่นคง

2.6.3 ควรลง วัน เดือน ปี เวลา เปิด-ปิด ตู้เก็บรักษาข้อมูลข่าวสารลับ และลงลายมือชื่อ ของผู้เปิด-ปิด

2.6.4 ตู้เก็บข้อมูลข่าวสารลับต้องเก็บไว้ในสถานที่ ซึ่งมีระบบการรักษาความปลอดภัยเกี่ยวกับสถานที่ ที่กำหนดให้เป็น “พื้นที่หวงห้าม”

2.6.5 ควรจัดให้มีตู้เก็บลูกกุญแจรวม เพื่อเป็นที่เก็บลูกกุญแจตู้เก็บข้อมูลข่าวสารลับทุกตู้ รวมไว้ที่เดียวกัน ตู้เก็บลูกกุญแจรวม ควรปิดล็อคด้วยกุญแจที่มีความมั่นคง และจัดที่เก็บไว้ในพื้นที่หวงห้าม

2.6.6 นายทะเบียนข้อมูลข่าวสารลับ ดูแลตู้เก็บลูกกุญแจรวม โดยผู้ที่รับผิดชอบ ตู้ข้อมูลข่าวสารลับ ควรนำลูกกุญแจตู้ที่ตนรับผิดชอบทั้งหมดมาเก็บไว้ในตู้เก็บกุญแจรวมหลังเสร็จภารกิจประจำวัน

2.6.7 ไม่ควรเก็บข้อมูลข่าวสารลับไว้ในเครื่องคอมพิวเตอร์จะต้องจัดเก็บลงในสื่อบันทึกข้อมูล เช่น แผ่นดิสก์ ซีดีรอม เทปบันทึก หรืออุปกรณ์อื่นที่ใช้จัดเก็บข้อมูลด้วยเครื่องคอมพิวเตอร์ โดยมีระบบรักษาความปลอดภัยในการจัดเก็บ และเรียกใช้ข้อมูลด้วยระบบรหัสผู้ใช้ และรหัสผ่าน

2.7 การยืมข้อมูลข่าวสารลับ ให้หัวหน้าหน่วยงานของรัฐ หรือผู้ได้รับมอบหมายเป็นผู้พิจารณาตรวจสอบคุณสมบัติของผู้ยืมว่า เป็นผู้มีอำนาจหน้าที่เกี่ยวข้องได้รับความไว้วางใจให้เข้าถึงชั้นความลับของข้อมูลข่าวสารที่จะยืม และสามารถปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ได้ พร้อมทั้งต้องบันทึกหลักฐานการยืมในทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3)

2.8 ข้อมูลข่าวสารลับของหน่วยงานของรัฐที่ไม่ประสงค์จะเก็บรักษา หรือมีอายุครบกำหนดการเก็บ ต้องส่งให้หอจดหมายเหตุแห่งชาติ กรมศิลปากร พิจารณาคัดเลือกไว้ให้ประชาชนได้ศึกษา ค้นคว้า ตามมาตรา 26 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 การทำลายให้พิจารณาจาก

2.8.1 ข้อมูลข่าวสารลับที่หอจดหมายเหตุแห่งชาติ พิจารณาแล้วว่าไม่มีคุณค่าในการเก็บรักษา

2.8.2 ข้อมูลข่าวสารลับ ชั้น “ลับที่สุด” ที่หากเก็บรักษาไว้จะเสี่ยงต่อการรั่วไหล อันอาจก่อให้เกิดอันตรายแก่ประโยชน์แห่งรัฐ หัวหน้าหน่วยงานของรัฐมีอำนาจสั่งทำลายได้ หากพิจารณาเห็นว่ามีความจำเป็นอย่างยิ่งที่จะต้องทำลาย

2.8.3 ต้องแต่งตั้ง คณะกรรมการทำลายข้อมูลข่าวสารลับ โดยมีนายทะเบียนข้อมูลข่าวสารลับเป็นประธาน และกรรมการอีกไม่น้อยกว่า 2 คน ซึ่งเป็นเจ้าหน้าที่ที่เกี่ยวข้อง และได้รับความไว้วางใจไม่ต่ำกว่าชั้นความลับของข้อมูลข่าวสารลับนั้น

2.8.4 จัดทำใบรับรองการทำลายข้อมูลข่าวสารลับ โดยนายทะเบียนข้อมูลข่าวสารลับต้องเก็บไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี

2.8.5 เมื่อทำลายข้อมูลข่าวสารลับแล้ว ให้นายทะเบียนข้อมูลข่าวสารลับ จดแจ้งในทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3) ด้วย

2.9 หากข้อมูลข่าวสารลับสูญหาย ให้ผู้ทราบข้อเท็จจริงรายงานให้หัวหน้าหน่วยงานของรัฐ ผู้ที่ได้รับมอบหมายที่ตนสังกัดทราบ เพื่อดำเนินการแต่งตั้งคณะกรรมการสอบสวน และให้นายทะเบียนข้อมูลข่าวสารลับบันทึกการสูญหายของข้อมูลข่าวสารลับลงในทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3)

2.10 ในกรณีขอให้เปิดเผยข้อมูลข่าวสารลับของราชการ หัวหน้าหน่วยงานของรัฐ อาจพิจารณาออกคำสั่งเปิดเผยหรือไม่เปิดเผยตามมาตรา15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 ได้ กรณีมีคำสั่งไม่เปิดเผย ให้หน่วยงานของรัฐพิจารณากำหนดวิธีรักษาข้อมูลข่าวสารลับตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544

การเปิดเผยข้อมูลข่าวสารลับ

1) การเปิดเผยข้อมูลข่าวสารลับแก่ผู้ใดต้องกระทำโดยระมัดระวัง ในกรณีจำเป็นให้กำหนดเงื่อนไขในการปฏิบัติให้เหมาะสม

2) ข้อมูลข่าวสารลับที่คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารมีคำวินิจฉัยให้เปิดเผย โดยไม่มีข้อจำกัดหรือเงื่อนไขใด ให้ถือว่าข้อมูลข่าวสารลับนั้นถูกยกเลิกชั้นความลับแล้ว เว้นแต่มีการฟ้องคดีต่อศาล และศาลมีคำสั่งหรือคำพิพากษาเป็นอย่างอื่น

3) ในกรณีที่หัวหน้าหน่วยงานของรัฐ หรือเจ้าหน้าที่ของรัฐตามมาตรา 20 (1) แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มีคำสั่งให้เปิดเผยข้อมูลข่าวสารลับใด โดยมีข้อจำกัดหรือเงื่อนไขเช่นใด ให้เปิดเผยข้อมูลข่าวสารลับตามข้อจำกัดและเงื่อนไขนั้น

4) ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 37 วรรค 2 คำวินิจฉัยของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารให้เป็นที่สุด

มติคณะรัฐมนตรีเมื่อ 11 เมษายน พ.ศ.2549 “ห้ามมิให้หน่วยงานของรัฐฟ้องคดีปกครองเพื่อเพิกถอนคำวินิจฉัยของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารที่มีคำวินิจฉัยให้หน่วยงานของรัฐเปิดเผยข้อมูลข่าวสารแก่ผู้อุทธรณ์”

5) กรณีที่ข้อมูลข่าวสารลับใดไม่มีเครื่องหมายแสดงชั้นความลับ เจ้าหน้าที่ที่เกี่ยวข้องสามารถเปิดเผยข้อมูลข่าวสารลับได้ เว้นแต่เจ้าหน้าที่นั้นได้รู้ หรือควรรู้ว่าข้อมูลข่าวสารนั้นได้มีการกำหนดชั้นความลับไว้

6) ข้อมูลข่าวสารตามมาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 เป็นข้อมูลข่าวสารที่ไม่ต้องเปิดเผย (ข้อมูลข่าวสารลับ) ถ้าเจ้าหน้าที่ดำเนินการเปิดเผยโดยสุจริต ตามที่ได้รับมอบหมาย และปฏิบัติต่อข้อมูลข่าวสารลับ โดยปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 เกิดความเสียหายให้ถือว่าเจ้าหน้าที่ของรัฐไม่ต้องรับผิด เพราะเป็นการกระทำโดยสุจริต

เจ้าหน้าที่ของรัฐตามมาตรา 20 (1) แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 หมายถึงเจ้าหน้าที่ผู้ปฏิบัติหน้าที่ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544

บทที่ 9

คู่มือการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

1. หัวหน้าหน่วยงานของรัฐ อาจมอบหมายให้มีผู้รับผิดชอบ

1.1 ด้านการรักษาความปลอดภัยทางระบบอิเล็กทรอนิกส์ มีหน้าที่ควบคุม กำกับดูแล ตรวจสอบ ให้คำแนะนำ ปรึกษา

1.2 ด้านการบริหารจัดการทางระบบอิเล็กทรอนิกส์ มีหน้าที่กำหนดผู้ใช้และสิทธิการเข้าถึงข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

2. การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

2.1 <u>การจัดทำ</u>

2.1.1 เจ้าหน้าที่ผู้จัดทำข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ต้องผ่านการตรวจสอบประวัติและพฤติการณ์ เพื่อรับรองความไว้วางใจก่อนปฏิบัติหน้าที่

2.1.2 สถานที่ที่ใช้จัดทำข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ กำหนดพื้นที่ให้เป็นพื้นที่หวงห้ามเด็ดขาด หรือหวงห้ามเฉพาะ ห้ามมิให้ผู้ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในพื้นที่ดังกล่าว โดยไม่ได้รับอนุญาต

2.1.3 การแสดงชั้นความลับของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

1) ให้แสดงชั้นความลับไว้ ณ ที่ที่แสดงข้อมูลข่าวสารลับนั้น เช่น เมื่อเรียกแฟ้มข้อมูลมาแสดงภาพที่หน้าจอภาพ ให้แสดงชั้นความลับทั้งหมดทุกหน้าของข้อมูลข่าวสารลับ ที่แสดงภาพบนจอนั้น และสื่ออิเล็กทรอนิกส์ที่จัดเก็บ เช่น แผ่นซีดีรอม แผ่นดิสก์ Flash drive เป็นต้น ให้แสดงชั้นความลับบนภาชนะที่บรรจุ

2) หรือใช้กระบวนการทางคอมพิวเตอร์ให้ปรากฏชั้นความลับเมื่อเรียกแฟ้มข้อมูลมาแสดงภาพ เช่น การจัดทำลายน้ำบนข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

2.2 <u>การจัดเก็บ</u>

2.2.1 ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ทุกชั้นความลับ ต้องเข้ารหัสด้วยเครื่องเข้ารหัสหรือโปรแกรมเข้ารหัส หากใช้โปรแกรมเข้ารหัส ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ต้องดำเนินการเข้ารหัสด้วยโปรแกรมเข้ารหัส ซึ่งปัจจุบันมี 2 ประเภทหลักคือ

1) กุญแจรหัสแบบสมมาตร (Symmetric Key) หรือ กุญแจเดี่ยวที่กำหนดใช้กุญแจลับ (Secret Key) เพียงหนึ่งเดียวในการเข้า และถอดรหัส

2) กุญแจรหัสแบบอสมมาตร (Asymmetric Key) หรือระบบกุญแจคู่ ที่กำหนดให้ใช้กุญแจสองตัว โดยกุญแจตัวหนึ่งใช้ในการเข้ารหัส (Public Key) และกุญแจอีกตัวหนึ่งใช้ในการถอดรหัส (Private Key) นอกจากนี้ยังสามารถประยุกต์ใช้กับการลงลายมือชื่ออิเล็กทรอนิกส์ เพื่อพิสูจน์ความเป็นเจ้าของ และตรวจสอบว่าเป็นข้อมูลข่าวสารลับที่มาจากผู้ส่งนั้นหรือไม่

การใช้กุญแจรหัสประเภทใดและจำนวนครั้งของการเข้ารหัสขึ้นอยู่กับความสำคัญของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ให้อยู่ในดุลพินิจของเจ้าของข้อมูลข่าวสารลับ และหัวหน้าหน่วยงานของรัฐ

2.2.2 ต้องมีระบบสำรองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์และเครื่องคอมพิวเตอร์แม่ข่ายสำรอง โดยแยกจัดเก็บในสถานที่ปลอดภัย เพื่อให้ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ดำเนินการได้อย่างต่อเนื่อง และความคงอยู่ของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ จึงควรมีการสำรองข้อมูลข่าวสารลับดังกล่าว โดยแยกสถานที่จัดเก็บไว้คนละแห่งกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ต้นฉบับ และเพื่อให้การใช้ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ได้อย่างต่อเนื่อง ควรมีเครื่องคอมพิวเตอร์แม่ข่ายสำรอง โดยแยกสถานที่จัดเก็บไว้คนละแห่งกับเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้งาน

2.3 การรับ-ส่ง

2.3.1 กำหนดระเบียบปฏิบัติการรับ-ส่ง ข้อมูลข่าวสารลับทางโทรคมนาคม เช่น

1) ข้อมูลข่าวสารลับ ที่กำหนดชั้นความลับ ลับ ลับมาก รับ-ส่งทางโทรคมนาคมจะต้องเข้ารหัสด้วยโปรแกรมเข้ารหัส 1 ชั้นขึ้นไป (ระบบกุญแจเดี่ยว หรือกุญแจคู่) หากมีความจำเป็นที่จะต้องรับ – ส่ง ข้อมูลข่าวสารลับที่กำหนดชั้น ลับที่สุด จะต้องเข้ารหัสด้วยโปรแกรมเข้ารหัสไม่น้อยกว่า 2 ชั้น (ระบบกุญแจเดี่ยว หรือกุญแจคู่ หรือ เครื่องเข้ารหัส)

2) จัดทำทะเบียนควบคุมการแจกจ่ายกุญแจรหัส เพื่อให้ทราบว่าบุคคลหรือหน่วยงานใดได้รับกุญแจรหัสชุดใด และมีกำหนดระยะเวลาการใช้งาน

3) กำหนดบุคคลรับผิดชอบในการสร้างกุญแจรหัส ซึ่งมิใช่บุคคลเดียวกันกับบุคคลที่จัดทำทะเบียนควบคุม และแจกจ่ายกุญแจรหัส โดยบุคคลดังกล่าวต้องได้รับมอบหมายจากหัวหน้าหน่วยงานของรัฐ

4) จะต้องมีการเปลี่ยนกุญแจรหัสตามห้วงเวลาและสถานการณ์ โดยไม่เป็นรูปแบบ และไม่ควรเก็บกุญแจรหัส ไว้ในเครื่องคอมพิวเตอร์ ควรจัดเก็บในสื่ออิเล็กทรอนิกส์ภายนอกอื่น เช่น แผนดิสก์ ซีดีรอม Flash Drive เป็นต้น

5) จะต้องมีการสำรองโปรแกรม และกุญแจรหัส ไม่น้อยกว่า 2 ชุด โดยแยกจัดเก็บรักษาไว้ในสถานที่ปลอดภัย ซึ่งควรเป็นสถานที่คนละแห่ง

6) จัดเครื่องคอมพิวเตอร์โดยเฉพาะในการเข้ารหัส และมีระบบการรักษาความปลอดภัยในการเข้าใช้งานเครื่องคอมพิวเตอร์

2.3.2 จัดทำทะเบียนเจ้าหน้าที่ควบคุมการรหัส และเจ้าหน้าที่การรหัส โดยบุคคลดังกล่าว มีหน้าที่ความรับผิดชอบ ดังนี้

<u>หน้าที่ของเจ้าหน้าที่ควบคุมการรหัส</u>

ดำเนินการทางการรหัสของหน่วยงาน ภายใต้การกำกับดูแลของ เจ้าหน้าที่ด้านการรักษาความปลอดภัยทางระบบอิเล็กทรอนิกส์ มีหน้าที่ความรับผิดชอบ ดังนี้

1. ควบคุมเจ้าหน้าที่ผู้เกี่ยวข้องกับการรหัสของหน่วยงานว่าเป็นบุคคลที่ได้รับรองความไว้วางใจ และควรผ่านการอบรมด้านการรักษาความปลอดภัยข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ แล้ว

2. จัดทำทะเบียนรายชื่อเจ้าหน้าที่การรหัส และมอบหมายหน้าที่เฉพาะส่วน

3. พิจารณาใช้ระบบการรหัสให้เหมาะสมกับชั้นความลับของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ และควบคุมการใช้ระบบการรหัสให้ถูกต้อง

4. หากพบการละเมิดการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ให้รายงานหัวหน้าหน่วยงานของรัฐ หรือเจ้าหน้าที่ด้านการรักษาความปลอดภัยทางระบบอิเล็กทรอนิกส์ทันที

<u>หน้าที่ของเจ้าหน้าที่การรหัส</u>

รับผิดชอบในการเข้า และถอดการรหัสของหน่วยงาน ภายใต้การอำนวยการควบคุม และกำกับดูแล ของเจ้าหน้าที่ควบคุมการรหัส โดยปฏิบัติ ดังนี้

1. ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ที่จะเข้าการรหัสต้องผ่านการพิจารณาจาก เจ้าหน้าที่ควบคุมการรหัสก่อน

2. ห้ามเปิดเผยข้อมูลเกี่ยวกับการเข้า หรือถอดรหัส แก่ผู้ที่ไม่มีหน้าที่เกี่ยวข้อง และต้องพิทักษ์รักษาข้อมูลเกี่ยวกับการรหัสให้ปลอดภัยตลอดเวลา

3. หากพบ หรือสงสัยว่ามีการละเมิดการรักษาความปลอดภัย ให้รายงานต่อเจ้าหน้าที่ควบคุมการรหัส ทันที

2.3.3 ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วยงาน ติดตามผลการปฏิบัติงาน เพื่อตรวจสอบการใช้งาน และการละเมิดการรักษาความปลอดภัย

2.4 การทำลาย

วิธีการทำลายข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ กรณีที่ข้อมูลจัดเก็บอยู่ในสื่ออิเล็กทรอนิกส์ เช่น แผ่นดิสก์ ฮาร์ดดิสก์ Flash Drive ที่สามารถใช้บันทึกซ้ำได้ ให้ใช้ชุดคำสั่งในระบบปฏิบัติการหรือโปรแกรมซึ่งทำหน้าที่ลบแฟ้มข้อมูลโดยไม่สามารถกู้กลับคืนได้ กรณีที่จัดเก็บอยู่ในสื่อที่ไม่สามารถใช้บันทึกซ้ำได้ ให้ใช้การทำลายด้วยวิธีทุบทำลายให้สิ้นสภาพการใช้งาน

บทที่ 10

คู่มือการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่

อาคารสถานที่ ทรัพย์สินมีค่าของแผ่นดินและความลับของทางราชการ รวมถึงบุคคลสำคัญของหน่วยงาน อาจเป็นเป้าหมายของการโจรกรรม การจารกรรม การก่อวินาศกรรม และการก่อการร้ายได้ ดังนั้นจึงจำเป็นต้องวางมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ เพื่อพิทักษ์รักษาบุคคลและทรัพย์สินของทางราชการให้ปลอดภัย หรือขัดขวาง หน่วงเหนี่ยวการดำเนินการของฝ่ายตรงข้ามมิให้สัมฤทธิ์ผล หรือมีผลเสียหายต่อหน่วยงานน้อยที่สุด และยังต้องประสานสอดคล้องกับมาตรการป้องกันภัยทางธรรมชาติ รวมถึงอุบัติภัยด้วย

ดังนั้นหน่วยงานของรัฐต้องกำหนดแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ของหน่วยงานตนเอง โดยสำรวจการรักษาความปลอดภัยเกี่ยวกับสถานที่ของหน่วยงานก่อน จากนั้นจึงนำผลจากการสำรวจเป็นข้อมูลพื้นฐานประกอบในการกำหนดแผน ซึ่งแผนดังกล่าวนี้เป็นเรื่องที่ต้องปฏิบัติเป็นกิจวัตร หน่วยงานเจ้าของแผนจึงต้องพิจารณาปรับปรุง แก้ไขแผนให้มีประสิทธิภาพอยู่ตลอดเวลา

การกำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ ต้องคำนึงถึงหลักการดังนี้

1. <u>กำหนดพื้นที่ที่มีการรักษาความปลอดภัย</u>

การกำหนดพื้นที่ที่มีการรักษาความปลอดภัย เพื่อเป็นการป้องกันผู้ไม่มีอำนาจหน้าที่ หรือผู้ไม่ประสงค์ดี เข้าไปในพื้นที่ โดยดำเนินการดังนี้ ต้องมีการเฝ้าตรวจ ผู้ที่จะเข้ามาในพื้นที่ ต้องมีการพิสูจน์ทราบว่าผู้ที่จะเข้ามาเป็นใคร มีวัตถุประสงค์ใด มีสิทธิ มีอำนาจหน้าที่หรือไม่ เป็นภัยหรือไม่ ต้องมีการขัดขวาง หากผู้ที่จะเข้ามาในพื้นที่เป็นผู้ที่ไม่มีอำนาจหน้าที่หรืออาจเป็นภัยได้

พื้นที่หรือบริเวณของส่วนราชการต่าง ๆ ควรกำหนดขอบเขตให้ชัดเจนว่าพื้นที่ใดควรได้รับการรักษาความปลอดภัยเป็นพิเศษ โดยแบ่งพื้นที่ ดังนี้

1. **พื้นที่ควบคุม** คือพื้นที่โดยรวมของหน่วยงาน อยู่ภายในขอบเขตของพื้นที่ที่มีการรักษาความปลอดภัยทั้งหมด ต้องมีระเบียบการควบคุมบุคคลและยานพาหนะเพื่อช่วยกลั่นกรองในชั้นหนึ่งก่อน มาตรการที่ใช้ควบคุมการผ่านเข้า-ออก เช่น การออกบัตรผ่าน และ/หรือบันทึกการผ่านเข้า-ออกของบุคคลและยานพาหนะ

2. **พื้นที่หวงห้าม** คือพื้นที่ที่มีการพิทักษ์รักษาสิ่งที่เป็นความลับต่าง ๆ ตลอดจนบุคคลสำคัญ ทรัพย์สินของทางราชการ ซึ่งแบ่งพื้นที่หวงห้ามออกเป็นดังนี้

2.1 “เขตหวงห้ามเฉพาะ” เช่น พื้นที่ซึ่งพิทักษ์รักษาสิ่งที่เป็นความลับ วัสดุอุปกรณ์ที่สำคัญ บุคคลสำคัญ ต้องมีการตรวจสอบบุคคลที่เข้าถึงอย่างเข้มงวด

2.2 “เขตหวงห้ามเด็ดขาด” เช่น พื้นที่ซึ่งมีสิ่งที่เป็นความลับตลอดจนบุคคลที่มีความสำคัญยิ่ง บุคคลที่ได้รับอนุญาตให้เข้าไปใน “เขตหวงห้ามเด็ดขาด” ต้องได้รับการไว้วางใจตามชั้นความลับที่เหมาะสม และใช้มาตรการเสริมเพิ่มเติม เช่น บัตรผ่านเข้า-ออก จะต้องใช้เฉพาะการผ่านเพียงครั้งเดียว และมีการบันทึกการ เข้า-ออก ทุกครั้ง

2. <u>การวางระบบป้องกันทางด้านวัตถุ</u>

เป็นมาตรการหน่วงเหนี่ยว จำกัด ขัดขวางการรุกล้ำ หรือป้องปราม เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยมีโอกาสตรวจสอบ พิสูจน์ทราบ และขัดขวาง หากมีการบุกรุก การป้องกันทางวัตถุอาจประกอบด้วย

2.1 เครื่องกีดขวางโดยรอบ แบ่งได้เป็น

1) เครื่องกีดขวางตามธรรมชาติ เช่น แม่น้ำ ลำคลอง เป็นต้น อาจพิจารณาดัดแปลง หรือปรับปรุงให้ใช้ประโยชน์เป็นเครื่องกีดขวางได้

2) เครื่องกีดขวางที่ประดิษฐ์ขึ้น เช่น รั้ว เครื่องกีดขวางบริเวณช่องทางเข้า-ออก เช่น แผงกั้นล้อเลื่อน แขนกั้นยานพาหนะ เป็นต้น

2.2 การให้แสงสว่าง

เพื่อให้มาตรการการรักษาความปลอดภัยสถานที่มีประสิทธิภาพ การให้แสงสว่าง เพื่อจะให้มองเห็นบริเวณรั้วและเขตหวงห้ามต่าง ๆ โดยชัดเจนในเวลามืดจะได้มองเห็นผู้ที่บุกรุกเข้ามาในสถานที่

3. <u>ระบบการติดต่อสื่อสารและระบบสัญญาณแจ้งภัย</u>

ระบบการติดต่อสื่อสารและสัญญาณแจ้งภัย จะช่วยให้การติดต่ออำนวยการควบคุมสถานการณ์ ตลอดจนรายงานผลการดำเนินการ เป็นไปได้อย่างรวดเร็วทันต่อเหตุการณ์ และมีประสิทธิภาพ

<u>ระบบการติดต่อสื่อสาร</u> เช่นโทรศัพท์ วิทยุสื่อสาร เป็นต้น ต้องสามารถติดต่อเจ้าหน้าที่ ผู้บังคับบัญชา เพื่อรายงานเหตุการณ์ รวมทั้งติดต่อหน่วยงานอื่น เพื่อระงับยับยั้ง และบรรเทาเหตุที่เกิดขึ้น

ระบบสัญญาณแจ้งภัย เช่น เครื่องมือทางอิเล็กทรอนิกส์ ไฟฟ้า เครื่องกล เป็นต้น ที่ทำให้เกิดสัญญาณเมื่อมีผู้บุกรุก หรือเกิดเหตุอื่น ๆ เช่น สัญญาณจับควัน สัญญาณจับคลื่นความร้อน เป็นต้น

4. การควบคุมบุคคลและยานพาหนะ

เป็นภารกิจหลักของการรักษาความปลอดภัยสถานที่ ผู้รับผิดชอบต้องตรวจสอบบุคคล และยานพาหนะอย่างละเอียด รอบคอบ ถี่ถ้วน เพื่อให้แน่ใจว่าผู้ที่ผ่านเข้ามาในพื้นที่มีสิทธิที่จะผ่านเข้ามา และไม่ก่อเหตุละเมิดการรักษาความปลอดภัย

การควบคุมบุคคล

บัตรผ่าน และป้ายแสดงตน เป็นหลักฐานแสดงสถานะต่อเจ้าหน้าที่รักษาการณ์ขณะผ่านจุดตรวจ หรือช่องทาง เข้า-ออก ทั้งนี้ถือเป็นการแสดงว่ามีสิทธิในการผ่าน เข้า-ออก และการเข้าถึงพื้นที่ที่มีการรักษาความปลอดภัยได้

บัตรผ่าน คือบัตรที่หน่วยงานของรัฐออกให้สำหรับบุคคล และยานพาหนะของผู้ที่ปฏิบัติงานอยู่ในพื้นที่นั้น และบุคคลภายนอกที่ต้องเข้ามาติดต่อเป็นการชั่วคราว โดยให้ เจ้าหน้าที่รักษาการณ์ทำการบันทึกหลักฐาน ตรวจสอบ และมอบบัตรผ่านให้ใช้ในการผ่านเข้า-ออกในแต่ละครั้ง

ป้ายแสดงตน คือหลักฐานใช้ควบคุมบุคคล ใช้สำหรับบุคคลทั้งภายในและภายนอก เพื่อแสดงสถานะในการเข้าในพื้นที่ที่มีการรักษาความปลอดภัย ป้ายแสดงตนต้องแสดงไว้ให้เห็นเด่นชัดตลอดเวลาที่อยู่ในพื้นที่

บันทึกหลักฐานการผ่านเข้า-ออก เป็นมาตรการควบคุมเสริมจากการใช้บัตรผ่าน หรือบัตรแสดงตน โดยจัดให้มีเจ้าหน้าที่บันทึกหลักฐาน สำหรับบุคคลที่ผ่านเข้า-ออก ในพื้นที่ที่มีการรักษาความปลอดภัย โดยให้มีการจดบันทึกรายละเอียดเช่นกัน ส่วนบุคคลภายนอกในกรณีผู้มาประชุม ติดต่อราชการ หรือพบปะเจ้าหน้าที่ของหน่วยงาน โดยให้มีรายละเอียด เช่น ชื่อ ที่อยู่ของผู้ที่ผ่านเข้า-ออก หน่วยงานที่สังกัด วัน เวลาที่ผ่านเข้า-ออก ชื่อผู้ที่มาติดต่อ เหตุผลในการผ่าน เข้า-ออก พื้นที่

การควบคุมยานพาหนะ

การควบคุมยานพาหนะ หมายรวมถึง การควบคุมทั้งบุคคล และสิ่งของต่าง ๆ บนยานพาหนะด้วย ยานพาหนะที่ได้รับการอนุญาตให้ผ่านเข้าไปในพื้นที่ ควรกำหนดเส้นทางและที่จอดรถทั้งของเจ้าหน้าที่ภายในและบุคคลภายนอกให้ชัดเจน

การบันทึกหลักฐานยานพาหนะที่ เข้า-ออก ควรมีรายละเอียดดังต่อไปนี้

1. วัน เวลา ที่ยานพาหนะผ่านเข้า-ออก
2. ชื่อผู้ขับ และชื่อผู้โดยสาร
3. ประเภท ชนิด สี เลขทะเบียนยานพาหนะ
4. ลักษณะ และจำนวนสิ่งของบนยานพาหนะนั้น
5. วัตถุประสงค์การเข้าพื้นที่ควบคุม

5. ระบบการรักษาการณ์

5.1 ระบบการรักษาการณ์ คือ การจัด และกำหนดเจ้าหน้าที่รักษาความปลอดภัย เจ้าหน้าที่เวรรักษาความปลอดภัยประจำวัน นายตรวจเวร เจ้าหน้าที่รักษาการณ์ และหรือยามรักษาการณ์ ปฏิบัติหน้าที่รักษาความปลอดภัยสถานที่ตามห้วงระยะเวลาที่กำหนด และให้รู้จักการใช้เครื่องมืออุปกรณ์ที่เสริมประสิทธิภาพในการปฏิบัติงานตลอดจนสนใจข่าวสารที่อาจส่งผลกระทบเป็นภัยต่อหน่วยงาน

5.2 กำลังและขีดความสามารถของเจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์เพียงพอกับการปฏิบัติหน้าที่ตามความสำคัญของสถานที่ของส่วนราชการนั้นๆ หรือไม่ มีการแก้ไขทดแทน หรือปรับปรุงจุดอ่อนเกี่ยวกับเรื่องนี้ด้วยวิธีใด มีการประสานแผนการรักษาความปลอดภัยกับส่วนราชการอื่นที่เกี่ยวข้องหรือไม่

5.3 ต้องมีการคัดเลือก ตรวจสอบประวัติและพฤติการณ์ เพื่อสรรหาตัวบุคคลที่ทำหน้าที่เจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ โดยพิจารณาจากคุณสมบัติด้านคุณธรรม จริยธรรม และสมรรถนะทางร่างกาย

5.4 ต้องมีการกำกับดูแล โดยเจ้าหน้าที่รักษาความปลอดภัยของหน่วยงานนั้น ๆ ด้วยวิธีการดังต่อไปนี้

5.4.1 การกำกับดูแลโดยบุคคล หมายถึงการตรวจการปฏิบัติงานโดยหัวหน้าเจ้าหน้าที่รักษาการณ์ตามลำดับชั้น การตรวจจะทำตั้งแต่ก่อนเริ่มปฏิบัติหน้าที่ตรวจสภาพทั่วไปของเครื่องมือ อุปกรณ์ อาวุธ ทบทวนคำสั่ง และระเบียบของสถานที่นั้นตรวจตามระยะเวลาระหว่างการปฏิบัติหน้าที่ เพื่อดูความพร้อม ความเคร่งครัด ความตื่นตัวในการปฏิบัติหน้าที่

5.4.2 การกำกับดูแลโดยเครื่องมือ เป็นการใช้เครื่องมือ หรือวิธีการที่เสมือนบังคับให้เจ้าหน้าที่รักษาการณ์ต้องปฏิบัติตามระยะเวลาที่ทำหน้าที่ เครื่องมือและวิธีการมีดังนี้

1) บันทึกการปฏิบัติ โดยใช้แบบฟอร์มรายงานการปฏิบัติ ให้เจ้าหน้าที่รักษาการณ์เป็นผู้ลงบันทึก ตามจุด และเวลาที่กำหนดไว้

2) ตรวจสอบการปฏิบัติงาน โดยเครื่องมือสื่อสาร เช่น วิทยุสื่อสาร โทรศัพท์ และสัญญาณอื่น ๆ ที่สามารถสื่อความหมายได้ โดยหัวหน้าเจ้าหน้าที่รักษาการณ์ หรือเจ้าหน้าที่รักษาความปลอดภัยของหน่วยงานเป็นผู้ตรวจสอบ

5.5 ต้องมีการฝึกอบรมและพัฒนาเจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ เพื่อให้การปฏิบัติหน้าที่มีประสิทธิภาพ ให้ตระหนักถึงภยันตรายที่อาจเกิดขึ้นแก่หน่วยงาน สร้างจิตสำนึกในการรักษาความปลอดภัย ฝึก ทบทวน การใช้เครื่องมือ อาวุธ อุปกรณ์ต่าง ๆ ตลอดจนทดสอบความสามารถ วินัยในการปฏิบัติหน้าที่

6. <u>การป้องกันและระงับอัคคีภัย</u>

หัวหน้าส่วนราชการต้องกำหนดแผนป้องกันและระงับอัคคีภัย โดยมีเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วยงาน เป็นผู้กำหนดรายละเอียดและกำกับดูแลให้เป็นไปตามกฎหมายเกี่ยวกับการป้องกันและระงับอัคคีภัย ในแต่ละหน่วยงานควรพิจารณา ดังนี้

6.1 <u>เจ้าหน้าที่ดับเพลิง</u> ควรกำหนดตัวบุคคล และหน้าที่ความรับผิดชอบให้ชัดเจน

6.1.1 **ในเวลาราชการ** ให้แบ่งกลุ่มเจ้าหน้าที่รับผิดชอบด้านต่าง ๆ เช่น กลุ่มที่ทำหน้าที่ดับเพลิง กลุ่มที่ทำหน้าที่ขนย้ายเอกสารและวัสดุอุปกรณ์ต่าง ๆ กลุ่มที่ทำหน้าที่ค้นหา ตรวจตราผู้ที่หลงเหลือในอาคาร เป็นต้น

6.1.2 **นอกเวลาราชการ** เป็นหน้าที่ของ เจ้าหน้าที่รักษาความปลอดภัย และเจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ประจำวันที่หน่วยงานกำหนดขึ้นเป็นผู้รับผิดชอบ

6.2 <u>การจัดเตรียมอุปกรณ์ในการดับเพลิง</u>

6.2.1 สัญญาณแจ้งเหตุเพลิงไหม้

6.2.2 เครื่องมือดับเพลิงชั้นต้น เช่น น้ำ ทราย ถัง เชือก ขวาน เป็นต้น อุปกรณ์ถังเคมีดับเพลิงที่เหมาะสมกับเพลิงไหม้ทุกประเภท

6.2.3 ตำแหน่งที่ติดตั้งควรอยู่ในตำแหน่งที่มองเห็นได้ชัดเจน และสามารถนำไปใช้ได้สะดวก

6.2.4 ตรวจสอบอุปกรณ์ทุกชนิดให้อยู่ในสภาพที่ใช้งานได้

6.2.5 หมายเลขโทรศัพท์ของหน่วยงานดับเพลิงที่ติดต่อได้สะดวก รวดเร็ว

6.3 การฝึกอบรมเรื่องการดับเพลิง

ให้จัดทำแผนป้องกันและระงับอัคคีภัย เส้นทางหนีไฟ และอบรมให้เจ้าหน้าที่ทุกคนในหน่วยงานระมัดระวังป้องกันการเกิดอัคคีภัย ฝึกซ้อมให้มีความรู้ ความชำนาญในการดับเพลิงเบื้องต้น การหนีไฟตามแผน โดยเจ้าหน้าที่ควรมีความรู้ในเรื่องต่าง ๆ ดังนี้

6.3.1 ประเภทของเพลิง เช่น จากวัสดุธรรมดา น้ำมัน วัตถุเคมี กระแสไฟฟ้าลัดวงจร เป็นต้น

6.3.2 เครื่องมืออุปกรณ์ที่ใช้ในการดับเพลิง ตำแหน่งที่ตั้ง วิธีการใช้

6.3.3 การติดต่อสื่อสาร แจ้งเหตุ แผนผังอาคาร เส้นทางเคลื่อนย้าย เส้นทางหนีไฟ

6.3.4 หมายเลขโทรศัพท์หน่วยดับเพลิง

7. อุปกรณ์เสริมมาตรการการรักษาความปลอดภัย

การติดตั้งอุปกรณ์เสริมมาตรการการรักษาความปลอดภัย หน่วยงานของรัฐควรพิจารณาตามความเหมาะสม เช่น ระบบกล้องโทรทัศน์วงจรปิด ซึ่งควรมีผู้รับผิดชอบในการควบคุม เฝ้าดู และตรวจสอบให้อยู่ในสภาพใช้งานได้ตลอดเวลา เป็นต้น

บทที่ 11

คู่มือการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยในการประชุมลับ

1. หัวหน้าหน่วยงานของรัฐเจ้าของเรื่องที่จะมีการประชุมลับเป็นผู้รับผิดชอบการรักษาความปลอดภัยเกี่ยวกับการประชุมลับนั้น หรืออาจมอบหมายให้บุคคลที่เหมาะสมเป็นผู้ดำเนินการแทนได้ โดยแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับและนายทะเบียนข้อมูลข่าวสารลับ รวมทั้งแจ้งให้ผู้เข้าร่วมการประชุมและผู้มีหน้าที่เกี่ยวข้องทุกฝ่ายทราบ

2. กรณีการประชุมลับหลายหน่วยงาน ต้องกำหนดหน่วยงานเจ้าภาพรับผิดชอบและแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ ทำหน้าที่ประสานงานในเรื่องการรักษาความปลอดภัยกับเจ้าหน้าที่รักษาความปลอดภัยในการประชุมลับของแต่ละหน่วยงาน ซึ่งจะต้องวางมาตรการการรักษาความปลอดภัยเฉพาะในฝ่ายตนให้สอดคล้องกับมาตรการการรักษาความปลอดภัยในการประชุมลับ

3. การรักษาความปลอดภัยในการประชุมลับต้องคำนึงถึงหลักการดังต่อไปนี้

3.1 บุคคลที่เกี่ยวข้องกับการประชุมลับ ต้องผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล พร้อมทั้งได้รับความไว้วางใจให้เข้าถึงความลับในการประชุมนั้น และการปฏิบัติงานให้อยู่ในความควบคุมของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับนั้น สำหรับผู้ที่ไม่มีอำนาจหน้าที่ ต้องไม่ได้รับทราบหรือครอบครองสิ่งที่เป็นความลับของทางราชการในการประชุม

3.2 ห้ามนำเครื่องมือสื่อสาร วัสดุอุปกรณ์ หรือเครื่องบันทึกภาพหรือเสียงเข้าไปในสถานที่ประชุม และต้องไม่นำเครื่องมือ วัสดุอุปกรณ์ หรือข้อมูลข่าวสารใด ๆ ออกนอกสถานที่ประชุมนั้น

4. การรักษาความปลอดภัยในการประชุมลับ ให้หน่วยงานของรัฐพิจารณาดำเนินการดังต่อไปนี้

4.1 กำหนดพื้นที่ที่มีการรักษาความปลอดภัยประกอบด้วยสิ่งดังต่อไปนี้

4.1.1 กำหนดอาณาเขตที่ใช้ในการประชุมลับ ที่ทำการของผู้เข้าประชุมลับและสถานที่ที่ใช้เก็บรักษาสิ่งที่เป็นความลับของทางราชการ และจัดให้มีมาตรการการรักษาความปลอดภัยตามความจำเป็นและเหมาะสมไว้ล่วงหน้าก่อนเปิดการประชุมลับ

4.1.2 กำหนดให้มีบัตรผ่านหรือป้ายแสดงตนสำหรับใช้ควบคุมบุคคล หลักเกณฑ์และวิธีปฏิบัติในการกำหนดพื้นที่ที่มีการรักษาความปลอดภัย ในการประชุมลับตามวรรคหนึ่ง ให้ดำเนินการตามมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่

4.2 ดำเนินการรักษาความปลอดภัย เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับต้องดำเนินการดังต่อไปนี้

4.2.1 ตรวจตราและตรวจสอบทางเทคนิคตลอดในพื้นที่ที่กำหนดให้มีการรักษาความปลอดภัยทั้งหมดอย่างละเอียดก่อนวันเปิดประชุมลับและระหว่างการประชุมลับ

4.2.2 ในกรณีที่การประชุมลับนั้นมีความสำคัญมาก หน่วยของรัฐอาจขอความช่วยเหลือจากองค์การรักษาความปลอดภัยได้ หลังจากที่องค์การรักษาความปลอดภัยตรวจสอบแล้ว ให้ส่งมอบความรับผิดชอบในพื้นที่นั้นเป็นลายลักษณ์อักษรแก่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับหรือผู้แทนหน่วยงานนั้น

การปฏิบัติต่อสิ่งที่เป็นความลับของทางราชการ การควบคุมดูแลการประชุมลับการทำลายข้อมูลข่าวสารลับที่ไม่ใช้แล้ว ให้อยู่ในความดูแลของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับและนายทะเบียนข้อมูลข่าวสารลับ

4.3 ประสานงานการรักษาความปลอดภัย

กรณีการประชุมลับหลายหน่วยงาน ต้องกำหนดหน่วยงานเจ้าภาพรับผิดชอบและแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ โดยผู้เข้าประชุมแต่ละฝ่ายจำเป็นต้องวางมาตรการการรักษาความปลอดภัยเฉพาะในฝ่ายตน ซึ่งการวางมาตรการดังกล่าวต้องสอดคล้องกับมาตรการการรักษาความปลอดภัยในการประชุมลับ

ทั้งนี้ เจ้าหน้าที่รักษาความปลอดภัยการประชุมลับ ทำหน้าที่ประสานงานในเรื่องการรักษาความปลอดภัยกับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ

4.4 กำหนดวิธีปฏิบัติต่อผู้มาติดต่อ

หลักเกณฑ์การปฏิบัติต่อผู้มาติดต่อในการประชุมลับ ให้ดำเนินการตามมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ โดยผู้ติดต่อกับผู้เข้าร่วมประชุมลับต้องเป็นบุคคลที่ได้รับอนุญาตให้ผ่านเข้าพื้นที่ที่มีการรักษาความปลอดภัย พื้นที่ควบคุม หรือพื้นที่หวงห้าม และกำหนดให้มีบัตรผ่านหรือป้ายแสดงตนสำหรับใช้ควบคุมบุคคล รวมทั้งจัดให้มีการบันทึกหลักฐานสำหรับผู้มาติดต่อ ทั้งนี้ จัดให้มีสถานที่พักรอสำหรับผู้มาติดต่อ

4.5 แถลงข่าวต่อสื่อมวลชน

กรณีจำเป็นต้องมีการแถลงข่าวเกี่ยวกับการประชุมลับ ให้ผู้รับผิดชอบจัดประชุมดำเนินการดังต่อไปนี้

4.5.1 จัดสถานที่ที่ใช้แถลงข่าวขึ้นโดยเฉพาะ และควรอยู่นอกพื้นที่ที่มีการรักษาความปลอดภัยในการประชุมลับ

4.5.2 กำหนดให้ผู้แถลงข่าว หัวข้อที่จะนำแถลง และข้อมูลข่าวสารที่จะเผยแพร่ ต้องได้รับอนุมัติจากที่ประชุมลับก่อน หรือในกรณีที่ที่ประชุมลับมอบหมายให้มีผู้แถลงข่าวหลายคน ผู้แถลงข่าวแต่ละคนต้องแถลงเฉพาะเรื่องที่ตนได้รับอนุมัติจากที่ประชุมลับเท่านั้น

4.5.3 ควบคุมให้การแถลงข่าวหรือการเผยแพร่ข้อมูลข่าวสารและผู้เข้ารับฟังเป็นไปด้วยความเหมาะสม

4.6 บรรยายหรือบรรยายสรุปเรื่องที่เป็นความลับ

ในกรณีที่เป็นการบรรยายหรือการบรรยายสรุปเรื่องที่เป็นความลับ นอกจากจะต้องปฏิบัติตามมาตรการในการรักษาความปลอดภัยในการประชุมลับแล้ว ให้ดำเนินการดังต่อไปนี้

4.6.1 กำหนดชั้นความลับของการบรรยายหรือการบรรยายสรุป โดยถือตามชั้นความลับที่สูงสุดในข้อมูลข่าวสาร หรือสิ่งที่ใช้ประกอบการบรรยายหรือการบรรยายสรุปนั้น

4.6.2 กำหนดให้ผู้เข้ารับฟังทุกคนต้องได้รับความไว้วางใจให้เข้าถึงชั้นความลับของการบรรยายหรือการบรรยายสรุปนั้น

4.6.3 เมื่อเริ่มและสิ้นสุดการบรรยายหรือการบรรยายสรุป ผู้บรรยายต้องแจ้งให้ผู้เข้ารับฟังรับทราบชั้นความลับของการบรรยาย และเน้นย้ำให้ดำเนินการรักษาความปลอดภัยต่อสิ่งที่ได้รับฟังจากการบรรยายหรือการบรรยายสรุปนั้น

บทที่ 12

คู่มือการปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

1. ให้เจ้าหน้าที่ของรัฐผู้พบเห็นหรือทราบ หรือสงสัยว่าจะมีหรือมีการละเมิดมาตรการการรักษาความปลอดภัย รีบดำเนินการเบื้องต้นเพื่อลดความเสียหายให้เหลือน้อยที่สุดและรายงานผู้บังคับบัญชา หรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือเจ้าหน้าที่ผู้รับผิดชอบ หรือแจ้งเจ้าของเรื่องเดิมทราบโดยเร็วที่สุด

2. ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือเจ้าหน้าที่ผู้รับผิดชอบดำเนินการดังต่อไปนี้

2.1 สำรวจและตรวจสอบความเสียหายอันเกิดจากการละเมิดมาตรการการรักษาความปลอดภัย

2.2 ดำเนินการเพื่อป้องกันหรือลดความเสียหายให้เหลือน้อยที่สุด

2.3 สำรวจตรวจสอบและค้นหาสาเหตุแห่งการละเมิดมาตรการการรักษาความปลอดภัย ตลอดจนจุดอ่อนและข้อบกพร่องต่าง ๆ

2.4 ดำเนินการแก้ไขมาตรการการรักษาความปลอดภัยให้รัดกุมยิ่งขึ้นเพื่อป้องกันมิให้มีการละเมิดมาตรการการรักษาความปลอดภัยเกิดขึ้นอีก

2.5 รายงานรายละเอียดเกี่ยวกับการละเมิดมาตรการการรักษาความปลอดภัยต่อผู้บังคับบัญชาตามลำดับชั้น หากมีข้อมูลข่าวสารลับสูญหายให้รายงานและบันทึกลงในทะเบียนควบคุมข้อมูลข่าวสารลับด้วย

2.6 หากปรากฏหลักฐานหรือข้อสงสัยว่าเกิดการจารกรรม หรือการก่อวินาศกรรมให้รายงานและขออนุมัติผู้บังคับบัญชาตามลำดับชั้น เพื่อแจ้งเรื่องให้เจ้าหน้าที่ผู้มีอำนาจหน้าที่ในด้านการสืบสวนดำเนินการต่อไป

3. เมื่อได้ดำเนินการตามข้อ 2 แล้ว ให้หัวหน้าหน่วยงานของรัฐ ดำเนินการดังต่อไปนี้

3.1 แจ้งให้หน่วยงานของรัฐซึ่งเป็นเจ้าของเรื่องเดิมหรือเจ้าของสถานที่หรือผู้ที่เกี่ยวข้องทราบทันที

3.2 สอบสวนเพื่อให้ทราบว่าผู้ใดเป็นผู้ละเมิดและผู้ใดเป็นผู้รับผิดชอบต่อการละเมิดนั้น

3.3 พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนั้นเกิดขึ้นซ้ำอีก

3.4 พิจารณาดำเนินการลงโทษตามกฎหมายต่อผู้ละเมิดมาตรการการรักษาความปลอดภัย หรือผู้จะละเมิด และผู้รับผิดชอบต่อการละเมิดนั้น

4. ให้หน่วยงานของรัฐซึ่งเป็นเจ้าของเรื่องเดิมหรือผู้ที่เกี่ยวข้อง ดำเนินการดังต่อไปนี้

4.1 พิจารณาว่าสมควรลดหรือยกเลิกชั้นความลับของสิ่งที่เป็นความลับของทางราชการนั้นหรือไม่

4.2 ขจัดความเสียหายอันเกิดจากการละเมิดมาตรการการรักษาความปลอดภัยที่จะมีต่อความมั่นคงและผลประโยชน์แห่งรัฐ ในการนี้ อาจต้องเปลี่ยนแปลงนโยบาย แผนงาน พร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นสมควร

บทที่ 13

แนวทางปฏิบัติเมื่อเกิดสถานการณ์ฉุกเฉิน

สังคมไทยในปัจจุบันอยู่ในสถานการณ์ที่มีความขัดแย้งด้วยแนวความคิดทางการเมือง รวมทั้งการก่อเหตุร้ายด้วยการสร้างความไม่สงบขึ้น โดยใช้รูปแบบต่างๆ เช่น การใช้วัตถุระเบิด การยิงอาวุธร้ายแรงจากระยะไกล การลอบวางเพลิง การปิดล้อมสถานที่เพื่อการข่มขู่/ต่อรอง

หน่วยงานของรัฐฝ่ายพลเรือน อาจได้รับผลกระทบจากสถานการณ์ความขัดแย้งทางการเมือง และการก่อเหตุร้ายด้วยอาวุธร้ายแรง เช่น การใช้วัตถุระเบิด อาวุธในราชการทหาร การก่อเหตุลอบวางเพลิง หรือการคุกคามด้วยการปิดล้อมบุกทำลาย ทำให้อาจจัดแบ่งหน่วยงานของรัฐตามความเสี่ยงที่อาจเกิดภัยคุกคามจากสถานการณ์ความขัดแย้งทางการเมืองและการก่อเหตุร้ายด้วยอาวุธร้ายแรงได้เป็น 2 กลุ่มใหญ่ คือ

1. หน่วยงานของรัฐที่มีความเสี่ยงสูงที่จะเกิดภัยคุกคาม
2. หน่วยงานของรัฐที่ไม่จัดอยู่ในกลุ่มที่มีความเสี่ยงสูง

1. <u>หน่วยงานของรัฐที่มีความเสี่ยงสูงที่จะเกิดภัยคุกคาม</u> ยังอาจจัดแบ่งออกเป็นกลุ่มที่อาจเกิดความเสี่ยงของภัยคุกคามได้ 3 กลุ่ม โดยตัวอย่างที่เกิดขึ้นผ่านมา คือ

1.1 หน่วยงานของรัฐที่เป็นกิจการโครงสร้างพื้นฐานแห่งชาติที่มีความสำคัญยิ่ง (National Critical Infrastructure : NCI) ซึ่งเป็นหน่วยงานที่เป็นส่วนหลักของสังคมสมัยใหม่ มีความสำคัญต่อความมั่นคงของชาติ ระบบเศรษฐกิจ และอุตสาหกรรม รวมทั้งเป็นเป้าหมายของการก่อวินาศกรรมหากเกิดความเสียหายหรือขัดข้องจะส่งผลกระทบต่อความมั่นคงทางเศรษฐกิจและสังคม ซึ่งหมายถึงกิจกรรมดังต่อไปนี้

1) การผลิตและแจกจ่ายกระแสไฟฟ้า
2) ระบบโทรคมนาคม
3) ระบบการผลิตน้ำประปา
4) การผลิตและการแจกจ่ายอาหาร,ผลิตด้านการเกษตร
5) ก๊าซธรรมชาติและพลังงานต่างๆ
6) ระบบขนส่งมวลชน ขนส่งพลังงาน
7) งานด้านสาธารณสุข
8) การให้บริการทางการเงิน
9) หน่วยงานให้ความปลอดภัยสาธารณะ เช่น ตำรวจ ทหาร

1.2 หน่วยงานที่มีภารกิจเกี่ยวกับผู้จัดการชุมนุมสาธารณะ เช่น หน่วยงานที่ได้รับมอบหมายให้ดำเนินการด้านความผิดของแกนนำการชุมนุม หน่วยงานของกองทัพที่ได้รับมอบหมายภารกิจเป็นกำลังหลักของการป้องกันเหตุร้ายในการชุมนุม สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติที่เกี่ยวข้องกับการตรวจสอบความผิดของแกนนำทางการเมือง สถานีโทรทัศน์ของกรมประชาสัมพันธ์ ซึ่งต้องประชาสัมพันธ์การดำเนินงานของฝ่ายรัฐที่มีผลกระทบต่อการชุมนุม ฯลฯ

1.3 หน่วยงานของรัฐที่มีที่ตั้งอยู่ในบริเวณใกล้เคียงกับสถานที่จัดชุมนุมทางการเมือง ทำให้แกนนำการชุมนุมทำการปิดล้อมเพื่อให้เป็นพื้นที่ เพื่อความปลอดภัยและป้องกันเจ้าหน้าที่ของรัฐใช้ประโยชน์ในการติดตามสถานการณ์การชุมนุม เช่น โรงพยาบาลตำรวจ สำนักงานตำรวจแห่งชาติ และโรงพยาบาลจุฬาลงกรณ์ สภากาชาดไทย ระหว่างการชุมนุมของกลุ่มต่างๆ

2. **<u>หน่วยงานของรัฐที่ไม่จัดอยู่ในกลุ่มที่มีความเสี่ยงสูง</u>** แต่ต้องระวังและเตรียมความพร้อมที่อาจจะเกิดจากการชุมนุม เช่น หน่วยงานที่ไม่ได้อยู่ติดกับพื้นที่การจัดชุมนุมทางการเมืองแต่อยู่ในเส้นทางที่ผู้จัดการชุมนุมจัดให้มีการเคลื่อนขบวนผู้ชุมนุมผ่านเส้นทาง อาทิ เช่น สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด ถนนดินแดง ธนาคารที่รัฐเป็นผู้ถือหุ้นและมีตู้เอทีเอ็มอยู่ในบริเวณสำนักงาน ซึ่งเคยได้รับผลกระทบจากการชุมนุมมาแล้ว

<u>การจัดทำแผนฉุกเฉินเพื่อรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้น</u>

จากสถานการณ์ต่างๆ ที่เกิดขึ้นในสังคม สถานการณ์บางอย่างอาจขยายตัวนำไปสู่การก่อความไม่สงบขึ้น และอาจส่งผลต่อความปลอดภัยของเจ้าหน้าที่ ทรัพย์สินของทางราชการ รวมทั้งอาคารสถานที่ของหน่วยงานของรัฐ ให้ได้รับความเสียหายได้ หัวหน้าหน่วยงานของรัฐจึงควรจัดให้มีการดำเนินการตามขั้นตอนต่อไปนี้ เพื่อรับมือกับสถานการณ์ที่อาจเกิดขึ้นต่อชีวิตทรัพย์สิน และอาคารสถานที่ของรัฐ คือ

1. แนวทางการป้องกันภัยจากเหตุร้ายในการก่อความไม่สงบ

1.1 เจ้าหน้าที่ในหน่วยงานของรัฐ ควรต้องติดตามสถานการณ์ที่เกิดขึ้นอย่างใกล้ชิด ผ่านการเสนอข่าวของสื่อมวลชนประเภทต่างๆ หรือการติดต่อขอรับทราบสถานการณ์จากหน่วยงานของรัฐที่ติดตามสถานการณ์ดังกล่าว

1.2 หน่วยงานของรัฐควรนำข้อมูลเกี่ยวกับสถานการณ์ที่เกิดขึ้นมาศึกษาวิเคราะห์รูปแบบที่เกิดขึ้นว่าจะส่งผลต่อหน่วยงานของรัฐอย่างไร หรือไม่

1.3 การศึกษาวิเคราะห์รูปแบบที่เกิดขึ้น ควรพิจารณาว่าการ ก่อเหตุนั้นๆ จะเกิดต่อหน่วยงานในความรับผิดชอบหรือไม่ ซึ่งอาจพิจารณาได้จาก

1) หน่วยงานเข้าไปเกี่ยวข้องกับสถานการณ์การชุมนุมหรือไม่

2) หน่วยงานเป็นเป้าหมายของการชุมนุมหรือไม่ จากการเป็นสัญลักษณ์ทางการเมือง มีส่วนได้ส่วนเสียในผลประโยชน์ของสถานการณ์การชุมนุม

3) อยู่ในพื้นที่เกี่ยวข้องของการชุมนุม หรือในเส้นทางการเคลื่อนไหวในการชุมนุม

1.4 หน่วยงานของรัฐควรวิเคราะห์กลุ่มที่จัดการชุมนุมและแรงจูงใจของกลุ่มตลอดจนเป้าหมายของการจัดชุมนุม เพื่อให้ทราบวัตถุประสงค์ของการชุมนุมว่าต้องการผลของการชุมนุมในระดับใด เพื่อจัดเตรียมมาตรการการรักษาความปลอดภัยของหน่วยงานต่อระดับของการชุมนุมนั้น

1.5 หน่วยงานของรัฐควรจัดให้มีการวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นต่อหน่วยงาน จุดอ่อน และความสำคัญของหน่วยงานต่อสถานการณ์ความเคลื่อนไหวของการจัดการชุมนุมทางการเมืองนั้น ๆ ว่าอยู่ในระดับใดเพื่อการเตรียมการระวังป้องกันให้เหมาะสมกับสถานการณ์

1.6 หน่วยงานของรัฐควรศึกษาและวิเคราะห์ถึงรูปแบบและวิธีการที่เหตุรุนแรงที่เกี่ยวข้องจะเกิดขึ้นต่อสถานที่ต่างๆ รวมถึงหน่วยงานของรัฐที่เกี่ยวข้อง เพื่อจะได้จัดมาตรการป้องกัน หรือลดความเสียหายที่อาจเกิดขึ้นได้อย่างเหมาะสมต่อไป

ในการติดตามสถานการณ์ วิเคราะห์ ประเมินความเสี่ยง ตลอดจนการเตรียมการระวังป้องกันเพื่อลดความเสียหาย หน่วยงานของรัฐอาจดำเนินการในรูปแบบของการจัดตั้งคณะทำงาน การหารือร่วมกันของหน่วยงานที่มีที่ตั้งใกล้เคียง โดยเชิญผู้แทนจากหน่วยงานให้ความปลอดภัยสาธารณะ และหน่วยงานอื่นๆ ที่พิจารณาว่ามีความเหมาะสมที่จะให้ข้อแนะนำที่จะเป็นประโยชน์เข้าร่วมประชุมหารือ เพื่อให้ได้ผลสรุปในทางปฏิบัติที่จะเป็นประโยชน์ต่อการดำเนินงานป้องกัน เพื่อไม่ให้เกิดความเสียหายต่อความปลอดภัยของเจ้าหน้าที่ ทรัพย์สิน และอาคารสถานที่ของหน่วยงานต่อไป

2. เพื่อเป็นการเตรียมความพร้อมล่วงหน้าในการรับสถานการณ์เหตุร้ายที่อาจเกิดขึ้น หน่วยงานของรัฐควรจัดให้มีการจัดทำแผนฉุกเฉินในสถานการณ์ต่างๆ ไว้ล่วงหน้าเพื่อจะได้จัดเตรียมคน อุปกรณ์ และแนวทางปฏิบัติ

2.1 แผนป้องกันอัคคีภัย

2.2 แผนป้องกันอุบัติภัย

2.3 แผนป้องกันการก่อวินาศกรรม

2.4 แผนป้องกันเหตุประท้วง/เรียกร้อง

2.5 แผนฉุกเฉินอื่นๆ ที่เกี่ยวข้อง

ในการจัดทำแผนฉุกเฉินต่างๆ ควรได้มีการหารือในระหว่างเจ้าหน้าที่ที่เกี่ยวข้องเพื่อให้แผนที่จัดทำมีความเหมาะสม สอดคล้องกับสถานการณ์ ปฏิบัติได้ในสถานการณ์ที่เกิดขึ้นจริง มีการชี้แจงต่อเจ้าหน้าที่ในหน่วยงานให้ได้รับทราบแนวทางปฏิบัติที่ถูกต้อง มีการซักซ้อมประเมินผล และปรับปรุงแผนให้สอดคล้องกับสถานการณ์อย่างเหมาะสม เพื่อให้เกิดประสิทธิภาพในการดำเนินการต่อไป

<u>ข้อแนะนำของการจัดทำแผนฉุกเฉิน</u>

แผนฉุกเฉินที่จัดทำจะต้องมีรายละเอียดที่เกี่ยวข้องครบถ้วน การเขียนแผนจะต้องสั้นกะทัดรัด สามารถนำไปปฏิบัติได้จริง ง่ายต่อการปฏิบัติ ในขั้นตอนการปฏิบัติควรมีความชัดเจนถึงการปฏิบัติต่างๆ ว่าสิ่งใดต้องปฏิบัติ ห้ามปฏิบัติ หรืออยู่ในดุลพินิจของเจ้าหน้าที่ และเพื่อให้การปฏิบัติตามแผนเป็นไปอย่างถูกต้องและเกิดประสิทธิภาพ จึงควรมีการซักซ้อมการปฏิบัติเป็นระยะตามความเหมาะสม เพื่อให้ผู้เกี่ยวข้องสามารถนำไปปฏิบัติได้เมื่อเกิดสถานการณ์ และมีการปรับแผนให้สอดคล้องกับสถานการณ์และแนวทางการปฏิบัติต่อไป

การจัดทำแผนฉุกเฉิน เพื่อให้เกิดความชัดเจนในการปฏิบัติตาม ควรจัดทำแผนภูมิแสดงขั้นตอนการปฏิบัติประกอบ ซึ่งหากสามารถจัดทำให้อยู่ในแผ่นกระดาษเดียวก็จะเหมาะสม และสามารถนำไปติดแสดงในหน่วยงาน เพื่อให้เจ้าหน้าที่ได้รับรู้ รับทราบได้อย่างกว้างขวาง ทั้งนี้แผนฉุกเฉินที่ดีควรมีองค์ประกอบที่สำคัญของแผน ได้แก่

1. มีความชัดเจนในคำสั่ง วัตถุประสงค์ และขอบเขต
2. มีความชัดเจนในขั้นตอนการปฏิบัติเมื่อเวลาเกิดเหตุ
3. มีความชัดเจนในสิ่งที่ต้องปฏิบัติ เช่น ชนิดของสัญญาณแสดงเหตุฉุกเฉิน สัญญาณแสดงเหตุฉุกเฉิน สัญญาณในการสั่งการขั้นตอนต่างๆ
4. แนวทางการประสานหน่วยงานภายนอกเมื่อเหตุการณ์ขยายตัวรุนแรงเกินที่หน่วยงานของรัฐจะระงับเหตุได้เพียงหน่วยงานเดียว

5. การดำเนินการภายหลังจากที่ควบคุมเหตุการณ์ได้
6. การเตรียมเจ้าหน้าที่เพื่อการแถลงข่าวต่อสื่อมวลชน
7. แนวทางการฟื้นฟูบูรณะเบื้องต้น เพื่อให้หน่วยงานสามารถปฏิบัติงานได้

3. องค์ประกอบของการจัดทำแผนฉุกเฉิน
   - 3.1 ประเมินภัยคุกคามหรือความเสี่ยงที่อาจเกิดขึ้น
   - 3.2 ประเมินขีดความสามารถของหน่วยงาน ในเรื่องคน เครื่องมือ อุปกรณ์ งบประมาณ ฯลฯ
   - 3.3 กำหนดวัตถุประสงค์ และลำดับความสำคัญ
   - 3.4 การจัดทำแผนผังเหตุการณ์ กำหนดผู้อำนวยการควบคุมภาวะฉุกเฉิน เพื่อปฏิบัติหน้าที่เมื่อเกิดเหตุฉุกเฉิน

4. ระดับของสถานการณ์และแผนรองรับเหตุการณ์ควรจัดทำแผนฉุกเฉินเพื่อรองรับสถานการณ์ของเหตุการณ์เป็น 3 ระดับ คือ
   - 4.1 สถานการณ์ฉุกเฉินที่หน่วยงานสามารถระงับ หรือควบคุมได้
   - 4.2 สถานการณ์ฉุกเฉินที่หน่วยงานไม่สามารถระงับ หรือควบคุมได้เอง จำเป็นต้องได้รับการสนับสนุนจากหน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานให้ความปลอดภัยสาธารณะหรือหน่วยงานข้างเคียง
   - 4.3 สถานการณ์ฉุกเฉินที่ลุกลามขยายตัวอย่างร้ายแรง ระดับจังหวัดหรือประเทศ ที่รัฐบาลจำเป็นต้องเข้ามาดำเนินการช่วยเหลือระงับเหตุ หรือองค์การระหว่างประเทศอื่นๆ เข้ามาเกี่ยวข้องดำเนินการ

แนวทางการจัดทำแผนฉุกเฉิน และมาตรการที่เกี่ยวข้องสำหรับหน่วยงานของรัฐ ที่มีความเสี่ยงสูง

นอกเหนือจากแนวทางจัดทำแผนฉุกเฉินตามข้อที่กล่าวถึงข้างต้นแล้ว หน่วยงานของรัฐที่มีความเสี่ยงภัยสูงควรดำเนินการเพิ่มเติม เพื่อให้เหมาะสมกับระดับของความเสี่ยงภัยที่หน่วยงานอาจได้รับผลกระทบดังนี้

1. การวิเคราะห์ความเสี่ยงที่อาจส่งผลต่อการทำงานของหน่วยงาน ซึ่งควรประกอบด้วยการวิเคราะห์สิ่งต่างๆ ว่าอาจเกิดได้อย่างไรบ้าง คือ

1.1 ภัยจากการโจรกรรมและอาชญากรรมทั่วไป

1.2 ภัยจากความผิดพลาดในการปฏิบัติหน้าที่ และจากบุคคลในหน่วยงาน

1.3 ภัยจากการใช้เครื่องมืออุปกรณ์ที่ไม่ได้คุณภาพเพียงพอ

1.4 ภัยจากการก่อการร้าย

1.5 ภัยจากสถานการณ์การก่อความไม่สงบ

2. หน่วยงานที่มีหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ด้านการรักษาความปลอดภัย จัดทำแผนงานที่เกี่ยวข้องกับการรักษาความปลอดภัย การบริหารจัดการความเสี่ยง แผนฉุกเฉินกรณีต่างๆ

3. หน่วยงานควรมีการเชิญหน่วยงานเกี่ยวข้องที่จะสนับสนุนการรักษาความปลอดภัยให้มีประสิทธิภาพยิ่งขึ้น เช่น หน่วยงานด้านการรักษาความสงบเรียบร้อยในพื้นที่ทั้งตำรวจ ทหาร หน่วยงานด้านการข่าวกรอง ที่จะสนับสนุนด้านข้อมูลที่เกี่ยวข้องกับสถานการณ์ หน่วยงานด้านการระงับเหตุการณ์ เช่น การดับเพลิง การบรรเทาสาธารณภัย หน่วยงานข้างเคียงในพื้นที่ และตัวแทนชุมชนโดยรอบพื้นที่ เพื่อสร้างให้เกิดเครือข่ายด้านการรักษาความปอลดภัย และการติดตามสถานการณ์ให้ทันต่อเหตุการณ์ รวมทั้งเพื่อการแลกเปลี่ยนประสบการณ์ในการปฏิบัติเพื่อรองรับสถานการณ์ ได้อย่างถูกต้องเหมาะสม
