มสขช. 01-2569

ประกาศใช้เมื่อ มกราคม 2569

มาตรฐานการรักษาความปลอดภัย หน่วยงานของรัฐฝ่ายพลเรือน

สำนักข่าวกรองแห่งชาติ

สำนักนายกรัฐมนตรี

มสขช. 01-2569

จัดทำโดย สำนักข่าวกรองแห่งชาติ สำนักนายกรัฐมนตรี
แจกจ่ายหน่วยงานของรัฐฝ่ายพลเรือนและเผยแพร่ในเว็บไซต์องค์การรักษา
ความปลอดภัยฝ่ายพลเรือน (www.secnia.go.th) โดยสามารถติดต่อ
สอบถามข้อมูลหรือขอคำแนะนำได้ตามที่อยู่ หมายเลขโทรศัพท์ และไปรษณีย์อิเล็กทรอนิกส์ ดังนี้
สำนักข่าวกรองแห่งชาติ
321 ถนนราชดำเนินนอก เขตดุสิต
กรุงเทพมหานคร
รหัสไปรษณีย์ 10300
โทร. 0 2279 7180 ต่อ 7304 7305 7310
ไปรษณีย์อิเล็กทรอนิกส์ : secnia@nia.go.th

คำนำ

การรักษาความปลอดภัยแห่งชาติ และการรักษาความลับของทางราชการ เป็นเรื่องสำคัญและจำเป็นที่หน่วยงานของรัฐต้องตระหนักและปฏิบัติตาม เรื่องนี้ได้มีข้อบัญญัติกำหนดไว้ในระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ซึ่งเป็นแนวปฏิบัติหลัก ขณะที่ ได้มีกฎหมาย ระเบียบ ข้อบังคับ มาตรฐาน และประกาศ ใช้จากหน่วยงานที่เกี่ยวข้อง ทำให้การปฏิบัติของหน่วยงานของรัฐจะต้องมีมาตรการรักษาความปลอดภัย และรักษาความลับของทางราชการ โดยปฏิบัติภายใต้ข้อกำหนด และแนวทางปฏิบัติ ที่ครบถ้วน ถูกต้อง และเหมาะสม

สำนักข่าวกรองแห่งชาติ ซึ่งมีภารกิจหลักในด้านการรักษาความปลอดภัยฝ่ายพลเรือน ตามที่บัญญัติไว้ในพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 มีหน้าที่ให้คำแนะนำ ช่วยเหลือ กำกับดูแลส่วนราชการฝ่ายพลเรือน รัฐวิสาหกิจ และหน่วยงานอื่นของรัฐในการดำเนินการเพื่อรักษาความปลอดภัยแก่เจ้าหน้าที่ สถานที่ ข้อมูลข่าวสาร และสิ่งของอื่น ๆ ของทางราชการให้พ้นจากภัยคุกคาม รวมทั้ง เป็นองค์การรักษาความปลอดภัยฝ่ายพลเรือน ตามที่ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม กำหนดไว้ ประกอบกับ ภายใต้บริบทภัยคุกคามรูปแบบเก่าที่ไม่หมดไป ทั้งยังรุนแรงและสร้างผลกระทบในวงกว้าง ขณะที่มีภัยคุกคามรูปแบบใหม่ ที่เกิดขึ้นหลายเรื่อง เป็นสิ่งที่คาดไม่ถึงยากต่อการรับมือ ทั้งหมดนี้เป็นความท้าทายให้หน่วยงานของรัฐต้องตั้งรับ และกำหนดมาตรการรักษาความปลอดภัยที่มีประสิทธิภาพรองรับ นอกจากนี้ กฎหมายที่เกี่ยวข้องกับการบริหารจัดการงานรักษาความปลอดภัย และการรักษาความลับของทางราชการ ตามระเบียบทั้งสองฉบับและกฎหมายอื่นๆ ที่ได้ปรับปรุงข้อกำหนดเพิ่มเติม และเชื่อมโยงในทางปฏิบัติระหว่างกัน

สำนักข่าวกรองแห่งชาติ ได้จัดทำมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน เพื่อเป็นเครื่องมือในการส่งเสริมและสนับสนุนให้หน่วยงานของรัฐฝ่ายพลเรือน สามารถดำเนินการด้านการรักษาความปลอดภัย ได้อย่างครบถ้วน ถูกต้อง และเหมาะสม โดยมาตรฐานดังกล่าวได้ผ่านการรับฟังความคิดเห็นจากหน่วยงานของรัฐฝ่ายพลเรือน (กลุ่มเป้าหมาย) หน่วยงานด้านการข่าว องค์การมหาชน สถาบันอุดมศึกษาของรัฐที่ไม่เป็นส่วนราชการแต่อยู่ในกำกับของรัฐ หรือองค์กรปกครองส่วนท้องถิ่น และหน่วยธุรการขององค์การของรัฐที่เป็นอิสระ รวมทั้ง การนำไปตรวจสอบเทียบเคียงกับมาตรฐานที่องค์การระหว่างประเทศว่าด้วยมาตรฐาน (International Organization for Standardization) เพื่อนำมาทบทวนและปรับปรุงให้เหมาะสมยิ่งขึ้น จากนั้นได้เสนอผ่านคณะกรรมการบริหารของสำนักข่าวกรองแห่งชาติ และคณะอนุกรรมการประสานการปฏิบัติตามนโยบายการรักษาความปลอดภัยแห่งชาติ (อป.กรช.) รวมทั้ง ได้แจ้งต่อคณะกรรมการนโยบายรักษาความปลอดภัยแห่งชาติ (กรช.) และคณะกรรมการข้อมูลข่าวสารของราชการ (กขร.) และคณะรัฐมนตรี รับทราบการเผยแพร่มาตรฐานฯ นี้ เพื่อให้หน่วยงานของรัฐได้

นำไปปรับใช้ รวมทั้ง หากเอกชนที่สนใจได้ศึกษาและทำความเข้าใจเพื่อร่วมเป็นส่วนหนึ่งในการต่อต้านภัยคุกคามในรูปแบบต่าง ๆ พร้อมกับเป็นการยกระดับการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน ที่จะช่วยกับสำนักข่าวกรองแห่งชาติขับเคลื่อนการรักษาความปลอดภัยแห่งชาติ รักษาไว้ซึ่งความมั่นคงแห่งรัฐและผลประโยชน์แห่งชาติ โดยมีกำหนดทบทวนมาตรฐานอย่างน้อยทุกห้าปี หรือเมื่อมีการปรับปรุง แก้ไข เพิ่มเติมกฎหมายหรือระเบียบหลักที่เกี่ยวข้อง

มาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือนฉบับนี้ ประกอบด้วยมาตรฐานการรักษาความปลอดภัยที่รวบรวมหลักการและแนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับบุคคล การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ การรักษาความปลอดภัยเกี่ยวกับสถานที่ การรักษาความปลอดภัยในการประชุมลับ และการปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

สำนักข่าวกรองแห่งชาติ ในฐานะองค์การรักษาความปลอดภัยฝ่ายพลเรือน มีความมุ่งหวังว่ามาตรฐานการรักษาความปลอดภัยฉบับนี้ จะเป็นเครื่องมือสำคัญในการยกระดับและพัฒนามาตรฐานการรักษาความปลอดภัยของหน่วยงานของรัฐฝ่ายพลเรือน ซึ่งมีความสำคัญต่อความมั่นคงปลอดภัยขององค์กรและความมั่นคงแห่งชาติ

สารบัญ

หน้า

หน้า

บทสรุปสำหรับผู้บริหาร

สำนักข่าวกรองแห่งชาติ จัดทำมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน ภายใต้บทบาทและหน้าที่ในภารกิจการรักษาความปลอดภัยฝ่ายพลเรือน ที่กำหนดไว้ในพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 และในฐานะองค์การรักษาความปลอดภัยฝ่ายพลเรือน ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม โดยมีวัตถุประสงค์เพื่อส่งเสริมและสนับสนุนให้การดำเนินการด้านการรักษาความปลอดภัยของหน่วยงานของรัฐฝ่ายพลเรือนมีประสิทธิภาพมากยิ่งขึ้น เพื่อเป็นการป้องปราม ป้องกัน หรือลดความเสียหายที่อาจเกิดจากภัยคุกคามหรือการกระทำต่าง ๆ ที่มุ่งบ่อนทำลาย จารกรรม ก่อวินาศกรรม หรือก่อการร้าย อันอาจก่อให้เกิดความเสียหายทั้งต่อเจ้าหน้าที่ของรัฐ ข้อมูลข่าวสาร และสถานที่ของราชการ ตลอดจนส่งผลกระทบต่อภาพลักษณ์ขององค์กร หรือขยายผลจนก่อให้เกิดความเสียหายในระดับประเทศได้

มาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน มีขอบข่ายการบังคับใช้ต่อหน่วยงานของรัฐที่เป็นหน่วยงานราชการส่วนกลาง และหน่วยงานราชการส่วนภูมิภาค ตามกฎหมายว่าด้วยการปรับปรุงกระทรวง ทบวง กรม และกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน รัฐวิสาหกิจ หน่วยงานอื่นของรัฐ อย่างไรก็ดี องค์กรปกครองส่วนท้องถิ่น หรือหน่วยงานอื่นใดของรัฐ หรือหน่วยงานรูปแบบใหม่ที่อยู่ในกำกับของฝ่ายบริหาร สามารถนำมาตรฐานนี้ไปใช้ได้โดยอนุโลม

มาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน ประกอบด้วยรายละเอียดของเนื้อหา 4 บท ได้แก่

บทที่ 1 กล่าวถึงความสำคัญ วัตถุประสงค์ วิธีการ และเครื่องมือในการขับเคลื่อนการดำเนินการตามมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน โดยกำหนดให้หน่วยงานตรวจสอบการปฏิบัติตามมาตรฐานด้วยตนเอง (Self-Assessment) ด้วยแบบตรวจสอบมาตรฐานการรักษาความปลอดภัย ภายใต้การสนับสนุนการดำเนินการจากสำนักข่าวกรองแห่งชาติ ซึ่งมีหน้าที่ให้คำแนะนำ ข้อชี้แนะ ตลอดจน ความช่วยเหลือในการรักษาความปลอดภัยแต่ละด้านให้เกิดประสิทธิภาพ ทั้งนี้ จุดเริ่มต้นในการดำเนินการให้เป็นไปตามมาตรฐาน คือ การแต่งตั้ง และมอบหมายผู้ปฏิบัติหน้าที่ในด้านต่าง ๆ โดยมีคำสั่งแต่งตั้งและมอบหมายหน้าที่เป็นลายลักษณ์อักษร ได้แก่

1) คำสั่งแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย นายทะเบียนข้อมูลข่าวสารลับ และผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ นายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์และผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์ คณะกรรมการตรวจสอบข้อมูลข่าวสารลับ คณะกรรมการทำลายข้อมูลข่าวสารลับ รวมถึง เจ้าหน้าที่นำสาร (ถ้ามี)

2) คำสั่งมอบหมายหน้าที่ผู้มีอำนาจกำหนดชั้นความลับ เพื่อใช้ดุลพินิจพิจารณากำหนดชั้นความลับ หรือปรับชั้นความลับของข้อมูลข่าวสารลับที่หน่วยงานเป็นเจ้าของเรื่อง

นิยามศัพท์ เป็นการอธิบายความหมายของคำศัพท์เฉพาะที่ระบุไว้ในมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน สำหรับคำศัพท์ หรือคำจำกัดความที่มีการกำหนดไว้แล้วตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม และกฎหมายหรือระเบียบอื่นที่มีการอ้างอิงในมาตรฐานฉบับนี้ มิได้นำมาอธิบายเพิ่มเติมไว้

นิยามศัพท์ที่ได้ให้ความหมายไว้ ได้แก่ มาตรฐานการรักษาความปลอดภัย การรักษาความปลอดภัยเกี่ยวกับบุคคล การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ การรักษาความปลอดภัยเกี่ยวกับสถานที่ การรักษาความปลอดภัยในการประชุมลับ หน่วยงานย่อย บุคคลภายนอก การรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) การรักษาสภาพพร้อมใช้งาน (Availability) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ อุปกรณ์เฉพาะ ภัยคุกคาม พื้นที่ควบคุม พื้นที่หวงห้าม เครื่องกีดขวาง แผนเผชิญเหตุ ผู้กระทำการละเมิด ผู้จะกระทำการละเมิด และผู้รับผิดชอบต่อการละเมิด

บทที่ 2 มาตรฐานการรักษาความปลอดภัย เป็นการกำหนดหลักการดำเนินการด้านมาตรฐานการรักษาความปลอดภัย ประกอบด้วย

1) มาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล การดำเนินการเพื่อคัดกรองบุคคลที่เข้ามาปฏิบัติหน้าที่ในหน่วยงาน โดยการตรวจสอบประวัติและพฤติการณ์บุคคล ให้ได้ผู้ที่มีคุณสมบัติเหมาะสม การรับรองความไว้วางใจบุคคลให้เข้าถึงสิ่งที่เป็นความลับของทางราชการ การอบรมให้ความรู้บุคลากรของหน่วยงาน เพื่อเสริมสร้างและกระตุ้นจิตสำนึกด้านการรักษาความปลอดภัย

2) มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ การดำเนินการเพื่อควบคุมและคุ้มครองข้อมูลข่าวสารลับของทางราชการ ไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง รั่วไหล หรือถูกเปิดเผยก่อนเวลาอันควร โดยให้ความสำคัญต่อการรับรองความไว้วางใจแก่บุคคล

ที่จะเข้าถึงข้อมูลข่าวสารลับ และให้เข้าถึงเฉพาะเรื่องที่ได้รับมอบหมายเท่านั้น การจัดให้มีระบบทะเบียนข้อมูลข่าวสารลับให้ครบถ้วน ได้แก่ ทะเบียนรับ (ทขล.1) ทะเบียนส่ง (ทขล.2) ทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3) แยกต่างหากจากทะเบียนงานสารบรรณปกติ ตลอดจนให้ความสำคัญต่อการตรวจสอบข้อมูลข่าวสารลับที่อยู่ในความครอบครอง (ทั้งในรูปแบบเอกสารและอิเล็กทรอนิกส์) อย่างสม่ำเสมอ เพื่อให้สามารถบริหารจัดการข้อมูลข่าวสารลับ ได้อย่างถูกต้องและเหมาะสม รวมถึงต้องจัดทำแผนการปฏิบัติในเวลาฉุกเฉินสำหรับข้อมูลข่าวสารลับ ได้แก่ แผนการเคลื่อนย้าย แผนการพิทักษ์รักษา และแผนการทำลาย และมีการควบคุม กำกับดูแลการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ ให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม

3) มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ การดำเนินการเพื่อควบคุมและคุ้มครองข้อมูลข่าวสารลับของทางราชการ ที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง หรือรั่วไหล โดยให้ความสำคัญต่อการรักษาความปลอดภัยเกี่ยวกับบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ได้แก่ ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ซึ่งสามารถเข้าถึงข้อมูลข่าวสารลับอิเล็กทรอนิกส์ของหน่วยงาน รวมถึงผู้ทำหน้าที่ติดตั้ง ซ่อมบำรุง หรือทำการอื่นใดต่อคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่ใช้ดำเนินการเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ตลอดจนจัดให้มีระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน เป็นลายลักษณ์อักษร

4) มาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ การดำเนินการเพื่อพิทักษ์รักษาที่สงวน อาคาร สถานที่ วัสดุอุปกรณ์ ศูนย์ข้อมูลสารสนเทศ ระบบสาธารณูปโภค ตลอดจนเจ้าหน้าที่ และข้อมูลข่าวสาร ให้พ้นจากภัยอันตราย หรือเหตุอื่นใดอันอาจทำให้เสียความสามารถในการปฏิบัติภารกิจของหน่วยงานของรัฐ โดยต้องมีการประเมินภัยคุกคาม ประเมินระดับความเสี่ยง และจัดระดับความเสี่ยงของหน่วยงาน เพื่อจะได้จัดทำแผนการรักษาความปลอดภัย ทั้งในสถานการณ์ปกติ สถานการณ์ไม่ปกติ และสถานการณ์ฉุกเฉิน ได้อย่างเหมาะสม ตลอดจนให้ความสำคัญต่อการทบทวนและซักซ้อมแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ อย่างน้อยปีละ 1 ครั้ง

5) มาตรฐานการรักษาความปลอดภัยในการประชุมลับ เป็นการดำเนินการเพื่อคุ้มครองและพิทักษ์รักษาบุคคล สถานที่ และข้อมูลข่าวสารลับที่เกี่ยวข้องในการประชุมลับนั้น ไม่ให้รั่วไหล ถูกรบกวนหรือขัดขวางการประชุม หรือถูกจารกรรม หรือวินาศกรรม โดยแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ เพื่อทำหน้าที่กำกับดูแล ตรวจสอบ

ผู้เกี่ยวข้องในการประชุมลับ กำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ กำกับดูแลการปฏิบัติต่อสิ่งที่เป็นความลับของทางราชการ รวมถึงควบคุมดูแลกรณีมีการแถลงข่าวหรือการบรรยายสรุปเกี่ยวกับการประชุมลับนั้น และมอบหมายหรือแต่งตั้งนายทะเบียนข้อมูลข่าวสารลับ ในการประชุมลับ เพื่อทำหน้าที่ดำเนินการเกี่ยวกับข้อมูลข่าวสารลับที่เกี่ยวข้องในการประชุมลับนั้น

6) มาตรฐานการปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย การกำหนดหลักการและแนวทางสำหรับเจ้าหน้าที่ของรัฐผู้พบเห็น หรือทราบ หรือสงสัยว่าจะมี หรือมีการละเมิดการรักษาความปลอดภัย เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือผู้รับผิดชอบ หัวหน้าหน่วยงานของรัฐ ที่เกิดการละเมิดการรักษา ความปลอดภัย และหัวหน้าหน่วยงานของรัฐที่เป็นเจ้าของเรื่องข้อมูลข่าวสารลับที่ถูกละเมิด เพื่อให้สามารถป้องกัน ลดความเสียหาย สำรวจและตรวจสอบความเสียหาย ค้นหาสาเหตุของการละเมิด จุดอ่อนและข้อบกพร่องต่าง ๆ เพื่อให้สามารถปรับปรุงและแก้ไขมาตรการการรักษาความปลอดภัยได้อย่างเหมาะสมมากยิ่งขึ้น ตลอดจนมีการสอบสวนให้ทราบผู้กระทำการละเมิด ผู้ที่ต้องรับผิดชอบต่อการละเมิดนั้น และดำเนินการลงโทษตามกฎหมาย เพื่อป้องกันหรือป้องปรามไม่ให้เกิดเหตุซ้ำอีก

บทที่ 3 แนวปฏิบัติด้านมาตรฐานการรักษาความปลอดภัย ประกอบด้วย แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับบุคคล แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับสถานที่ แนวปฏิบัติการรักษาความปลอดภัยในการประชุมลับ และแนวปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย โดยเป็นการกำหนดรายละเอียดการปฏิบัติไล่เรียงตามหลักการมาตรฐานการรักษาความปลอดภัยทั้ง 6 ด้าน

บทที่ 4 การประเมินมาตรฐานการรักษาความปลอดภัย กำหนดให้มีกระบวนการตรวจสอบและประเมินมาตรฐานการรักษาความปลอดภัย โดยหน่วยงานของรัฐตรวจสอบตนเองตามแบบตรวจสอบมาตรฐานการรักษาความปลอดภัย อย่างน้อยปีละ 1 ครั้ง และสำนักข่าวกรองแห่งชาติ ทำหน้าที่สนับสนุนด้านการประเมินผลการตรวจสอบ เพื่อที่จะสามารถให้คำแนะนำชี้แนะ และช่วยเหลือด้านการรักษาความปลอดภัยแก่หน่วยงานของรัฐฝ่ายพลเรือน ได้อย่างเหมาะสม

ผนวก กำหนดให้มีแบบเอกสาร เพื่อเป็นเครื่องมือสำคัญต่อการปฏิบัติตามมาตรฐานการรักษาความปลอดภัย ได้แก่

1) แบบสำรวจมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ เพื่อให้หน่วยงานของรัฐใช้ในการสำรวจและกำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ (ในสถานการณ์

ปกติ) ให้เหมาะสม รวมถึงสามารถพิจารณาปรับปรุง เพิ่มเติมมาตรการการรักษาความปลอดภัย ให้รองรับสถานการณ์ไม่ปกติ และสถานการณ์ฉุกเฉินได้

2) แบบตรวจสอบมาตรฐานการรักษาความปลอดภัย ซึ่งถือเป็นเครื่องมือสำคัญที่จะช่วยให้การขับเคลื่อนมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน สามารถบรรลุตามวัตถุประสงค์ในการส่งเสริมและสนับสนุนให้เกิดประสิทธิภาพด้านการรักษาความปลอดภัย โดยหน่วยงานของรัฐต้องแต่งตั้งคณะกรรมการตรวจสอบมาตรฐานการรักษาความปลอดภัยของหน่วยงาน (คมป.) เพื่อทำหน้าที่ตรวจสอบ (Check List) ตามแบบตรวจสอบมาตรฐานการรักษาความปลอดภัย อย่างน้อยปีละ 1 ครั้ง และส่งแบบตรวจสอบ ให้สำนักข่าวกรองแห่งชาติ เพื่อเป็นข้อมูลสำหรับการสนับสนุนการดำเนินการ ให้คำแนะนำ หรือช่วยเหลือในเรื่องการรักษาความปลอดภัยและการรักษาความลับของทางราชการ

.....

มาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน

บทที่ 1
บททั่วไป

ความสำคัญ

สำนักข่าวกรองแห่งชาติ มีภารกิจหน้าที่ด้านการรักษาความปลอดภัยฝ่ายพลเรือน ตามพระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. 2562 และในฐานะองค์การรักษาความปลอดภัยฝ่ายพลเรือน ตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 มีหน้าที่ให้คำแนะนำ ให้คำปรึกษา ช่วยเหลือ กำกับดูแล ตรวจสอบ พร้อมทั้งพิจารณาแก้ไขข้อบกพร่อง เพื่อให้ระบบการรักษาความปลอดภัยของหน่วยงานของรัฐฝ่ายพลเรือน ได้ผลสมบูรณ์และมีประสิทธิภาพอยู่เสมอ

เพื่อให้สามารถขับเคลื่อนบทบาทหน้าที่ ในฐานะองค์การรักษาความปลอดภัยฝ่ายพลเรือน ได้อย่างเหมาะสม สำนักข่าวกรองแห่งชาติได้จัดทำมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน โดยกำหนดหลักเกณฑ์และแนวปฏิบัติด้านการรักษาความปลอดภัย ประกอบด้วย การรักษาความปลอดภัยเกี่ยวกับบุคคล การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ การรักษาความปลอดภัยเกี่ยวกับสถานที่ การรักษาความปลอดภัยในการประชุมลับ และการปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย ให้หน่วยงานของรัฐฝ่ายพลเรือนนำไปใช้ปฏิบัติเพื่อรองรับและป้องกันผลกระทบอันอาจเกิดจากภัยคุกคามต่าง ๆ ได้อย่างเหมาะสมและมีประสิทธิภาพ

วัตถุประสงค์

เพื่อให้หน่วยงานของรัฐฝ่ายพลเรือน ซึ่งตามมาตรฐานนี้ เรียกว่า “หน่วยงานของรัฐ” ประกอบด้วย หน่วยงานราชการส่วนกลาง หน่วยงานราชการส่วนภูมิภาค ตามกฎหมายว่าด้วยการปรับปรุงกระทรวง ทบวง กรม และกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน รัฐวิสาหกิจ หน่วยงานอื่นของรัฐ สามารถนำหลักการและแนวทางปฏิบัติด้านมาตรฐานการรักษาความปลอดภัย ไปใช้เพื่อเสริมประสิทธิภาพความปลอดภัยขององค์กร โดยมีกลไกและเครื่องมือที่ชัดเจน ครอบคลุม และปฏิบัติได้จริง สามารถตรวจสอบการปฏิบัติ และประเมินการดำเนินการ เพื่อจะได้ปรับปรุงและพัฒนาการรักษาความปลอดภัย ให้มีประสิทธิภาพอยู่เสมอ

วิธีการ

มาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน มีกลไกและเครื่องมือในการตรวจสอบและประเมินมาตรฐานการรักษาความปลอดภัย ดังนี้

1. หน่วยงานของรัฐตรวจสอบผลการปฏิบัติของหน่วยงานตนเอง ตามแบบตรวจสอบมาตรฐานการรักษาความปลอดภัย

2. สำนักข่าวกรองแห่งชาติ ประเมินผลการปฏิบัติของหน่วยงานของรัฐ เพื่อสามารถให้คำแนะนำ ชี้แนะ และช่วยเหลือด้านการรักษาความปลอดภัย ได้อย่างเหมาะสม

เพื่อให้สามารถขับเคลื่อนการดำเนินการให้เป็นไปตามมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน หัวหน้าหน่วยงานของรัฐ ต้องมีคำสั่งแต่งตั้งผู้มีหน้าที่รับผิดชอบหรือมอบหมายหน้าที่ให้กับผู้ใต้บังคับบัญชาอย่างเหมาะสม ได้แก่

1. แต่งตั้งผู้มีหน้าที่รับผิดชอบ เป็นลายลักษณ์อักษร ได้แก่

1.1 “เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ” เพื่อทำหน้าที่ดำเนินการ ควบคุมตลอดจนให้คำปรึกษาเกี่ยวกับการรักษาความปลอดภัยของหน่วยงานให้เป็นไปตามมาตรฐานการรักษาความปลอดภัย

1.2 “นายทะเบียนข้อมูลข่าวสารลับและผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ” ของหน่วยงานของรัฐและหน่วยงานย่อย เพื่อทำหน้าที่ดำเนินการทางทะเบียนข้อมูลข่าวสารลับของหน่วยงานของรัฐและหน่วยงานย่อย และดำเนินการอื่นใดที่เกี่ยวข้องตามที่กำหนดไว้ในระเบียบว่าด้วยการรักษาความลับของทางราชการพ.ศ. 2544 และที่แก้ไขเพิ่มเติม

1.3 “นายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์และผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์” ของหน่วยงานของรัฐและหน่วยงานย่อย เพื่อทำหน้าที่ดำเนินการทางทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์ของหน่วยงานของรัฐและหน่วยงานย่อย และดำเนินการอื่นใดที่เกี่ยวข้องตามที่กำหนดไว้ในระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ทั้งนี้ นายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์และผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์ อาจเป็นบุคคลเดียวกับนายทะเบียนข้อมูลข่าวสารลับและผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ ตามข้อ 1.2 ก็ได้

1.4 “คณะกรรมการตรวจสอบข้อมูลข่าวสารลับ” เพื่อทำหน้าที่ตรวจสอบการมีอยู่จริงของข้อมูลข่าวสารลับ และตรวจสอบการปฏิบัติที่ถูกต้องตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติมตามรายการข้อมูลข่าวสารลับที่แจ้งไว้ในทะเบียนข้อมูลข่าวสารลับ

1.5 “คณะกรรมการทำลายข้อมูลข่าวสารลับ” เพื่อทำหน้าที่พิจารณาข้อมูลข่าวสารลับที่ขอทำลาย และควบคุมการทำลายข้อมูลข่าวสารลับ

1.6 “เจ้าหน้าที่นำสาร” เพื่อทำหน้าที่ดูแลรักษาและจัดส่งข้อมูลข่าวสารลับ ไปยังหน่วยงานของรัฐหรือหน่วยงานอื่น อย่างปลอดภัย

2. มอบหมาย “ผู้มีอำนาจกำหนดชั้นความลับ” เป็นลายลักษณ์อักษรเพื่อทำหน้าที่กำหนดชั้นความลับ หรือปรับชั้นความลับของข้อมูลข่าวสารลับที่หน่วยงานเป็นเจ้าของเรื่อง

นิยามศัพท์

นิยามศัพท์ เป็นการอธิบายความหมายของคำที่มีการกล่าวไว้ในมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน โดยไม่รวมถึงคำศัพท์ และคำจำกัดความที่มีการกำหนดไว้แล้วตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 รวมถึงกฎหมายหรือระเบียบอื่นที่ได้มีการอ้างอิงในมาตรฐานฉบับนี้ โดยนิยามศัพท์ ประกอบด้วย

“มาตรฐานการรักษาความปลอดภัย” หมายความว่า หลักการและแนวทางปฏิบัติในการรักษาความปลอดภัยเกี่ยวกับบุคคล ข้อมูลข่าวสารลับ และสถานที่ ให้พ้นจากการรั่วไหล การจารกรรม การบ่อนทำลาย การก่อวินาศกรรม การโจรกรรม และการกระทำอื่นใดที่เป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ รวมถึงลดความเสียหายที่อาจเกิดขึ้นจากการละเมิดการรักษาความปลอดภัย

“การรักษาความปลอดภัยเกี่ยวกับบุคคล”หมายความว่า หลักการและแนวทางปฏิบัติเพื่อคัดกรองบุคคลที่เข้ามาปฏิบัติหน้าที่ในหน่วยงาน ให้มีคุณสมบัติเหมาะสมโดยเชื่อมั่นว่าไม่เป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ

“การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ” หมายความว่า หลักการและแนวทางปฏิบัติ เพื่อคุ้มครองข้อมูลข่าวสารลับไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง รั่วไหล หรือถูกเปิดเผยก่อนเวลาอันควร

“การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์” หมายความว่า หลักการและแนวทางปฏิบัติ เพื่อคุ้มครองข้อมูลข่าวสารลับที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง รั่วไหล หรือถูกเปิดเผยก่อนเวลาอันควร

“การรักษาความปลอดภัยเกี่ยวกับสถานที่”หมายความว่าหลักการและแนวทางปฏิบัติ เพื่อพิทักษ์รักษาที่สงวน อาคาร สถานที่ วัสดุอุปกรณ์ ศูนย์ข้อมูลสารสนเทศ ระบบสาธารณูปโภค ตลอดจนเจ้าหน้าที่ และข้อมูลข่าวสารที่อยู่ในความครอบครอง

ให้พ้นจากภัยอันตราย หรือเหตุอื่นใดอันอาจทำให้เสียความสามารถในการปฏิบัติภารกิจของหน่วยงานของรัฐ

“การรักษาความปลอดภัยในการประชุมลับ” หมายความว่าหลักการและแนวทางปฏิบัติ เพื่อพิทักษ์รักษาสิ่งที่เป็นความลับในการประชุม ไม่ให้รั่วไหล หรือถูกเปิดเผยก่อนเวลาอันควร รวมถึง คุ้มครองบุคคล เครื่องมืออุปกรณ์และสถานที่ ในการประชุมลับ

“หน่วยงานย่อย” หมายความว่า หน่วยงานระดับสำนัก หรือกอง หรือฝ่าย หรือเทียบเท่าที่มีชื่อเรียกอย่างอื่นของหน่วยงานของรัฐ

“บุคคลภายนอก” หมายความว่า บุคคลที่ไม่สังกัดหน่วยงานของรัฐนั้น แต่ได้รับมอบหมายหรือได้รับการทำสัญญาว่าจ้างให้ปฏิบัติงานให้กับหน่วยงานของรัฐ เป็นการชั่วคราว

“การรักษาความลับ” (Confidentiality) หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต โดยนิยามนี้ ใช้เพื่อวัตถุประสงค์ในการรักษาความลับของข้อมูลข่าวสารลับอิเล็กทรอนิกส์เป็นการเฉพาะ

“การรักษาความครบถ้วน” (Integrity) หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

“การรักษาสภาพพร้อมใช้งาน” (Availability) หมายความว่า การจัดทำ ให้ทรัพย์สินสารสนเทศ สามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“อุปกรณ์เฉพาะ” หมายความว่า คอมพิวเตอร์และอุปกรณ์ต่อพ่วงหรืออุปกรณ์อิเล็กทรอนิกส์ ที่ใช้สำหรับดำเนินการต่อข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ซึ่งหน่วยงานของรัฐได้ขึ้นทะเบียนควบคุมไว้แล้ว

“ภัยคุกคาม” หมายความว่า ภาวะหรือสถานการณ์ที่ก่อให้เกิดความไม่มั่นคง ซึ่งเป็นปัญหาที่มีความรุนแรง สลับซับซ้อน หากไม่ดำเนินการแก้ไขจะเกิดผลกระทบต่อหน่วยงานหรือความมั่นคงแห่งชาติ

“พื้นที่ควบคุม” หมายความว่า พื้นที่ที่มีมาตรการควบคุมการเข้าถึงของบุคคลและยานพาหนะ เพื่อควบคุม ดูแลรักษาสิ่งที่เป็นความลับของทางราชการ บุคคล และทรัพย์สินของทางราชการ ไม่ให้ได้รับความเสียหายหรือเกิดภัยอันตรายขึ้นได้

“พื้นที่หวงห้าม” หมายความว่า พื้นที่ที่มีมาตรการควบคุมการเข้าถึงของบุคคลและยานพาหนะ ในระดับที่สูงกว่าพื้นที่ควบคุม โดยอาจแบ่งเป็น “เขตหวงห้ามเฉพาะ” และ “เขตหวงห้ามเด็ดขาด” ตามความสำคัญของพื้นที่

“เครื่องกีดขวาง” หมายความว่า สิ่งใด ๆ ที่สามารถใช้ป้องกัน ขัดขวาง หรือหน่วงเหนี่ยวบุคคลหรือยานพาหนะที่ไม่มีสิทธิเข้าไปในพื้นที่ควบคุมของหน่วยงานของรัฐ ซึ่งแบ่งออกเป็นเครื่องกีดขวางตามธรรมชาติ เช่น แม่น้ำ คูน้ำ ลำคลอง ภูเขา และเครื่องกีดขวางที่ประดิษฐ์ขึ้น เช่น กำแพง หรือรั้ว หรือเครื่องกั้นประจำประตู หรือช่องทางเข้าออก

“แผนเผชิญเหตุ” หมายความว่า แผนซึ่งจัดทำเป็นลายลักษณ์อักษรและเผยแพร่ให้ผู้เกี่ยวข้องได้รับทราบ โดยระบุวัตถุประสงค์ที่จัดทำแผนในภาพรวมสำหรับการจัดการเหตุฉุกเฉิน อาจรวมถึงการกำหนดทรัพยากรที่จะใช้ในการปฏิบัติงาน ภารกิจที่มอบหมาย และข้อมูลข่าวสารสำหรับจัดการเหตุฉุกเฉินระหว่างช่วงระยะเวลาการปฏิบัติการช่วงหนึ่งหรือหลายช่วง

“ผู้กระทำการละเมิด” หมายความว่า บุคคลที่กระทำการละเมิดการรักษาความปลอดภัย โดยจงใจหรือประมาทเลินเล่อ อันเป็นเหตุให้สิ่งที่เป็นความลับของทางราชการรั่วไหล หรือเป็นเหตุให้เจ้าหน้าที่ของรัฐ หรือวัสดุอุปกรณ์ หรือทรัพย์สินของรัฐได้รับความเสียหาย

“ผู้จะกระทำการละเมิด” หมายความว่า บุคคลที่พยายามกระทำการละเมิดการรักษาความปลอดภัย อันอาจเป็นเหตุให้สิ่งที่เป็นความลับของทางราชการรั่วไหล หรือเป็นเหตุให้เจ้าหน้าที่ของรัฐ หรือวัสดุอุปกรณ์ หรือทรัพย์สินของรัฐได้รับ ความเสียหาย

“ผู้รับผิดชอบต่อการละเมิด” หมายความว่า ผู้มีหน้าที่รับผิดชอบในการปฏิบัติ กำกับดูแลด้านการรักษาความปลอดภัยของหน่วยงานของรัฐ ตลอดจนผู้บังคับบัญชาของผู้กระทำการละเมิด อันพิสูจน์ทราบได้ว่าละเลยหรือย่อหย่อนในการปฏิบัติหน้าที่หรือการกำกับดูแล จนเป็นเหตุให้เกิดการกระทำละเมิด

บทที่ 2
มาตรฐานการรักษาความปลอดภัย

มาตรฐานการรักษาความปลอดภัย เป็นการดำเนินการด้านการรักษาความปลอดภัยเกี่ยวกับบุคคล ข้อมูลข่าวสารลับ ข้อมูลข่าวสารลับอิเล็กทรอนิกส์ สถานที่ การประชุมลับ และการละเมิดการรักษาความปลอดภัย โดยมีแนวทางปฏิบัติ ดังนี้

1. **การรักษาความปลอดภัยเกี่ยวกับบุคคล**

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล เป็นการดำเนินการ เพื่อคัดกรองบุคคลที่เข้ามาปฏิบัติหน้าที่ในหน่วยงาน โดยการตรวจสอบประวัติและพฤติการณ์บุคคล ให้ได้ผู้ที่มีคุณสมบัติเหมาะสม การรับรองความไว้วางใจบุคคลให้เข้าถึงสิ่งที่เป็นความลับของทางราชการ การอบรมให้ความรู้บุคลากรของหน่วยงาน เพื่อเสริมสร้างและกระตุ้นจิตสำนึกด้านการรักษาความปลอดภัย โดยดำเนินการ ดังนี้

เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ต้องจัดให้มีการดำเนินการ ได้แก่

1.1 ตรวจสอบประวัติและพฤติการณ์บุคคล

1.1.1 บุคคลที่ต้องตรวจสอบประวัติและพฤติการณ์

(1) ผู้ที่อยู่ระหว่างรอว่าจ้าง บรรจุ หรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ ลูกจ้างทดลองงาน หรือฝึกงานก่อนบรรจุเข้าปฏิบัติงาน หรือผู้ที่ขอกลับเข้ารับราชการใหม่

(2) ผู้ที่ได้รับมอบหมายให้ปฏิบัติงานในหน้าที่ หรือตำแหน่งที่สำคัญของทางราชการ หรือที่เกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการ หรือทรัพย์สิน มีค่าของแผ่นดิน

(3) ผู้ได้รับทุนการศึกษาของหน่วยงานของรัฐ หรือทุนอื่นใด เพื่อศึกษาในประเทศหรือต่างประเทศ และมีข้อผูกพันให้เข้าปฏิบัติงานให้แก่หน่วยงานของรัฐ เมื่อสำเร็จการศึกษาแล้ว

(4) เจ้าหน้าที่ของรัฐที่ยังมิได้รับการตรวจสอบประวัติและพฤติการณ์ หรือผู้ที่ขอโอนมารับราชการยังหน่วยงาน แม้ได้รับการตรวจสอบประวัติและพฤติการณ์จากหน่วยงานเดิมแล้วก็ตาม

สำหรับบุคคลภายนอก หน่วยงานของรัฐต้องจัดให้มีการรักษาความปลอดภัยเกี่ยวกับบุคคล ตามความเหมาะสม

1.1.2 บุคคลที่ต้องตรวจสอบประวัติและพฤติการณ์โดยละเอียด

(1) บุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการ ชั้นลับที่สุด ลับมาก หรือการรหัส

(2) บุคคลที่มีพฤติการณ์ หรือปรากฏข่าวสารหรือติดต่อกับบุคคล หรือองค์การทั้งภายในและภายนอกประเทศที่จะเป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ

(3) บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ในภารกิจหรือตำแหน่งหน้าที่สำคัญ หรือแต่งตั้งให้ดำรงตำแหน่งที่สำคัญในหน่วยงานของรัฐ รวมถึงบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวข้องกับทรัพย์สินมีค่าของแผ่นดิน

1.2 รับรองความไว้วางใจบุคคล กรณีมีการมอบหมายให้บุคคลเข้าถึงสิ่งที่เป็นความลับของทางราชการ หรือปฏิบัติในภารกิจหรือตำแหน่งหน้าที่สำคัญ

1.3 ทบทวน แก้ไข เพิ่มเติมข้อมูลประวัติบุคคลของเจ้าหน้าที่ เมื่อมีการเปลี่ยนแปลง หรือจัดให้มีการติดตาม ทบทวน อย่างน้อยทุกสามปี

1.4 อบรมด้านการรักษาความปลอดภัยในระหว่างการปฐมนิเทศเจ้าหน้าที่ใหม่ สำหรับบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่หรือเข้าถึงสิ่งที่เป็นความลับของทางราชการ ต้องผ่านการชี้แจงก่อนปฏิบัติงาน และทบทวนเพิ่มเติมระหว่างปฏิบัติงาน

1.5 รักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม และมาตรฐานการรักษาความมั่นคงปลอดภัย ตามที่มีกำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ เป็นการดำเนินการเพื่อควบคุมและคุ้มครองข้อมูลข่าวสารลับของทางราชการ ไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง รั่วไหล หรือถูกเปิดเผยก่อนเวลาอันควร ตลอดจนให้ความสำคัญต่อการตรวจสอบข้อมูลข่าวสารลับที่อยู่ในความครอบครอง (ทั้งในรูปแบบเอกสารและอิเล็กทรอนิกส์) อย่างสม่ำเสมอ เพื่อให้สามารถบริหารจัดการข้อมูลข่าวสารลับ ได้อย่างถูกต้องและเหมาะสม และสอดคล้องกับหลักธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) โดยดำเนินการ ดังนี้

2.1 เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ต้องดำเนินการ ได้แก่

2.1.1 จัดให้มีการรับรองความไว้วางใจแก่บุคคลที่จะเข้าถึงข้อมูลข่าวสารลับ โดยให้เข้าถึงเฉพาะเรื่องที่ได้รับมอบหมายเท่านั้น

2.1.2 จัดให้มีทะเบียนข้อมูลข่าวสารลับของหน่วยงานของรัฐและหน่วยงานย่อย ประกอบด้วย ทะเบียนรับ (ทขล.1) ทะเบียนส่ง (ทขล.2) ทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3) แยกต่างหากจากทะเบียนงานสารบรรณปกติ

2.1.3 จัดให้มีการตรวจสอบการมีอยู่จริงของข้อมูลข่าวสารลับ เพื่อให้สามารถบริหารจัดการข้อมูลข่าวสารลับได้อย่างเหมาะสมและถูกต้องตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติมตามรายการข้อมูลข่าวสารลับที่แจ้งไว้ในทะเบียนข้อมูลข่าวสารลับ อย่างน้อยทุก6 เดือน (ห้วง 1 มกราคม ถึง 30 มิถุนายน)และห้วง (1 กรกฎาคม ถึง 31 ธันวาคม) โดยคณะกรรมการตรวจสอบข้อมูลข่าวสารลับ ประกอบด้วย นายทะเบียนข้อมูลข่าวสารลับเป็นประธาน และเจ้าหน้าที่ของรัฐที่ได้รับความไว้วางใจให้เข้าถึงชั้นความลับของข้อมูลข่าวสารลับ ไม่น้อยกว่าสองคนเป็นกรรมการ และให้คณะกรรมการตรวจสอบข้อมูลข่าวสารลับรายงานผลการตรวจสอบ ดังนี้

(1) รายงานผลการตรวจสอบข้อมูลข่าวสารลับ ตามแบบรายงานการตรวจสอบข้อมูลข่าวสารลับต่อหัวหน้าหน่วยงานของรัฐ อย่างน้อยทุก 6 เดือน

(2) นำเสนอรายงานผลการปฏิบัติประจำปี ตามแบบรายงานผลการปฏิบัติเกี่ยวกับข้อมูลข่าวสารลับ ประจำปี พ.ศ. .... ต่อหัวหน้าหน่วยงานของรัฐ เพื่อรายงานต่อคณะกรรมการข้อมูลข่าวสารของราชการ (กขร.) ภายในเดือนมีนาคมของปีถัดไป

2.1.4 จัดให้มีแผนการปฏิบัติในเวลาฉุกเฉินสำหรับข้อมูลข่าวสารลับและข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ได้แก่ แผนการเคลื่อนย้าย แผนการพิทักษ์รักษา และแผนการทำลาย

2.1.5 ควบคุมและกำกับดูแลการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ ได้แก่ การจัดทำ การสำเนาและการแปล การโอน การส่ง การรับ การเก็บรักษา การยืม การทำลาย การปฏิบัติในเวลาฉุกเฉิน การเปิดเผย และกรณีสูญหายให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 และที่แก้ไขเพิ่มเติม รวมถึงคำแนะนำการปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 หรือระเบียบอื่นๆที่เกี่ยวข้อง

2.2 ผู้มีอำนาจกำหนดชั้นความลับของหน่วยงานของรัฐที่เป็นผู้จัดทำข้อมูลข่าวสารลับ (เจ้าของเรื่อง) มีหน้าที่ดำเนินการ ดังนี้

2.2.1 กำหนดชั้นความลับ ให้เหตุผลประกอบการกำหนดชั้นความลับของข้อมูลข่าวสารลับนั้น และต้องแสดงชั้นความลับของข้อมูลข่าวสารลับให้ชัดเจน

2.2.2 พิจารณาปรับเพิ่ม ลด ยกเลิกชั้นความลับ

3. การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ เป็นการดำเนินการเพื่อควบคุมและคุ้มครองข้อมูลข่าวสารลับของทางราชการ ที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง ถูกเปิดเผยก่อนเวลาอันควร หรือรั่วไหล โดยดำเนินการ ดังนี้

เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ต้องจัดให้มีการดำเนินการ ได้แก่

3.1 การรักษาความปลอดภัยเกี่ยวกับบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ได้แก่ ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ซึ่งสามารถเข้าถึงข้อมูลข่าวสารลับอิเล็กทรอนิกส์ของหน่วยงาน รวมถึงผู้ทำหน้าที่ติดตั้ง ซ่อมบำรุง หรือทำการอื่นใดต่อคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ใช้ดำเนินการเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ โดยดำเนินการ ดังนี้

3.1.1 ผู้ใช้งานและผู้ดูแลระบบ

(1) ผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล

(2) ได้รับการรับรองความไว้วางใจบุคคล

(3) ได้รับอนุญาตจากผู้บังคับบัญชาในการเข้าถึงและการใช้งานคอมพิวเตอร์และระบบคอมพิวเตอร์

(4) ผ่านการชี้แจงหรืออบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การใช้งานระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบเครือข่าย และอินเทอร์เน็ต โดยคำนึงถึงการรักษาความลับ (Confidentiality) การรักษา ความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ตามที่มีกฎหมายกำหนดไว้

(5) ได้รับใบรับรองการใช้หรือดูแลระบบในระดับต่างๆ ตามระดับและความหลากหลายของหลักสูตร เพื่อเข้าสู่กระบวนการการปฏิบัติหน้าที่การรักษาความปลอดภัยข้อมูลข่าวสารลับอิเล็กทรอนิกส์ และสอดคล้องกับความมุ่งหมายของหน่วยงาน ครอบคลุมตามภารกิจที่ได้รับมอบหมายที่เกี่ยวข้องกับการดูแลความปลอดภัยข้อมูลข่าวสารลับอิเล็กทรอนิกส์

(6) การกำหนดกลุ่มและจัดทำบัญชีรายชื่อของผู้เข้าใช้งานระบบหน้าที่เกี่ยวข้องกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ และต้องมีการกำหนดสิทธิ์การใช้งานที่เกี่ยวข้องกับการ อ่าน เขียน ลบ ไฟล์ข้อมูลข่าวสารลับอิเล็กทรอนิกส์ รวมถึง การกำหนดสิทธิ์การเข้าถึงข้อมูลที่จำเป็นต่อการใช้งานเท่านั้น ร่วมไปกับการปรับปรุงการกำหนดกลุ่มหรือบัญชีรายชื่อให้ทันสมัยอยู่เสมอ

(7) จัดเก็บรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เป็นความลับ

(8) ผู้ปฏิบัติงานของหน่วยงานที่เกี่ยวข้องกับภารกิจข้อมูลข่าวสารลับอิเล็กทรอนิกส์ต้องติดบัตรแสดงตนหรือใบอนุญาตในพื้นที่กำหนดของแต่ละส่วนงานด้านข้อมูลข่าวสารลับอิเล็กทรอนิกส์

(9) ผู้ใช้งานและผู้ดูแลระบบต้องได้รับอนุญาตจากผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ของหน่วยงาน

(10) เมื่อผู้ปฏิบัติงานด้านข้อมูลข่าวสารลับอิเล็กทรอนิกส์ของหน่วยพ้นจากการปฏิบัติหน้าที่ ให้ตัดชื่อออกจากทะเบียนความไว้วางใจของบุคคล พร้อมทั้งจัดทำรายชื่อบุคคลดังกล่าวไว้เป็นหลักฐานเพื่อการตรวจสอบ และให้ลงชื่อในบันทึกการรับรองการรักษาความลับเมื่อพ้นจากตำแหน่ง หรือ หน้าที่

(11) ผู้ใช้งานและผู้ดูแลระบบต้องไม่เปิดประตูเข้าพื้นที่ทิ้งไว้ หรือยินยอมให้บุคคลอื่นที่ไม่ได้รับอนุญาตติดตามเข้ามาในพื้นที่เกี่ยวข้องกับภารกิจข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ที่เป็นพื้นที่ควบคุม “เขตหวงห้ามเด็ดขาด” และ หรือ “เขตหวงห้ามเฉพาะ”

3.1.2 บุคคลภายนอก

(1) ผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล ก่อนการปฏิบัติงาน

(2) ได้รับการรับรองความไว้วางใจบุคคล

(3) ได้รับอนุญาตในการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์จากหัวหน้าหน่วยงานของรัฐ

(4) ผ่านการชี้แจงให้ทราบเกี่ยวกับระเบียบและข้อปฏิบัติเกี่ยวกับการรักษาความลับและการรักษาความปลอดภัย และกฎหมายที่เกี่ยวข้อง

(5) ได้รับการกำกับดูแลระหว่างดำเนินการ ภายใต้การบริหารจัดการของหน่วยงาน

(6) บุคคลภายนอกผู้มาตรวจสอบข้อมูลหรือเข้าสืบค้นข้อมูล ต้องได้รับการตรวจสอบเหตุผลและความจำเป็นที่จะอนุญาตให้บุคคลภายนอกเข้าพื้นที่ใช้งานระบบข้อมูล

ข่าวสารลับอิเล็กทรอนิกส์ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกข้อมูลของบุคคล และการเข้าออกไว้เป็นหลักฐาน พร้อมจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี

3.2 การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยดำเนินการ ดังนี้

3.2.1 กำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(2) ระบบสารสนเทศและระบบสำรองของสารสนเทศ ต้องอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติ อย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

3.2.2 กำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

(1) จัดทำแนวปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(2) ประกาศนโยบายและแนวปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถปฏิบัติตามนโยบายและแนวปฏิบัติได้

(3) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(4) ทบทวน ปรับปรุงนโยบายและแนวปฏิบัติ ให้เป็นปัจจุบันอยู่เสมอ

(5) กำหนดให้ อาคาร สถานที่ซึ่งเป็นที่ตั้งของระบบสารสนเทศ และพื้นที่ใช้งานระบบสารสนเทศที่ใช้สำหรับจัดเก็บและประมวลผลข้อมูลสารสนเทศ เป็นพื้นที่หวงห้าม

(6) การพิจารณาใช้วิธีการกำหนดชั้นความลับให้กับข้อมูลสารสนเทศที่ต้องจัดเก็บ

(7) การจำกัดการเข้าถึงข้อมูลและระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น การกำหนดสิทธิ์การใช้งานให้เหมาะสมกับหน้าที่ความรับผิดชอบ และมีการตรวจสอบและบันทึกการเข้าใช้งาน

(8) การจัดทำเอกสารนโยบายและขั้นตอนการปฏิบัติงานที่ชัดเจนและเป็นปัจจุบัน รวมถึงการกำหนดบทลงโทษสำหรับผู้ที่ไม่ปฏิบัติตาม

3.3 การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์

3.3.1 กำหนดอุปกรณ์เฉพาะที่ใช้ในการจัดทำข้อมูลข่าวสารลับอิเล็กทรอนิกส์และจัดทำทะเบียนควบคุมอุปกรณ์ดังกล่าว

3.3.2 จัดเก็บข้อมูลข่าวสารลับอิเล็กทรอนิกส์ โดยดำเนินการ ดังนี้

(1) เข้ารหัสข้อมูลข่าวสารลับอิเล็กทรอนิกส์ที่ต้องการบันทึกหรือจัดเก็บก่อนการดำเนินการจัดเก็บ

(2) การจัดทำระเบียนการจัดเก็บในสื่ออิเล็กทรอนิกส์ หรืออุปกรณ์ ที่มีทะเบียนควบคุมหรือในระบบซึ่งกำหนดไว้เป็นการเฉพาะให้เป็นหมวดหมู่และง่ายต่อการค้นหา

(3) การดำเนินการให้สื่ออิเล็กทรอนิกส์ หรืออุปกรณ์ หรือระบบที่จัดเก็บต้องตั้งอยู่ในพื้นที่ที่มีการรักษาความปลอดภัย

(4) การจัดเก็บอุปกรณ์ที่เกี่ยวข้องจัดเก็บข้อมูล ได้แก่ (Personal Computer) คอมพิวเตอร์แม่ข่าย (Servers) เครื่องคอมพิวเตอร์ลูกข่าย (Clients) รวมถึงอุปกรณ์ที่ใช้ร่วมกับระบบเครือข่าย ซอฟต์แวร์และแอปพลิเคชั่น ให้อยู่ในระดับที่เหมาะสมในทุกระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (Defense in depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (Multiple layers of security controls) เพื่อลดความเสี่ยงในกรณีที่มาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

3.3.3 การส่งและรับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ โดยดำเนินการ ดังนี้

(1) การเข้ารหัสข้อมูลข่าวสารลับ หรือข้อมูลที่ถูกบันทึกในรูปแบบต่างๆก่อนดำเนินการจัดส่ง

(2) การจัดทำใช้ช่องทางสื่อสารที่มั่นคงปลอดภัย หรือช่องทางของหน่วยงานของรัฐ เช่น ระบบจดหมายอิเล็กทรอนิกส์กลางเพื่อการสื่อสารของหน่วยงานภาครัฐ

(3) การใช้ซอฟต์แวร์ที่หน่วยงานกำหนดและสอดคล้องกับระบบพื้นฐานทางอิเล็กทรอนิกส์ของหน่วยโดยภาพรวม

(4) การใช้ซอฟต์แวร์และแอพพลิเคชั่นที่จัดทำ หรือพัฒนาโดยหน่วยงานภาครัฐ

(5) การจัดทำแพลตฟอร์มการทำงานออนไลน์ผ่านระบบ Mail Chat Meeting Share File หรือ Document และบริการอื่นๆในอนาคต ให้สามารถทำงานร่วมกันได้บนแพลตฟอร์มเดียวกัน

(6) การจัดทำระบบพิสูจน์ยืนยันตัวตนผ่าน Digital ID หรือ Single Sign-On ให้พร้อมการยืนยันตัวตน เพื่อรองรับการส่งและการรับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ร่วมไปกับการใช้งานผ่านการพิสูจน์ตัวตันด้วยปัจจัยหลายอย่าง (Muti-Factor Authentication) กับอุปกรณ์ชนิดต่างๆที่มีความหลากหลาย

(7) ห้ามมิให้ผู้ใช้งาน ใช้อุปกรณ์การส่งและการรับข้อมูลข่าวสารลับอิเล็กทรอนิกส์อิเล็กทรอนิกส์ของหน่วยโดยปราศจากการตรวจสอบหรืออนุญาตของผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายให้กำกับดูแล

ทั้งนี้ ข้อมูลข่าวสารลับ ชั้น “ลับที่สุด” ห้ามดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

3.3.4 การทำลาย ให้ดำเนินการตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม รวมถึงกฎหมายอื่นที่เกี่ยวข้องด้วยวิธีการลบถาวร หรือแนวทางการทำลายตามมาตรฐานสากล (International Standards) หรือจนไม่สามารถนำมาใช้ประโยชน์ได้

(1) การดำเนินการตามข้อกำหนดการทำลายข้อมูลข่าวสารลับ

(2) การทำลายด้วยวิธีการลบถาวร

(3) กระบวนการทำลายข้อมูลควรสามารถทำให้ข้อมูลไม่สามารถกู้คืนได้และไม่สามารถนำกลับมาใช้ หรือ ค้นหาข้อมูลได้อีกจากระบบที่เก็บข้อมูล

(4) การใช้เครื่องมือและกระบวนการทำลายที่เหมาะสมและมุ่งเน้นการทำลายข้อมูลดิจิทัลโดยใช้เครื่องมือที่มีความปลอดภัย

(5) การจัดทำบันทึกข้อมูลเกี่ยวกับการทำลายข้อมูลเป็นสิ่งสำคัญ เพื่อเป็นหลักฐานในการแสดงว่าข้อมูลถูกทำลายอย่างถูกต้องและปลอดภัย

(6) การทำลายต้องระบุข้อมูลที่ต้องการทำลายอย่างชัดเจน เพื่อป้องกันไม่ให้ข้อมูลที่สำคัญถูกลบออกไป

(7) การใช้โปรแกรมในการลบที่ผ่านการรับรองตามมาตรฐานสากล (Data Wiping หรือ Data Sanitization) หลังจากการทำลายข้อมูลแล้วหน่วยความจำสามารถนำกลับมาใช้งานได้อย่างปลอดภัย

(8) การลบโดยการทำลายสนามแม่เหล็ก (Degaussing)โดยใช้เครื่องที่ผ่านการรับรองตามมาตรฐานสากล หลังจากการทำลายด้วยวิธีนี้จะทำให้หน่วยความจำไม่สามารถนำกลับมาใช้งานได้อีก

(9) การทำลายหน่วยความจำทางกายภาพ (Physical Destruction) โดยการบด (Shredding) การเจาะ (Drilling) วิธีการนี้จะทำให้หน่วยความจำไม่สามารถนำกลับมาใช้งานได้อีก

3.3.5 การปฏิบัติในเวลาฉุกเฉิน ให้จัดทำแผนปฏิบัติสำหรับข้อมูลข่าวสารลับและข้อมูลข่าวสารลับอิเล็กทรอนิกส์ กรณีเกิดเหตุฉุกเฉิน

(1) การสำรองข้อมูลทั้งหมดก่อนย้ายข้อมูลเพื่อความปลอดภัย ร่วมไปกับการใช้อุปกรณ์บันทึกข้อมูลแบบที่ถอดย้ายได้ (Removable Storage Device)

(2) การทดสอบการขนถ่ายข้อมูลในขั้นตอนขององค์กร

(3) การจัดทำแผนการเคลื่อนย้ายข้อมูลข่าวสารลับอิเล็กทรอนิกส์ และจัดทำทะเบียนควบคุมอุปกรณ์ก่อนดำเนินการเคลื่อนย้ายออกจากที่ตั้ง

(4) การจัดทำแผนการพิทักษ์รักษาข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ขณะเคลื่อนย้ายออกจากที่ตั้งเก่าไปยังที่ตั้งแห่งใหม่ เพื่อปกป้องข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต รวมถึงการป้องกันการสูญหายของข้อมูลภายใต้สถานการณ์ที่ไม่ปลอดภัยขณะอยู่ระหว่างการเคลื่อนย้าย

(5) การจัดทำแผนการทำลายข้อมูลข่าวสารลับอิเล็กทรอนิกส์ในสถานการณ์ฉุกเฉินที่มีความจำเป็นอย่างเร่งด่วนในการป้องกันไม่ให้ข้อมูลข่าวสารลับอิเล็กทรอนิกส์ถูกนำไปโดยผู้ที่ไม่ได้รับอนุญาต

4. การรักษาความปลอดภัยเกี่ยวกับสถานที่

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ เป็นการดำเนินการ เพื่อพิทักษ์รักษาที่สงวน อาคาร สถานที่ วัสดุอุปกรณ์ ศูนย์ข้อมูลสารสนเทศ ระบบสาธารณูปโภค ตลอดจนเจ้าหน้าที่ และข้อมูลข่าวสาร ให้พ้นจากภัยอันตราย หรือเหตุอื่นใดอันอาจทำให้เสียความสามารถในการปฏิบัติภารกิจของหน่วยงานของรัฐ โดยหน่วยงานต้องจัดทำแผนการรักษาความปลอดภัยทั้งในสถานการณ์ปกติ สถานการณ์ไม่ปกติ และสถานการณ์ฉุกเฉิน ตลอดจนให้ความสำคัญต่อการทบทวนและซักซ้อมแผน อย่างน้อยปีละ 1 ครั้ง โดยดำเนินการ ดังนี้

เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ต้องจัดให้มีการดำเนินการ ได้แก่

4.1 ประเมินภัยคุกคาม ประเมินระดับความเสี่ยง และจัดระดับความเสี่ยงของหน่วยงาน

4.1.1 หากผลการประเมินความเสี่ยงพบว่า ไม่มีภัยคุกคามหรือความเสี่ยงในระดับที่ต้องมีการปรับมาตรการการรักษาความปลอดภัย ให้จัดทำแผนการรักษาความปลอดภัยในสถานการณ์ปกติ

4.1.2 หากผลการประเมินความเสี่ยงพบว่า อาจมีภัยคุกคามหรือความเสี่ยงในระดับที่ต้องมีการปรับมาตรการการรักษาความปลอดภัย แต่อยู่ในวิสัยที่หน่วยงานสามารถเผชิญและควบคุมสถานการณ์ได้ ให้จัดทำแผนการรักษาความปลอดภัยในสถานการณ์ไม่ปกติ

4.1.3 หากผลการประเมินความเสี่ยงพบว่า มีภัยคุกคามหรือเกิดเหตุละเมิดขึ้น และจำเป็นต้องเข้าระงับเหตุให้ทันท่วงที ต้องขอความช่วยเหลือ จากหน่วยงานข้างเคียง หรือหน่วยงานเฉพาะที่มีทักษะและความชำนาญในการบริหารจัดการสถานการณ์ ในกรณีนี้ ให้จัดทำแผนการรักษาความปลอดภัยในสถานการณ์ฉุกเฉิน (แผนเผชิญเหตุ)

4.2 จัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ ให้สอดคล้องกับผลการประเมินภัยคุกคามและความเสี่ยง รวมทั้ง ระดับผลกระทบที่อาจก่อให้เกิดความเสียหาย โดยการจัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ ควรมีการทบทวนและซักซ้อมแผนให้รองรับภัยคุกคามอยู่เสมอ

4.3 กำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ ให้สอดคล้องตามแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ ในสถานการณ์ต่าง ๆ

4.4 สำรวจและตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่

การสำรวจการรักษาความปลอดภัยเกี่ยวกับสถานที่ เป็นการดำเนินการสำหรับหน่วยงานของรัฐที่ยังไม่มีการกำหนดมาตรการการรักษาความปลอดภัยมาก่อน ส่วนการตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่ เป็นการดำเนินการกรณีต้องการทบทวนหรือปรับปรุงมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ของหน่วยงานของรัฐ

4.5 จัดให้มีการซักซ้อมแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีสถานการณ์ที่กระทบต่อการรักษาความปลอดภัย

4.6 ทบทวนและปรับปรุงแผนให้มีความเหมาะสมกับสถานการณ์ปัจจุบันหรือเมื่อเกิดเหตุละเมิดการรักษาความปลอดภัย หรืออย่างน้อยทุกห้าปี

5. การรักษาความปลอดภัยในการประชุมลับ

มาตรฐานการรักษาความปลอดภัยในการประชุมลับ เป็นการดำเนินการ เพื่อคุ้มครองและพิทักษ์รักษาบุคคล สถานที่ และข้อมูลข่าวสารลับ ที่เกี่ยวข้องในการประชุมลับนั้น ไม่ให้รั่วไหล ถูกรบกวนหรือขัดขวางการประชุม หรือถูกจารกรรม หรือวินาศกรรม โดยต้องแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ และนายทะเบียนข้อมูลข่าวสารลับในการประชุมลับ เพื่อทำหน้าที่กำกับดูแลการประชุมลับนั้น โดยดำเนินการ ดังนี้

5.1 หัวหน้าหน่วยงานของรัฐเจ้าของเรื่อง ที่จะจัดการประชุมลับเป็นผู้รับผิดชอบภาพรวมในการจัดประชุม และมาตรการรักษาความปลอดภัยเกี่ยวกับการประชุมลับนั้น โดยหัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมาย แต่งตั้งบุคคล เพื่อทำหน้าที่ “เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ” และ “นายทะเบียนข้อมูลข่าวสารลับในการประชุมลับ” เป็นลายลักษณ์อักษร หรืออย่างน้อยอาจมอบให้บุคคลที่เหมาะสมเป็นผู้ดำเนินการแทนได้ รวมทั้งแจ้งให้ผู้เข้าร่วมประชุม และผู้มีหน้าที่เกี่ยวข้องทุกฝ่ายทราบ ทั้งนี้ การแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ และนายทะเบียนข้อมูลข่าวสารลับในการประชุมลับ หากหน่วยงานได้มีการแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย และนายทะเบียนข้อมูลข่าวสารลับของหน่วยงานเพื่อปฏิบัติงานไว้แล้ว หน่วยงานสามารถมอบหมายให้ทำหน้าที่ในการประชุมลับได้ตามความเหมาะสม

5.2 หัวหน้าหน่วยงานของรัฐเจ้าของเรื่อง ต้องกำหนดมาตรการเพื่อพิทักษ์รักษาสิ่งที่เป็นความลับของทางราชการที่ปรากฏในการประชุมลับ ไม่ให้มีการรั่วไหล หรือถูกจารกรรม หรือถูกเปิดเผยไปถึงผู้ไม่มีส่วนเกี่ยวข้อง รวมทั้ง ป้องกันการถูกรบกวน หรือขัดขวางการประชุมลับจากการก่อวินาศกรรม รวมทั้งการคุ้มครองบุคคลและสถานที่ที่เกี่ยวข้องกับการประชุมลับนั้น

5.3 เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ ต้องจัดให้มีการดำเนินการ ดังนี้

5.3.1 กำกับดูแล ตรวจสอบผู้เกี่ยวข้องในการประชุมลับว่า ผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล พร้อมทั้งรับรองความไว้วางใจจากหน่วยงานต้นสังกัด ให้เข้าถึงชั้นความลับในไม่ต่ำกว่าชั้นความลับของการประชุมลับนั้น

5.3.2 กำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ รวมถึงตรวจตราและตรวจสอบทางเทคนิคในพื้นที่ที่กำหนด ทั้งก่อน ระหว่าง และหลังการประชุมลับ

5.3.3 กำหนดข้อห้ามในการนำเครื่องมือ วัสดุอุปกรณ์ อุปกรณ์ อิเล็กทรอนิกส์ที่สามารถสื่อสารหรือบันทึกข้อมูลข่าวสารของการประชุม เข้าไปในสถานที่ที่มีการประชุมลับ และต้องไม่นำเครื่องมือ วัสดุอุปกรณ์หรือข้อมูลข่าวสารใดๆ ออกนอกสถานที่ประชุมนั้น

5.3.4 กำกับดูแลการปฏิบัติต่อสิ่งที่เป็นความลับของทางราชการในการประชุมลับให้เป็นไปตามมาตรฐานการรักษาความปลอดภัย

5.2.5 กรณีมีการแถลงข่าวหรือการบรรยายสรุป ผู้แถลงข่าวหรือผู้บรรยายสรุป เรื่องที่แถลงหรือบรรยายสรุป ต้องได้รับอนุมัติจากที่ประชุมลับก่อน และจัดสถานที่ขึ้นเป็นการเฉพาะบริเวณนอกพื้นที่ที่ไม่เกี่ยวข้องกับการรักษาความปลอดภัยในการประชุมลับ

5.2.6 การบรรยายสรุปผลการประชุมเรื่องที่เป็นความลับต้องปฏิบัติเช่นเดียวกับการรักษาความปลอดภัยในการประชุมลับ ประกอบด้วย

1) การกำหนดให้ผู้เข้ารับฟังต้องได้รับความไว้วางใจให้เข้าถึงชั้นความลับไม่ต่ำกว่าชั้นความลับของข้อมูลในการบรรยายสรุป

2) การกำหนดชั้นความลับของการบรรยายสรุป

3) ผู้บรรยายต้องแจ้งระดับชั้นความลับของการบรรยายสรุปให้ผู้เข้ารับฟังทราบ

5.2.7 กรณีผู้เข้าประชุมแต่ละฝ่ายจำเป็นต้องวางมาตรการการรักษาความปลอดภัยเฉพาะในฝ่ายตน ต้องประสานแนวทางปฏิบัติการรักษาความปลอดภัยในการประชุมลับ ให้เป็นไปตามที่กำหนด

5.2.8 กรณีจัดการประชุมลับในพื้นที่ภายนอก หรือในพื้นที่ของหน่วยงานของรัฐอื่น ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ ประสานความร่วมมือกับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือเจ้าหน้าที่ผู้รับผิดชอบของหน่วยงานหรือของพื้นที่นั้น

5.2.9 การจัดแถลงข่าวและข้อมูลรายละเอียดของการประชุมลับ ต้องได้รับการอนุมัติจากที่ประชุมลับก่อนนำไปเผยแพร่ โดยผู้ปฏิบัติหน้าที่แถลงข่าวต้องเป็นผู้ได้รับมอบหมายให้ดำเนินการแถลงข่าวเป็นการเฉพาะเรื่องตามที่รับมอบหมาย/อนุมัติจากที่ประชุมลับเท่านั้น

5.2.10 การจัดเตรียมพื้นที่แถลงข่าวจากการประชุมลับให้เป็นไปด้วยความเหมาะสมและสอดคล้องกับผู้เข้ารับทราบข้อมูล

5.3 นายทะเบียนข้อมูลข่าวสารลับในการประชุมลับ ต้องดำเนินการต่อข้อมูลข่าวสารลับในการประชุมลับ ให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

5.4 กรณีจัดการประชุมลับทางระบบสารสนเทศหรือออนไลน์ ต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานของรัฐ และปฏิบัติตามพระราชกำหนดว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ ที่ต้องกำหนดมาตรการให้ครอบคลุมเป็นไปตามหลักการสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย

1) การรักษาความลับ (Confidentiality) เพื่อป้องกันการเข้าถึง ใช้ หรือเปิดเผยข้อมูลโดยผู้ไม่มีสิทธิ

2) การรักษาความถูกต้องครบถ้วน (Integrity) เพื่อป้องกันข้อมูลไม่ให้ถูกแก้ไข สูญหาย เสียหาย หรือถูกทำลายโดยไม่ได้รับอนุญาต

3) การรักษาสภาพพร้อมใช้งาน (Availability) เพื่อให้ข้อมูลอิเล็กทรอนิกส์สามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

4) การคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล โดยหน่วยงานผู้จัดประชุมลับต้องดำเนินการตามข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการประชุมผ่านสื่ออิเล็กทรอนิกส์

5.5 บุคคลผู้เข้าประชุมลับ ต้องผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล พร้อมทั้งได้รับความไว้วางใจให้เข้าถึงความลับในการประชุมนั้น และการปฏิบัติให้อยู่ในความควบคุมของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับนั้น สำหรับผู้ที่ไม่มีอำนาจหน้าที่ต้องไม่ได้รับทราบ หรือครอบครองสิ่งที่เป็นความรับของราชการในที่ประชุม

5.6 การกำหนดพื้นที่ที่ใช้ในการประชุมลับ ที่ทำการของผู้เข้าประชุมลับ สถานที่ใช้เก็บรักษาสิ่งที่เป็นความลับของทางราชการ และจัดให้มีมาตรการรักษาความปลอดภัยตามความจำเป็นและเหมาะสมไว้ล่วงหน้าก่อนเปิดการประชุมลับ

5.7 เจ้าหน้าที่ผู้มีภารกิจควบคุมการรักษาความปลอดภัยการประชุมลับต้องดำเนินการดังนี้

5.7.1 การตรวจสอบและตรวจตราทางเทคนิคครอบคลุมบริเวณโดยรอบพื้นที่ที่ถูกกำหนดให้มีการรักษาความปลอดภัยอย่างละเอียด ก่อนวันเปิดประชุมลับและระหว่างการประชุมลับ

5.7.2 กรณีที่การประชุมลับนั้นมีความสำคัญ หน่วยงานของรัฐเจ้าของเรื่องอาจประสานงานขอให้องค์การรักษาความปลอดภัย (สำนักข่าวกรองแห่งชาติ) ดำเนินการให้ได้ โดยหลังจากที่องค์การรักษาความปลอดภัยตรวจสอบแล้ว ให้ส่งมอบความรับผิดชอบในพื้นที่นั้นเป็นลายลักษณ์แก่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ หรือผู้แทนหน่วยงานนั้น การปฏิบัติต่อสิ่งที่เป็นความลับของทางราชการ การควบคุมดูแลการประชุมลับ การทำลายข้อมูลข่าวสารลับ ที่ไม่ใช้แล้ว ให้อยู่ในความดูแลของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ และนายทะเบียนข้อมูลข่าวสารลับ

สำหรับหน่วยงานที่มีความพร้อมในการดำเนินการตรวจสอบและตรวจตราทางเทคนิค หรือมีความประสงค์ที่จะดำเนินการเอง สามารถขอคำแนะนำหรือแนวทางปฏิบัติจากสำนักข่าวกรองแห่งชาติได้

ทั้งนี้ ในการขอรับการสนับสนุนให้สำนักข่าวกรองแห่งชาติ ดำเนินการทั้งการตรวจสอบ ตรวจตราทางเทคนิค หรือการให้คำแนะนำหรือถ่ายทอดแนวทางปฏิบัติ ให้หน่วยงานจัดทำหนังสือขอรับการสนับสนุนเป็นลายลักษณ์อักษร ถึงผู้อำนวยการสำนักข่าวกรองแห่งชาติ

5.8 หากพบว่ามีผู้มาติดต่อกับผู้เข้าร่วมประชุมลับ เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ ต้องดำเนินการตรวจสอบว่าผู้มาติดต่อกับผู้เข้าร่วมประชุมลับเป็นบุคคลที่ได้รับอนุญาตให้ผ่านเข้ามาในพื้นที่ที่ใช้ในการประชุมลับ ที่ทำการของผู้เข้าประชุมลับ สถานที่ใช้เก็บรักษาสิ่งที่เป็นความลับของทางราชการหรือไม่

6. การละเมิดการรักษาความปลอดภัย

การละเมิดการรักษาความปลอดภัย อาจเกิดจากการขาดจิตสำนึก และขาดวินัยในการรักษาความปลอดภัยของบุคคลที่เกี่ยวข้อง ทั้งโดยเจตนาหรือไม่เจตนา ได้แก่ ความประมาทเลินเล่อ ความไม่รอบคอบ ความเกียจคร้านและย่อหย่อนต่อหน้าที่ ความรู้เท่าไม่ถึงการณ์ ความเห็นแก่ประโยชน์ส่วนตัว เป็นต้น รวมถึงการกระทำของฝ่ายตรงข้าม โดยการจารกรรมหรือการก่อวินาศกรรม

มาตรฐานการปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย เป็นการกำหนดหลักการและแนวทางให้มีการป้องกัน ลดความเสียหาย สำรวจและตรวจสอบ ความเสียหาย ค้นหาสาเหตุของการละเมิด จุดอ่อนและข้อบกพร่องต่าง ๆ โดยมีขั้นตอนดำเนินการ ดังนี้

6.1 เจ้าหน้าที่ของรัฐผู้พบเห็น หรือทราบ หรือสงสัยว่าจะมี หรือมีการละเมิดการรักษาความปลอดภัย ต้องดำเนินการตามขั้นตอน ดังนี้

6.1.1 ดำเนินการเบื้องต้นเพื่อลดความเสียหาย

6.1.2 รายงานผู้บังคับบัญชา หรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือผู้รับผิดชอบ หรือแจ้งเจ้าของเรื่องเดิมทราบโดยเร็ว

6.2 เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือผู้รับผิดชอบ ต้องดำเนินการ ดังนี้

6.2.1 สำรวจและตรวจสอบความเสียหาย

6.2.2 ดำเนินการเพื่อป้องกันหรือลดความเสียหาย

6.2.3 ค้นหาสาเหตุแห่งการละเมิดการรักษาความปลอดภัย หากปรากฏหลักฐานหรือข้อสงสัยว่าเกิดการจารกรรมหรือการก่อวินาศกรรม ต้องประสานเจ้าหน้าที่หรือหน่วยงานที่เกี่ยวข้องด้านการสืบสวน ดำเนินการต่อไป

6.2.4 ปรับปรุงแก้ไขมาตรการการรักษาความปลอดภัยให้มีประสิทธิภาพยิ่งขึ้น

6.2.5 รายงานผลการดำเนินการข้างต้นต่อผู้บังคับบัญชา

6.3 หัวหน้าหน่วยงานของรัฐ ต้องดำเนินการ ดังนี้

6.3.1 แจ้งหน่วยงานของรัฐซึ่งเป็นเจ้าของเรื่องเดิมทราบ (กรณีเกี่ยวข้องกับข้อมูลข่าวสารลับที่หน่วยงานของรัฐอื่นเป็นเจ้าของเรื่อง)

6.3.2 แต่งตั้งคณะกรรมการสอบสวนข้อเท็จจริง

6.3.3 พิจารณาดำเนินการตามกฎหมายต่อผู้กระทำการละเมิด หรือผู้จะกระทำการละเมิด หรือผู้รับผิดชอบต่อการละเมิดนั้น ไม่ว่าโดยเจตนาหรือไม่ก็ตาม

6.4 หัวหน้าหน่วยงานของรัฐ ซึ่งเป็นเจ้าของเรื่องเดิมหรือผู้ที่เกี่ยวข้อง ต้องดำเนินการดังนี้

6.4.1 พิจารณาว่าสมควรลดหรือยกเลิกชั้นความลับของสิ่งที่เป็นความลับของทางราชการนั้นหรือไม่

6.4.2 ขจัดความเสียหายอันเกิดจากการละเมิดการรักษาความปลอดภัย และปรับปรุงแก้ไขมาตรการการรักษาความปลอดภัย เพื่อป้องกันไม่ให้เกิดเหตุละเมิดซ้ำ

ทั้งนี้ เมื่อเกิดเหตุละเมิดการรักษาความปลอดภัย ให้พิจารณาแนวทางการดำเนินการให้เป็นไปตามกฎหมายที่เกี่ยวข้อง ประกอบด้วย อาทิ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

บทที่ 3
แนวปฏิบัติด้านมาตรฐานการรักษาความปลอดภัย

แนวปฏิบัติด้านมาตรฐานการรักษาความปลอดภัย เป็นการกำหนดรายละเอียดการปฏิบัติเพื่อให้สามารถดำเนินการด้านการรักษาความปลอดภัยให้เป็นไปตามมาตรฐานการรักษาความปลอดภัย ประกอบด้วย แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับบุคคล แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับสถานที่ แนวปฏิบัติการรักษาความปลอดภัยในการประชุมลับ และแนวปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย โดยหน่วยงานของรัฐสามารถปฏิบัติ ดังนี้

1. แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับบุคคล ประกอบด้วย การตรวจสอบประวัติและพฤติการณ์บุคคล การตรวจสอบประวัติและพฤติการณ์บุคคลโดยละเอียด การรับรองความไว้วางใจบุคคล การบันทึกการเปลี่ยนแปลงประวัติบุคคล โดยปฏิบัติ ดังนี้

1.1 การตรวจสอบประวัติและพฤติการณ์บุคคล

1.1.1 ให้เจ้าของประวัติกรอกรายละเอียดในแบบประวัติบุคคล (รปภ.1) ให้ครบถ้วน ภายใต้การควบคุมดูแลของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วยงานของรัฐ หรือเจ้าหน้าที่ที่ได้รับมอบหมายจากเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย

1.1.2 ให้หน่วยงานของรัฐทำหนังสือถึงกองทะเบียนประวัติอาชญากร สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ หรือหัวหน้าสถานีตำรวจนครบาล หรือหัวหน้าสถานีตำรวจภูธร ที่เจ้าของประวัติมีภูมิลำเนาอยู่ เพื่อพิมพ์ลายนิ้วมือและดำเนินการตรวจสอบลายพิมพ์นิ้วมือและประวัติอาชญากรจากฐานข้อมูลกองทะเบียนประวัติอาชญากร สำนักงานพิสูจน์หลักฐานตำรวจ สำนักงานตำรวจแห่งชาติ โดยระบุให้กองทะเบียนประวัติอาชญากร หรือสถานีตำรวจนครบาล หรือสถานีตำรวจภูธร ที่ดำเนินการตรวจสอบ แจ้งผลการตรวจสอบลายพิมพ์นิ้วมือและประวัติอาชญากร ถึงหน่วยงานของรัฐเจ้าของเรื่องโดยตรง

1.1.3 ในกรณีที่ปรากฏความผิดหรือมีผลของคดี ให้หัวหน้าหน่วยงานของรัฐพิจารณาว่าจะสั่งบรรจุ หรือว่าจ้าง หรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ หรือให้บุคคลนั้นพ้นจากการปฏิบัติหน้าที่ และให้ดำเนินการตามกฎหมายที่เกี่ยวข้องต่อไป

1.1.4 กรณีที่หัวหน้าหน่วยงานของรัฐสั่งบรรจุ หรือว่าจ้าง หรือแต่งตั้งบุคคลตามข้อ 1.1.3 ให้หน่วยงานของรัฐส่งสำเนาแบบประวัติบุคคล (รปภ.1) ที่เจ้าของประวัติได้ลงลายมือชื่อเพื่อรับรองสำเนาถูกต้องทุกหน้า และสำเนาผลการตรวจสอบลายพิมพ์นิ้วมือและประวัติอาชญากรที่เจ้าหน้าที่ที่ได้รับมอบหมาย ลงลายมือชื่อ เพื่อรับรองสำเนาถูกต้องทุกหน้า ให้สำนักข่าวกรองแห่งชาติดำเนินการตามอำนาจหน้าที่

1.2 การตรวจสอบประวัติและพฤติการณ์บุคคลโดยละเอียด

1.2.1 ให้ดำเนินการตรวจสอบประวัติและพฤติการณ์ ตามแนวทาง การตรวจสอบประวัติและพฤติการณ์บุคคล

1.2.2 ตรวจสอบและหาข้อมูล เพื่อรวบรวมข่าวสารเพิ่มเติมจากกลุ่มบุคคลใกล้ชิดหรือบุคคลอื่นที่เกี่ยวข้อง

ทั้งนี้ การดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล ต้องคำนึงถึงหลักการตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ตลอดจนการดำเนินการตรวจสอบประวัติและพฤติการณ์บุคคลโดยละเอียด สามารถขอคำแนะนำ หรือขอให้สำนักข่าวกรองแห่งชาติ ดำเนินการแทนได้

1.3 การรับรองความไว้วางใจบุคคล

1.3.1 ตรวจสอบประวัติและพฤติการณ์บุคคล ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่สำคัญหรือเข้าถึงสิ่งที่เป็นความลับของทางราชการตามชั้นความลับที่จะได้รับมอบหมาย

1.3.2 จัดทำใบรับรองความไว้วางใจ (รปภ.4) โดยหัวหน้าหน่วยงานของรัฐหรือผู้ได้รับมอบหมายเป็นผู้ลงนาม

1.3.3 จัดอบรมหรือชี้แจงเรื่องการรักษาความปลอดภัย ตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติมรวมถึงกฎหมายอื่นที่เกี่ยวข้อง

1.3.4 ให้ผู้ได้รับมอบหมายภารกิจลงนามในบันทึกรับรองการรักษาความลับเมื่อเข้ารับการปฏิบัติหน้าที่ในภารกิจหรือตำแหน่งหน้าที่ (รปภ.3)

1.3.5 จัดเก็บเอกสารหลักฐานด้านการรักษาความปลอดภัย ไว้ในแฟ้มประวัติบุคคลของผู้นั้น

1.3.6 บันทึกชื่อลงในทะเบียนความไว้วางใจ (รปภ.5) และเมื่อมีการเปลี่ยนแปลงระดับความไว้วางใจ หรือพ้นจากภารกิจหน้าที่ ต้องแก้ไขทะเบียนความไว้วางใจให้เป็นปัจจุบัน

1.3.7 กรณีบุคคลพ้นจากภารกิจหรือตำแหน่งหน้าที่ ให้ลงชื่อในบันทึกรับรองการรักษาความลับเมื่อพ้นจากการปฏิบัติหน้าที่ในภารกิจหรือตำแหน่งหน้าที่(รปภ.6) และมอบคืนข้อมูลข่าวสารของราชการให้กับหัวหน้าหน่วยงานของรัฐหรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือผู้ที่ได้รับมอบหมาย

1.4 การบันทึกการเปลี่ยนแปลงประวัติบุคคล

1.4.1 เจ้าของประวัติ

(1) บันทึกการเปลี่ยนแปลงข้อมูลส่วนบุคคล เช่น ชื่อ ชื่อสกุล สถานภาพ วุฒิการศึกษา ที่อยู่อาศัย (ที่อยู่ปัจจุบัน ที่อยู่ตามทะเบียนบ้าน) เป็นต้น ในบันทึกเปลี่ยนแปลงประวัติบุคคล (รปภ.2) หรือแบบอื่นตามความเหมาะสม

(2) ส่งบันทึกเปลี่ยนแปลงประวัติบุคคล (รปภ.2) หรือแบบอื่นตามความเหมาะสม และแนบสำเนาเอกสารที่มีการรับรองสำเนาถูกต้องโดยเจ้าของประวัติ เช่น ใบแจ้งเปลี่ยนชื่อ/ชื่อสกุล ใบสำคัญการสมรส ใบวุฒิการศึกษา เป็นต้น ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือผู้ที่ได้รับมอบหมาย

1.4.2 เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือผู้ที่ได้รับมอบหมาย

(1) เก็บรวบรวมบันทึกเปลี่ยนแปลงประวัติบุคคล หรือแบบอื่นตามความเหมาะสม และสำเนาเอกสารหลักฐานไว้ในแฟ้มประวัติของเจ้าของประวัติ

(2) แก้ไข เพิ่มเติมข้อมูลประวัติตามที่ได้รับแจ้งจากเจ้าของประวัติให้เป็นปัจจุบัน (เฉพาะในส่วนที่สามารถแก้ไขเพิ่มเติมได้)

2. แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ ประกอบด้วยการกำหนดชั้นความลับและการแสดงชั้นความลับ การปรับชั้นความลับ โดยปฏิบัติ ดังนี้

2.1 การกำหนดชั้นความลับและการแสดงชั้นความลับ

2.1.1 การกำหนดชั้นความลับ

(1) กำหนดชั้นความลับและให้เหตุผลประกอบการกำหนดชั้นความลับสอดคล้องตามข้อมูลข่าวสารที่ไม่ต้องเปิดเผยตามมาตรา 14 และ 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และพิจารณากำหนดชั้นความลับให้เหมาะสม (ชั้น “ลับ” “ลับมาก” “ลับที่สุด”) ตามองค์ประกอบ ได้แก่ ความสำคัญของเนื้อหา แหล่งที่มาของข้อมูลข่าวสาร วิธีการนำไปใช้ประโยชน์ จำนวนบุคคลที่ควรรับทราบ ผลกระทบหากมีการเปิดเผย และหน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่องหรือผู้อนุมัติ

(2) นายทะเบียนข้อมูลข่าวสารลับหรือผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับต้องบันทึกเหตุผลย่อของการกำหนดชั้นความลับในช่องการดำเนินการของทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3)

2.1.2 การแสดงชั้นความลับ

(1) เครื่องหมายแสดงชั้นความลับของข้อมูลข่าวสารลับและข้อมูลข่าวสารลับอิเล็กทรอนิกส์ให้ใช้สีแดงหรือสีอื่นที่สามารถมองเห็นได้อย่างเด่นชัดและขนาดตัวอักษรใหญ่กว่าตัวอักษรธรรมดา

(2) ข้อมูลข่าวสารลับที่มีสภาพเป็นเอกสารและในรูปแบบอิเล็กทรอนิกส์ ให้แสดงชั้นความลับไว้ที่กึ่งกลางด้านบนและด้านล่าง ทุกหน้าที่ปรากฏข้อความหรือรูปภาพหรืออื่น ๆ ที่สามารถสื่อความหมายได้ และกรณีเก็บในลักษณะม้วนหรือพับให้แสดงชั้นความลับไว้ให้เห็นชัดเจนในขณะม้วนหรือพับไว้ด้วย

(3) ข้อมูลข่าวสารลับที่จัดทำในลักษณะรูปเล่ม ให้แสดงชั้นความลับไว้ที่ด้านนอกของปกหน้าและปกหลังด้วย

(4) ข้อมูลข่าวสารลับที่อยู่ในรูปแบบสิ่งบันทึกอื่น ๆ ที่สามารถแสดงผล หรือสื่อความหมายโดยกรรมวิธีใด ๆ ให้แสดงชั้นความลับไว้บนซองหรือกล่อง หรือหีบห่อที่บรรจุข้อมูลข่าวสารลับนั้นด้วย

2.2 การปรับชั้นความลับ

2.2.1 หน่วยงานของรัฐเจ้าของเรื่อง

(1) ผู้มีอำนาจกำหนดชั้นความลับ หรือผู้ได้รับมอบหมาย

- ขีดฆ่าชั้นความลับ และแสดงชั้นความลับใหม่ (ถ้ามี) ทุกหน้าของข้อมูลข่าวสารลับ

- แสดงข้อความแจ้งการปรับชั้นความลับ ไว้ที่หน้าแรกใกล้กับเครื่องหมายแสดงชั้นความลับเดิมของเอกสารลับนั้น หรือซอง หรือกล่อง หรือหีบห่อที่บรรจุข้อมูลข่าวสารลับนั้น

- แจ้งหน่วยงานที่แจกจ่ายทุกหน่วยงาน ให้ทำการแก้ไขชั้นความลับทั้งในส่วนของข้อมูลข่าวสารและทะเบียนข้อมูลข่าวสารลับ ให้ตรงกัน

(2) นายทะเบียนข้อมูลข่าวสารลับหรือผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับแก้ไขชั้นความลับในทะเบียนข้อมูลข่าวสารลับ (ทขล.2 และ ทขล.3) ให้ถูกต้อง และจดแจ้งการปรับชั้นความลับในช่องการดำเนินการของทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3)

2.2.2 หน่วยงานของรัฐที่ครอบครองข้อมูลข่าวสารลับ ต้องแก้ไขให้ตรงตามที่ได้รับแจ้งจากหน่วยงานของรัฐเจ้าของเรื่อง ดังนี้

(1) ผู้ครอบครองข้อมูลข่าวสารลับ ขีดฆ่าชั้นความลับ และแสดงชั้นความลับใหม่ (ถ้ามี) และแสดงข้อความแจ้งการปรับชั้นความลับ ไว้ที่หน้าแรกใกล้กับเครื่องหมายแสดงชั้นความลับเดิมของเอกสารลับนั้น หรือซอง หรือกล่อง หรือหีบห่อที่บรรจุข้อมูลข่าวสารลับ

(2) นายทะเบียนข้อมูลข่าวสารลับหรือผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับแก้ไขชั้นความลับในทะเบียนข้อมูลข่าวสารลับ (ทขล.1 และ ทขล.3) และจดแจ้งการปรับชั้นความลับในช่องการดำเนินการของทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3)

2.2.3 การปรับชั้นความลับล่วงหน้า เพื่อเป็นการลดขั้นตอนดำเนินการหรือการบริหารจัดการข้อมูลข่าวสารลับ ดำเนินการดังนี้

(1) ผู้มีอำนาจกำหนดชั้นความลับหรือผู้ได้รับมอบหมายของหน่วยงานของรัฐเจ้าของเรื่อง แสดงข้อความแจ้งการปรับชั้นความลับล่วงหน้าไว้ที่หน้าแรกใกล้กับเครื่องหมายแสดงชั้นความลับของเอกสารลับนั้น หรือซอง หรือกล่อง หรือหีบห่อที่บรรจุข้อมูลข่าวสารลับนั้น

(2) เมื่อถึงกำหนดเวลาที่ระบุไว้ หน่วยงานของรัฐเจ้าของเรื่อง (จัดเก็บสำเนา) และหน่วยงานของรัฐที่ครอบครอง สามารถทำการแก้ไขชั้นความลับของข้อมูลข่าวสารลับและแก้ไขชั้นความลับในระบบทะเบียนข้อมูลข่าวสารลับ ได้โดยไม่ต้องยืนยันให้ทราบอีก

ทั้งนี้ มีมติคณะรัฐมนตรี เมื่อวันที่ 11 มีนาคม 2546 เรื่อง แนวทางปฏิบัติในการปรับชั้นความลับ สำหรับเรื่องที่เสนอคณะรัฐมนตรี (หนังสือสำนักเลขาธิการคณะรัฐมนตรี ที่ นร 0505/ว 71 ลงวันที่ 14 มีนาคม 2546)

3. แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์

ประกอบด้วยการรักษาความปลอดภัยเกี่ยวกับบุคคลสำหรับผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอก การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ โดยปฏิบัติ ดังนี้

3.1 การรักษาความปลอดภัยเกี่ยวกับบุคคล สำหรับผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอก ที่ปฏิบัติหน้าที่เกี่ยวข้องกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ โดยเป็นบุคคลที่สามารถเข้าถึงชั้นความลับของข้อมูลข่าวสารลับ หรือทำหน้าที่ติดตั้ง ซ่อมบำรุง หรือทำการอื่นใดต่อคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่ใช้ดำเนินการเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์

3.1.1 ตรวจสอบประวัติและพฤติการณ์บุคคล ตามแนวทางปฏิบัติ การตรวจสอบประวัติและพฤติการณ์บุคคล ข้อ 1.1 ทั้งนี้ หากบุคคลที่ได้รับมอบหมายสามารถเข้าถึงชั้นความลับของข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ชั้น “ลับมาก”หรือสามารถเข้าถึงข้อมูลสำคัญของหน่วยงาน

ที่ประเมินแล้วว่าหากข้อมูลดังกล่าว สูญหาย หรือรั่วไหล จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง ต้องจัดให้มีการตรวจสอบประวัติและพฤติการณ์บุคคลโดยละเอียด ตามแนวทางปฏิบัติการตรวจสอบประวัติและพฤติการณ์บุคคลโดยละเอียด ข้อ 1.2

3.1.2 เมื่อบุคคลดังกล่าว ผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล ให้ดำเนินการรับรองความไว้วางใจบุคคล ตามแนวทางปฏิบัติการรับรองความไว้วางใจ ข้อ 1.3

3.1.3 ชี้แจงหรืออบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การใช้งานระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบเครือข่าย และอินเทอร์เน็ต กรณีเป็นบุคคลภายนอก ต้องชี้แจงให้ทราบระเบียบและข้อปฏิบัติเกี่ยวกับการรักษาความลับและการรักษาความปลอดภัย รวมถึงกฎหมายอื่นที่เกี่ยวข้อง

3.1.4 ให้มีเจ้าหน้าที่ของหน่วยงานทำหน้าที่ควบคุม กำกับดูแล ระหว่างดำเนินงานของบุคคลภายนอก

ทั้งนี้ กรณีมีเหตุจำเป็นเร่งด่วน อาทิ ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ใช้ดำเนินการเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ชำรุดหรือติดขัดจนส่งผลกระทบต่อการปฏิบัติภารกิจอย่างร้ายแรง หัวหน้าหน่วยงานของรัฐ อาจอนุญาตให้บุคคลภายนอกเข้ามาดำเนินการซ่อมแซมได้ โดยไม่ต้องรอผลการตรวจสอบประวัติและพฤติการณ์บุคคล หากผลการตรวจสอบประวัติและพฤติการณ์พบว่ามีความไม่เหมาะสม ต้องแจ้งผู้เกี่ยวข้องตรวจสอบการปฏิบัติงานและพิจารณาดำเนินการตามขั้นตอนอื่นต่อไป

3.2 การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยต้องกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานให้เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และที่แก้ไขเพิ่มเติม

3.3 การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์

3.3.1 กำหนดอุปกรณ์เฉพาะและจัดทำทะเบียนควบคุมอุปกรณ์ที่ใช้ในการจัดทำข้อมูลข่าวสารลับอิเล็กทรอนิกส์

3.3.2 จัดเก็บข้อมูลข่าวสารลับอิเล็กทรอนิกส์ โดยดำเนินการ ดังนี้

(1) เข้ารหัสข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ก่อนการจัดเก็บตามมาตรฐานการเข้ารหัสที่เป็นสากล เช่น AES (Advanced Encryption Standard) หรือมาตรฐานที่หน่วยงานองค์กรกำหนด

(2) จัดเก็บในสื่ออิเล็กทรอนิกส์ หรืออุปกรณ์ที่มีทะเบียนควบคุม หรือในระบบซึ่งกำหนดไว้เป็นการเฉพาะ

(3) สื่ออิเล็กทรอนิกส์ หรืออุปกรณ์ หรือระบบที่จัดเก็บ ต้องตั้งอยู่ในพื้นที่ที่มีการรักษาความปลอดภัย

3.3.3 ส่งและรับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ โดยดำเนินการ ดังนี้

(1) เข้ารหัสข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ที่ส่งผ่านเครือข่ายด้วยโปรโตคอลที่ปลอดภัย เช่น HTTPS TLS หรือ SSL และแจ้งช่องทางติดต่อขอรับรหัสผ่านเพื่อเปิดไฟล์ข้อมูลข่าวสารลับ เช่น หมายเลขโทรศัพท์ หรือไปรษณีย์อิเล็กทรอนิกส์ หรือช่องทางอื่นใดตามที่หน่วยงานกำหนด โดยห้ามแจ้งรหัสผ่านไปพร้อมกับการส่งไฟล์ข้อมูลข่าวสารลับนั้น และเมื่อผู้ส่งได้รับการติดต่อเพื่อขอรับรหัสผ่าน ต้องมีการสอบถามและบันทึกชื่อ ตำแหน่ง และส่วนงานของผู้ติดต่อขอรับรหัสผ่าน เพื่อเป็นการยืนยันตัวตน

(2) ใช้ช่องทางสื่อสารที่มั่นคงปลอดภัย หรือช่องทางที่หน่วยงานของรัฐกำหนด เช่น ระบบสารบรรณอิเล็กทรอนิกส์ หรือระบบไปรษณีย์อิเล็กทรอนิกส์กลางของหน่วยงาน

(3) การรับข้อมูลข่าวสารลับผ่านช่องทางไปรษณีย์อิเล็กทรอนิกส์กลางของหน่วยงาน ให้ผู้รับยืนยันการรับโดยการตอบกลับ (reply) ทางช่องทางนั้น หรือช่องทางอื่นตามที่ผู้ส่งได้ระบุไว้ ทั้งนี้ การตอบกลับอย่างน้อยต้องระบุข้อความว่า หน่วยงานได้รับข้อมูลข่าวสารลับพร้อมแจ้งหมายเลขโทรศัพท์ของหน่วยงานผู้รับไว้ด้วย ทั้งนี้ กรณีส่งผิดหน่วยงาน ให้ผู้รับรีบแจ้งหน่วยงานผู้ส่งทราบทันที พร้อมทั้งลบทำลายไฟล์ข้อมูลดังกล่าว

(4) กำหนดสิทธิผู้ใช้ (user) เป็นรายบุคคลให้กับนายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับอิเล็กทรอนิกส์หรือบุคคลอื่นที่เกี่ยวข้องในการเปิด รับ หรือส่งข้อมูลข่าวสารลับอิเล็กทรอนิกส์

3.3.4 การดำเนินการอื่น ๆ เกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์ ได้แก่ การจัดทำการสำเนาและการแปล การโอน การส่ง การรับ การเก็บรักษา การยืม การทำลาย การปฏิบัติในเวลาฉุกเฉิน การเปิดเผย และกรณีสูญหาย ให้ดำเนินการตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม รวมถึงคำแนะนำการปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ในส่วนที่เกี่ยวข้องกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์

4. แนวปฏิบัติการรักษาความปลอดภัยเกี่ยวกับสถานที่ ประกอบด้วย การประเมินภัยคุกคามและความเสี่ยงที่มีโอกาสที่จะเกิดการละเมิดการรักษาความปลอดภัยเกี่ยวกับสถานที่ การจัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ การกำหนดมาตรการการรักษาความปลอดภัย

เกี่ยวกับสถานที่ การสำรวจและตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่ การดำเนินการฝึกซ้อมแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ โดยปฏิบัติ ดังนี้

4.1 การประเมินภัยคุกคามและความเสี่ยงที่มีโอกาสที่จะเกิดการละเมิด การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Security Risk Analysis and Assessment)

4.1.1 วิเคราะห์ความเสี่ยง โดยคำนึงถึงบทบาท สถานภาพ ภารกิจของหน่วยงาน จำนวนบุคลากร ข้อมูลข่าวสาร ครุภัณฑ์ ระบบเทคโนโลยีสารสนเทศ และทรัพย์สินที่ต้องรับผิดชอบดูแลรักษา ประกอบกับเป้าหมายการดำเนินการ ของหน่วยงานในอนาคต และเหตุการณ์ที่เคยเกิดเหตุละเมิด หรือเสี่ยงจะเกิดเหตุละเมิด ทั้งนี้ ใช้หลักการวิเคราะห์โอกาสที่จะเกิดกับผลกระทบและความรุนแรง เมื่อเกิดเหตุการณ์นั้น ๆ ตามเครื่องมือหรือวิธีการที่เหมาะสม อาทิ เกณฑ์การประเมินภัยคุกคามและความเสี่ยง ดังนี้

ระดับของความเสี่ยง

=

ค่าระดับความรุนแรง (มูลค่าความเสียหาย/ผลกระทบ) × ค่าโอกาสที่จะเกิดความเสี่ยง

Risk Assessment matrix			ความถี่ที่เกิดขึ้น				
			ต่ำมาก/น้อยมาก	ต่ำ/น้อย	ปานกลาง	สูง/บ่อย	สูงมาก/บ่อยมาก
			1	2	3	4	5
ผลกระทบและความรุนแรง	สูงมาก/หายนะ I	5	5	10	15	20	25
	สูง /วิกฤต G,H	4	4	8	12	16	20
	ปานกลาง E,F	3	3	6	9	12	15
	ต่ำ/น้อย B,C,D	2	2	4	6	8	10
	น้อยมาก A	1	1	2	3	4	5
			ระดับของความเสี่ยง				

รูปที่ 1 ตารางตัวอย่างแสดงการวิเคราะห์ประเมินภัยคุกคามและความเสี่ยง

4.1.2 จัดระดับความเสี่ยงของภัยต่าง ๆ ที่จะส่งผลต่อการละเมิดการรักษาความปลอดภัยเกี่ยวกับสถานที่ เพื่อกำหนดแผนการรักษาความปลอดภัยสถานที่ ให้เหมาะสมกับระดับความเสี่ยง โดยคำนึงถึงองค์ประกอบในการบริหารความเสี่ยง ได้แก่ การระบุหรือค้นหาความเสี่ยง การลดความสูญเสีย การควบคุมความเสี่ยง

โอกาสที่จะเกิดความเสี่ยง	ความถี่โดยเฉลี่ย	ค่าคะแนน
สูงมาก	1 เดือนต่อครั้ง หรือมากกว่า	5
สูง	1 – 6 เดือนต่อครั้ง แต่ไม่เกิน 5 ครั้ง	4
ปานกลาง	1 ปีต่อครั้ง	3
น้อย	2 – 3 ปีต่อครั้ง	2
น้อยมาก	5 ปีต่อครั้ง	1

รูปที่ 2 ตารางสรุปค่าคะแนนโอกาสที่จะเกิดความเสี่ยงตามระดับความถี่

ระดับของความรุนแรง	มูลค่าความเสียหาย	ค่าคะแนน
สูงมาก	มากกว่า 10 ล้านบาท	5
สูง	มากกว่า 2.5 ล้านถึง 10 ล้านบาท	4
ปานกลาง	มากกว่า 1 ล้านถึง 2.5 ล้านบาท	3
น้อย	ตั้งแต่ 1 แสนถึง 1 ล้านบาท	2
น้อยมาก	น้อยกว่า 1 แสนบาท	1

รูปที่ 3 ตารางสรุปค่าคะแนนระดับความรุนแรงต่อมูลค่าความเสียหาย

ระดับของความรุนแรง	ผลกระทบกับความต่อเนื่องในการปฏิบัติงาน	ค่าคะแนน
สูงมาก	หน่วยงานต้องยุติการปฏิบัติงานและต้องปฏิบัติงานในพื้นที่สำรอง ไม่เกิน 2 เดือนขึ้นไป	5
สูง	หน่วยงานต้องยุติการปฏิบัติงาและต้องปฏิบัติงานในพื้นที่สำรอง ไม่เกิน 2 เดือน	4
ปานกลาง	หน่วยงานไม่สามารถปฏิบัติงานได้ตามปกติ เกิดภาวะชะงักงันอย่างมีนัยสำคัญทำให้กระทบต่อการปฏิบัติงานตามแผนงาน/โครงการ	3
ระดับของความรุนแรง	**ผลกระทบกับความต่อเนื่องในการปฏิบัติงาน**	**ค่าคะแนน**
น้อย	หน่วยงานได้รับผลกระทบต่อการปฏิบัติงานโดยอาจต้องปรับเปลี่ยนวิธีการหรือรูปแบบการทำงานบางส่วน	2
น้อยมาก	หน่วยงานได้รับผลกระทบต่อการปฏิบัติงานโดยอาจต้องปรับเปลี่ยนวิธีการหรือรูปแบบการทำงานเพียงเล็กน้อยเท่านั้น	1

รูปที่ 4 ตารางสรุปค่าคะแนนผลกระทบความเสี่ยงกับความต่อเนื่องในการปฏิบัติงาน

ระดับของความเสี่ยง	ระดับคะแนน	การดำเนินการเกี่ยวกับมาตรการการรักษาความปลอดภัยในหน่วยงาน
สูงมาก (สีแดง)	20-25	ผู้รับผิดชอบต้องดำเนินการปรับระดับมาตรการการรักษาความปลอดภัยและปฏิบัติตามแผน เผชิญเหตุทันทีอย่างเคร่งครัด (แผนการรักษาความปลอดภัยในสถานการณ์ฉุกเฉิน)
สูง (สีส้ม)	11-19	ผู้รับผิดชอบต้องดำเนินการปรับระดับมาตรการการรักษาความปลอดภัยและกำกับดูแลให้มีการปฏิบัติอย่างครบถ้วน (แผนการรักษาความปลอดภัยในสถานการณ์ไม่ปกติ)
ปานกลาง (สีเหลือง)	5-10	ผู้รับผิดชอบต้องดำเนินการกำกับดูแลการปฏิบัติตามแผนการรักษาความปลอดภัยที่กำหนดไว้ โดยเน้นย้ำในส่วนที่เห็นว่ามีความจำเป็น หรือกำหนดมาตรการเสริมเป็นการเฉพาะกรณี (แผนการรักษาความปลอดภัยในสถานการณ์ปกติ)
น้อย (สีเขียว)	3-4	ผู้รับผิดชอบต้องดำเนินการกำกับดูแลการปฏิบัติตามแผนการรักษาความปลอดภัยที่กำหนดไว้ และจัดเก็บข้อมูลหรือสถานการณ์ดังกล่าวมาปรับปรุงและพัฒนาแผนการรักษาความปลอดภัย รวมทั้งมาตรการการรักษาความปลอดภัยสถานที่ให้เหมาะสมอย่างมีประสิทธิภาพ (จัดทำ Best Practice ตามวงรอบของการตรวจสอบมาตรการการรักษาความปลอดภัยสถานที่)
น้อยมาก (สีเทา)	1-2	

รูปที่ 5 ตารางสรุปเกณฑ์ประเมินความเสี่ยง

4.2 การจัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่

เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ต้องจัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ โดยพิจารณาจากองค์ประกอบ ดังนี้

4.2.1 ระดับความสำคัญของหน่วยงาน พิจารณาจากภารกิจ หน้าที่และสิ่งที่ต้องพิทักษ์รักษา

4.2.2 สภาพแวดล้อมของหน่วยงานเชิงภูมิศาสตร์ เช่น ที่ตั้ง ลักษณะพื้นที่ข้างเคียง รวมถึงทัศนคติของชุมชนแวดล้อมที่มีต่อหน่วยงานและภาพลักษณ์ของหน่วยงาน

4.2.3 ข่าวสาร สิ่งบอกเหตุ ตลอดจนข้อมูลหรือสถิติเกี่ยวกับการเกิดเหตุละเมิดการรักษาความปลอดภัย

4.2.4 ประสิทธิภาพในการเตือนภัย รวมทั้งการร้องขอการสนับสนุน จากหน่วยงานต่าง ๆ

4.2.5 จำนวนบุคลากรในหน่วยงาน เจ้าหน้าที่รักษาความปลอดภัย พื้นที่ที่ต้องกำกับดูแล

4.2.6 งบประมาณที่มีในการดำเนินการตามมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่

4.2.7 ระบบและช่องทางการติดต่อสื่อสารภายในหน่วยงานและการติดต่อสื่อสารกับหน่วยงานอื่น ๆ

4.2.8 การฝึกซ้อมและปรับปรุงแผนการรักษาความปลอดภัยสถานที่

4.2.9 แนวทางการรายงานผลการสำรวจหรือการตรวจสอบการรักษาความปลอดภัยต่อผู้บังคับบัญชา

ทั้งนี้ การจัดทำแผนการรักษาความปลอดภัยสถานที่ ต้องคำนึงถึงองค์ประกอบข้างต้น รวมทั้งการประเมินภัยคุกคาม ความเสี่ยง โอกาสที่จะเกิดและผลกระทบทั้งในด้านมูลค่าความเสียหายและความต่อเนื่องในการปฏิบัติงานเพื่อจัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ ทั้ง 3 ระดับ ได้แก่

(1) แผนการรักษาความปลอดภัยในสถานการณ์ปกติ หมายถึง สถานการณ์ที่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมายวิเคราะห์ประเมินแล้วว่า ไม่มีภัยคุกคามหรือความเสี่ยงในระดับที่จะเกิดผลกระทบในแง่ของมูลค่า ความเสียหายและความต่อเนื่องในการปฏิบัติงาน ให้จัดทำแผนการรักษาความปลอดภัยในสถานการณ์ปกติ คือ กำหนดมาตรการการรักษาความปลอดภัยสถานที่ให้เหมาะสมและรองรับกับภัยคุกคามในสถานการณ์ทั่วไป

(2) แผนการรักษาความปลอดภัยในสถานการณ์ไม่ปกติ หมายถึง สถานการณ์ที่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมายวิเคราะห์ประเมินแล้วว่าอาจมีภัยคุกคามหรือความเสี่ยงในระดับที่จะเกิดผลกระทบในแง่ของมูลค่าความเสียหายและความต่อเนื่อง

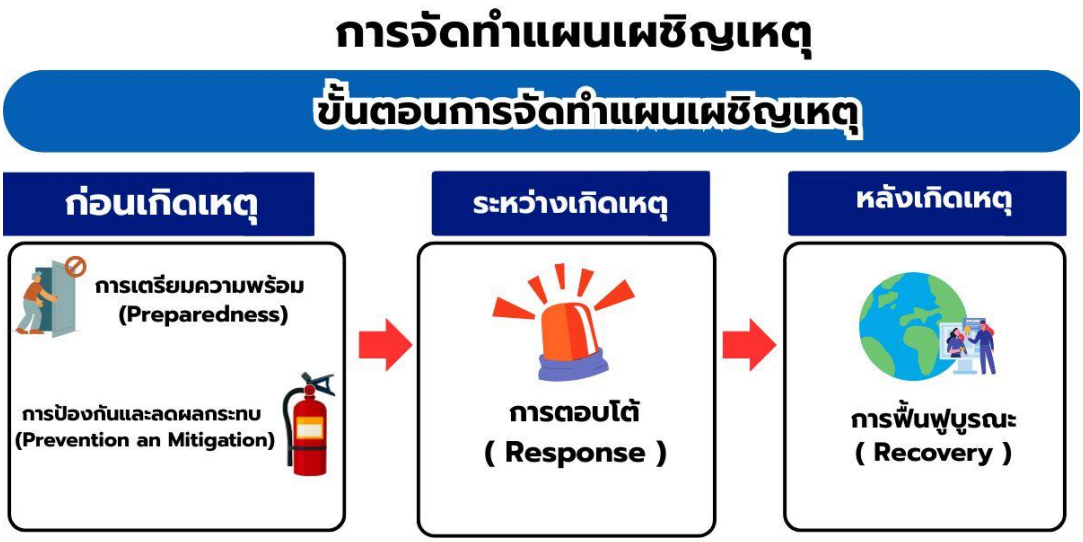
ในการปฏิบัติงาน แต่อยู่ในวิสัยที่หน่วยงานสามารถเผชิญและควบคุมสถานการณ์ได้ ในสถานการณ์เช่นนี้ต้องจัดทำแผนการรักษาความปลอดภัยในสถานการณ์ไม่ปกติ โดยการปรับระดับมาตรการการรักษาความปลอดภัยให้เข้มข้นขึ้น ตลอดจนมีการจัดทำแผนเผชิญเหตุ เพื่อรองรับภัยคุกคามต่าง ๆ

(3) แผนการรักษาความปลอดภัยในสถานการณ์ฉุกเฉิน (แผนเผชิญเหตุ) หมายถึง สถานการณ์ที่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมายวิเคราะห์ประเมินแล้วว่า มีภัยคุกคามหรือเกิดเหตุละเมิดขึ้นและจำเป็นต้องเข้าระงับเหตุให้ทันท่วงที โดยอาจต้องประสานขอความช่วยเหลือจากหน่วยงานข้างเคียง หน่วยงานเฉพาะที่มีทักษะและความชำนาญการในการบริหารจัดการสถานการณ์ ในกรณีนี้เจ้าหน้าที่ภายในหน่วยงานจะต้องปฏิบัติตามแผนรักษาความปลอดภัยในสถานการณ์ฉุกเฉิน ที่กำหนดไว้โดยเคร่งครัด

การจัดทำแผนเผชิญเหตุ (Incident Action Plan) ควรให้ครอบคลุม3 ขั้นตอน คือ ก่อนเกิดเหตุ ระหว่างเกิดเหตุ และหลังเกิดเหตุ โดยแผนเผชิญเหตุ ประกอบด้วยหัวข้อที่สำคัญ ได้แก่

- คำจำกัดความและคำย่อต่าง ๆ
- หลักการและเหตุผล วัตถุประสงค์ ขอบเขต
- แนวทางและวิธีการปฏิบัติเมื่อเกิดเหตุภาวะฉุกเฉิน
- แผนผังการควบคุมเหตุภาวะฉุกเฉิน (Flow chart) ในแต่ละระดับความรุนแรง
- ผังการติดต่อสื่อสารภายในหน่วยงาน (Call Tree)
- ขั้นตอนการแจ้งเหตุ หมายเลขโทรศัพท์ฉุกเฉินในการประสานงานและรายงานกับหน่วยงานภายนอก
- แผนการปฏิบัติในเวลาฉุกเฉินสำหรับข้อมูลข่าวสารลับและข้อมูลข่าวสารลับอิเล็กทรอนิกส์
- การอพยพ
- การเคลื่อนย้ายไปปฏิบัติงานในพื้นที่สำรอง
- การฟื้นฟูบูรณะคืนสู่สภาวะปกติ (Recovery)

ทั้งนี้ แผนผังการควบคุมเหตุภาวะฉุกเฉินในแต่ละระดับความรุนแรง อ้างอิงตามกฎหมาย อาทิ พระราชบัญญัติควบคุมอาคาร พ.ศ. 2522 และที่แก้ไขเพิ่มเติม พระราชบัญญัติป้องกันและบรรเทาสาธารณภัย พ.ศ. 2550 พระราชบัญญัติความปลอดภัย อาชีวอนามัยและสภาพแวดล้อมในการทำงาน พ.ศ. 2554 มติคณะรัฐมนตรี เมื่อ 7 พฤศจิกายน 2543 เรื่อง มาตรการและแนวทางในการป้องกันการเกิดอัคคีภัยในสถานที่ราชการ หน่วยงานของรัฐ และรัฐวิสาหกิจ



รูปที่ 6 ขั้นตอนการจัดทำแผนเผชิญเหตุ

หมายเหตุ : การพิจารณาจัดทำแผนการรักษาความปลอดภัยหน่วยงานของรัฐให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 พระราชบัญญัติป้องกันและบรรเทาสาธารณภัย พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้อง อาทิ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และให้มีการซักซ้อมแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่อย่างน้อยปีละ 1 ครั้ง เพื่อนำมาพิจารณาปรับปรุงให้เหมาะสมกับสถานการณ์ปัจจุบัน

4.3 การกำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่

4.3.1 มาตรการการรักษาความปลอดภัยในสถานการณ์ปกติ เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมาย ต้องดำเนินการ ดังนี้

(1) กำหนดพื้นที่ควบคุมสำหรับเจ้าหน้าที่ บุคคลภายนอก และ ผู้มาติดต่อ

(2) มีเครื่องกีดขวางและอุปกรณ์กีดขวางการเข้าออกพื้นที่ควบคุม พื้นที่หวงห้าม ได้แก่ แนวรั้วรอบพื้นที่ควบคุม อุปกรณ์กีดขวางการบุกรุกเข้าพื้นที่บริเวณประตูช่องทางเข้าออกหลัก ประตูช่องทางเข้าออกอาคารที่ทำการ และประตูช่องทางเข้าออกหน่วยงานภายใน

(3) มีระบบแสงสว่างบริเวณแนวรั้ว บริเวณภายในพื้นที่ควบคุมรอบนอกตัวอาคาร โดยต้องติดตั้งไม่ให้ปรากฏจุดอับแสงหรือพื้นที่ทึบแสงในเวลากลางคืน และบริเวณพื้นที่ภายในอาคาร

(4) มีระบบสัญญาณเตือนภัยระบบไฟฉุกเฉินและช่องทางเข้าออกฉุกเฉิน เพื่อเตือนภัยและเป็นช่องทางหลบหนี กรณีเกิดเหตุเพลิงไหม้หรือเหตุฉุกเฉินอื่น ๆ

(5) กำหนดมาตรการเพื่อควบคุมบุคคล ได้แก่ มีบัตรแสดงตน เพื่อเป็นการพิสูจน์ตัวตน และแยกความชัดเจนระหว่างเจ้าหน้าที่ บุคคลภายนอกและผู้มาติดต่อ

(6) กำหนดมาตรการเพื่อควบคุมยานพาหนะ โดยแยกพื้นที่จอดรถยนต์ รถจักรยานยนต์ ระหว่างเจ้าหน้าที่ บุคคลภายนอก และผู้มาติดต่อ

(7) จัดเจ้าหน้าที่รักษาความปลอดภัยประจำวัน อย่างน้อยประกอบด้วย เจ้าหน้าที่เวรรักษาความปลอดภัย เจ้าหน้าที่รักษาการณ์ (พนักงานจ้างเหมาบริการ โดยมีคุณสมบัติตามที่พระราชบัญญัติธุรกิจรักษาความปลอดภัย พ.ศ. 2558 กำหนดไว้) ปฏิบัติหน้าที่ตรวจตราและตรวจสอบความเรียบร้อย เพื่อป้องกันการละเมิดการรักษาความปลอดภัยบริเวณภายในพื้นที่ควบคุมรอบนอกอาคาร

(8) จัดให้มีระบบการป้องกันอัคคีภัย แผนการป้องกันอัคคีภัยหรือแผนปฏิบัติในสถานการณ์ฉุกเฉิน หรือสถานการณ์ไม่ปกติอื่น ๆ โดยการวิเคราะห์และประเมินความเสี่ยงของหน่วยงาน

ทั้งนี้ ระบบการป้องกันอัคคีภัย ระบบสัญญาณเตือนภัย ความเข้มของแสงสว่าง หรืออื่น ๆ ที่เกี่ยวข้องต่อการกำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้เป็นไปตามพระราชบัญญัติควบคุมอาคาร พ.ศ. 2522 และที่แก้ไขเพิ่มเติม

(9) จัดให้มีเครื่องมือและอุปกรณ์การรักษาความปลอดภัย อาทิ กล้องโทรทัศน์วงจรปิด (Closed Circuit Television : CCTV) ให้เพียงพอและเหมาะสมกับพื้นที่ โดยขั้นต่ำให้เป็นไปตามคุณลักษณะพื้นฐาน ตามประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม หรืออื่น ๆ ที่เกี่ยวข้อง ระบบควบคุมการเข้าออกอัตโนมัติ (Access Control System)

(10) สำรวจและตรวจสอบเครื่องมือและอุปกรณ์การรักษาความปลอดภัยทุกประเภทให้อยู่ในสภาพพร้อมใช้งาน อย่างน้อยปีละหนึ่งครั้ง

4.3.2 มาตรการการรักษาความปลอดภัยในสถานการณ์ไม่ปกติเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานของรัฐ ปรับระดับมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้มีความเข้มข้นขึ้น อาทิ ไม่อนุญาตให้จอดรถภายในหน่วยงาน ไม่อนุญาตให้บุคคล (ตามที่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบุ) เข้ามาในพื้นที่ของหน่วยงาน เพิ่มเติมอุปกรณ์เกี่ยวกับการรักษาความปลอดภัย เช่น เครื่องมือการตรวจค้นวัตถุต้องสงสัย

4.3.3 มาตรการการรักษาความปลอดภัยในสถานการณ์ฉุกเฉิน เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานของรัฐ ปรับระดับมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้มีความเข้มข้นและควบคุมกำกับดูแลอย่างเคร่งครัด โดยต้องมีการประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง หรือหน่วยงานที่มีอำนาจหน้าที่กำกับตามกฎหมายในเรื่องนั้น ๆ ระบุไว้ เช่น กฎหมายว่าด้วยดิจิทัล

4.4 การสำรวจและตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่

4.4.1 การสำรวจเพื่อกำหนดมาตรการการรักษาความปลอดภัยสถานที่ เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย ต้องพิจารณาเพื่อกำหนดมาตรการการรักษาความปลอดภัยที่เหมาะสม อาทิ ที่ตั้งทางภูมิศาสตร์ ภารกิจของหน่วยงาน ความสัมพันธ์กับมวลชนโดยรอบ สถานการณ์ทางการเมือง ข่าวสารสิ่งบอกเหตุ ผลการประเมินภัยคุกคามและระดับความเสี่ยงที่หน่วยงานจะต้องเผชิญทั้งในปัจจุบันและอนาคต รวมทั้งผลกระทบและความเสียหายที่จะเกิดขึ้นหากเกิดการละเมิดมาตรการการรักษาความปลอดภัย ให้ทราบถึงจุดอ่อน ข้อขัดข้องหรือความบกพร่อง ในด้านต่าง ๆ โดยจะนำมาศึกษาทบทวน เพื่อกำหนดแนวทางวางมาตรการที่เหมาะสม รัดกุมและมีประสิทธิภาพ ตลอดจนควรดำเนินการสำรวจทุกครั้งที่มีการปรับปรุงเปลี่ยนแปลง ทางกายภาพของที่ทำการ ตามขั้นตอน ดังนี้

<u>ขั้นที่หนึ่ง</u> ศึกษาข้อมูลความบกพร่องด้านการรักษาความปลอดภัยสถานที่ ที่เคยเกิดขึ้นจากรายงานและข้อมูลข่าวสารที่รวบรวมได้ทั้งภายในพื้นที่ทำการและพื้นที่บริเวณใกล้เคียงโดยรอบของหน่วยงานของรัฐ อาทิ รายงานเกี่ยวกับการโจรกรรม เหตุเพลิงไหม้ สภาพสังคม เช่น ย่านชุมชนแออัด แหล่งลักลอบค้ายาเสพติด บ่อนการพนัน สถานเริงรมย์ พฤติกรรมโดยรวมของประชาชนที่อาศัยในบริเวณนั้น เป็นต้น ตลอดจนความตระหนักถึงความสำคัญด้านการรักษาความปลอดภัยของเจ้าหน้าที่ภายในหน่วยงาน

<u>ขั้นที่สอง</u> สำรวจพื้นที่และอาคารสถานที่ที่จะกำหนดมาตรการการรักษาความปลอดภัยโดยละเอียด ทั้งในเวลาราชการ นอกเวลาราชการ และวันหยุดราชการ ทั้งกลางวันและกลางคืน เพื่อนำมาประกอบกับข้อมูลที่ได้จากขั้นที่หนึ่ง และนำมาประมวลเพื่อใช้กำหนดรายละเอียดของมาตรการและประเภทของเครื่องมืออุปกรณ์สำหรับการรักษาความปลอดภัยสถานที่ ให้รองรับกับระดับความสำคัญของหน่วยงาน และเป็นมาตรการที่เจ้าหน้าที่และบุคคลภายนอก สามารถปฏิบัติได้จริง โดยคำนึงถึงงบประมาณที่เหมาะสม

<u>ขั้นที่สาม</u> จัดทำรายงานผลการสำรวจการรักษาความปลอดภัยเกี่ยวกับสถานที่ โดยชี้ให้เห็นถึงอุปสรรค ข้อบกพร่อง จุดอ่อน แนวทางแก้ไข ผลกระทบหากไม่มีการกำหนด

มาตรการการรักษาความปลอดภัย ตลอดจนความสำคัญและความจำเป็นของการกำหนดมาตรการเสนอผู้บังคับบัญชาเพื่อพิจารณา

ในการสำรวจมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ หน่วยงานของรัฐอาจนำแบบสำรวจมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่หน่วยงานของรัฐฝ่ายพลเรือนตามผนวกนี้เป็นแนวทางในการดำเนินการสำรวจ

4.4.2 การตรวจสอบมาตรการการรักษาความปลอดภัยสถานที่ในสภาวะปกติ

หน่วยงานของรัฐต้องกำหนดห้วงเวลาการตรวจสอบ เช่น ทุก 6 เดือน หรือ 1 ปีขึ้นอยู่กับบริบทของแต่ละหน่วยงานทั้งในด้านระดับความสำคัญ หน้าที่ ความรับผิดชอบ พื้นที่ตั้งและสภาพแวดล้อม โดยให้ส่วนงานรักษาความปลอดภัย เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วยงาน หรือผู้ที่ได้รับมอบหมายทำการตรวจสอบหาข้อบกพร่องหรือทบทวนมาตรการที่กำหนด เพื่อจัดทำรายงานเสนอผู้บังคับบัญชาพิจารณา

4.4.3 การตรวจสอบมาตรการการรักษาความปลอดภัยสถานที่ เมื่อเกิดการละเมิดการรักษาความปลอดภัย

เมื่อเกิดการละเมิดการรักษาความปลอดภัยขึ้นในหน่วยงานของรัฐหลังการปฏิบัติตามแผนการรักษาความปลอดภัยในสถานการณ์ฉุกเฉิน (แผนเผชิญเหตุ) หัวหน้าหน่วยงานของรัฐต้องดำเนินการตามข้อบัญญัติแห่งระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 หมวด 7 การละเมิดการรักษาความปลอดภัย

ทั้งนี้ การละเมิดการรักษาความปลอดภัยสถานที่ มีผลกระทบตั้งแต่ระดับที่สามารถควบคุมได้จนถึงระดับรุนแรง โดยหากพิจารณาเหตุละเมิดที่มีลักษณะผลกระทบที่รุนแรง คือ การก่อวินาศกรรมมีหลายรูปแบบขึ้นอยู่กับความต้องการใช้งานของกลุ่มผู้กระทำ เพราะจุดมุ่งหมายของการก่อวินาศกรรมมี 2 หลักใหญ่ คือ ต้องการสร้างความเสียหายแก่ชีวิตและทรัพย์สินของรัฐ หรือต้องการสร้างความตื่นตระหนก เพื่อบั่นทอนความน่าเชื่อถือของหน่วยงานของรัฐ การก่อวินาศกรรมมีหลายรูปแบบ แต่ที่ปรากฏการก่อเหตุ คือ

(1) การลอบวางเพลิง ซึ่งการป้องกันก็เช่นเดียวกับการป้องกันอัคคีภัย

(2) การใช้วัตถุระเบิด

(3) การใช้สารเคมีหรือก๊าซพิษ

(4) การใช้เชื้อโรค-ชีวภาพ

(5) การใช้แร่ธาตุกัมมันตรังสี

ในการตรวจสอบมาตรการการรักษาความปลอดภัยสถานที่เมื่อเกิดการละเมิดการรักษาความปลอดภัยจำเป็นต้องพิจารณาถึงมาตรการที่มีอยู่ รวมทั้งแนวทางปฏิบัติตาม

แผนการรักษาความปลอดภัยในสถานการณ์ฉุกเฉิน(แผนเผชิญเหตุ) เพื่อทบทวนและปรับปรุงให้เหมาะสม สามารถป้องกันหรือลดความเสียหายที่จะเกิดการละเมิดซ้ำในครั้งต่อไป โดยแนวทางปฏิบัติที่หน่วยงานควรกำหนดและเผยแพร่เพื่อให้ถือปฏิบัติ อาทิ แนวทางปฏิบัติต่อเหตุการณ์ก่อวินาศกรรม แนวทางปฏิบัติกรณีการข่มขู่ว่าจะก่อการร้ายหรือลอบวางระเบิดทางโทรศัพท์ แนวทางปฏิบัติ เมื่อพบวัตถุต้องสงสัยว่าเป็นวัตถุระเบิด การตรวจสอบยานพาหนะ เพื่อป้องกันการก่อวินาศกรรม เช่น อาวุธ วัตถุระเบิด แนวทางปฏิบัติในการตรวจสอบสถานที่ที่อาจมีการนำวัตถุระเบิดมาซ่อนพราง แนวทางปฏิบัติต่อการพบสิ่งต้องสงสัยว่าเป็นกล่องของขวัญ พัสดุภัณฑ์หรือจดหมายระเบิด แนวทางปฏิบัติต่อพัสดุภัณฑ์หรือจดหมายที่ต้องสงสัยว่าภายในบรรจุเชื้อโรค (แนวทางปฏิบัติเพื่อรองรับสถานการณ์ต่าง ๆ ศึกษาได้จากคำแนะนำการปฏิบัติตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 และที่แก้ไขเพิ่มเติม)

เมื่อดำเนินการตรวจสอบมาตรการการรักษาความปลอดภัยสถานที่ตามห้วงเวลาที่กำหนดไว้ หรือเมื่อมีสถานการณ์ที่ต้องมีการปรับมาตรการการรักษาความปลอดภัย ควรมีการทบทวนหลังการปฏิบัติ (After Action Review) เป็นการสรุปบทเรียนที่เกิดขึ้น เพื่อนำมาพิจารณาปรับปรุง เพิ่มเติมมาตรการการรักษาความปลอดภัยสถานที่ ให้เหมาะสมกับสถานการณ์ปัจจุบัน

4.5 การดำเนินการฝึกซ้อมแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่

4.5.1 การฝึกซ้อมแผนบนโต๊ะ (Table Top Exercise : TTX) เป็นการฝึกซ้อมแผนที่มุ่งเน้นการระบุจุดแข็ง จุดอ่อน รวมทั้งการทำความเข้าใจในแผน นโยบาย ข้อตกลงความร่วมมือและขั้นตอนการปฏิบัติที่ใช้อยู่ของหน่วยงานที่เกี่ยวข้อง ใช้การอภิปรายกลุ่มแบบไม่เป็นทางการบนพื้นฐานของสถานการณ์สมมติที่กำหนดขึ้นโดยมีวิทยากรกระบวนการ (Facilitators) เป็นผู้นำการอภิปรายให้เป็นไปตามแนวทางและวัตถุประสงค์ของการฝึกซ้อม ผู้เข้าร่วมฝึกซ้อมควรเป็นเจ้าหน้าที่ระดับสูง เจ้าหน้าที่ที่รับผิดชอบ หรือบุคลากรหลักในเรื่องนั้น ๆ รูปแบบการฝึกซ้อมไม่มีการเคลื่อนย้ายทรัพยากร ทำให้ประหยัดและเกิดประสิทธิภาพ สามารถฝึกแก้ไขปัญหาตามสถานการณ์สมมติที่เฉพาะเจาะจงภายใต้สภาวะที่ไม่มีความกดดัน ผู้เข้าร่วมฝึกซ้อมได้แลกเปลี่ยนข้อมูลระหว่างกัน

นอกจากนี้ การฝึกซ้อมแผนบนโต๊ะสามารถกำหนดหรือระบุให้เป็นการฝึกซ้อมในที่บังคับการ (Command Post Exercise : CPX) ได้อีกด้วย โดยมีรูปแบบเดียวกัน แต่เน้นเฉพาะสำหรับการฝึกด้านการวิเคราะห์ วางแผน และวินิจฉัยสั่งการแก่เจ้าหน้าที่และผู้นำ โดยการฝึกซ้อมในลักษณะนี้จะนำเสนอปัญหาที่ซับซ้อนและสมจริง

4.5.2 การฝึกซ้อมแผนเฉพาะหน้าที่ (Functional Exercise : FEX) เป็นการฝึกซ้อมภายในหน่วยงานหรือระหว่างหน่วยงานที่มีการจำลองสถานการณ์ฉุกเฉิน ให้สมจริงมากที่สุดเท่าที่

จะเป็นไปได้ โดยมีการเคลื่อนย้ายวัสดุอุปกรณ์หรือบุคลากรตามสถานการณ์สมมติ วัตถุประสงค์ในการฝึกซ้อมลักษณะนี้ เพื่อทดสอบหรือประเมินขีดความสามารถของบุคคล และบทบาทหน้าที่ที่กำหนดไว้ตามแผนและขั้นตอนการปฏิบัติว่า มีความเหมาะสมเพียงพอต่อการตอบโต้กับสถานการณ์ฉุกเฉิน

4.5.3 การฝึกซ้อมเต็มรูปแบบ (Full-scale Exercise : FSX) เป็นการฝึกซ้อมที่มีความซับซ้อนและใช้ทรัพยากรมากที่สุดในบรรดาการฝึกซ้อมรูปแบบอื่น ๆ รวมทั้งเกี่ยวข้องกับบุคลากรจากหลากหลายหน่วยงานและหลายระดับ โดยมีการเคลื่อนย้ายทรัพยากรและบุคลากรเพื่อตอบโต้กับสถานการณ์จริง การฝึกซ้อมเต็มรูปแบบสามารถทดสอบการตอบโต้และบรรเทาเหตุฉุกเฉินในหลายมิติ โดยมุ่งเน้นการปฏิบัติตามแผน นโยบาย และขั้นตอนกระบวนการที่พัฒนาหรือกำหนดขึ้น จาก TTX หรือ CPX เหตุการณ์ต่าง ๆ นำเสนอโดยใช้บทสถานการณ์สมมติในการฝึกซ้อม (Script Exercise Scenario) นอกจากนี้ ในการจัด FSX นั้น จะกำหนดเวลาจริง (Real Time) และอยู่ภายใต้สภาวะแวดล้อมที่กดดันเสมือนเหตุการณ์จริง ดังนั้น เจ้าหน้าที่และทรัพยากรจึงต้องมีการเคลื่อนย้ายไปยังพื้นที่เกิดเหตุการณ์ซึ่งจัดไว้สำหรับปฏิบัติการ ด้วยเหตุนี้ FSX จึงเป็นการฝึกซ้อมที่ใช้ในการประเมินแผน ขั้นตอนการปฏิบัติ รวมทั้งการประสานการปฏิบัติในการตอบโต้เหตุการณ์ภายใต้เงื่อนไขภาวะวิกฤติ

ทั้งนี้ หน่วยงานอาจดำเนินการฝึกซ้อมตามกระบวนการ โดยอาจเพิ่มเติมขั้นตอนการทำความเข้าใจและทดสอบแผนโดยการเดินทดสอบ (Walk-through Drill) นอกเหนือจากการฝึกซ้อมแผนบนโต๊ะ หรือการซ้อมแผนตามหน้าที่ เพื่อให้ผู้เข้าร่วมฝึกซ้อมเข้าใจถึงขั้นตอนการปฏิบัติในสถานที่จริงได้อย่างดียิ่งขึ้น เป็นการเฉพาะแต่ละกรณี โดยไม่จำเป็นต้องดำเนินการฝึกซ้อมเต็มรูปแบบ ให้พิจารณาตามความเหมาะสมและงบประมาณ

5. แนวปฏิบัติการรักษาความปลอดภัยในการประชุมลับ ประกอบด้วย มาตรการการรักษาความปลอดภัยในการประชุมลับ การดำเนินการรักษาความปลอดภัยในการประชุมลับ

5.1 มาตรการการรักษาความปลอดภัยในการประชุมลับ เป็นการนำมาตรการด้านการรักษาความปลอดภัยเกี่ยวกับบุคคล การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับและการรักษาความปลอดภัยเกี่ยวกับสถานที่ มาใช้ประกอบกัน โดยอยู่ในความควบคุมและกำกับดูแลของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ และนายทะเบียนข้อมูลข่าวสารลับในการประชุมลับ ที่มีการแต่งตั้งเป็นลายลักษณ์อักษร ดังนี้

5.1.1 การรักษาความปลอดภัยเกี่ยวกับบุคคล ต้องมีการตรวจสอบประวัติและพฤติการณ์บุคคล รับรองความไว้วางใจบุคคลที่จะเข้าถึงหรือเกี่ยวข้องกับการประชุมลับทุกคน

5.1.2 การรักษาความปลอดภัยเกี่ยวกับสถานที่ ต้องมีการกำหนดขอบเขต/ระดับความสำคัญของพื้นที่การประชุม เช่น พื้นที่หวงห้าม (เขตหวงห้ามเฉพาะหรือเขตหวงห้ามเด็ดขาด) และมีการตรวจสอบพื้นที่การประชุม

5.1.3 การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ และข้อมูลข่าวสารสำคัญที่เกี่ยวข้องในการประชุมลับ โดยต้องดำเนินการตามระเบียบว่าด้วย การรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม รวมทั้งกำหนดมาตรการในการรักษาความปลอดภัยเกี่ยวกับระบบเครือข่ายสารสนเทศ เช่น โทรศัพท์เคลื่อนที่ คอมพิวเตอร์แบบพกพา หรืออุปกรณ์อื่น ๆ

5.2 การดำเนินการรักษาความปลอดภัยในการประชุมลับ

5.2.1 กำหนดพื้นที่ควบคุมที่จะใช้ในการประชุมลับ รวมถึงสถานที่จัดเก็บข้อมูลข่าวสารลับ โดยมีมาตรการควบคุมการเข้าถึงพื้นที่ที่เข้มงวด (กำหนดเป็นพื้นที่หวงห้าม)

5.2.2 มีการตรวจสอบพื้นที่ ทั้งก่อน ระหว่าง และหลังการประชุมลับโดยใช้เครื่องมือทางเทคนิค ได้แก่ เครื่องมือตรวจสอบการดักฟัง เครื่องมือตรวจสอบ การล่วงล้ำ เครื่องมือตรวจสอบการก่อวินาศกรรม เป็นต้น ทั้งนี้ การตรวจสอบดังกล่าวต้องดำเนินการโดยเจ้าหน้าที่ที่มีความเชี่ยวชาญเฉพาะ เพื่อเป็นการยืนยันได้ว่าผู้ไม่มีส่วนเกี่ยวข้องในการประชุมลับนั้นจะไม่สามารถได้ยินเรื่องราว หรือได้เห็นความเป็นไปในห้องประชุม ไม่มีเครื่องมือที่ใช้เพื่อการจารกรรม ก่อวินาศกรรม และหรือเอกสาร หรือสิ่งที่ใช้เพื่อการก่อกวน บ่อนทำลาย อยู่ในสถานที่ประชุมและพื้นที่ที่มีการรักษาความปลอดภัย

5.2.3 มีมาตรการควบคุมบุคคล โดยผู้เกี่ยวข้องในการประชุมลับ ต้องได้รับอนุญาตจากเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับและจัดให้มีบัตรผ่านหรือบัตรแสดงตนสำหรับผู้เกี่ยวข้องในการประชุมลับ ได้แก่ ผู้เข้าประชุม เจ้าหน้าที่บันทึกเสียงการประชุม ผู้จดรายงานการประชุม เจ้าหน้าที่เทคนิค เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย เจ้าหน้าที่บริการ เป็นต้น

5.2.4 กำหนดข้อห้ามนำเครื่องมือสื่อสาร เครื่องถ่ายภาพ และอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ที่ใช้ในการบันทึก จัดเก็บ และหรือส่งภาพ หรือข้อความ เข้าไปในห้องประชุม เว้นแต่ได้รับอนุญาตจากเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับนั้น

5.2.5 การประสานงานการรักษาความปลอดภัย หากผู้เข้าประชุมแต่ละฝ่ายเห็นว่าจำเป็นต้องวางมาตรการการรักษาความปลอดภัยเพื่อใช้เฉพาะฝ่ายตนขึ้น มาตรการที่กำหนดขึ้นนั้นจะต้องสอดคล้องกับมาตรการการรักษาความปลอดภัยในการประชุมลับของส่วนรวมด้วย โดยต้อง

ประสานงานในเรื่องการรักษาความปลอดภัยกับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับนั้น

5.2.6 การแถลงข่าวเกี่ยวกับการประชุมลับ ต้องจัดสถานที่สำหรับแถลงข่าวขึ้นโดยเฉพาะ โดยผู้แถลงข่าวต้องได้รับการแต่งตั้ง และเรื่องที่จะแถลงต้องได้รับอนุมัติจากที่ประชุม ในกรณีมีผู้แถลงข่าวหลายคน แต่ละคนจะต้องแถลงเฉพาะเรื่องที่ตนได้รับอนุมัติเท่านั้น

5.2.7 การบรรยายหรือการบรรยายสรุปเรื่องที่เป็นความลับ ผู้บรรยายจะต้องแจ้งชั้นความลับของเรื่องที่บรรยายให้ผู้ฟังทราบ โดยผู้เข้าฟังการบรรยายต้องได้รับความไว้วางใจไม่ต่ำกว่าชั้นความลับของเรื่องที่บรรยาย และต้องกำหนดมาตรการการรักษาความปลอดภัยในการบรรยายหรือการบรรยายสรุปเรื่องที่เป็นความลับนั้น เช่นเดียวกับการรักษาความปลอดภัยในการประชุมลับ

5.2.8 กำกับดูแล และดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ หรือสิ่งที่เป็นความลับของทางราชการในการประชุมลับ ให้เป็นไปตามมาตรฐานการรักษาความปลอดภัย ระเบียบ และกฎหมายที่เกี่ยวข้อง

5.2.9 กรณีจัดการประชุมลับทางระบบสารสนเทศหรือออนไลน์ ต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานของรัฐ และปฏิบัติตามพระราชกำหนดว่าด้วย การประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์

6. แนวปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย ประกอบด้วย การปฏิบัติของผู้พบเห็นหรือทราบว่ามีการละเมิดการรักษาความปลอดภัย หรือสงสัยว่าจะมีการละเมิดการรักษาความปลอดภัย เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือเจ้าหน้าที่ผู้รับผิดชอบ และหัวหน้าหน่วยงานของรัฐ ที่เกิดการละเมิดการรักษา ความปลอดภัย รวมถึงหัวหน้าหน่วยงานของรัฐที่เป็นเจ้าของเรื่องข้อมูลข่าวสารลับที่ถูกละเมิด โดยปฏิบัติ ดังนี้

6.1 ผู้พบเห็น หรือทราบว่ามีการละเมิดการรักษาความปลอดภัย หรือสงสัยว่าจะมีการละเมิดการรักษาความปลอดภัยเกิดขึ้น ต้องดำเนินการ ดังนี้

6.1.1 กรณีการละเมิดการรักษาความปลอดภัยเกิดขึ้นภายในหน่วยงานของตน ให้รีบดำเนินการลดความเสียหายเบื้องต้นให้เหลือน้อยที่สุด และรายงานให้ผู้บังคับบัญชา หรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือเจ้าหน้าที่ผู้รับผิดชอบ ทราบโดยเร็วที่สุด

6.1.2 กรณีการรักษาความปลอดภัยของหน่วยงานอื่นถูกละเมิด และไม่อยู่ในวิสัยที่จะดำเนินการเพื่อลดความเสียหายเบื้องต้นได้ ต้องรีบแจ้งหน่วยงานนั้นหรือรายงานผู้บังคับบัญชาของตน เพื่อแจ้งให้หน่วยงานที่ถูกละเมิด ทราบโดยเร็วที่สุด

6.2 เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือเจ้าหน้าที่ผู้รับผิดชอบของหน่วยงานของรัฐที่เกิดการละเมิดการรักษาความปลอดภัย ต้องดำเนินการ ดังนี้

6.2.1 สำรวจและตรวจสอบความเสียหายอันเกิดจากการละเมิดการรักษาความปลอดภัย

6.2.2 ดำเนินการลดความเสียหายให้เหลือน้อยที่สุด

6.2.3 สำรวจ ตรวจสอบ และค้นหาสาเหตุแห่งการละเมิดการรักษาความปลอดภัยตลอดจนจุดอ่อนและข้อบกพร่องต่าง ๆ

6.2.4 รายงานรายละเอียดเกี่ยวกับการละเมิดการรักษาความปลอดภัยให้ผู้บังคับบัญชาตามลำดับชั้นทราบโดยเร็ว ถ้าการละเมิดการรักษาความปลอดภัยนั้นมีข้อมูลข่าวสารลับสูญหาย ให้แจ้งนายทะเบียนข้อมูลข่าวสารลับ เพื่อบันทึกการสูญหายของข้อมูลข่าวสารลับในทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3) ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

6.2.5 แก้ไขมาตรการการรักษาความปลอดภัยให้รัดกุมยิ่งขึ้น เพื่อป้องกันมิให้เกิดการละเมิดการรักษาความปลอดภัยขึ้นอีก

6.2.6 หากปรากฏหลักฐานหรือสงสัยว่าถูกจารกรรม หรือถูกก่อวินาศกรรม ให้รายงานขออนุมัติผู้บังคับบัญชาตามลำดับชั้น เพื่อพิจารณาดำเนินการต่อไป เช่น แต่งตั้งคณะกรรมการสืบสวนข้อเท็จจริง หรือคณะกรรมการสอบสวนข้อเท็จจริง หรือคณะกรรมการตรวจสอบข้อเท็จจริง หรือแจ้งเจ้าหน้าที่ตำรวจ หรือขอคำแนะนำจากองค์การรักษาความปลอดภัย เป็นต้น

6.3 เมื่อได้ดำเนินการตามข้อ 6.2 แล้ว ให้หัวหน้าหน่วยงานของรัฐ พิจารณาดำเนินการดังนี้

6.3.1 แต่งตั้งคณะกรรมการสืบสวนข้อเท็จจริง หรือคณะกรรมการสอบสวนข้อเท็จจริง หรือคณะกรรมการตรวจสอบข้อเท็จจริง เพื่อหาผู้กระทำการละเมิด และผู้รับผิดชอบต่อการละเมิดนั้น ซึ่งอาจเป็นผู้ครอบครองสิ่งที่เป็นความลับของทางราชการ หรือผู้มีหน้าที่ดูแลรักษาสถานที่ของหน่วยงาน

6.3.2 พิจารณาลงโทษผู้กระทำการละเมิดการรักษาความปลอดภัยหรือผู้รับผิดชอบการละเมิดนั้น โดยอาศัยข้อเท็จจริงจากผลการสืบสวนและสอบสวนเป็นแนวทางในการพิจารณาลงโทษ

6.3.3 สั่งการให้มีการพิจารณาแก้ไขข้อบกพร่อง ปรับปรุงมาตรการการรักษาความปลอดภัยให้รัดกุมและเหมาะสมยิ่งขึ้น เพื่อป้องกันไม่ให้เกิดการละเมิดการรักษาความปลอดภัยขึ้นอีก

6.3.4 กรณีการละเมิดการรักษาความปลอดภัยเกี่ยวข้องกับข้อมูลข่าวสารลับที่หน่วยงานของรัฐอื่นเป็นเจ้าของเรื่อง ต้องแจ้งเรื่องการละเมิดการรักษาความปลอดภัยที่เกิดขึ้นให้แก่หน่วยงานเจ้าของเรื่อง ทราบทันที

6.4 เมื่อหน่วยงานเจ้าของเรื่อง หรือผู้เกี่ยวข้อง ได้รับแจ้งว่ามีการละเมิดการรักษาความปลอดภัยเกิดขึ้น ต้องดำเนินการ ดังนี้

6.4.1 พิจารณาว่าการละเมิดได้ทำให้ความสำคัญของสิ่งที่เป็นความลับของทางราชการเปลี่ยนแปลงไปหรือไม่ สมควรที่จะลดชั้นหรือยกเลิกชั้นความลับของสิ่งที่เป็นความลับของทางราชการนั้นหรือไม่ อย่างไร

6.4.2 ขจัดความเสียหายอันเกิดจากการละเมิดที่จะมีขึ้นต่อหน่วยงานของตนหรือหน่วยงานอื่น ในการนี้ อาจต้องปรับนโยบาย แผนการดำเนินงาน พร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องด้วย

บทที่ 4
การประเมินมาตรฐานการรักษาความปลอดภัย

การประเมินมาตรฐานการรักษาความปลอดภัย เป็นการกำหนดแนวทางการตรวจสอบและประเมินมาตรฐานการรักษาความปลอดภัย โดยมีรายการตรวจสอบ (Check List) เป็นเครื่องมือให้หน่วยงานของรัฐสามารถตรวจสอบการดำเนินการและการปฏิบัติด้านการรักษาความปลอดภัย ให้เป็นไปตามมาตรฐานการรักษาความปลอดภัย และสำนักข่าวกรองแห่งชาติในฐานะองค์การรักษาความปลอดภัยฝ่ายพลเรือน มีหน้าที่ติดตาม พิจารณา และประเมินการดำเนินการ เพื่อสามารถให้คำแนะนำ ส่งเสริม สนับสนุน และช่วยเหลือด้านการรักษาความปลอดภัย ได้อย่างถูกต้องและเหมาะสม เพื่อเสริมการรักษาความปลอดภัยของหน่วยงานของรัฐให้มีประสิทธิภาพมากยิ่งขึ้น โดยดำเนินการ ดังนี้

1. หน่วยงานของรัฐ

หน่วยงานของรัฐ ตรวจสอบการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน ตามแบบตรวจสอบมาตรฐานการรักษาความปลอดภัย อย่างน้อยปีละ 1 ครั้ง โดยหัวหน้าหน่วยงานของรัฐ แต่งตั้งคณะกรรมการตรวจสอบมาตรฐานการรักษาความปลอดภัยของหน่วยงาน (คมป.) ซึ่งมีองค์ประกอบและหน้าที่ ดังนี้

1.1 องค์ประกอบของคณะกรรมการ ประกอบด้วย ประธานกรรมการ ที่หัวหน้าหน่วยงานของรัฐมอบหมาย และกรรมการอีกไม่น้อยกว่า 4 คน โดยมีเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย และนายทะเบียนข้อมูลข่าวสารลับของหน่วยงาน เป็นกรรมการ

1.2 คณะกรรมการ มีหน้าที่

1.2.1 ตรวจสอบผลการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน ตามแบบตรวจสอบมาตรฐานการรักษาความปลอดภัย และรายงานผลการตรวจสอบต่อหัวหน้าหน่วยงานของรัฐ อย่างน้อยปีละ 1 ครั้ง

1.2.2 เสนอแนะ ปรับปรุง และพัฒนา ตลอดจนติดตามผลและรายงานความคืบหน้าต่อหัวหน้าหน่วยงานของรัฐ กรณีการปฏิบัติไม่เป็นไปตามแนวทางที่กำหนด

1.2.3 จัดส่งแบบตรวจสอบมาตรฐานการรักษาความปลอดภัย ไปยังสำนักข่าวกรองแห่งชาติ

1.2.4 ดำเนินการด้านการรักษาความปลอดภัยอื่น ๆ ตามที่หัวหน้าหน่วยงานของรัฐมอบหมาย

หมายเหตุ : คณะกรรมการ อาจแต่งตั้งคณะทำงานของหน่วยงาน เพื่อให้มีหน้าที่ดำเนินการตามข้อ 1.2.1 และ 1.2.2 ด้วยก็ได้

2. สำนักข่าวกรองแห่งชาติ

สำนักข่าวกรองแห่งชาติ มีหน้าที่ในการติดตามและประเมินผลการดำเนินการตามมาตรฐานการรักษาความปลอดภัย ภายใต้บทบัญญัติที่กฎหมายกำหนดไว้ โดยผู้อำนวยการสำนักข่าวกรองแห่งชาติ แต่งตั้งคณะกรรมการประเมินการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยหน่วยงานของรัฐฝ่ายพลเรือน โดยมีหน้าที่ ดังนี้

2.1 ตรวจสอบและประเมินผลการปฏิบัติของหน่วยงานของรัฐ

2.2 แจ้งผลการตรวจประเมินต่อหัวหน้าหน่วยงานของรัฐ ตลอดจนให้คำแนะนำและข้อเสนอแนะด้านการรักษาความปลอดภัย

2.3 รายงานผลการดำเนินการต่อผู้อำนวยการสำนักข่าวกรองแห่งชาติ เพื่อนำเสนอต่อคณะกรรมการนโยบายรักษาความปลอดภัยแห่งชาติ (กรช.) และคณะกรรมการข้อมูลข่าวสารของราชการ (กขร.)

2.4 คณะกรรมการ อาจแต่งตั้งหรือมอบหมายให้มีเจ้าหน้าที่ดำเนินการ ตามข้อ 2.1 และรายงานผลไปยังคณะกรรมการ ได้

.....

ผนวก

- แบบสำรวจมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่
- แบบตรวจสอบมาตรฐานการรักษาความปลอดภัย

แบบสำรวจมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่

แบบสำรวจมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ ฉบับนี้ ใช้สำหรับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือผู้ที่ได้รับมอบหมายให้รับผิดชอบเกี่ยวกับการรักษาความปลอดภัยสถานที่ เพื่อกำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ให้เหมาะสมกับบริบทของแต่ละหน่วยงาน ตามรายละเอียดดังต่อไปนี้

เจ้าหน้าที่ผู้ดำเนินการสำรวจ.....วัน/เดือน/ปี ที่ทำการสำรวจ.....

1. สภาพแวดล้อมภายนอกหน่วยงาน เช่น แหล่งชุมชนแออัด ย่านธุรกิจ หน่วยงานราชการ สถานที่สำคัญใกล้เคียงที่อาจมีผลกระทบต่อการรักษาความปลอดภัยของหน่วยงาน

   .....

   .....

   1) ทิศเหนือ ติด.....

   2) ทิศใต้ ติด.....

   3) ทิศตะวันออก ติด.....

   4) ทิศตะวันตก ติด.....

   หน่วยงานตั้งอยู่ในพื้นที่ ☐ ของตนเอง ☐ เช่าโดยตั้งอยู่เพียงหน่วยงานเดียว
   ☐ เช่าพื้นที่ของเอกชน ☐ ใช้/เช่าพื้นที่หน่วยงานรัฐร่วมกัน

2. หน่วยงานที่จะมอบหมายให้รับผิดชอบด้านการรักษาความปลอดภัยสถานที่ คือ

   .....

3. อาคาร/สถานที่ของหน่วยงานที่กำหนดให้เป็นพื้นที่ควบคุม โดยแบ่งเป็นพื้นที่ควบคุม และพื้นที่หวงห้าม ได้แก่ เขตหวงห้ามเด็ดขาด และเขตหวงห้ามเฉพาะ

   1) .....

   ☐ มีป้ายสัญลักษณ์บอกพื้นที่หวงห้าม ☐ ไม่มีการแสดงป้ายสัญลักษณ์
   ☐ มีการตรวจสอบก่อนเข้าพื้นที่หวงห้าม ☐ ไม่มีการตรวจสอบ

2) .....

☐ มีป้ายสัญลักษณ์บอกพื้นที่หวงห้าม ☐ ไม่มีการแสดงป้ายสัญลักษณ์

☐ มีการตรวจสอบก่อนเข้าพื้นที่หวงห้าม ☐ ไม่มีการตรวจสอบ

3) .....

☐ มีป้ายสัญลักษณ์บอกพื้นที่หวงห้าม ☐ ไม่มีการแสดงป้ายสัญลักษณ์

☐ มีการตรวจสอบก่อนเข้าพื้นที่หวงห้าม ☐ ไม่มีการตรวจสอบ

4. เครื่องกีดขวาง (ประดิษฐ์ขึ้นหรือตามธรรมชาติ)

1) รั้ว จำนวน.....ด้าน ความสูง ประมาณ.....เมตร
สภาพของแนวรั้ว.....

.....

.....

2) เครื่องกีดขวางทางธรรมชาติ เช่น คลอง ลำธาร
จำนวน.....ด้าน ความกว้าง ประมาณ.....เมตร
สภาพ.....

.....

.....

3) เครื่องกีดขวางบริเวณช่องทางเข้า-ออก เพื่อหน่วงเหนี่ยวการเข้าถึงพื้นที่ เช่น แผงกั้นล้อเลื่อน แขนกั้นยานพาหนะ เครื่องกั้นปีกผีเสื้อ จำนวน.....จุด
ติดตั้งบริเวณ.....

.....

5. ช่องทางเข้า-ออก รวมจำนวน.....ช่องทาง แยกเป็น
ช่องทางเข้า-ออก หลัก.....ช่องทาง
ช่องทางเข้า-ออก รอง.....ช่องทาง
ช่องทางเข้า-ออก ฉุกเฉิน.....ช่องทาง

ทั้งนี้ ควรคำนึงถึงการผ่านเข้า-ออกได้ทั้งบุคคลและยานพาหนะ หรือพิจารณาให้ชัดเจนว่าช่องทางใดอนุญาตให้ผ่านเข้า-ออกได้เป็นการเฉพาะ ทั้งในด้านบุคคล/ยานพาหนะ (เจ้าหน้าที่/บุคคลภายนอก) และเวลาเปิด-ปิด

1) ช่องทางเข้าหลัก คือ.....
เปิด-ปิด เวลา.....
2) ช่องทางออกหลัก คือ.....
เปิด-ปิด เวลา.....
3) ช่องทางเข้า-ออก รอง คือ.....
เปิด-ปิด เวลา.....
4) ช่องทางเข้า-ออก ฉุกเฉิน คือ.....
เปิด-ปิด เวลา.....
<u>หมายเหตุ</u> กรณีมีช่องทางเข้า-ออก มากกว่าจำนวนที่ปรากฏในแบบสำรวจฯ สามารถเพิ่มเติมข้อมูลได้ตามความเป็นจริง

6. การให้แสงสว่าง (บางครั้งมีการติดตั้งอย่างเพียงพอ แต่เปิดใช้บางส่วน ตามนโยบายการประหยัดพลังงาน)
1) แสงสว่างบริเวณแนวรั้ว ☐ เพียงพอ ☐ ไม่เพียงพอ
2) แสงสว่างภายในพื้นที่รอบนอกอาคาร ☐ เพียงพอ ☐ ไม่เพียงพอ
3) แสงสว่างภายในอาคาร ☐ เพียงพอ ☐ ไม่เพียงพอ
4) ระบบไฟส่องสว่าง สำหรับพื้นที่อับแสง/พื้นที่ควบคุมเป็นกรณีพิเศษ
☐ ดำเนินการติดตั้ง ☐ ไม่ได้ดำเนินการติดตั้ง
5) ระบบไฟฟ้าสำรอง..... สามารถใช้งานได้ภายใน.....นาที
ระยะเวลาในการสำรองได้นาน..... ช.ม.
ใช้งานได้เต็มระบบ หรือบางส่วน โดยติดตั้งไว้ที่.....
.....

7. ระบบการติดต่อสื่อสารของการรักษาการณ์ (นายตรวจเวรรักษาความปลอดภัย/เวรรักษาความปลอดภัยประจำวัน/เจ้าหน้าที่ยามรักษาการณ์) โดย (โทรศัพท์ภายใน/โทรศัพท์เคลื่อนที่/โซเชียลเน็ตเวิร์ก/วิทยุสังเคราะห์ความถี่).....
ระหว่าง.....กับ.....

<u>หมายเหตุ</u> จัดให้มีช่องทางการติดต่อสื่อสารสำรอง/ฉุกเฉิน ในกรณีที่ช่องทางการติดต่อสื่อสารหลักไม่สามารถใช้งานได้

8. ระบบสัญญาณแจ้งเตือนภัย (สัญญาณแจ้งเหตุอัคคีภัย/สัญญาณแจ้งเหตุฉุกเฉิน/สัญญาณแจ้งเมื่อมีผู้บุกรุกเข้าพื้นที่ควบคุม/สัญญาณขอความช่วยเหลือ)

   1) ภายในหน่วยงาน.....

   2) ภายนอกหน่วยงาน.....

9. การควบคุมบุคคล

   มีการจัดทำบัตรผ่านเข้า-ออกพื้นที่ให้แก่บุคคล (แบ่งประเภทของบุคคลที่ผ่านเข้า-ออก เช่น เจ้าหน้าที่ บุคคลภายนอก ผู้มาประชุม ผู้มาติดต่อ).....

   .....

   มีการบันทึกและเก็บหลักฐานการผ่านเข้า-ออกสำหรับบุคคลภายนอก โดยจัดเก็บรายละเอียด .....

   .....

   เจ้าหน้าที่ผู้ทำการบันทึก คือ.....

   มีการใช้ระบบอุปกรณ์อิเล็กทรอนิกส์ในการควบคุมบุคคลผ่านเข้า-ออกพื้นที่/พื้นที่ควบคุม

   .....

   .....

10. การควบคุมยานพาหนะ

   มีการจัดทำบัตรผ่านเข้า-ออกพื้นที่สำหรับยานพาหนะ (แบ่งประเภทของยานพาหนะ เช่น ของหน่วยงาน เจ้าหน้าที่ บุคคลภายนอก ผู้มาประชุม ผู้มาติดต่อ).....

   .....

   มีการบันทึกและเก็บหลักฐานการผ่านเข้า-ออกของยานพาหนะ ได้แก่ .....

   .....

   กำหนดพื้นที่จอดรถ แยกระหว่างเจ้าหน้าที่ของหน่วยงาน และบุคคลทั่วไป

   .....

11. การควบคุมระบบกุญแจของหน่วยงาน

   1) กุญแจประตูทางเข้า-ออกพื้นที่ อยู่ในความควบคุมของ.....

   .....

2) กุญแจประตูทางเข้า-ออกอาคาร อยู่ในความควบคุมของ.....
.....

3) กุญแจประตูเข้า-ออกห้องต่าง ๆ ภายในอาคาร อยู่ในความควบคุมของ.....
.....

4) ห้องควบคุมระบบกุญแจ/กุญแจสำรองของหน่วยงานทั้งหมด อยู่ในความรับผิดชอบของ
.....

5) เจ้าหน้าที่ในหน่วยงานมีกุญแจสำรองเองหรือไม่ ผู้ถืออยู่ในตำแหน่ง/ปฏิบัติหน้าที่ส่วนงานใด.....
.....

12. ระบบการรักษาการณ์ความปลอดภัย

1) จัดจ้างเจ้าหน้าที่ยามรักษาการณ์ (เจ้าหน้าที่ รปภ.) จาก.....
จำนวน.....นาย
ปฏิบัติหน้าที่วันละ.....ผลัด ผลัดละ.....นาย ตั้งแต่เวลา.....
.....
พื้นที่ที่ดูแลรับผิดชอบ.....
.....
.....

อุปกรณ์ในการรักษาความปลอดภัยของเจ้าหน้าที่ยามรักษาการณ์ ได้แก่ ไฟฉาย กระบอง กุญแจมือ เป็นต้น

☐ มี ☐ ไม่มี

รายละเอียดของอุปกรณ์ที่จัดเตรียมไว้ .....
.....

2) จัดเจ้าหน้าที่ของหน่วยงาน ปฏิบัติหน้าที่เวรรักษาความปลอดภัยประจำวัน วันละ.....คน
แบ่งเป็น.....ผลัด ผลัดละ.....คน ตั้งแต่เวลา.....
.....
พื้นที่ที่ดูแลรับผิดชอบ.....
.....

3) การกำหนดจุดตรวจ จำนวน.....จุด ได้แก่.....
.....
ตรวจตามห้วงเวลาทุก ๆ .....ช.ม.
<u>หมายเหตุ</u> การกำหนดจุดตรวจและห้วงเวลาในการตรวจ สำหรับเจ้าหน้าที่ยามรักษาการณ์และเจ้าหน้าที่เวรรักษาความปลอดภัยประจำวัน (เจ้าหน้าที่ของหน่วยงาน) อาจเหมือนหรือแตกต่างกันได้

13. การป้องกันและระงับอัคคีภัย
    1) อุปกรณ์ในการแจ้งเตือนและอุปกรณ์ดับเพลิง อาทิ เครื่องตรวจจับควัน/ความร้อน สปริงเกอร์ ถังดับเพลิง สายฉีดน้ำดับเพลิง มีจำนวนเพียงพอ เหมาะสมต่อประเภทของเพลิง และติดตั้งในจุดที่พร้อมใช้งาน.....
    การตรวจสอบความพร้อมในการใช้งาน ทุกห้วงระยะเวลา.....เดือน
    โดยหน่วยงาน.....
    2) การฝึกอบรมในการป้องกันและระงับอัคคีภัยเบื้องต้นให้แก่เจ้าหน้าที่.....
    (ทุกระดับ/เฉพาะบางกลุ่ม) ตามห้วงระยะเวลาทุก ๆ.....เดือน
    โดยหน่วยงาน.....

14. อุปกรณ์เกี่ยวกับการรักษาความปลอดภัย
    1) การติดตั้งกล้องโทรทัศน์วงจรปิด จำนวน.....จุด รวม.....ตัว
    แบ่งเป็นประเภท Standard Camera .....ตัว Infrared Camera.....ตัว
    Dome Camera.....ตัว Speed Dome Camera .....ตัว
    ครอบคลุมพื้นที่บริเวณ.....
    .....
    ระยะเวลาในการตรวจสอบความพร้อมใช้งาน ทุก ๆ.....เดือน
    การจัดเก็บสัญญาณภาพระบบโทรทัศน์วงจรปิด (ห้องมอนิเตอร์) อยู่ในความควบคุมดูแลของ.....
    .....

2) อุปกรณ์ตรวจสอบการเข้า-ออกพื้นที่ เช่น เครื่องตรวจวัตถุต้องสงสัย จำนวน.....จุด รวม.....ตัว ติดตั้งในบริเวณพื้นที่.....
.....
โดยการควบคุมดูแลของ.....
3) ระบบควบคุมการเข้า-ออกอาคาร อาทิ ระบบประตูรหัส (Access Control) มีการติดตั้งทุกอาคาร หรือบางอาคาร ได้แก่.....
.....
โดยการควบคุมดูแลของ.....
4) ข้อมูลเพิ่มเติมเกี่ยวกับอุปกรณ์รักษาความปลอดภัยอื่น ๆ .....
.....
.....

15. การฝึกอบรมเกี่ยวกับการรักษาความปลอดภัยสถานที่ ตามห้วงเวลา ทุก ๆ.....เดือน จัดโดย.....
หลักสูตรที่เคยจัด/กำลังจะจัด.....

16. หน่วยงานมีแผนเกี่ยวกับการรักษาความปลอดภัย (แผนระงับอัคคีภัย/แผนอพยพเคลื่อนย้าย ในสถานการณ์ต่าง ๆ เช่น เกิดเหตุเพลิงไหม้ มีการชุมนุมปิดล้อม เป็นต้น).....
.....
จัดทำโดย.....วัน/เดือน/ปี ที่จัดทำ.....

17. แผนการอพยพเคลื่อนย้ายบุคคลและสิ่งของออกจากพื้นที่ กรณีเกิดเหตุฉุกเฉิน อาทิ การชุมนุมปิดล้อม เหตุเพลิงไหม้.....
การฝึกซ้อมการอพยพตามแผน ทุกห้วงระยะเวลา.....เดือน
สถานที่ปฏิบัติงานสำรอง คือ .....
.....

18. หน่วยงานมีการจัดทำแผนเผชิญเหตุ หรือไม่.....
แผนที่ดำเนินการจัดทำ คือ .....
.....

19. การละเมิดการรักษาความปลอดภัยที่เคยเกิดขึ้นในหน่วยงาน จำนวน.....ครั้ง
เหตุที่เกิด .....
.....
สาเหตุ .....
.....
สิ่งที่ดำเนินการ .....
.....
การปรับปรุงมาตรการการรักษาความปลอดภัย.....
.....
ข้อมูลเพิ่มเติม .....
.....
.....

<u>หมายเหตุ</u> กรณีการละเมิดการรักษาความปลอดภัยไม่ได้เกิดขึ้นภายในหน่วยงาน แต่เจ้าหน้าที่ในหน่วยงานพบเห็น หรือสงสัย และแจ้งเตือนหรือดำเนินการอื่นใด ให้ระบุไว้ใน “ข้อมูลเพิ่มเติม”

20. หน่วยงานที่ทำหน้าที่ด้านการรักษาความปลอดภัยเกี่ยวกับสถานที่ โดยตรง
☐ ไม่มี
☐ มี หน่วยงาน.....

21. การส่งเสริมให้มีจิตสำนึกด้านการรักษาความปลอดภัย เช่น ฝึกซ้อมแผน อบรม/ทบทวน
.....
.....

22. ปัญหา-อุปสรรค ในการดำเนินการรักษาความปลอดภัยเกี่ยวกับสถานที่
.....
.....
.....

23. การขอรับการสนับสนุนจากองค์การรักษาความปลอดภัยฝ่ายพลเรือน

.....

.....

.....

<u>คำอธิบาย</u> ในการตรวจสอบมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ สามารถนำแบบสำรวจดังกล่าวเป็นจุดเริ่มต้นสำหรับทบทวนมาตรการฯ ที่กำหนดไว้ว่า มีความเหมาะสมขณะดำเนินการตรวจสอบ มากน้อยเพียงใด ทั้งนี้ แบบสำรวจฯ เป็นเพียงการนำมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ที่ระบุไว้ในระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 มาเรียบเรียงไว้เบื้องต้นเท่านั้น การพิจารณากำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ จำเป็นต้องวิเคราะห์และประเมินภัยคุกคาม ความเสี่ยงของแต่ละหน่วยงาน ประกอบกับบริบทอื่น ๆ ให้เหมาะสม เพื่อกำหนดมาตรการที่สอดคล้องกับงบประมาณและความจำเป็นในการดำเนินการ เพื่อรองรับภัยคุกคามที่แตกต่างกันของแต่ละหน่วยงาน ได้อย่างมีประสิทธิภาพ

แบบตรวจสอบมาตรฐานการรักษาความปลอดภัย

การตรวจสอบ ประจำปี พ.ศ. ..... **ชื่อหน่วยงานของรัฐ**.....

<u>คำชี้แจง</u> **คณะกรรมการตรวจสอบมาตรฐานการรักษาความปลอดภัย** ใส่เครื่องหมาย √ ในช่อง “ผลการปฏิบัติ” หรือ “ไม่มีการปฏิบัติ”

1. **“ผลการปฏิบัติ”** หมายถึง มีการดำเนินการในประเด็นนั้น ๆ โดย

   1.1 <u>ดำเนินการ</u> หมายถึง ดำเนินการตามมาตรฐานการรักษาความปลอดภัย

   1.2 <u>ไม่ดำเนินการ</u> หมายถึง ดำเนินการไม่เป็นไปตามมาตรฐานการรักษาความปลอดภัย

   ทั้งนี้ กรณีมีการดำเนินการตามแนวทางอื่น หรือตามระเบียบภายในของหน่วยงาน ให้ชี้แจงในช่อง “หมายเหตุ” หรือจะระบุไว้ในส่วนความคิดเห็นของคณะกรรมการตรวจสอบการปฏิบัติตามมาตรฐานการรักษาความปลอดภัย ด้วยก็ได้

2. **“ไม่มีการปฏิบัติ”** หมายถึง ไม่มีการดำเนินการ เนื่องจากไม่มีเหตุหรือกรณีที่ต้องปฏิบัติในประเด็นนั้น ๆ

<u>หมายเหตุ</u> ใส่เครื่องหมาย √ ในช่อง “ผลการปฏิบัติ” หรือ “ไม่มีการปฏิบัติ” ให้ตรงตาม**รายการตรวจสอบ**มาตรฐานการรักษาความปลอดภัย โดยพิจารณารายละเอียดการดำเนินการตามมาตรฐาน และคำอธิบายที่ปรากฏตามแบบตรวจสอบมาตรฐานการรักษาความปลอดภัย

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**การแต่งตั้ง** “เจ้าหน้าที่ควบคุมการรักษาความปลอดภัย” **การรักษาความปลอดภัยเกี่ยวกับบุคคล** **1. ตรวจสอบประวัติและพฤติการณ์บุคคล** 1) ผู้ที่อยู่ระหว่างรอว่าจ้าง บรรจุ หรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ ลูกจ้างทดลองงาน หรือฝึกงานก่อนบรรจุเข้าปฏิบัติงาน หรือผู้ที่ขอกลับเข้ารับราชการใหม่ 2) ผู้ที่ได้รับมอบหมายให้ปฏิบัติงานในหน้าที่ หรือตำแหน่งที่สำคัญของทางราชการ หรือที่เกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการ หรือทรัพย์สินมีค่าของแผ่นดิน 3) ผู้ได้รับทุนการศึกษาของหน่วยงานของรัฐ หรือทุนอื่นใดเพื่อศึกษาในประเทศหรือต่างประเทศ และมีข้อผูกพันให้เข้าปฏิบัติงานให้แก่หน่วยงานของรัฐ เมื่อสำเร็จการศึกษาแล้ว 4) เจ้าหน้าที่ของรัฐที่ยังมิได้รับการตรวจสอบประวัติและพฤติการณ์ หรือผู้ที่ขอโอนมารับราชการยังหน่วยงาน แม้ได้รับการตรวจสอบประวัติและพฤติการณ์จากหน่วยงานเดิมแล้วก็ตาม 5) บุคคลภายนอกที่ปฏิบัติงานให้หน่วยงานของรัฐ	ทำหน้าที่ดำเนินการ ควบคุม ตลอดจนให้คำปรึกษาเกี่ยวกับการรักษาความปลอดภัยของหน่วยงาน - ตามแนวทางปฏิบัติการตรวจสอบประวัติและพฤติการณ์บุคคล - หน่วยงานของรัฐต้องจัดให้มีมาตรการการรักษาความปลอดภัยเกี่ยวกับบุคคล สำหรับบุคคลภายนอกที่ปฏิบัติงานให้หน่วยงานของรัฐ ตามความเหมาะสม - มีระบบการจัดเก็บประวัติบุคคลที่มีความปลอดภัย ถูกต้อง ครบถ้วน และพร้อมใช้งาน				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**2. ตรวจสอบประวัติและพฤติการณ์บุคคล<u>โดยละเอียด</u>** 1) บุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการชั้นลับที่สุด ลับมาก หรือการรหัส 2) บุคคลที่มีพฤติการณ์ หรือปรากฏข่าวสารหรือติดต่อกับบุคคล หรือองค์การทั้งภายในและภายนอกประเทศที่จะเป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ 3) บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ในภารกิจหรือตำแหน่งหน้าที่สำคัญหรือแต่งตั้งให้ดำรงตำแหน่งที่สำคัญในหน่วยงานของรัฐ รวมถึงบุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวข้องกับทรัพย์สินมีค่าของแผ่นดิน	- ดำเนินการหรือปรับใช้ตามแนวทางปฏิบัติการตรวจสอบประวัติและพฤติการณ์บุคคลโดยละเอียด - กรณีขอให้สำนักข่าวกรองแห่งชาติดำเนินการตรวจสอบแทน ให้ปฏิบัติตามแนวทางที่สำนักข่าวกรองแห่งชาติกำหนด				
	3. การรับรองความไว้วางใจบุคคล มีการรับรองความไว้วางใจบุคคล ให้เข้าถึงสิ่งที่เป็นความลับของทางราชการหรือปฏิบัติในภารกิจหรือตำแหน่งหน้าที่สำคัญ	ตามแนวทางปฏิบัติการรับรองความไว้วางใจบุคคล				
	4. **การทบทวน แก้ไข เพิ่มเติมข้อมูลประวัติบุคคลของเจ้าหน้าที่ ให้เป็นปัจจุบันอยู่เสมอ**	ตามแนวทางปฏิบัติการบันทึกการเปลี่ยนแปลงประวัติบุคคล เมื่อมีการเปลี่ยนแปลงข้อมูลประวัติ หรือมีการติดตาม ทบทวน อย่างน้อยทุก 3 ปี				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**5. การอบรมและทบทวนการปฏิบัติแก่เจ้าหน้าที่ของรัฐ** 1) ปฐมนิเทศ 2) ทบทวนเพิ่มเติม	- อบรมให้แก่เจ้าหน้าที่ใหม่ก่อนการปฏิบัติงาน - ทบทวนเพื่อกระตุ้นจิตสำนึกในการรักษาความปลอดภัย อย่างสม่ำเสมอ				
	การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ	ดำเนินการเป็นลายลักษณ์อักษร				
	1. หัวหน้าหน่วยงานของรัฐ ต้องดำเนินการ ดังนี้ 1) ให้การรับรองความไว้วางใจแก่บุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการ 2) มอบหมายหน้าที่ผู้มีอำนาจกำหนดชั้นความลับให้กับผู้ใต้บังคับบัญชา 3) แต่งตั้ง 3.1) นายทะเบียนข้อมูลข่าวสารลับ ผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ 3.1.1) หน่วยงานของรัฐ 3.1.2) หน่วยงานย่อย 3.2) เจ้าหน้าที่นำสารของหน่วยงาน	แต่งตั้งนายทะเบียนข้อมูลข่าวสารลับ ผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับในระดับหน่วยงานของรัฐและหน่วยงานย่อย - ผู้ทำหน้าที่นำส่งข้อมูลข่าวสารลับออกนอกหน่วยงานของรัฐ				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**2. ระบบทะเบียนข้อมูลข่าวสารลับ** 1) ของหน่วยงานของรัฐ 1.1) ทะเบียนรับ (ทขล.1) 1.2) ทะเบียนส่ง (ทขล.2) 1.3) ทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3) 2) ของหน่วยงานย่อย 2.1) ทะเบียนรับ (ทขล.1) 2.2) ทะเบียนส่ง (ทขล.2) 2.3) ทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3) **3. การตรวจสอบข้อมูลข่าวสารลับ อย่างน้อยทุก 6 เดือน** 1) แต่งตั้งคณะกรรมการตรวจสอบข้อมูลข่าวสารลับ 2) รายงานการตรวจสอบข้อมูลข่าวสารลับต่อหัวหน้าหน่วยงานของรัฐ อย่างน้อยทุก 6 เดือน 3) รายงานผลการปฏิบัติเกี่ยวกับข้อมูลข่าวสารลับ ประจำปี..... ต่อประธานคณะกรรมการข้อมูลข่าวสารของราชการ (กขร.)	- ระบบทะเบียนข้อมูลข่าวสารลับต้องแยกต่างหากจากระบบทะเบียนข้อมูลข่าวสารที่ไม่มีชั้นความลับ - นายทะเบียนข้อมูลข่าวสารลับ หรือผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับเป็นผู้มีหน้าที่บันทึกทางทะเบียน - ตรวจสอบข้อมูลข่าวสารลับที่มีอยู่จริงและตรวจสอบการปฏิบัติที่ถูกต้องตามระเบียบ - ส่งแบบรายงานผลการปฏิบัติเกี่ยวกับข้อมูลข่าวสารลับประจำปี.... ภายในเดือนมีนาคมของปีถัดไป - แบบรายงานการตรวจสอบข้อมูลข่าวสารลับและแบบรายงานผลการปฏิบัติเกี่ยวกับข้อมูลข่าวสารลับประจำปี.... ตามระเบียบว่าด้วยการ				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย		รักษาความลับของทางราชการ (ฉบับที่ 2) พ.ศ. 2561				
	4. การกำหนดชั้นความลับของข้อมูลข่าวสารลับ 1) กำหนดชั้นความลับของข้อมูลข่าวสารลับไว้ชัดเจน 2) บันทึกเหตุผลย่อของการกำหนดชั้นความลับของข้อมูลข่าวสารลับ ในช่องการดำเนินการของทะเบียนควบคุมข้อมูลข่าวสารลับ (ทขล.3)	ตามแนวทางปฏิบัติการกำหนดชั้นความลับและแสดงชั้นความลับ (การกำหนดชั้นความลับ)				
	5) การจัดทำข้อมูลข่าวสารลับ	- มีการแสดงชั้นความลับ ตามแนวทางปฏิบัติการกำหนดชั้นความลับและแสดงชั้นความลับ (การแสดงชั้นความลับ) - แสดงเลขที่ชุด เลขที่หน้า ไว้อย่างชัดเจนและถูกต้อง				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**6. การสำเนา / การแปล / การเข้ารหัส / การถอดรหัสข้อมูลข่าวสารลับ**	มีการบันทึกจำนวนชุด ยศ ชื่อ ตำแหน่งของผู้ดำเนินการ และชื่อหน่วยงานของรัฐที่จัดทำไว้ที่ข้อมูลข่าวสารลับฉบับต้นและฉบับสำเนา แปล เข้ารหัส ถอดรหัส				
	7. การโอนข้อมูลข่าวสารลับ กรณีมีการปรับเปลี่ยน โครงสร้างภารกิจ ต้องโอนข้อมูลข่าวสารลับในความครอบครองให้ไปเป็นของหน่วยงานที่มีภารกิจและอำนาจหน้าที่เกี่ยวข้อง ตามโครงสร้างภารกิจที่ปรับใหม่	- มีแบบบันทึกการโอนและการรับโอนข้อมูลข่าวสารลับ - บันทึกในช่องการดำเนินการ ทขล.3				
	8. การส่งข้อมูลข่าวสารลับ 1) ส่งออกนอกบริเวณหน่วยงานภายในประเทศ โดยเจ้าหน้าที่นำสาร หรือทางไปรษณีย์ลงทะเบียนตอบรับ	- มีการบรรจุซองหรือภาชนะทึบแสง 2 ชั้น - แนบใบตอบรับ - บันทึกใน ทขล.3 กรณีส่งแล้วไม่มีผู้รับ - กรณีส่งทางไปรษณีย์ลงทะเบียนตอบรับ หรือทางโทรคมนาคม ต้องดำเนินการตามที่กำหนดไว้ใน				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย		ระเบียบภายใน คำสั่ง หรือประกาศการอนุญาตของหัวหน้าหน่วยงานของรัฐ				
	2) ส่งออกภายนอกประเทศ	- มีการบรรจุซองหรือภาชนะทึบแสง 2 ชั้น และแนบใบตอบรับ - ปฏิบัติตามระเบียบกระทรวงการต่างประเทศว่าด้วยถุงเมล์การทูต				
	3) ส่งภายในบริเวณหน่วยงาน	- ใช้ใบปกปิดทับตามชั้นความลับของข้อมูลข่าวสาร - ผู้นำส่ง ต้องเป็นเจ้าของเรื่องหรือนายทะเบียนข้อมูลข่าวสารลับหรือผู้ช่วยฯ				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**9. การรับข้อมูลข่าวสารลับ**	- ผู้รับ ต้องเป็นนายทะเบียนข้อมูลข่าวสารลับ หรือผู้ช่วยฯ หรือบุคคลตามจ่าหน้าของหนังสือ หรือผู้ได้รับมอบความไว้วางใจให้เข้าถึงชั้นความลับของข้อมูลข่าวสารลับ - ส่งคืนใบตอบรับ ให้แก่หน่วยงานผู้ส่ง				
	10. การยืมข้อมูลข่าวสารลับ	- มีบันทึกการยืม - บันทึกในช่องการดำเนินการ ทขล.3				
	11. การเก็บรักษาข้อมูลข่าวสารลับ	มีระบบการเก็บรักษาที่มีความปลอดภัย ถูกต้อง ครบถ้วน พร้อมใช้งาน				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**12. การปรับชั้นความลับของข้อมูลข่าวสารลับ** 1) หน่วยงานของรัฐเจ้าของเรื่องพิจารณาปรับชั้นความลับโดยผู้มีอำนาจกำหนดชั้นความลับหรือผู้บังคับบัญชาตามสายงาน 2) หน่วยงานผู้ครอบครองข้อมูลข่าวสารลับแก้ไขชั้นความลับให้ตรงกัน 3) แก้ไขชั้นความลับในระบบทะเบียนข้อมูลข่าวสารลับ **13. การทำลายข้อมูลข่าวสารลับ** 1) แต่งตั้งคณะกรรมการทำลายข้อมูลข่าวสารลับ 2) ส่งบัญชีรายชื่อหนังสือให้สำนักหอจดหมายเหตุแห่งชาติพิจารณาคุณค่าก่อนทำลาย 3) จัดทำใบรับรองการทำลายข้อมูลข่าวสารลับ	ตามแนวทางปฏิบัติการปรับชั้นความลับ - คณะกรรมการทำลายข้อมูลข่าวสารลับ มีหน้าที่พิจารณารายการหนังสือขอทำลาย และควบคุมการทำลายข้อมูลข่าวสารลับ - ใบรับรองการทำลายข้อมูลข่าวสารลับ ต้องเก็บไว้ไม่น้อยกว่า 1 ปี - บันทึกการทำลายในช่องการดำเนินการ ทบล.3				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**14. กรณีสูญหาย**	- รายงานผู้บังคับบัญชา - บันทึกใน ทบล.3 - แต่งตั้งคณะกรรมการสอบสวน				
	15. การเปิดเผย โดย 1) เจ้าหน้าที่ของรัฐใช้ดุลยพินิจในการเปิดเผย 2) ได้รับความเห็นชอบจากผู้บังคับบัญชา ก่อนการเปิดเผย 3) ตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ โดยปฏิบัติตามคำวินิจฉัยให้เปิดเผยของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสาร (กวฉ.)	- เจ้าหน้าที่ของรัฐ (ผู้เป็นเจ้าของเรื่อง) ในระดับตามที่กำหนดในกฎกระทรวง ออกตามความในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 เป็นผู้มีอำนาจใช้ดุลยพินิจสั่งให้เปิดเผยข้อมูลข่าวสารลับตามมาตรา 15				
	กรณีข้อมูลข่าวสารลับที่ครบอายุกำหนดตามมาตรา 26 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 1) ส่งบัญชีรายชื่อหนังสือให้สำนักหอจดหมายเหตุแห่งชาติพิจารณาคุณค่า 2) ขออนุมัติต่อขยายระยะเวลาไม่เปิดเผยข้อมูลข่าวสารลับนั้น	ผู้มีอำนาจพิจารณาอนุมัติการขอขยายระยะเวลาไม่เปิดเผยข้อมูลข่าวสารลับ ตามกฎกระทรวง ฉบับที่ 3 (พ.ศ.2541) ออกตามความในพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**การรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับอิเล็กทรอนิกส์** **1. การรักษาความปลอดภัยเกี่ยวกับบุคคล** 1) ผู้ใช้งานและผู้ดูแลระบบ	- ผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล - ได้รับการรับรองความไว้วางใจบุคคล - ได้รับอนุญาตในการเข้าถึงและใช้งานคอมพิวเตอร์ - ผ่านการชี้แจงหรืออบรมเกี่ยวกับการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ การใช้งานคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบเครือข่ายและอินเทอร์เน็ต โดยคำนึงถึงการรักษาความลับ (Confidentiality), การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability)				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	2) บุคคลภายนอก	- ผ่านการตรวจสอบประวัติและพฤติการณ์บุคคล - ได้รับการรับรองความไว้วางใจบุคคล - ได้รับอนุญาตในการเข้าถึงคอมพิวเตอร์และระบบคอมพิวเตอร์จากหัวหน้าหน่วยงานของรัฐ - ผ่านการชี้แจงให้ทราบเกี่ยวกับระเบียบและข้อปฏิบัติเกี่ยวกับการรักษาความลับและการรักษาความปลอดภัย - ได้รับการกำกับดูแลขณะดำเนินการโดยใกล้ชิด				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มี การปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**2. การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ** 1) มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ 2) มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553				
	3. การดำเนินการเกี่ยวกับข้อมูลข่าวสารอิเล็กทรอนิกส์ 1) กำหนดอุปกรณ์เฉพาะที่ใช้ในการจัดทำข้อมูลข่าวสารลับอิเล็กทรอนิกส์ และมีทะเบียนควบคุมอุปกรณ์ 2) จัดเก็บข้อมูลข่าวสารลับอิเล็กทรอนิกส์	- เข้ารหัสก่อนการจัดเก็บ - สื่อบันทึกหรืออุปกรณ์หรือระบบที่ใช้จัดเก็บ มีการขึ้นทะเบียนหรือควบคุม - สื่อบันทึกหรืออุปกรณ์หรือระบบที่ใช้จัดเก็บ ตั้งอยู่ในพื้นที่ที่มีการรักษาความปลอดภัย				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**4. การส่งและการรับข้อมูลข่าวสารลับอิเล็กทรอนิกส์** 1) ไม่แจ้งรหัสผ่านไปพร้อมกับการส่งไฟล์ข้อมูลข่าวสารลับ 2) ไม่ส่งและรับข้อมูลข่าวสารลับ ชั้น “ลับที่สุด”	- เข้ารหัส (Encryption) ก่อนการส่ง - ใช้ช่องทาง (Channels) ที่มั่นคงปลอดภัย - ใช้ซอฟต์แวร์ของหน่วยงานของรัฐ เช่น WorkD - ไม่มีการดำเนินการต่อข้อมูลข่าวสารลับ ชั้น “ลับที่สุด”				
	5. การทำลาย	- ดำเนินการตามข้อกำหนดการทำลายข้อมูลข่าวสารลับ - ทำลายด้วยวิธีการลบถาวร				
	6. การปฏิบัติในเวลาฉุกเฉิน 1) แผนการเคลื่อนย้าย 2) แผนการพิทักษ์รักษา 3) แผนการทำลาย	มีแผนปฏิบัติสำหรับข้อมูลข่าวสารลับ และข้อมูลข่าวสารลับอิเล็กทรอนิกส์ กรณีเกิดเหตุฉุกเฉิน				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**การรักษาความปลอดภัยเกี่ยวกับสถานที่** **1. การประเมินภัยคุกคามและความเสี่ยง** 1) ระบุภัยคุกคามและความเสี่ยง 2) ประเมินระดับความเสี่ยง 3) จัดระดับความเสี่ยง **2. แผนและมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่** 1) การจัดทำแผนและมาตรการการรักษาความปลอดภัย 1.1) แผนและมาตรการการรักษาความปลอดภัยในสถานการณ์ปกติ 1.1.1) กำหนดพื้นที่ที่มีการรักษาความปลอดภัยโดยกำหนดอาณาเขตและกำหนดสิทธิการเข้าถึงพื้นที่ 1.1.2) การใช้เครื่องกีดขวาง 1.1.3) ระบบแสงสว่าง ได้แก่ ไฟแสงสว่าง ไฟส่องสว่าง ไฟสำรอง	ตามแนวทางปฏิบัติการประเมินภัยคุกคามและความเสี่ยง เช่นหลักการวิเคราะห์ความเสี่ยง (SWOT หรืออื่นๆ) ตามแนวทางปฏิบัติการจัดทำแผนและมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ - มีป้ายข้อความแสดงการกำหนดพื้นที่ที่ชัดเจน โดยเฉพาะพื้นที่ที่เป็นเขตหวงห้าม - มีเครื่องกีดขวาง อาทิ รั้ว แผงกั้น - มีระบบแสงสว่างเพียงพอต่อการมองเห็น ทั้งในเวลากลางวันกลางคืน และบริเวณพื้นที่อับแสง				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	1.1.4) ระบบสัญญาณเตือนภัย 1.1.5) การควบคุมบุคคลในการเข้า-ออก และอยู่ในพื้นที่ 1.1.6) การควบคุมยานพาหนะในการเข้า-ออก และอยู่ในพื้นที่ 1.1.7) การจัดเจ้าหน้าที่รักษาความปลอดภัยสถานที่ทั้งในส่วนเจ้าหน้าที่ของหน่วยงานและเจ้าหน้าที่ยามรักษาการณ์	- มีระบบสื่อสารและสัญญาณแจ้งเตือนภัยที่พร้อมใช้งาน - มีบัตรผ่าน บัตรแสดงตน และบันทึกการเข้า-ออก สำหรับบุคคลและยานพาหนะ - กรณีอยู่ในพื้นที่ควบคุม ต้องมีมาตรการเพิ่มเติมในการควบคุมบุคคล - นายตรวจเวรรักษาความปลอดภัยประจำวัน - เจ้าหน้าที่เวรรักษาความปลอดภัยประจำวัน - ยามรักษาการณ์ - มีการรายงานผลการปฏิบัติประจำวัน ตามแบบการรายงานผลที่หน่วยงานกำหนด				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	1.1.8) การป้องกันอัคคีภัย โดยพิจารณาให้สอดคล้องกับกฎหมายว่าด้วยการควบคุมอาคาร 1.1.9) อุปกรณ์เกี่ยวกับการรักษาความปลอดภัย อาทิ กล้องโทรทัศน์วงจรปิด (CCTV) ระบบควบคุมการเข้า-ออก (Access Control) 1.2) แผนและมาตรการการรักษาความปลอดภัยในสถานการณ์ไม่ปกติ	ปรับระดับมาตรการให้มีความเข้มข้นขึ้น อาทิ ไม่อนุญาตให้จอดรถภายในหน่วยงาน ไม่อนุญาตให้บุคคล (ตามที่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบุ) เข้ามาในพื้นที่ของหน่วยงาน เพิ่มเติมอุปกรณ์เกี่ยวกับการรักษาความปลอดภัย เช่น เครื่องตรวจโลหะแบบเดินผ่าน (Walk Through)				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	1.3) แผนและมาตรการการรักษาความปลอดภัยในสถานการณ์ฉุกเฉิน (แผนเผชิญเหตุ)	จัดทำแผนเผชิญเหตุ (Incident Action Plan) โดยกำหนดมาตรการให้ครอบคลุมทั้งก่อนเกิดเหตุ ระหว่างเกิดเหตุ และหลังเกิดเหตุ				
	2) การซักซ้อมแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่อย่างน้อยปีละ 1 ครั้ง	ตามแนวทางปฏิบัติการดำเนินการฝึกซ้อมแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่				
	3) การทบทวนปรับปรุงแผนให้มีความเหมาะสมกับสถานการณ์ปัจจุบัน					

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**3. การสำรวจและตรวจสอบมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่** 1) การสำรวจเพื่อกำหนดมาตรการการรักษาความปลอดภัย 1.1) รวบรวมข้อมูลข่าวสารและศึกษาข้อมูลความบกพร่องด้านการรักษาความปลอดภัยสถานที่ 1.2) สำรวจพื้นที่และอาคารสถานที่ที่จะกำหนดมาตรการการรักษาความปลอดภัยโดยละเอียด 1.3) จัดทำรายงานผลการสำรวจการรักษาความปลอดภัยเกี่ยวกับสถานที่ 2) การตรวจสอบมาตรการการรักษาความปลอดภัย 2.1) การตรวจสอบในสภาวะปกติสถานการณ์ปกติ 2.2) การตรวจสอบเมื่อเกิดการละเมิดการรักษาความปลอดภัย	ตามแนวทางปฏิบัติการสำรวจและตรวจสอบการรักษาความปลอดภัยเกี่ยวกับสถานที่				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**การรักษาความปลอดภัยในการประชุมลับ** **1. แต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย** ในการประชุมลับ **2. แต่งตั้งนายทะเบียนข้อมูลข่าวสารลับ** ในการประชุมลับ **3. ตรวจสอบการรับรองความไว้วางใจ**ไม่ต่ำกว่าชั้นความลับของการประชุมลับ สำหรับผู้ที่เกี่ยวข้อง **4. กำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่** ทั้งก่อน ระหว่าง และหลังการประชุมลับ **5. ห้ามนำเครื่องมือ วัสดุอุปกรณ์ อุปกรณ์อิเล็กทรอนิกส์** ที่สามารถสื่อสารหรือบันทึกข้อมูลข่าวสารของการประชุม เข้าไปในสถานที่ที่มีการประชุมลับ **6. ห้ามนำข้อมูลข่าวสารจากการประชุมลับ** ออกนอกสถานที่ที่มีการประชุมลับ **7. ดำเนินการต่อสิ่งที่เป็นความลับของทางราชการ ตามกฎหมายและระเบียบที่เกี่ยวข้อง**	มีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร มีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร กรณีพบข้อสงสัยว่ามีการละเมิดการรักษาความปลอดภัยในการประชุมลับ ต้องดำเนินการสำรวจตรวจสอบสถานที่หลังการประชุมลับเสร็จสิ้นด้วย				

	รายการตรวจสอบ	รายละเอียด/คำอธิบาย	ผลการปฏิบัติ		ไม่มีการปฏิบัติ	หมายเหตุ
			ดำเนินการ	ไม่ดำเนินการ		
มาตรฐานการรักษาความปลอดภัย	**8. การแถลงข่าวหรือการบรรยายสรุป** **การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย** **1. มีการดำเนินการเบื้องต้นเพื่อลดความเสียหาย และรายงาน** ผู้บังคับบัญชา หรือผู้มีหน้าที่เกี่ยวข้อง **2. สำรวจและตรวจสอบความเสียหาย** **3. ปรับปรุงมาตรการการรักษาความปลอดภัย** **4. รายงานสรุปผลการดำเนินการต่อผู้บังคับบัญชา** **5. แจ้งหน่วยงานของรัฐซึ่งเป็นเจ้าของเรื่องเดิมทราบ** (กรณีเกี่ยวข้องกับข้อมูลข่าวสารลับที่หน่วยงานของรัฐอื่นเป็นเจ้าของเรื่อง) **6. แต่งตั้งคณะกรรมการสอบสวนข้อเท็จจริง** **7. ดำเนินการตามกฎหมาย**ต่อผู้กระทำการละเมิด หรือผู้จะกระทำการละเมิด หรือผู้รับผิดชอบต่อการละเมิด	- ผู้แถลงข่าวหรือผู้บรรยายสรุปเรื่องที่แถลงหรือบรรยายสรุปต้องได้รับอนุมัติจากที่ประชุมลับก่อน และจัดสถานที่ขึ้นเป็นการเฉพาะ - การบรรยายสรุปเรื่องที่เป็นความลับ ต้องตรวจสอบการรับรองความไว้วางใจผู้เข้ารับฟัง				

ความคิดเห็นของคณะกรรมการตรวจสอบมาตรฐานการรักษาความปลอดภัยของหน่วยงาน

.....

.....

.....

.....

.....

.....

.....

.....

ลงชื่อ.....ประธาน

(.....)

ลงชื่อ.....กรรมการ

(.....)

ลงชื่อ.....กรรมการ

(.....)

ลงชื่อ.....กรรมการ

(.....)

ลงชื่อ.....กรรมการและเลขานุการ

(.....)

วันที่.....

บรรณานุกรม

กฎหมาย

พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540.

ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544. และที่แก้ไขเพิ่มเติม.

ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552. และที่แก้ไขเพิ่มเติม

ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ (ฉบับที่ 4) พ.ศ. 2564.

คำแนะนำ

คำแนะนำการปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544. และที่แก้ไขเพิ่มเติม. สำนักข่าวกรองแห่งชาติ.

คำแนะนำการปฏิบัติตามระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552. และที่แก้ไขเพิ่มเติม. สำนักข่าวกรองแห่งชาติ.

ประกาศ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีแบบปลอดภัย พ.ศ. 2555. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของการประชุมผ่านสื่ออิเล็กทรอนิกส์ พ.ศ. 2563. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล.

เว็บไซต์

<https://www.slideshare.net/paladtai/ddpm> สืบค้นเมื่อ 23 กันยายน 2564. พงศธร ศิริสาคร. (2557) การจัดทำแผนเผชิญเหตุ.